Draft ‘Statutory’ Code of Practice

Publication Draft – Jan 2022

This is a draft document and subject to change.

© Crown Copyright 2022
The text in this document (excluding the Forensic Science Regulator’s logo, any other logo, and material quoted from other sources) may be reproduced free of charge in any format or medium providing it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown Copyright and its title specified. This document is not subject to the Open Government Licence.

The Forensic Science Regulator Act 2021

This is the Code of Practice issued by the Forensic Science Regulator pursuant to the provisions of s2 of The Forensic Science Regulator Act 2021.

In accordance with the provisions of the Act this Code has been:

1. Prepared and published by the Forensic Science Regulator [as required by s2];
2. Approved by the Secretary of State [as required by s3(3)(b)] on [Date to be inserted];
3. Laid before Parliament by the Secretary of State [as required by s3(3)(b)] on [Date to be inserted];
4. Approved by the House of Commons [as required by s3(3)(c)] on [Date to be inserted]; and
5. Approved by the House of Lords [as required by s3(3)(c)] on [Date to be inserted].

In accordance with s3(4) of the Act the provisions of this Code come into force at 00:00:01 on [Date to be inserted].

Table of Contents

Introduction

1. Introduction

1.1 General

1.1.1 Forensic science is a critical and important part of criminal investigations and the administration of justice, not only to identify offenders and provide expert evidence to the courts, but it is one of the strongest safeguards against false allegation and wrongful conviction. Forensic science examinations carry significant risks and the consequences of a quality failure can be profound, particularly where there is a system rather than an individual failure. The former could lead to the review of hundreds or even thousands of results generated by a flawed technique or method. The purpose of forensic science regulation is to minimise the risk of a quality failure and ensure that accurate and reliable scientific evidence is used in criminal investigations and in criminal trials.

1.1.2 The model for regulation of forensic science in England and Wales is based on each forensic unit operating an effective quality management system that meets the requirements of this Code. This will provide the necessary control of processes and minimise the risk of quality failure. The implementation of quality management systems by forensic science organisations in the UK began in the early 1990’s, first with certification to a management standard and then with accreditation to technical standards.

1.1.3 By the early 2000’s forensic science organisations in the UK and overseas had developed quality management systems with a scope that covered a wide range of laboratory-based activities.

1.1.4 The key elements of an effective quality management system are;

a. Validation of techniques with a focus on understanding and managing the risk of quality failure;

b. Defining, demonstrating and testing the competence of practitioners; and

c. Having documented and controlled procedures, audit to ensure they are effective and being followed, complemented by processes that encourage and support continuous improvement.

1.1.5 The establishment of an effective quality management system provides the basis for forensic units to understand and manage the risk of a quality failure. Quality management systems in forensic units in the UK are, where accreditation is required, assessed by the United Kingdom Accreditation Service ® (UKAS ®) [1] against international standards and guidance, primarily BS EN ISO/IEC 17025:2017 [1] and BS EN ISO/IEC 17020:2012 [2] and ILAC G19:08/2014 [3]. Similar provisions will apply with other accreditation bodies. The role of the non-statutory Forensic Science Regulator was established in 2007 [2] under the Royal Prerogative to set standards for forensic science and ensure compliance with those standards. This was achieved through the establishment of the Codes of Practice and Conduct [4], appendices covering different sectors of forensic science and general guidance documents. In 2011 [5] the House of Commons Science and Technology Select Committee called for the Forensic Science Regulator to be given statutory powers, it reinforced this in two further reports [6] [7] and the House of Lords Science and Technology Select Committee also called for statutory powers [8]. A Private Members Bill [9] to establish statutory powers for the Forensic Science Regulator was introduced in Parliament in 2020 and, following modification, the Forensic Science Regulator Act 2021 (the ‘2021 Act’) [10] received Royal Assent on 29 April 2021 [11]. [3]

1.1.6 The role of the Forensic Science Regulator (the ‘Regulator’ under the 2021 Act was introduced on ###.

---

1 The terms ‘United Kingdom Accreditation Service’ and ‘UKAS’ are registered trademarks of the United Kingdom Accreditation Service which is the national accreditation body for the United Kingdom.

2 Written Ministerial Statement of 12 July 2007 by Meg Hillier MP (then a Minister at the Home Office). [12]

3 On Royal Assent certain administrative provisions of the Act became law. All other provisions of the Act were to be brought into effect by Regulations issued by the Secretary of State [see s13 2021 Act [10]].

1.2 The Forensic Science Regulator Act 2021

1.2.1 The 2021 Act [10] requires the Regulator to prepare and publish a code of practice about the carrying on of forensic science activities in England and Wales. This document is the Code of Practice (the ‘Code’) required by Section 2 of the 2021 Act [10]. This Code builds on the non-statutory Codes of Practice and Conduct [4] incorporating much of their content.

1.2.2 The 2021 Act [10] introduced powers for the Regulator to intervene where there is reason to believe that a person [4] may be carrying on a forensic science activity to which the Code applies in a way that creates a substantial risk (that being a risk which is more than theoretical) [5] of;

a. Adversely affecting any criminal investigation, or

b. Impeding or prejudicing the course of justice in any proceedings. [6]

1.2.3 The powers introduced include one to investigate [see s5 2021 Act [10]] and one to require compliance [see s6 2021 Act [10]].

1.2.4 Every effort should be made by all those who work in forensic science to avoid the situation arising where there is an unacceptable risk to a criminal investigation or the administration of justice. The Senior Accountable Individual (see section 17) shall be responsible for the monitoring and mitigation of the risk of quality failures. To facilitate this all forensic units which are subject to this Code issued under the 2021 Act [10] are, if the Code demands accreditation, required to sign a confidentiality disclosure waiver to allow UKAS (and/or any other accreditation body the unit uses) to disclose any relevant information to the Regulator.

---

4 The term ‘persons’ is defined in The Interpretation Act 1978 [15] and that definition includes any ‘body of persons corporate or unincorporate’.

5 The term ‘substantial risk’ in the 2021 Act [10] has not yet been considered by the courts. The term is used in the Contempt of Court Act 1981 [103] and the meaning has been considered by the courts in that context. See, for example, Her Majesty’s Attorney General v. Express Newspapers [2004] EWHC 2859 (Admin).

6 Neither the investigations nor proceedings are limited to those in the Criminal Justice System in England and Wales.

1.2.5 The 2021 Act [10] makes further provision for the Regulator to require persons to provide copies of documents and other information in the person’s possession or control as part of a Regulator’s investigation.

1.3 The Code

1.3.1 This Code is based on the regulatory model historically (i.e. prior to the introduction of the 2021 Act [10]) in use for forensic science in England and Wales in that it requires each forensic unit to operate an effective quality management system and, where required by this Code, achieve/maintain accreditation to a suitable international standard and/or this Code. There are additions to this Code to cover the provisions set out in the 2021 Act [10] including Regulator’s investigations, issuing of compliance notices, issuing completion certificates, appeals and other functions of the Regulator. [7]

1.3.2 This Code applies to all those undertaking forensic science activities subject to the Code, whether individual practitioners, academics, public or private sector forensic science providers, and refers to all as forensic units. These can be small teams in larger organisations, sole practitioners or large providers and can be instructed by the prosecution or the defence.

1.3.3 This Code applies, directly, to forensic science activities undertaken for matters related to the Criminal Justice System in England and Wales. Future versions of the code can be applied to other jurisdictions and/or purposes by order of the Secretary of State [see s11(2)(c) of the 2021 Act [10]. It is open to other jurisdictions, or bodies, to voluntarily adopt the code (perhaps subject to relevant adjustment for differences in the legal systems) if appropriate stakeholders agree. [8]

1.3.4 This Code is not intended to be a substitute for the complete version of the international standards referred to herein. Section 42 of this Code cross

---

[7] The coverage of these issues in this Code is limited to what is needed to understand the operation of this Code. These matters are dealt with, in more detail, in relevant policy documents issued by the Regulator.

[8] The adoption of this Code by other jurisdictions, or bodies, does not extend the role of the Regulator unless the adoption follows, or involves, the enactment of regulations under s11(2)(c) of the 2021 Act [10].

references to some of the key clauses that appear in the normative references (see section 12.3 herein); this is not intended to be a comprehensive analysis of the provisions. Forensic units applying for, or holding, accreditation to one, or more, of the international standards (issued by the International Organization for Standardization) remain responsible for ensuring they are aware of all relevant requirements within, or related to, those standards.

Part A – Legal Position

2. The Forensic Science Regulator

2.1.1 The 2021 Act [10] placed the Regulator on a statutory basis (as a new legal entity) and provided the Regulator with legal powers. Those include, but are not limited to, the power to:

a. Issue a code of practice;

b. Investigate concerns; and

c. Protect the CJS from poor practice in forensic science.

2.1.2 While the 2021 Act [10] makes no reference to ‘quality’ or ‘standards’ the Written Ministerial Statement, in 2007 [12], made clear that the role of the Regulator related to quality standards in forensic science. The explanatory memorandum [13] which accompanied the bill (which became the 2021 Act [10]) and the Parliamentary debates [9] on the bill were clear that the main aim of the bill was to transfer the existing role to a statutory basis and provide additional powers.

2.1.3 The role of the Regulator therefore focusses on quality standards in forensic science as opposed to any other aspect of the provision of forensic science.

3. Basis of Appointment of the Forensic Science Regulator and Legal Powers

3.1.1 Those sections of the 2021 Act [10] which did not become effective on Royal Assent [see s13 of the 2021 Act [10] were brought into effect by Regulations issued by the Secretary of State [see s13(4) of the 2021 Act [10]]. Those Regulations are as follows.

a. ### brought sections ### into effect on ###.

---

9 The debates on the bill were as follows. In the House of Commons - the first reading [105], the second reading [106], the money resolution [109], the committee stage [107] and the third reading [108]. In the House of Lords – the first reading [110], the second reading [111], the committee stage [112] and the third reading [113]. Royal Assent was recorded on the 29th April 2021 [11].

b. ### brought sections ### into effect on ###.

4. Employment Rights Act 1996 [14]

Text to be developed

5. Forensic Science Activities

5.1 Legal Basis

5.1.1 The role of the Regulator covers forensic science. The creation of a statutory role meant it was necessary to define what is meant by the term ‘forensic science’ or at least those areas of ‘forensic science’ which would be subject to this Code.

5.1.2 The approach taken in the 2021 Act [10] [see s11] was to establish the concept of ‘forensic science activities’ (FSA). The definition adopted was, deliberately, one which could cover anything which might conceivably be considered forensic science. The 2021 Act [10] [see s2] requires the Regulator to define the FSA which are subject to the code. This places responsibility on the Regulator for defining, with sufficient clarity, what activities are FSA subject to this Code.

5.2 Definition

5.2.1 Section 11 of the 2021 Act [10] defines FSA as follows.

(1) In this Act “forensic science activity” means an activity relating to the application of scientific methods for a purpose mentioned in subsection (2).

(2) Those purposes are—

(a) purposes relating to the detection or investigation of crime in England and Wales;

(b) purposes relating to the preparation, analysis or presentation of evidence in criminal proceedings in England and Wales;

(c) such other purposes as the Secretary of State may specify in regulations made by statutory instrument.

5.2.2 At the time of publication of the first issue of this Code no regulations have been issued under the provisions of s11(2)(c).

5.2.3 The s11 definition is clearly a wide one which could cover a significant range of activities.

5.3 Limits on FSA

Link to Crime

5.3.1 The definition above, see section 5.2.1, makes clear that FSA must be undertaken for one of the purposes set out in s11(2) 2021 Act [10].

5.3.2 The definition refers to ‘crime’ rather than a specific crime so that the work does not have to be related to a specific offence or suspected offence.

5.3.3 The 2021 Act [10] uses the text ‘relating to’ which indicates the work does not have to be directly for the purposes stated.

Territorial Extent

5.3.4 The 2021 Act [10] creates a territorial limit to the scope of FSA by reference to ‘England and Wales’.

5.3.5 In relation to s11(2)(a) of the 2021 Act [10] the limit is taken to mean that the work must relate to crime in England and Wales. It imposes no restriction on where the FSA may be undertaken.

5.3.6 In relation to s11(2)(b) of the 2021 Act [10] the limit is taken to mean the criminal proceedings must occur in England and Wales. It imposes no restriction on:

a. Where the crime, or suspected crime, occurred; or

b. Where the FSA is undertaken.

Approach

5.3.7 The general requirements for FSA (see section 46 of this Code) are intended to give effect to the limitations set out above.

5.4 Levels

5.4.1 The 2021 Act [10] provides, see s2, that the Regulator shall issue a code of practice and, in that code, shall define which FSA are subject to the code. The Regulator powers to investigate [see s5 2021 Act [10]] and issue compliance notices [see s6 2021 Act [10]] apply only to FSA which are subject to the code.

5.4.2 In contrast, the Regulator powers to provide guidance [see s9(1) 2021 Act [10]] and provide advice [see s9(2) 2021 Act [10]] are available in relation to all FSA.

5.4.3 This means that the Regulator can define activities which might be considered forensic science (or some related field or undertaking) into levels as follows.

a. Activities which are not FSA.

b. Activities which are FSA, but which are not subject to the code.

c. Activities which are FSA and are subject to the code.

5.4.4 The Regulator has no direct role in respect of those activities which are defined not to be FSA.

5.4.5 Where an activity is defined as an FSA the extent of the Regulator’s powers depend on whether it is subject to this Code. Were an FSA is not subject to this Code the powers in s9 2021 Act [10] apply. Where an FSA is subject to this Code then the powers for a Regulator’s investigation [see s5 2021 Act [10]] and enforcement [see s6 2021 Act [10]] also apply. [10]

5.5 Approach to FSA Definition

5.5.1 To provide a structure to the FSA definitions the Regulator has set out a series of ‘sectors’ covering broad classes of activities which might be viewed as forensic science (or a related field or undertaking). Within these ‘sectors’ the Regulator has listed a series of ‘sub-sectors’ which describe relatively broad fields within the sector. In each of the ‘sub-sectors’ the Regulator has listed a series of ‘activities’ describing aspects of the work.

5.5.2 This structure is set out in the table in section 9 herein.

5.5.3 For each ‘sub-sector’ in the Table there is an appendix to this Code. The first section of each appendix is a detailed definition of each of the FSA listed for that ‘sub-sector’. It is stressed that in the table in section 9 herein, the ‘sectors’ and the ‘sub-sectors’ exist only to provide a structure for the definition of the

[10] The manner in which the powers in sections 5 and 6 2021 Act [10] apply is affected by the provisions of section 12.

FSA. They do not affect the definition of any FSA. The definitions of the FSA are those set out in the appendices to this Code.

5.5.4 The 2021 Act [10], see s2(2)(a), requires that this Code sets out which FSA are subject to the provisions of the Code. The primary purpose of the definition of FSA in this Code is to satisfy that requirement. It follows that a declaration that an activity is an FSA subject to the Code is conclusive on that issue in relation to this issue of the Code. Similarly, if the Code defines an FSA and states that it is not subject to the Code that is conclusive of that issue in relation to this issue of the Code. The FSA covered, and not covered, by the Code may be different in different issues of the Code.

5.5.5 The fact that an activity is not defined as an FSA in this Code should not be taken as evidence that it is not an FSA. Only a clear statement by the Regulator, in this Code, or by regulatory notice, will achieve this.

5.5.6 The nature of FSA means that the definitions of some FSA may appear to overlap with other FSA definitions. To ensure it is clear what is covered, and which standards apply for each FSA the definitions may include exclusions. In some cases, these exclusions will make clear that activities which are not considered FSA are excluded from a particular definition. This means that some activities, which are not considered FSA, also have to be defined. These are set out in the appendices to this Code.

5.5.7 There are several aspects of the definition of FSA which will be common across all, or most, definitions.

5.5.8 Section 48 of this Code sets out these general provisions and requirements which apply to all FSA definitions unless clear language to the contrary is included in a specific FSA definition.

5.6 Scope of FSA

5.6.1 A forensic unit which undertakes any part of an FSA is carrying on that FSA.

5.6.2 In general, a forensic unit which is carrying on an FSA is not required to deliver every aspect of the description of the FSA. However, there are FSA where a service of an appropriate quality can only be delivered is a minimum set of the aspects are delivered. In such cases the Regulator has established a ‘minimum

service requirement’. These are set out in the FSA definition in the relevant appendix to this Code.

5.7 Restrictions

5.7.1 The definition of FSA in the 2021 Act [10] is, deliberately, wide enough to cover most areas where scientific methods are used in the Criminal Justice System. In defining the FSA which are subject to this Code the Regulator has focussed on those FSA which have historically been considered forensic science.

5.7.2 In future editions of this Code the scope of activities which are covered by the Code may expand.

5.8 Significance

5.8.1 The purpose of defining activities as FSA is to delineate the remit of the Regulator. It is not intended, by itself, to make any comment on the nature or quality of any activity (whether an FSA or not).

6. The Code

6.1 General

6.1.1 Section 2 of the 2021 Act [10] requires the Regulator to “prepare and publish a code of practice about the carrying on of forensic science activities in England and Wales”.

6.2 Territorial Extent

6.2.1 The provisions of s2 of the 2021 Act [10] mean that this Code only applies to FSA which are undertaken in England and Wales.

6.2.2 The terms ‘England’ and ‘Wales’ are defined in The Interpretation Act 1978 [15]. An FSA will, subject to the point in section 6.2.3, be undertaken within England and Wales if the activity occurs within the areas covered in those definitions.

6.2.3 The following activities shall always be considered to occur in England and Wales regardless of the location of the forensic unit.

a. The reporting of the outcome of any activities; and/or

b. The provision of evidence (whether written or oral).

6.2.4 The definition of FSA also incorporates territorial restrictions. These are discussed in section 5 of this Code.

7. Transitional Provisions

7.1.1 The 2021 Act [10] [see s13(7)] allows the Secretary of State to implement transitional provisions as part of the commencement process.

Text to be developed.

8. International Obligations

Text to be developed.

Part B - Summary of Requirements

9. Summary of Requirements

9.1.1 This section provides a summary of the requirements set out in the appendices for each FSA. This is a summary and, in the event of any inconsistencies with the content of the appendices the appendices shall prevail.

Text to be developed

Part C - The Code

10. Legal Basis

10.1.1 This document is the code of practice issued by the Forensic Science Regulator pursuant to the provisions of s2 of the 2021 Act [10].

10.1.2 In accordance with the provisions of the 2021 Act [10] this Code has been:

a. Prepared and published by the Forensic Science Regulator [as required by s2];

b. Approved by the Secretary of State [as required by s3(3)(b)] on [Date to be inserted]

c. Laid before Parliament by the Secretary of State [as required by s3(3)(b)] on [Date to be inserted];

d. Approved by the House of Commons [as required by s3(3)(c)] on [Date to be inserted]; and

e. Approved by the House of Lords [as required by s3(3)(c)] on [Date to be inserted].

10.1.3 In accordance with s3(4) of the 2021 Act [10] the provisions of this Code come into force at 00:00:01 on [Date to be inserted].

11. Structure

11.1.1 This Code is formed of several parts as set out below.

a. Part A - Sets out the legal background to this Code.

b. Part B - Provides a summary of the requirements established for each FSA.

c. Part C – Sets out legal issues related to this Code.

d. Part D - Sets out the standards of conduct.

e. Part E - Sets out the standards of practice.

f. Part F - Contains information which is general to this Code.

g. Part G - Contains appendices to this Code. These may contain, inter alia, the following.

i. Information about specific issues.

ii. Definitions of FSA (and other definitions relevant to the delineation of FSA).

iii. Standards and requirements which are relevant to a specific FSA or groups of FSAs.

iv. The means of demonstrating compliance with this Code relevant to a specific FSA or group of FSAs.

12. General

12.1 Transitional Provisions

Introduction of the Code

Text to be developed.

Changes to the Code

12.1.1 This Code will change over time. This Code has, or in time will, replace the Codes of Practice and Conduct [4] issued by the non-statutory Forensic Science Regulator.

12.1.2 It is inevitable that there will be circumstances where the work on an individual case will transcend an issue of this Code.

12.1.3 All work should be performed in accordance with the Code which is in effect at the time the work was undertaken. There is no requirement to revisit work which has already been done if this Code changes.

12.2 Scope

12.2.1 This Code applies to any forensic unit undertaking an FSA to which this Code applies. The FSA which are subject to this Code are set out in the FSA definitions (see the appendices).

12.2.2 This Code specifies the requirements for competence for undertaking FSA. Where relevant, appropriate legal, regulatory and information security provisions are included.

12.3 Normative References

12.3.1 The following normative references are cited in this Code and, in areas where accreditation to an international standard is required by this Code, form the basis of demonstration of compliance with the requirements of this Code. References:

a. BS EN ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories; [1]

b. ILAC-G19:08/2014, Modules in a Forensic Science Process; [3]

c. BS EN ISO/IEC 17020:2012, General criteria for the operation of various types of bodies performing inspection; [2]

d. ILAC-P15:07/2016, Application of ISO/IEC 17020:2012 for the Accreditation of Inspection Bodies; [16]

e. UKAS-RG 201:2015, Accreditation of Bodies Carrying Out Scene of Crime Examination (Edition 2); [17]

f. BS EN ISO 15189:2012, Medical laboratories. Requirements for quality and competence; [18] and

g. BS EN ISO/IEC 17000:2020, Conformity assessment. Vocabulary and general principles. [19]

12.4 Terms and Definitions

12.4.1 For the purposes of this Code, the definitions of terms are provided in section 41 - Glossary.

12.4.2 The meanings of abbreviations and acronyms are given in section 40 - Acronyms and Abbreviations.

12.4.3 The word ‘shall’ is used in this Code where the clause is a requirement; the word ‘should’ is used to indicate the clause is a recommendation based on generally accepted practice in the forensic science profession.

12.5 Application of Standards

The Code

12.5.1 This Code sets out the standards, and other requirements, which apply to each FSA. The way this is done may be different for different FSA.

12.5.2 For each FSA this Code may demand compliance with any combination of the following.

a. The Standards of Conduct.

b. The Standards of Practice contained in the main Code (i.e. not the appendices).

c. The Standards of Practice contained in one, or more, of the appendices to this Code.

12.5.3 For each FSA which is subject to this Code the requirements in this Code operate from the date this Code becomes effective (the date specified in section 10 herein). All forensic units must comply with the provisions of the Code from the effective date set out in section 10.

12.5.4 This Code may include provisions with regard to demonstration of compliance (either generally or for specific FSAs) which are not operative from the date this Code takes effect (i.e. the date may be set in the future). In these areas the requirements of this Code must be complied with from the effective date but the demonstration of compliance (e.g. by accreditation) is not required until the date specified. It is open to forensic units to achieve the requirement before the date specified.

Non-Code Standards Documents

12.5.5 The Regulator may work with other bodies (e.g. professional bodies or regulators) to support the production of standards or requirements for certain fields of forensic science.

12.5.6 Unless such documents are incorporated into this Code, they do not form part of the code to be issued under the provisions of s2 2021 Act [10].

Other Documents

12.5.7 The Regulator may issue other documents (e.g. guidance documents). These do not form part of the code issued under s2 2021 Act [10].

12.6 General Provisions

12.6.1 In this Code any reference to legislation (e.g. statute or secondary legislation) should be taken to mean the following.

a. The legislation as amended.

b. Any secondary legislation created under powers contained within the statute.

c. Where the legislation is repealed and replaced the new provisions.

12.6.2 In this Code any reference to a specific body (e.g. a Government department) shall be taken to mean the body regardless if the name is altered and, should it be abolished, any successor body.

13. Modification

13.1.1 This is the first issue of the Code.

13.2 Tracking

13.2.1 Subsequent issues of the Code will adopt the following approach.

a. Significant changes from the previous issue will be highlighted in grey, significant deletions will be marked as “[deleted text]”.

b. Where sections are inserted, moved or renumbered, the subsequent renumbering of sections that follow will not generally be marked.

c. To comply with the Regulations on accessibility [20] the changes will be listed in a footnote from this section.

13.3 Approach

13.3.1 The Regulator will, under normal circumstances, modify this Code in the following manner.

a. The Regulator shall publish a notice of intent to modify this Code setting out the proposed changes. The proposed timescales for the changes will be set out.

b. The notice of intention to modify this Code will provide at least six months’ notice of the proposed changes.

c. The Regulator shall undertake a consultation, as required by the 2021 Act [10], on the proposed changes before finalising the changes which will be made to this Code.

d. The Regulator shall publish the Code which is to be submitted for approval under the provisions of s3 2021 Act [10].

e. Where common commencement dates have been introduced by HM Government for implementation of regulation consideration shall be given to the use of those dates.

13.3.2 While the above text sets out the normal approach it must be recognised that the role of the Regulator is, in part, to protect the CJS. Circumstances may arise where this process will not be followed.

13.4 Review

13.4.1 This document is subject to review at regular intervals. Comments should be sent to the address, or email provided, at: www.gov.uk/government/organisations/forensic-science-regulator.

14. Supremacy Provision

14.1 General

14.1.1 It may be necessary to publish a modified version of this Code (e.g. a version in a different language or one addressing specific accessibility issues). If such a version is published, its nature as a secondary version of this Code, will be made clear in the document.

14.1.2 In all cases the original version of this Code, or any issue of this Code, is to be taken as the definitive version of the document. In the event of any discrepancy

between the prime version and a secondary version the text of the normal version shall prevail.

14.2 Online Publication

14.2.1 This Code may be published online as both PDF and HTML versions.

14.2.2 In all cases the PDF version, of any issue of this Code, is to be taken as the definitive version of this Code.

Part D - Standards of Conduct

15. Standards of Conduct

15.1.1 The Regulator sets out, for all persons carrying on any FSA to which this Code applies (and this Code specifies compliance in the FSA definition), regardless of the source of the instruction, the values and ideals the profession stands for. These Standards of Conduct provide a clear statement to commissioning parties, the Criminal Justice System and the public of what they have a right to expect.

15.1.2 The Standards of Conduct are set out in section 43 herein.

15.1.3 Where this Code requires compliance with the Standards of Conduct, all practitioners shall comply with the Standards of Conduct and shall declare this compliance (or otherwise) as set out in section 37 herein.

Part E - Standards of Practice

16. Application

16.1.1 The Standards of Practice, subject to the point in section 16.1.2, apply to all forensic units carrying on an FSA to which this Code applies where compliance is specified in the FSA definition (see the appendices).

16.1.2 It is recognised that the Criminal Justice System may require the assistance of an expert who does not normally operate in the area of forensic science. Where such an expert is instructed in relation to a FSA to which this Code applies and compliance with the Standards are required, the expert shall not be subject to the provisions of the Standards of Practice set out in the main Code but shall comply with the provisions of section 44.2 herein.

17. Management Requirements

17.1 General

17.1.1 Where this Code, for an FSA, specifies accreditation, the forensic unit shall have a Schedule of Accreditation covering compliance with the standards identified in this Code for the methods, products and services it is, subject to the provisions in this Code with regard to infrequently commissioned experts (see section 44 herein) and infrequently used methods (see section 29.3.48 et seq herein), providing.

17.1.2 The forensic unit shall define all roles that could influence the performance of the forensic science activities undertaken and detail the competences (see section 27.3 herein) required for these roles. These roles include all those performing the following as part of a forensic science activity.

a. Planning and performing inspection activities.

b. Tests, including sampling.

c. Operating specific equipment.

d. Performing critical findings checks and peer review.

e. Signing/issuing certificates or test reports.

f. Providing interpretations/opinion.

g. Software installation, authorisation for software changes and administration of firmware and software (e.g. analytical software, anti-malware software).

h. Development, validation, and verification of new, adopted or adapted methods.

17.1.3 Where top management is referred to in relevant normative references (see section 12.3 herein), this should usually be at Chief Officer or board level and, in this Code, is referred to as the Senior Accountable Individual (see 17.2 herein).

17.2 Senior Accountable Individual

Appointment

17.2.1 Where a forensic unit is comprised of two, or more, practitioners it shall appoint a senior manager (that being at director, partner, board level, chief officer level or equivalent) to be the Senior Accountable Individual.

17.2.2 Where a forensic unit is comprised of only one practitioner that practitioner shall be the Senior Accountable Individual.

Role

17.2.3 The Senior Accountable Individual shall be responsible for the strategic leadership of the forensic unit’s compliance with this Code and to manage the risks related to any FSA undertaken by, or under the control of, the forensic unit. There should be particular focus on any risks which could adversely affect a criminal investigation or impede or prejudice the course of justice in any proceedings.

17.2.4 The 2021 Act [10] makes provision for circumstances where the Regulator has reason to believe that a person may be carrying on a forensic science activity to which this Code applies in a way that creates a substantial risk of:

a. Adversely affecting any criminal investigation, or

b. Impeding or prejudicing the course of justice in any proceedings. [10]

17.2.5 The Senior Accountable Individual shall take responsibility, on behalf of the forensic unit, in relation to any Regulator’s investigation or compliance action by the Regulator. [11]

17.2.6 The Senior Accountable Individual shall have the authority to make decisions and deploy resources to address quality matters in the forensic unit.

17.2.7 The name, and contact details, of the Senior Accountable Individual shall be notified to the Regulator. The Senior Accountable Individual will be the route through which any communications related to action under sections 5 and/or 6 of the 2021 Act [10] will be sent to the forensic unit

17.2.8 The forensic unit shall promptly (and in any event within 30 days) notify the Regulator, of any change in the information provided about the Senior Accountable Individual.

18. Business Continuity

18.1.1 The forensic unit shall have procedures to be implemented following interruption to, or failure of, business critical processes, to maintain or restore operations and ensure availability of information (at a level which prevents significant interruption to operations), and both confidentiality and integrity of that information. [12] [13]

18.1.2 The business continuity procedures shall include:

a. An IT incident management plan retrieval of critical data (see section 31 Control of Data (e.g. Backups, Recovery and Business Continuity); and

---

11 The responsibilities of the forensic unit in relation to investigations and compliance action by the Regulator are discussed in section 24.3 of this Code.

12 Further guidance, if required, can be obtained from ISO 22313:2020 Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301. [120] [122]

13 Commissioning party’s should ensure that their own business continuity plans have addressed the risk that a provider goes out of business with no legal successor, to ensure retained material, case files and associated paperwork is available (e.g. continuity and access records, validation records, competency records, calibration and maintenance records). Ideally this should be through stipulation in a contract, clarifying that copies of certain information need to be supplied with the case files.

b. Consideration of what additional supporting information would be required to support case file data (e.g. validation reports, calibration records).

18.1.3 A forensic unit may need to use externally provided services in the undertaking of all (or any part of) an FSA (see section 23 herein). The commissioning forensic unit should ensure that its business continuity procedures include provision to preserve and/or recover any material transferred to, or generated in the facility commissioned to perform the work. Where externally provided services are performed by a separate legal entity, these business continuity procedures should include the safeguards should that legal entity go out of business with no legal successor (e.g. through stipulation in a contract with the legal entity in question to assist in receivership disputes).

18.1.4 The business continuity procedures shall be tested on an annual basis and the results documented. [14] Any identified need for action to modify the plans shall be implemented and the plans re-tested.

19. Independence, Impartiality and Integrity

19.1.1 The forensic unit shall ensure that all of its practitioners are made aware of, and adhere to, the Standards of Conduct in respect of their independence, impartiality and integrity, and that the organisational structure, policies and procedures support this rather than hinder it.

19.1.2 Conflicts of interest, perceived or otherwise, and threats to impartiality may include a practitioner:

a. Having, or being perceived to have, an interest in the outcome of the case;

b. Being coerced or having the perception of being coerced, openly or secretively; [15]

---

[14] This should be scaled based upon risk, in some circumstances a desk-top exercise may be justifiable.

[15] The question of perception may be judged by reference to the test for apparent bias of members of the judiciary. In Magill v. Porter [2001] UKHL 67 the court noted “[The Court] must then ask whether those circumstances would lead a fair-minded and informed observer to conclude that there was a real possibility that the tribunal was biased”.

c. Being asked to disregard critical findings that support/undermine either the prosecution’s or the defence’s position;

d. Being asked (except where there is a clear legal reason for doing so) to limit the information being provided to the court including, but not limited to, findings that contradict any issued report(s);

e. Being the sole reviewer of their critical findings;

f. Being involved with activities that could be perceived as witness coaching or being coached, rather than training or familiarisation;

g. Being over-familiar with, or trusting, another person instead of relying on objective evidence;

h. Having organisational and management structures that could be perceived to reward, encourage or support bias;

i. Having a close/significant personal or financial relationship with a party likely to be affected by the outcome of:

   i. The practitioner’s work; and/or

   ii. The case.

j. Having a close/significant personal or financial relationship with any person acting as an expert witness in the case; or

k. Acting in self-interest.

19.1.3 It is possible for a conflict of interest to arise as a result of information held by a practitioner. This could be information, perhaps obtained from other parties to the case or previous dealings with some of the parties, making it difficult for the practitioner to adhere to their obligations to the CJS or their client.

19.1.4 Experts should consider relevant hypotheses for their findings prior to presenting their findings in the case.

19.1.5 The required policies and procedures shall not only aim to prevent internal and external influence on the results of their examinations and tests, but also cover the corrective action (such as formal disclosure) to be taken if there is a possibility of a practitioner’s judgement having been, or perceived to have been, compromised.

20. Confidentiality

20.1.1 The forensic unit shall have documented policies and procedures detailing confidentiality requirements, including any disclosure requirements, and shall ensure that those requirements are applied to any subcontractors. The procedures shall address the following.

a. The material held by the forensic unit which is subject to an obligation of confidentiality.

b. The nature of the confidentiality obligation and its application to all staff and external service providers.

c. The potential legal liability for breach of confidentiality.

d. The conditions that may allow the confidentiality to be waived or legally overridden and the process the forensic unit shall follow in such circumstances.

21. Document Control

21.1.1 The forensic unit shall apply document/version control procedures to the following where they are integral to the forensic process, including but not limited to:

a. Both hard copy and electronic copies;

b. Procedures – technical and quality;

c. Software;

d. Technical methods;

e. Forms;

f. Locally held copies of key external documents; and

g. Statutory documents (e.g. licences for possession of materials such as drugs or firearms).

21.1.2 The retention period for obsolete/superseded documents should be defined and should take into account commissioning party [21], regulatory [16] and legal requirements. [17]

22. Review of Requests, Tenders and Contracts

22.1.1 The processes surrounding the review of requests, tenders and contracts may occur at several different levels and at several key stages through the processing of forensic work.

22.1.2 The issues to be addressed shall include the following.

a. Whether the forensic unit can legally perform the work (e.g. does it have all required licences etc).

b. Whether the forensic unit meets the standards required for the work and the necessary means of demonstrating compliance.

c. Whether the practitioners have the level of background checks (e.g. security checks) the commissioning party requires for the work (see section 27 of this Code);

d. Whether the proposed work would properly address the issues for the CJS.

22.1.3 Further issues which should be considered may include, but not be limited to:

a. The processes leading to the documentation of an overarching Service Level Agreement (SLA)/contract between the commissioning party and the forensic unit;

b. The management of the adherence to the agreed SLA/contract;

c. The format and language of any report or disclosable information;

---

16 For example the Code of Practice issued under the provisions of s23 Criminal Procedure and Investigations Act 1996 [96] and the requirements of this Code.

17 Some documents, such as standard operating procedures or validation reports, may be required for the life of the techniques and a blanket 30 years is often applicable from the last time the technique they refer to was used and/or reported.

d. The documentation and review of more detailed case-specific requirements through the use of submission forms etc;

e. Outcomes from case conferences; and

f. Significant discussions with the Officer In Charge (OIC), solicitors etc.

22.1.4 The aspects discussed and agreed as part of the review of requests, tenders and contracts may include, but not be limited to:

a. Turnaround times;

b. Report format;

c. Items to be examined;

d. Case assessment and strategy;

e. Sequence of examination;

f. Precautions to be taken to preserve additional evidence;

g. Methods to be used;

h. Products to be delivered;

i. Costs;

j. Collection/transfer of items; and

k. Retention, destruction or return of items (see 35.6 Exhibit Return and Disposal).

22.1.5 A documented policy is required, which shall include recording of all relevant instances when work requirements are discussed and reviewed such that a demonstrable audit trail, including appropriate justifications and authorisations, is available for each piece of work undertaken.

23. Externally Provided Products and Services

23.1 Externally Provided Services

23.1.1 A forensic unit may obtain services from outside the forensic unit (externally provided services) [18] as part of the undertaking of all, or any part, of an FSA. This section applies to any externally provided service which could directly affect the quality of the forensic unit’s undertaking of an FSA.

23.1.2 The use of externally provided services, as described in the paragraph, shall only occur if the commissioning party has agreed in advance. The forensic unit commissioning the work shall ensure that:

a. All work meets the requirements of this Code;

b. All continuity, security and recording requirements are met; and

c. The provider of the external services has all required licenses and/or approvals necessary to perform the work (see section 23.1.6 of this Code).

23.1.3 The forensic unit obtaining the externally provided services remains responsible for the overall quality of the work, including that of any external element. [19]

23.1.4 Forensic units shall have a procedure for: [20]

a. Defining, reviewing and approving the forensic unit’s requirements for using externally provided services;

b. Specifying the requirements of the services to the external provider; and

c. Ensuring that external providers conform to relevant requirements of this Code.

23.1.5 Forensic units intending to obtain external services related to the undertaking of any FSA, or part of FSA, shall include in its business continuity procedure the arrangements that have been made to preserve retained material [21] should their

---

18 Externally provided services can be obtained through any model (contractual or otherwise) including subcontracts.

19 If the externally provided service is a forensic science activity which is subject to this Code, the externally provided services work will also be subject to this Code.

20 Forensic units conducting activities which require accreditation to ISO 17025 [1] should note that although there is overlap with the standard’s clause 6.6 Externally Provided Products and Services, the standard has wider requirements which also apply.

21 Including relevant data, reports and records.

external provider or its contracted storage facility cease business and have no legal successor.

23.1.6 Where any externally provided work is subject to any requirement for approvals or licences established by law, rules or convention, (such as work connected to firearms examination, child exploitation, drug analysis or for inclusion on the National DNA Database ® [22]), the external provider must be appropriately approved or licensed.

23.2 Externally Provided Products

23.2.1 Forensic units shall ensure that any swabs, consumables, sampling/collection kits, packaging and/or chemicals they use are fit for purpose and the forensic unit should assist commissioning parties in understanding the forensic unit’s acceptance criteria for items submitted. [23] Demonstration of fitness for purpose of chemicals (e.g. reagents) is through initial validation and appropriate quality control of chemicals used in the method.

24. Quality Issues

24.1 Control of Non-Conforming Examination and Testing

24.1.1 The forensic unit shall have policies and procedures to identify non-conforming work and, in addition, policies and procedures that are implemented when non-conforming work is identified.

24.1.2 Non-conforming examination and testing refers to any aspect of the forensic unit’s work that does not conform to the forensic unit’s policies, procedures, or customer expectations including the following. [3]

a. Scene examination.

---

22 The National DNA Database is a registered trademark of the Secretary of State for the Home Department.

23 The manner in which this can be demonstrated may include consumable manufacturers and kit assemblers meeting the requirements set out in the Publicly Available Specification (PAS) 377:2012 Specification for consumables used in the collection, preservation and processing of material for forensic analysis - Requirements for product, manufacturing and forensic kit assembly [104] and/or BS ISO 18385:2016 Minimising the risk of human DNA contamination in products used to collect, store and analyse biological material for forensic purposes [118].

b. Laboratory examination.

c. Sampling.

d. Testing.

e. Results.

f. Witness testimony.

24.1.3 Examples of non-conforming testing include are not limited to, significant instances of:

a. Unexpected performance in proficiency testing/inter-laboratory comparison (see 36.1 Inter-Laboratory Comparisons (Proficiency Tests and Collaborative Exercises));

b. Unauthorised access to restricted areas or information;

c. Missing or compromised items/case files;

d. Equipment failing to receive timely calibration or maintenance;

e. Staff failing to follow procedures or norms of integrity that impact on quality;

f. Judicial criticism;

g. Potential criminal activity by staff;

h. Withdrawal of security clearance from staff;

i. Contamination incidents which may have an adverse impact on the CJS (e.g. those not identified through the use of quality controls within the method); [24]

j. A technical method being found to be producing erroneous results;

k. Any standards/reference materials, equipment or reagents being found to have defects or deficiencies; or

[24] Where contamination incidents which are detected by the routine safeguards do not normally warrant notification to the Regulator a significant number of such events may indicate an underlying issue worthy of reporting.

l. Anything likely to cause a disruption to the provision of service at the expected quality, including but not limited to, removal/suspension of accreditation.

24.1.4 The forensic unit shall maintain a record of non-conformities which:

a. Is capable of being used to identify trends;

b. Includes any concessions obtained to use non-conforming work;

c. Includes any review reports;

d. Details any corrective and/or preventive actions taken; and

e. Is retained in line with the case file retention period.

24.1.5 Initially the significance of a non-conformity in relation to the validity of examination or test results shall be evaluated and its root cause identified. This review shall include assessment of any impact on casework already reported, remedial action required on the individual non-conformity as well as whether the root cause analysis points to wider systemic issues which could indicate risk of reoccurrence or previously unidentified occurrence.

24.1.6 The forensic unit shall inform the Regulator about any non-conforming test if it has potential to significantly disaffect the commissioning party such that it could attract adverse public comment, be against the public interest or lead to a miscarriage of justice, and shall be provided with an report on the review of the non-conformity. [25]

24.2 Complaints

24.2.1 The forensic unit shall have policies and procedures for dealing with complaints. These procedures shall define what constitutes a complaint [26] in relation to the work undertaken by the forensic unit and shall ensure that appropriately scaled reviews are instigated on receipt of any complaints.

---

[25] The Regulator shall be informed at the earliest opportunity once a reportable issue has been confirmed as a quality failure rather than after a potentially prolonged review. Basic information on the incident and likely timescale for the review is often all that is needed at the notification stage.

[26] A commonly accepted definition is any expression of negative feedback.

24.2.2 The forensic unit shall inform the Regulator via fsrenquiries@homeoffice.gov.uk or to the address given at www.gov.uk/government/organisations/forensic-science-regulator at the earliest opportunity about any complaint or non-conforming examination and/or test if it has significantly disaffected the commissioning party such that it could attract adverse public comment, be against the public interest or lead to a miscarriage of justice. [27] The policies and procedures relating to complaints shall also indicate the escalation criteria and the individual/role holder responsible for notifying the Regulator.

24.2.3 Reviews prompted by complaints shall include examination of the potential impact on any work that has already been completed by the forensic unit. In the event that it is shown that there could have been an impact on any previous work this should be dealt with through the non-conforming work process (see 24.1 - Control of Non-Conforming Examination and Testing).

24.2.4 The forensic unit shall retain records of all complaints and of the subsequent reviews and outcomes in line with the case file retention period. Where the complaint has been referred to the Regulator, a copy of the report on the finding of the review shall be provided to the Regulator.

24.2.5 Complaints may be received from many sources including the commissioning party, persons professing to be victims of crime, police forces, and other departments within the same forensic unit (e.g. laboratory, scene of crime unit, investigation unit) and the judicial system (including adverse court decisions pertinent to the work).

24.3 Regulator’s Consideration of Quality Issues

General

24.3.1 The Regulator may become aware of quality issues in a forensic unit in several ways. These include, but are not limited to, the following.

---

27 In this Code the term ‘miscarriage of justice’ means (a) an unsafe conviction, (b) a wrongful acquittal, (c) the inability to bring an offender to justice (d) delaying bringing an offender to justice and (e) the inability to clear the innocent.

a. Notification by a forensic unit under the provisions of section 24.1.6 above;

b. Notification by a forensic unit under the provisions of section 24.2.2above;

c. Notification by a third party; and/or

d. Information in the public domain (e.g. a court judgment or media reports).

24.3.2 The Regulator’s response to such quality issues depends on the nature of the issues and their potential impact. The options include, but are not limited to, the following.

a. To work with the forensic unit as part of the normal quality monitoring process to determine the nature of the issues and the appropriate response to reviews into non-conforming examinations and tests.

b. To initiate a Regulator’s investigation under the provisions of s5 2021 Act [10]; and/or

c. To initiate compliance action under the provisions of s6 2021 Act [10].

24.3.3 The manner in which the Regulator deals with the appropriate response is set out elsewhere [22] .

24.3.4 The following parts of section 24.3 of this Code sets out what the Regulator expects of forensic units when any quality issues are being considered by the Regulator.

Monitoring of Quality

24.3.5 Forensic units are involved in the operation of the CJS and, as a consequence, shall act in the interests of the CJS at all times.

24.3.6 Where the Regulator is considering a potential quality issue in a forensic unit that forensic unit shall:

a. Co-operate with the Regulator to the extent permitted by law;

b. Provide, as far as permitted by law, all information sought by the Regulator, or potentially relevant to the Regulator’s consideration;

c. Ensure sufficient resources are employed to address the issue in a suitable timescale;

d. Act in the interests of the CJS.

Regulator’s Investigations [s5 2021 Act [10]]

24.3.7 Where it is appropriate to initiate a Regulator’s investigation into any aspect of the work of a forensic unit the forensic unit shall, in addition to the requirements set out above in relation to monitoring (see section 24.3.6 above):

a. Familiarise itself with the provisions of s5 2021 Act [10];

b. Ensure that all representatives involved in the Regulator’s investigation are:

i. Aware of the provisions of s5 2021 Act [10];

ii. Aware of the potential consequences of non-compliance with notices issued under s5 2021 Act [10].

Compliance Action [ss6-8 2021 Act [10]]

24.3.8 Where the Regulator initiates compliance processes in relation to any aspect of the work of a forensic unit that unit shall, in addition to the requirements set out above in relation to monitoring (see section 24.3.6 above):

a. Familiarise itself with the provisions of sections 6-8 2021 Act [10];

b. Ensure all representatives involved in the Regulator’s investigation are:

i. Aware of the provisions of sections 6-8 2021 Act [10];

ii. Aware of the consequences of non-compliance with any notice issued.

Reporting

24.3.9 The existence of a Regulator’s investigation or compliance action (i.e. the issue of a compliance notice, the application for and/or granting of an injunction, the initiation of contempt proceedings or finding of contempt) may need to be disclosed in reports. Similarly, the fact that a Regulator’s investigation or compliance action has previously taken place may need to be disclosed in reports. This is discussed in section 37.6 below.

25. Control of Records

25.1 General

25.1.1 The forensic unit shall establish retention times that satisfy the requirements of legislation, [28] its accrediting body, the party commissioning the work [21] and this Code.

25.1.2 Records shall be stored and subsequently disposed of in a manner appropriate to their sensitivity and/or protective marking (e.g. incinerated or shredded to a specified standard which has been notified to the commissioning party).

25.1.3 Protective marking (e.g. with a Government Security Classification [23]) does not, by itself, provide an exemption to disclosure obligations. [24]

25.1.4 Where records are distributed across systems and/or locations, the forensic unit shall have a procedure to be able to retrieve and collate records required for reporting cases. The procedure shall detail the data types covered (see also procedural requirements in 31 Control of Data).

25.2 Technical Records

25.2.1 As a minimum, the technical records [29] shall contain all relevant information relating to the following.

a. The collection and movement of material (physical items, data and records), including:

   i. The date on which the material was taken or received;

   ii. The date of subsequent movement of the material to another party;

   iii. From whom or where and to whom or where the material was moved; and

---

28 At the time of issue of this Code, the relevant requirements are set out in the Code of Practice issued under the provisions of s23 Criminal Procedure and Investigations Act 1996 [96].

29 Technical records include accumulations of data and information that result from carrying out tests – see Glossary.

iv. The means by which the material was received or passed from/to another party (see 35. Handling of Test Items).

b. Sufficient relevant detail to be able to trace any analytical output to:

i. A specific instrument;

ii. Instrument configuration, e.g. software version or, if relevant, firmware;

iii. The operator; and

iv. The date of the analysis.

c. The examination of items, and materials recovered from items, and whether made by the practitioner or an assistant.

d. Verbal and other communications, including reports and statements.

e. Meetings attended and telephone conversations, including points of agreement or disagreement, and agreed actions.

f. Emails and other electronic transmissions (e.g. images) sent or received.

25.2.2 The records, in whatever form, shall be clear and comprehensive, and expressed in such a manner and in sufficient detail that another practitioner in the same field, and in the absence of the original practitioner, can follow the nature of the work undertaken, any interpretations/opinions made, and the inferences drawn from the work. This is particularly important in situations where an insufficient quantity of the exhibit remains for independent re-examination or testing, or the form of the exhibit is altered.

25.2.3 Whenever practicable, technical records shall be produced contemporaneously with the examination. The practitioner shall begin making records from the time instructions are received and shall continue making records throughout their involvement in the case. If there is any discussion about the case, or advice on tasking or submission was sought, prior or during contract review it may be appropriate to start making records before receiving formal instructions from the commissioning party.

25.2.4 When an examination, test result or observation is rejected, the reasons shall be recorded.

25.2.5 For the period of record retention, traceability shall be maintained for all names, initials and/or identifiers. These should be legible and understandable.

25.2.6 It shall be possible to associate all changes to critical data with the person having made those changes. [30] [31] Reasons for the changes shall be recorded.

25.2.7 Hard copy records generated by the forensic unit used as part of the case file shall be paginated using a page numbering system which indicates the total number of pages. [32]

a. Each page of every document in the case record shall be traceable to the practitioner responsible for the sampling and/or performance of each examination or test, to a uniquely identified case and uniquely identified item/exhibit. [33]

b. It shall be clear from the case record who has performed all stages of the analysis or examination and when each stage of the analysis or examination was performed.

c. Alterations or comments in the records shall be clear and be signed, or otherwise be attributable to the individual who made them and dated.

25.3 Checking and Review

25.3.1 The forensic unit shall have a procedure for checking and review. For methods that require calculations [34] and/or critical data transfers that are not part of a validated electronic process, the procedure shall include a requirement for effective checks of those calculations and/or critical data transfers to be carried out.

---

30 A system, for example, with timed and dated electronic signatures could achieve this aim.

31 Changes to critical data shall be traceable, however it is accepted that systems may not always facilitate this. It is therefore acceptable for the records to be located in different systems or locations.

32 See ILAC-G19 [3] section 3.5, however assurance of adequate control of electronic records will also need to be demonstrated.

33 Items should have an identifier which is unique within the organisation rather than simply within the case. Initials and number and/or date is not considered unique and although would not devalue or invalidate the exhibit if properly handled, it does add a risk which should be avoided.

34 Including those embedded in spreadsheets.

25.3.2 The forensic unit shall have a procedure for carrying out checks on critical findings and designate competent individuals authorised to carry out such checks. [35] [36] Where checks on critical findings are carried out, the records shall indicate that each critical finding has been checked and whether it was agreed, or not and by whom and when the checks were performed. The procedure should include a process for resolving any discordant results or findings.

25.3.3 Where the forensic unit has deemed [37] the procedure requires an independent check, the organisation should define this level of independence [38] and records should be kept to demonstrate this.

25.3.4 The forensic unit shall have documented policies and procedures and authorised practitioners for the review of case records, including reports and statements. The review shall establish from the case notes and discussion with the practitioner that the work carried out is:

a. Appropriate to the requirements of the case;

b. Fully documented in the case notes, with appropriate checks on critical findings, calculations and data transfers;

c. In compliance with the forensic unit’s documented policies and procedures; and

d. Consistent with the contents of the report or statement.

25.3.5 In all reviews, the case record shall indicate that the review has been carried out, by whom and when.

25.3.6 The checks and reviews shall be recorded as entries against each finding or on a summary of findings or on a report, as appropriate.

---

35 The forensic unit may identify individuals external to the unit to conduct critical findings checks.

36 The forensic unit shall demonstrate the competence of persons conducting critical findings checks (e.g. inclusion in the forensic unit’s proficiency trials), this includes persons external to the unit if they perform this role.

37 For instance, this determination may be at the identification of end-user requirements in the validation study.

38 ILAC-G19 [3] section 4.7.5 requires this check to be conducted without knowledge of the original result where the critical findings check is the only quality control.

25.3.7 If the checker/reviewer disagrees on any point and the matter cannot be resolved, the reason(s) for the disagreement and any action taken as a result shall be recorded.

26. Internal Audits

26.1.1 The annual audit programme shall cover all aspects of the management system. This shall include, but not be limited to:

a. Implementation of the management system;

b. Records of individual files; and

c. Security and integrity of information and data (also 31.3 Electronic Information Security).

26.1.2 A risk assessment-based approach should be taken to determine the frequency of the audit schedule, but methods shall be audited at least once every four-year cycle. [39]

26.1.3 Where the forensic unit undertakes to make statements of opinions and interpretations, the audits shall include a review of the process by which these are made and of the competence requirements of the individuals authorised to make such statements.

26.1.4 Where examination and testing activities are delivered from a number of different operational sites, the internal audits shall cover all sites and all aspects of the management system.

26.1.5 When the results of the audit cast doubt on the effectiveness of examinations, or the correctness or validity of the forensic unit’s test results to the extent that misleading information may have been reported, the forensic unit shall treat the audit result as a non-conforming result.

---

[39] The frequency of audits should take account of the length of time (and stability of) the quality managements system has been in place, the size of the organisation, the complexity of the work being audited, the frequency of use of specific technical methods or procedures, and the potential consequences of noncompliance with the requirements. The value of occasional unannounced audits should also be considered.

27. Personnel Requirements

27.1 General

27.1.1 The forensic unit shall ensure appropriate background checks (e.g. security checks) have been completed on all candidates for employment and contractors in accordance with relevant laws, regulations and ethics. These checks shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. [40]

27.1.2 The commissioning party shall be notified of the level of background checks held in the forensic unit by staff with access to the data and items to allow a determination of whether the level is acceptable (see section 22 - Review of Requests, Tenders and Contracts).

27.1.3 The contracts for all staff, permanent and temporary, shall contain confidentiality agreements, [41] setting out their own and the forensic unit’s responsibility for information security, and details of their expected conduct.

27.2 Standards of Conduct

27.2.1 The forensic unit shall have a Code of Conduct compatible with the Standards of Conduct provided in section 43 herein. Practitioners shall be made familiar with how the Code of Conduct relates to their role in the administration of justice and details of how this was achieved shall be recorded.

27.3 Competence

---

40 The required level of clearance for prolonged or unsupervised access to case material is normally Security Check (SC) [114] or Non-Police Personnel Vetting (NPPV) level 3 [115], or equivalent. The clearance level required may however be varied in writing by the commissioning party, the controller of the data or the Senior Accountable Individual of the commissioning party (where the party and the forensic unit are part of the same organisation).

41 The confidentiality agreements should cover the intellectual property of the forensic unit and all information relating to casework, and shall not conflict with any disclosure requirements.

General

27.3.1 The forensic unit shall determine and document the requirements for competency and ongoing competency for each role, as set out in section 17 herein, including the competences required for reporting findings.

27.3.2 The forensic unit shall determine the appropriate competence framework for practitioners, [42] this should include the following.

a. Education.

b. Qualification.

c. Training.

d. Technical knowledge.

e. Skills and experience.

f. The nature of the competence assessment.

g. The frequency of reassessment of competence.

h. Whether observation of any testing or inspection work is required, and if so, the frequency of this.

27.3.3 The forensic unit shall have processes to address the following.

a. Remedial actions when competence is found to have lapsed. See also 24.1 - Control of Non-Conforming Examination and Testing.

b. Remedial actions required should there be an event which undermines the credibility of a practitioner or the forensic unit. Such events may include, but not be limited to, the following.

i. Judicial criticism.

ii. Complaints.

iii. Criticism by a professional body.

iv. Criticism by the Regulator.

---

[42] This may be a locally or nationally devised framework.

Competence Required for Reporting

27.3.4 Forensic units shall ensure that all practitioners who provide factual evidence based on scientific methodology are additionally able to demonstrate, if required:

a. Whether there is a body of specialised literature relating to the field;

b. That the principles, techniques and assumptions they have relied on are valid;

c. An understanding of where factual reporting in the forensic science activity ends, and where expert evidence with interpretation and opinions begins.

d. That assumptions they have relied upon are reasonable; and

e. The impact that the uncertainty of measurement associated with the application of a given method could have on any conclusion.

27.3.5 Forensic units shall ensure that all practitioners who provide expert evidence have a sufficient level of experience, knowledge, integrity and, where appropriate, qualifications, relevant to the type of evidence being adduced, to give credibility to the reliability of the work undertaken and the conclusions drawn. They shall also ensure that they are able to explain their methodology and reasoning, both in writing and orally, concisely in a way that is comprehensible to a lay person and not misleading.

27.3.6 In determining competence, the forensic unit shall consider whether any issues, other than those listed in section 27.3.5 above, show that an otherwise apparently suitable person is not competent. Relevant issues include, but are not limited to, the following.

a. Adverse judicial comments.

b. Adverse findings by the Forensic Science Regulator.

c. Adverse findings by professional or regulatory bodies.

27.3.7 Forensic units shall ensure that all practitioners who provide expert evidence based on their practical experience and/or their professional knowledge are additionally able to provide: [43]

a. An explanation of their methodology and reasoning;

b. Reference to a body of up to date specialised literature relating to the field of expertise and the extent to which this supports or undermines their methodology and reasoning;

c. An assessment that any database they have relied on is relevant and sufficient in size and quality to justify the nature and breadth of inferences drawn from it, that the inferences are logically sound and that alternative hypotheses in the investigative mode and alternative propositions in the evaluative mode have been properly considered;

d. A demonstration that their methodology, assumptions and reasoning have been considered by other scientists and are regarded as sound, or, where challenged, the concerns have been satisfactorily addressed;

e. An assessment of the extent to which their methodology and reasoning are accepted by their peers, together with details of any outstanding concerns;

f. Relevant information to support claims of expertise, as well as anything that may adversely affect credibility or competence (e.g. adverse judicial findings); [24] [44] and

g. The statement of understanding and truth in expert reports for the CJS in England and Wales, as required in Criminal Practice Directions V 19b (see 37.1.9 herein and Criminal Practice Directions v 19b.1.13) [25].

27.3.8 Expertise cannot be simply measured in years, number of cases examined, educational achievements, post-nominals or seniority, nor is it equivalent to

---

43 Also see the list included in the Criminal Practice Directions V (19A.5c) [25].

44 Note the Criminal Procedure Rules 19.3-(3c) [34] requires experts to provide “notice of anything of which the party serving it is aware which might reasonably be thought capable of detracting substantially from the credibility of that expert.” This provision applies to experts regardless of the source of instruction.

credibility or eloquence although all these elements may contribute. The broad range of case circumstances encountered in any discipline of forensic science means that a particular expert will have more relevant experience and expertise in some cases than in others.

a. The competence of each expert in each discipline in which they claim expertise shall be assessed, both initially and thereafter at appropriate intervals.

b. Continuing Professional Development (CPD) is an important element of ensuring ongoing competence, as is ensuring that experts remain up to date with their knowledge of the scientific literature relevant to their field. This enables them to comply with their obligations under CrimPR 19.4 (b) and (f).

c. Experts should participate in regular calibration of their expertise [26] [27] through, for example, proficiency tests that are representative of the complexity encountered in casework.

27.4 Competence Records

27.4.1 The forensic unit and/or individual practitioners, including those in external provider roles (and other providing external services) shall maintain, and keep readily available, records of education, training, skills and experience in sufficient detail to provide evidence of proper training and formal competence assessment. [45] These records shall include, but not be limited to:

a. Academic and/or professional qualifications;

b. Internal/external courses attended;

c. Relevant training/retraining received whilst employed by the forensic unit;

d. Any subsequent remedial action from any substantive complaints, errors or adverse judicial comments;

---

45 This may include records of Continuous Professional Development.

e. Any substantive accolades, commendations, etc. pertinent to skills and experience;

f. The tasks for which the individual has been assessed as competent and authorised to carry out; and

g. The date(s) on which competence and authorisation were confirmed.

27.4.2 The competence system shall be fully documented, and the forensic unit shall have a policy for retention of training manuals, training and competence assessment records in line with the policy for retention of case files.

28. Accommodation and Environmental Conditions

28.1 Laboratory/Examination Facilities

28.1.1 The laboratory/examination facilities shall include, as appropriate (to the work being undertaken):

a. Suitable laboratory accommodation and appliances (e.g. laboratory benches, safety cabinets, refrigerators, freezers) and space (per employee) to carry out the work to the required standard safely and without cross-contamination;

b. Provision of appropriate environmental conditions (e.g. lighting, temperature, humidity, ventilation/air flow) required to facilitate correct performance of examinations or tests, and not adversely affect the required quality of any measurement or invalidate results;

c. Proportionate protection against likely risks, such as arson, theft or interference with items/exhibits;

d. Archive/storage facilities with adequate storage conditions to prevent loss, deterioration and contamination, and to maintain the integrity and identity of documents/records/test items/exhibits before, during and after examinations or tests have been performed; and

e. Facilities for the secure disposal of confidential waste and the safe disposal of hazardous materials.

28.1.2 The access and use of item/exhibit storage areas and server rooms should be controlled in addition to laboratory areas where work is carried out. The forensic unit shall hold on record a list of all staff who are authorised to enter these areas. This shall be reviewed and updated regularly.

28.1.3 Delivery and loading areas, and other points where unauthorised persons may enter the building, shall be isolated from casework and information processing areas and access shall also be controlled. Unauthorised persons needing to enter controlled areas shall be escorted at all times by authorised staff and a record of these entries shall be maintained.

28.2 Contamination Avoidance, Monitoring and Detection [28] [29] [30]

28.2.1 The forensic unit shall have policies and procedures relevant to the nature of the casework for the prevention, monitoring and detection of contamination that could interfere with the analyte of interest.

28.2.2 The steps in establishing procedures relevant to contamination control in recently introduced (or amended) methods [46] for trace evidence shall include, [47] but not be limited to:

a. Conducting a hazard or risk-based analysis of the entire method with respect to contamination (e.g. process mapping);

b. Identifying critical control points in the process where contamination events could occur (e.g. consumable selection, transfers, etc.) and for these critical control points:

   i. Establish acceptable contamination control limits at each point;

   ii. Establish monitoring requirements (e.g. frequency); and

---

46 This is taken to be methods introduced or put forward for accreditation from October 2016.

47 With new methods involving data or digital media, steps in establishing procedures relevant to data contamination control shall include 28.2.2 a, b, and e, although if exhibits are likely to also require trace evidence analysis this should be conducted first, or all these issues may still apply.

iii. Establish preventative and corrective actions (e.g. when acceptable or control limits are found to be exceeded);

c. Establishing effective methods for both routine and deep cleaning/decontamination of facilities and surfaces;

d. Establishing requirements for record keeping; and

e. Establishing procedures for verifying that the contamination control process remains fit for purpose.

28.2.3 The processes and procedures for the management of contamination for trace evidence shall also include, but not limited to, consideration of the following.

a. Limiting and recording, and where necessary preventing, access by internal and external visitors to any areas where FSA are undertaken where any recent activity by the visitor relevant to the FSA being undertaken could have an adverse effect on that FSA. Such activity could include, but not be limited to:

i. Incident scene attendance;

ii. Examination of complainant and/or suspect (e.g. for the purposes of taking samples);

iii. Prisoner handling; and

iv. Handling of, or exposure to, relevant materials (e.g. firearm and drugs).

b. Effective separation [48] of incompatible activities to prevent cross-contamination. This includes, but is not limited to, the handling of:

i. Un-amplified and amplified DNA;

ii. High and low-level drugs work;

---

48 The extent of physical separation will dictate if objective evidence is needed to demonstrate effectiveness; for instance, a different facility versus simply an adjacent room with potentially shared access routes or service such as air conditioning will require different approaches. However, if temporal separation is the intention, then objective evidence to show the effectiveness of the approach is expected.

iii. Toxicology work involving samples likely to have high and low levels of drugs;

iv. Examination of firearms and firearm discharge residues;

v. Examination of accelerant and fire scene debris; and

vi. Examination of test items from suspects, complainants and scenes.[49]

c. Policy on use of disposable equipment in specified areas and/or performing specific FSAs (e.g. gloves, face masks and mop caps).

d. Testing of consumables and chemicals in all stages of the examination/analytical processes and, where appropriate, testing for specific contaminants that could interfere with the success or interpretation of the examination or test (see also 28.2.2 herein).

e. Good working practices, such as:

i. Protecting test items/samples in wrapping/containers when not being worked on or used;

ii. Using only new, or suitably cleaned equipment to remove solvent, standard or reagent from stock bottles;

iii. Not pouring unused portions of solvent, standard or reagent back into bulk supplies; and

iv. Frequent changing of solvent used for rinsing equipment.

f. Good housekeeping practices.

g. Analysis of blank controls.

h. Environmental sampling/monitoring with particular reference to acceptable levels of relevant potential contaminants. This should include equipment, work areas, consumables and clothing to ensure that any contamination of

[49] The same examiner should not examine the complainant and a suspect in relation to the same alleged incident.

accommodation and/or equipment that does occur is recognised and controlled.

i. Using methods for both routine and deep cleaning/decontamination which include consideration of the following:

    i. The nature of contaminants relevant to the operation of the FSA and/or the forensic unit;

    ii. Work surfaces, walls, doors, flooring, ceiling, ducting, other fixtures and fittings and the likely vectors of contaminant transmission;

    iii. The materials/chemicals appropriate for use in contamination control;

    iv. Appropriate training and competence of staff deployed in cleaning/decontamination processes; and

    v. Governance and oversight by senior management.

28.2.4 The policies and procedures shall ensure access to areas, other than scenes of incidents, where FSA are undertaken is restricted to authorised individuals. These individuals shall be required to provide samples, and any necessary consent (e.g. for analysis and use of data), for elimination databases relevant to the nature of the work undertaken in areas they access (e.g. DNA analysis, dactyloscopic analysis) and any results found in casework screened against them as detailed in the forensic unit’s policies and procedures. These databases may be locally or remotely maintained.

28.2.5 Policies and procedures for elimination databases of laboratory staff, internal/external visitors and equipment suppliers should include, but are not limited to:

a. Reporting policies;

b. Data formats;

c. Searching policies;

d. Validation of searching procedures;

e. Security and access;

f. Retention periods;

g. Sharing agreements (i.e. between laboratories/forensic units);

h. Agreements/consents; and

i. Release forms.

29. Methods and Method Validation

29.1 General

29.1.1 The general requirement is that all technical methods and procedures used by a forensic unit shall be fit for purpose.

29.1.2 This involves establishing that the method operates in the expected manner, that the limitations of the method are properly understood, that the planned use of the method is appropriate and the approach to reporting is sensible.

29.1.3 Validation allows a proper understanding of the risks involved in the use of a method.

29.2 Selection of Methods

29.2.1 This section details the principles of the requirement for validated methods, the next section, 29.3 Validation of Methods, details the required processes.

29.2.2 Forensic units with methods already [50] within the schedule of accreditation will normally only be required to collate the existing validation paperwork to form as comparable a validation library as possible, and produce the short statement of validation completion as described in 29.3.63 herein. [51]

29.2.3 Even where a method is considered standard and is in widespread use, scientific validity will still need to be demonstrated. The topic of verification of the validation of adopted methods is discussed below although many of the other validation steps are likely also to apply. If a method is being newly

---

50 This is taken to be methods introduced or put forward for accreditation prior to October 2016. However, at least one example of a validation compliant with the Codes will be required for assessment to include the Codes in the schedule of accreditation.

51 Subsequent releases of these Codes may extend the requirement to existing methods. However, updates in technology, reviews of existing methods and the need for continuous improvement are expected to prompt validation studies.

included in the forensic unit’s scope of accreditation and validation has not been conducted at the laboratory site where it is to be implemented, the forensic unit will have to follow the adopted methods procedure, which ends in the production of a validation library and statement of completion as well as demonstrating the method works in their hands.

29.2.4 If a method requires the use of portable equipment (i.e. equipment intended to be used at different locations) for any reason, the validation study shall include testing any additional controls as well as assessing any additional aspects that may impact on the tests. For ISO 17020 [2] applications see, for example, Process Requirements section 7.1.1 in UKAS-RG 201 [17] (including but not limited to temperature, humidity, surfaces, cross reactivity, lighting, cross contamination control, handling controls).

29.2.5 The forensic unit should have validated the method, product or service prior to use in casework in accordance with the requirements of this Code. If the implementation plan requires a period of pilot after the validation study for the validation to be considered complete, such as might be the case for novel [52] techniques, non-routine or infrequently used activities, or if there is any other deviation from the validation requirements set out in this Code, the forensic unit should ensure that the status of the validation for the product, method or service is clearly understood by the commissioning party prior to agreeing use in casework.

29.3 Validation of Methods

29.3.1 The forensic unit shall use methods of demonstrable validity (see the Standards of Conduct in section 43 herein).

29.3.2 Validation should be conducted prior to implementation of the method. This may be performed in its entirety by the forensic unit, or the studies to produce the data may be performed by the manufacturer or another forensic unit; in which

[52] Major breakthroughs, novel uses of existing science, or significant changes might warrant wider stakeholder consultations. In these cases, it would be useful to inform the Regulator, who may advise on the most expedient method of ensuring that the CJS requirements are understood.

case the forensic unit implementing the method shall review the data to determine if it is adequate, reliable and relevant to the purpose it intends for the method (see Verification of the Validation of Adopted Methods 29.3.39 to 29.3.45).

29.3.3 Except where the method has been validated for incident scene use (see, for example, UKAS-RG 201 [17]), if the validation has not been conducted at the site that will be using the method the forensic unit shall verify the scope of the validation with the required steps in 29.3.6 herein. This may be scaled up or down according to the adequacy and relevance of the available existing validation study. In such cases, following review of validation data to determine if the validation is adequate, the forensic unit’s own practitioners trained and signed off as competent in the procedure shall demonstrate such adopted methods perform reliably at the given location by following the validation process. [53] [3] [31] [32]

29.3.4 The validation policy or procedure shall set out roles and responsibilities of practitioners involved in conducting validation, authorisation of key stages and reviewing outcomes.

29.3.5 To ensure validation studies are conducted on the final method, there should be a clear boundary between development and validation. It is important that any significant unexpected outcomes are not corrected during validation, but that the method is declared to have failed validation. The method should then be amended, and validation repeated. [54] If a method is amended during validation, then the validation is invalid. The procedure should include consideration of how to prevent inadvertent re-entering of the development process once validation has started.

---

53 See ILAC-G19 [3] (3.10): “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.” The Codes expect the review to be against the end-user’s requirements with the production of the statement of validation completion see section 29.3.63.

54 Should validation need to be repeated, consideration of whether using the same dataset or item introduces a potential risk of optimising the method to the validation sample set itself, so separation of stages in name only.

29.3.6 The validation procedure shall include where relevant, but is not limited to:

a. Determining the end-user’s requirements;

b. Determining the specification;

c. Risk assessment of the method;

d. A review of the end-user’s requirements and specification;

e. Setting the acceptance criteria;

f. The validation plan;

g. The outcomes of the validation exercise;

h. Assessment of acceptance criteria compliance;

i. Validation report;

j. Statement of validation completion; and

k. Implementation plan.

29.3.7 In certain circumstances implemented methods will require revalidation, e.g. when:

a. Quality control indicates that an established method is changing with time;

b. Equipment that was not validated to be mobile or portable is moved to a new location;

c. Deficiencies have become apparent after the method has been implemented; or

d. The end-user identifies a change in requirement.

Determining the End-User’s Requirements

29.3.8 The process of innovation ending in the implementation of a validated method is more likely to be instigated by the forensic unit than the end-user. However, to meet the needs of the CJS, which is the key end-user, the requirements of all intermediate users of a method through to the expectations of the court (e.g. Criminal Practice Directions [25] V 19A.5, relevant case law [33]) need to be determined.

29.3.9 The amount of direct input from the CJS end-user should be determined by the forensic unit, based on the type of innovation; certain requirements may be generic and form a set of core requirements to the casework type.

29.3.10 The Criminal Practice Directions V (i.e. 19A.5) [25] that supplement Part 19 of the Criminal Procedure Rules [34] should be considered as providing an insight as to the expectations of the CJS end-user. These expectations apply regardless of whether the result is evidence of fact or opinion.

29.3.11 The end-user’s requirement shall take account of, as appropriate:

a. Who will operate or use the new method, product or service post-delivery, and in what environment;

b. What the new method or product is intended to deliver for the end-user’s;

c. What statutory and regulatory requirements related to development and use of the method or product apply;

d. Whether there are any compatibility issues to be considered, e.g. data output formats;

e. What level of quality performance is expected; and

f. By what date the new method, product or service is required for implementation.

29.3.12 End-user’s requirements should conform to the following rules:

a. Each requirement is a single statement;

b. Each requirement is testable;

c. Each requirement specifies something that the solution will do, not how it will do it;

d. Each requirement specifies in its wording whether it is mandatory or desirable; and

e. Each requirement is written in a language that can be understood by the non-technical stakeholders.

29.3.13 Where the method is part of a service to be provided to a specified commissioning party, the forensic unit shall also ensure their formal agreement of the method selection.

Determining the Specification

29.3.14 A detailed specification shall be written for the method, product or service, and shall include the technical quality standards. It may be an extension of the end-user’s requirements document or a separate document.

29.3.15 The specification adds detail to the requirements captured in end-user requirement from the range of users (e.g. analysts, reporting officers). It also draws in other technical requirements and is ultimately what is to be tested, encapsulating what this method is to do, the configuration, and what the method can and cannot be used for.

29.3.16 At this stage the list contained in the ILAC-G19 [3] (3.10) should be considered, even if the points listed were not explicitly raised in the end-user requirement capture exercise. The specification may also draw on technical details from a review of the scientific literature.

Risk Assessment of the Method

29.3.17 Once the method has been designed or determined, there shall be an assessment to identify any risks, or potential risks, to the CJS related to the use of the method or amendment to the method, including ad hoc methods. The process shall include, but not be limited to:

a. Identifying, on the basis of the use to which the results may be put, the possible impact on the CJS of any errors in the results, associated materials or procedures; and

b. Identifying areas where the operation of the method, or interpretation of the results, requires specialist skills or knowledge to prevent ambiguous or misleading outputs or outcomes.

29.3.18 The forensic unit should use a formal risk assessment method. This Code requires risk assessment in various sections including in contamination (see section 28.2.2 herein) and control of data (see section 31.1.3 herein). The methodology recommended in both is based upon process mapping and

identifying the critical control points for the risks or failure modes [55] at those stages. One process map may be used to cover the whole method against different risks.

29.3.19 Where the method relies on a scientific model or theory the risk assessment should address the following in a forensic science context:

a. The validity of the theory/model;

b. Any assumptions incorporated within the theory/model; and

c. Limits on the application of the theory/model.

29.3.20 In light of the assessment there shall be recommendations for modification of the specification, specific studies to be included in the validation exercise or additional procedures and/or safeguards that should be implemented. Examples would include, but not be limited to:

a. Caveats about the use of the method;

b. Circumstances in which the use of the method would be inadvisable; and

c. Additional work that should be undertaken in combination with the method.

29.3.21 Where test items provided by an end-user, or data derived from these, are required for the development work or validation, the forensic unit shall obtain prior permission, from those with responsibility for the items and/or data (e.g. the commissioning party or prosecuting authority) for their use and include their use in the risk assessment. [35] Given the risks involved in the use of casework items/data the Senior Accountable Individual for the forensic unit shall be informed of the proposed use.

29.3.22 The risk assessment shall be subject to version control and should feed into the statement of validation completion.

---

[55] Examples of how Failure Mode Effect Analysis may assist are included in guidance published by the Regulator. [31]

Review of the End-User’s Requirements

29.3.23 The forensic unit shall review the requirements collated to ensure that requirements considered essential/mandatory have been translated correctly into the specification and the specification is fit for purpose. Where appropriate, the end-user’s specifying the requirement (e.g. analysts, reporting officers) may be involved in this review process.

29.3.24 When a review identifies that there are risks, or that there are compatibility, legality or ethical issues, the forensic unit shall produce a revised end-user’s requirements and/or specification.

29.3.25 Any subsequent changes to the specification shall then be only made in line with the forensic unit’s change control procedures and only following further review and acceptance of the impact of the changes by the intended end-user’s.

29.3.26 The forensic unit shall ensure that all practitioners involved in the development and validation/verification of the method are informed of any agreed changes to the end-user’s requirements or specification.

The Acceptance Criteria

29.3.27 The acceptance criteria should be clearly stated, based upon the specification, the risk analysis, and any control strategies put in place to control identified risks.

29.3.28 The acceptance criteria shall be used to demonstrate the effectiveness of the method and control strategy within measurable and set tolerances.

The Validation Plan

29.3.29 The validation shall be carried out according to a documented validation plan. The validation plan shall identify and define the functional and performance requirements, the relevant parameters and characteristics to be studied and the acceptance criteria for the results obtained to confirm that the specified requirements for the method, product or service have been met.

29.3.30 Where appropriate, the validation plan shall also include a requirement to check the relevant parameters and characteristics of the procedures for sampling, handling and transportation. The same level of confidence in the results

obtained shall be required whether the method is to be used routinely or infrequently.

29.3.31 The validation shall be carried out using simulated casework material in the first instance and subsequently, where possible, permitted and appropriate, with actual casework material to confirm its robustness. [56]

29.3.32 The validation plan should be tailored depending on whether it is intended for the:

a. Validation of measurement-based methods;

b. Validation of interpretive methods;

c. Verification of the validation of adopted methods; and/or

d. Verification of the impact of minor changes to methods.

29.3.33 The validation plan should be signed off by a suitably competent individual who was independent from the development of the method and has sufficient knowledge of the relevant field under study.

29.3.34 Particularly where this is a plan for the validation of a new method rather than an adopted method (see 29.3.8), it is accepted additional individuals may be needed to provide the necessary breadth of technical knowledge to evaluate the plan. [57] In such cases these individuals shall be listed in the validation report and their role in supporting the person responsible for sign-off should be recorded.

Validation of Measurement-Based Methods

29.3.35 The validation plan should ensure the required parameters and characteristics are studied:

---

[56] Legal advice may be required for the use of casework material where the exemption in relevant legislation ‘for law enforcement purposes’ may not apply. Validation studies on casework material generates disclosure requirements and a protocol with guidance on the issue of handling differences between results obtained with existing and the new methods. [35]

[57] Good experimental design ensures the study tests the features required and can reduce the overall experimental effort.

a. By an analyst or examiner competent in the field of work under study, who has sufficient knowledge of the work to be able to make appropriate decisions from the observations made as the study progresses; and

b. Using equipment that is within specification, working correctly and, where appropriate, calibrated.

29.3.36 The functional and performance requirements, and the relevant parameters and characteristics for measurement-based methods [58] that shall be considered include the following.

a. Competence requirements of the analyst/user.

b. Environmental constraints.

c. Item/sample size.

d. Item/sample handling.

e. Item/sample homogeneity.

f. Ability of the sampling process to provide a representative sample of the item.

g. Efficiency of recovery of the substance(s) to be identified/measured (i.e. analyte) during sample preparation for analysis.

h. Presence or absence of the analyte(s) of interest in the sample analysed.

i. Minimum quantity of each analyte that can be reliably detected.

j. Minimum amount of each analyte that can be accurately quantified.

k. Identification/measurement relates to the analyte(s) alone, and is not compromised by the presence of some matrix or substrate effect or interfering substance.

---

[58] The applicability of the parameter should be considered against the aim and the nature of the test. Determining a limit of quantification 29.3.36j may be evaluated as not applicable in an entirely qualitative test, but there may still be a requirement to estimate the uncertainty (see 30. Estimation of Uncertainty).

l. Results are consistent, reliable, accurate, robust and with an uncertainty measurement.

m. Compatibility with results obtained by other analysts using different equipment and different methods.

n. Limitations of applicability.

Validation of Interpretive Methods [59]

29.3.37 The functional and performance requirements for interpretive methods are less prescriptive than for measurement-based methods although should include testing against representative ground truth data. [60] They concentrate on the competence requirements for the practitioners involved and how the practitioners shall demonstrate that they can provide consistent, reproducible, valid and reliable results that are compatible with the results of other competent practitioners. This may be achieved by a combination of:

a. Independent confirmation of results/opinions by another competent examiner (i.e. without prior knowledge of the first result/opinion provided);

b. Participating in inter-laboratory comparisons (collaborative exercises or proficiency tests); and

c. Designing frequent in-house assessment into the process using positive and negative competence tests.

29.3.38 An interpretive method shall require only the relevant subset of the parameters and characteristics for measurement-based methods to be determined.

Verification of the Validation of Adopted Methods

29.3.39 Verification is defined as confirmation, through the assessment of existing objective evidence or through experiment, that a method, process or device is fit (or remains fit) for the specific purpose intended.

---

59 Examples of interpretive methods may include the comparison of marks, handwriting, microscopic comparisons etc.

60 Examples of data where the truth is known (not inferred) include datasets created from known donors of samples or call data records created by staged calls at specific coordinates.

29.3.40 Each of the steps of the validation process are to be completed (i.e. as detailed in 29.3.6), whether the user is producing the objective evidence for relevance, reliability and completeness themselves or objectively reviewing data produced by others. [61] The required end-user requirement and specification form the purpose that the forensic unit is assessing against. If a specification is being also adopted from elsewhere, this should be assessed for suitability for the forensic unit’s requirements also.

29.3.41 The assessment to identify any risks, or potential risks, to the CJS related to the use of the method or amendment to the method should be included. If the method is to be deployed in a different manner than the study that provided the data the forensic unit intended to review the specification against, the differences require to be risk-assessed and may prompt a fuller validation study.

29.3.42 Where the validation has not been conducted at the site [62] that will be using the method, the forensic unit must verify the scope of the validation with the study scaled up or down according to the adequacy and relevance of the available existing validation study.

29.3.43 The amount of work required to be carried out in verification exercises when introducing methods developed and validated elsewhere, shall take account of the adequacy of the available existing validation data and the familiarity and experience within the forensic unit of the techniques, equipment and facilities involved.

29.3.44 The forensic unit shall check its performance against the specification for the method it is required to produce rather than simply against existing published data, as the requirements may differ.

29.3.45 The validation report shall have as a minimum a summary of the experimental work/review, results, specification used in the review, the risk assessment, practitioner training/competence requirement and assessment plans. The

---

61 External developers of methods or tools are encouraged to conduct their developmental validation exercises in a comparable manner to the requirements set out in this Code, as well as making the data available..

62 See UKAS RG 201 for methods intended for incident scene use. [17]

required validation library and statement of validation completion shall be produced.

Minor Changes in Methods

29.3.46 Replacing like-for-like equipment [63] or minor changes to methods used by the forensic unit may not always require a full revalidation exercise. The impact of the change shall be risk assessed, verified against the original validation and authorised in line with other validation studies.

29.3.47 A revalidation exercise shall be carried out when changes are assessed to have the potential to influence the results obtained.

Infrequently Used Methods

29.3.48 Infrequently used methods pose a challenge in maintaining competence and capability for any FSA. While the use of such methods is acceptable there need to be appropriate safeguards.

29.3.49 Methods used less than once in every three-month period should be considered to be infrequently used. However, the forensic unit is required to define the period as some methods may be risk assessed during validation as requiring additional competence checks prior to use if even used on a monthly basis.

29.3.50 All methods the forensic unit intends using, including infrequently used methods, shall have been validated in line with this Code and the forensic unit shall demonstrate competence to perform the method. The validation, verification or re-verification shall include the steps in 29.3.6 herein and, as with all methods, a validation library is required. [64]

29.3.51 Forensic units shall have a procedure to identify infrequently performed examinations/tests and their maintenance or use including:

a. The definition of infrequently performed examinations/test;

---

63 Replacing the same make and model may still need some assessment as minor modifications, including software and firmware, might affect the operation.

64 As with all validations the study should be scaled according to user requirement and case circumstances the adequacy and relevance of the available existing validation study, however the forensic unit must still verify the scope of the validation with the required steps in 29.3.6 herein, even if these are brief.

b. Responsibility for confirming the validation or verification remains appropriate;

c. How competence will be maintained or is demonstrated, ILAC G19 [3] recommends:

   i. Regular use of control samples even when casework samples are not being analysed; or

   ii. Re-verification before the examination/test in question is performed on a casework sample involving at least the use of an appropriate reference material, followed by replicate examination/testing of the real sample;

d. The sign-off procedure for use in casework including justification of method choice; and

e. How the status of the method will be reported in statements or reports.

29.3.52 Infrequently used methods may be maintained on the forensic unit’s schedule of accreditation through regular use of mock casework, competence assessments and any other measures agreed with the accreditation body. [36] In order to be retained within the schedule of accreditation, UKAS requires each FSA to be assessed at least once within the four-year accreditation cycle and details the requirements in its publication TPS 68 [36]. [65]

29.3.53 If not included on the schedule of accreditation, then the methods shall be re-verified in accordance with the requirements of these Code prior to each use in casework (see 29.3.51 herein as well as ILAC G19 [3]). If these activities are to become part of the routine activities of the forensic unit (i.e. used more frequently than once every three months), and the FSA requires it, accreditation shall be sought and obtained by the date set in the FSA definition.

Validation Outcomes

29.3.54 A summary of the outcome of the validation exercise shall be included in the validation report, which shall normally be retained for 30 years after the last use

---

65 Other accreditation bodies may have similar requirements.

of the method. A full record of the validation exercise will normally be retained by the forensic unit for a similar period, but as a minimum shall be maintained for the functional life of the method and shall include:

a. The authorised validation plan and any subsequent changes to the plan, with justifications and authorisations for the changes;

b. All experimental results from the validation exercise;

c. A detailed comparison of the experimental results with the specified requirements;

d. Independent evaluation of the extent to which the results obtained conform or otherwise to the specified requirements;

e. Any corrective actions identified; and

f. Independent approval of the validation. [66]

Assessment of Acceptance Criteria Compliance

29.3.55 The independent evaluation of compliance of the experimental results with specified requirements shall be carried out by a person (or persons) not involved in the development of the method or conducting the validation process.

29.3.56 The person(s) shall have demonstrated they have sufficient knowledge of the issues involved to be able to identify and assess the significance of any deficiencies. [67]

29.3.57 The independent authorisation shall typically establish whether:

a. The validation work is adequate and has fully demonstrated compliance of the method with the acceptance criteria for the agreed specification; and

b. The method is fit for its intended use.

---

66 The same person may carry out both the independent evaluation and the independent authorisation, if competent to do so.

67 The person(s) may be employed by the forensic unit, contracted by the forensic unit to carry out the evaluation, or be wholly independent of the forensic unit. If employed by the forensic unit, the evaluator/authoriser would need to be able to demonstrate the appropriate level of independence.

29.3.58 If the forensic unit were to plan to implement methods rated as high risk and/or likely to attract challenge once implemented, the Regulator should be consulted as to the need for any wider review and/or publication prior to implementation.

Validation Report [68]

29.3.59 The forensic unit shall produce a validation report in sufficient detail to allow independent assessment of the adequacy of the work carried out in demonstrating that the method, product or service conforms to the specification and is fit for purpose. The report need not contain all the experimental data, but a summary of this data shall be provided, and the raw data shall be available for inspection if required.

29.3.60 The content of the validation report shall depend on the type and extent of validation carried out, but as a general guide it should include, as appropriate:

a. A title and unique identifier;

b. A description of the purpose of the method, product or service;

c. The specification;

d. The name, version number and manufacturer of any equipment used;

e. The name(s) and signature(s) of the person(s) accountable for the development of the validation processes;

f. The validation plan;

g. The risk assessment;

h. Any authorised changes to the validation plan and justifications for the changes;

---

68 Forensic units with methods within the schedule of accreditation, on or before 1 November 2016, will often only be required to compile the validation library for those specific methods, which contains a validation report in its original format and the comparable information that the end-user requirement and/or specification would contain (i.e. what the method was intended to be able to do). It is good practice to review the completeness of the validation at this stage and take any further steps to ensure that the method can be said to be valid on the basis of the records held.

i. A summary of the experimental work and outcomes in sufficient detail to ensure that the tests could be independently replicated by a competent person;

j. Details of any review reports produced;

k. Conformity with the acceptance criteria (expected compared with actual results and any pass/fail criteria);

l. Any limitations/constraints applicable;

m. Any related published papers and similar methods in use by the forensic unit;

n. Any recommendations relating to the implementation of the method, product or service; and

o. The date of the report.

29.3.61 The forensic unit shall submit the validation report for review by persons suitably qualified and independent of the validation process; any issues arising should be dealt with expeditiously.

29.3.62 All the required records relating to the development and validation of the method, product or service shall be archived, together with the means of accessing the records, and will normally be kept for 30 years following the method’s last use in casework. [69]

Statement of Validation Completion

29.3.63 The aim of the statement of validation completion is to provide those making decisions on the use of the results with a short executive summary of the validation steps performed, and key issues surrounding the validation. The intention is that the statement will be no more than two sides of A4 paper in plain language. [70]

---

69 The blanket retention period is an alternative to tracking a method’s use in casework and applying the correct retention period in accordance with the Criminal Procedure and Investigations Act 1996 [96], as amended.

70 See also the CPS Core Foundation Principles for Forensic Science Providers [83] and the list of questions in direction 19A.5 contained in the Criminal Practice Directions. [82]

29.3.64 The approval by the forensic unit on the scope of the validation must be clear.

29.3.65 The forensic unit should provide any further information that would be useful to the CJS. Examples would include, but not be limited to:

a. Caveats about the use of the method;

b. The approved uses of the method, which could be by case type or exhibit type;

c. Circumstances in which the use of the method would be inadvisable; and

d. Additional work that should be undertaken in combination with the result.

Validation Library

29.3.66 The forensic unit shall have available a library of documents relevant to the authorisation of the new method through validation or verification. Where the following are not already distinct sections in the validation report, the content of this library shall include, but not be limited to:

a. The specification for the method approved (see earlier sub-section Determining the specification);

b. Any associated supporting material, such as academic papers or technical reports that were used to support or provide evidence on the applicability of the method; [71]

c. The risk assessment for the method approved;

d. The validation plan for the method approved;

e. The validation report;

f. The record of approval; and

g. The statement of validation completion.

---

71 The literature review also ensures the body of knowledge requirement as outlined in R v. Bonython [1984] 38 SASR 45 can be demonstrated as well as supporting the application of direction 19A.5d of the Criminal Practice Directions V [25].

29.3.67 Where the method implements a scientific theory/model or an interpretation or evaluation model, the library should include a record of information supporting the use of the theory/model.

29.3.68 Where the method relies on reference collections or databases, the nature, access and their availability should be described.

29.3.69 The information in the library may be disclosable in criminal proceedings [72] and should be prepared with that possibility in mind.

Implementation Plan and Any Constraints

29.3.70 The forensic unit shall have a plan for implementation of methods, products or services new to the forensic unit. This plan shall address, where relevant:

a. Whether revisiting old cases should be explored, where the revised or new method offers new analytical opportunities and, if relevant, the benefits or risks communicated to the commissioning party;

b. The standard operating procedure (including the process for assessment/interpretation/reporting of results) or instructions for use;

c. Requirements for staff training, competence assessment and on-going monitoring of staff competence;

d. Integration of the method with what is already in place;

e. If the method is intended to be included in the scope of accreditation and what steps are required to achieve this;

f. The monitoring mechanisms to be used to demonstrate that the method remains under satisfactory control during its use;

g. The protocols for calibration, monitoring and maintenance of any equipment;

h. The supply and traceability of any standards/reference materials;

---

[72] Commercial-in-confidence does not override the disclosure requirements of the Criminal Procedure and Investigations Act 1996 [96] and a refusal to disclose may prevent methods, products or services being used.

i. The supply and quality control of key materials, consumables and reagents;

j. The exhibit handling and any anti-contamination protocols;

k. The accommodation plan;

l. Any specific health and safety, environmental protection, data protection and information security arrangements;

m. The communication plan; and

n. The schedule for post-implementation review.

30. Estimation of Uncertainty

30.1.1 A forensic unit performing testing [73] is required to evaluate measurement uncertainty; testing is the determination of one or more characteristics according to a procedure and although typically quantitative, it can be qualitative (e.g. a presumptive test with a colour change).

30.1.2 Qualitative testing may be for the presence or absence of a defined analyte but there will be uncertainty associated with the underlying test conditions. Where the test method precludes rigorous evaluation of measurement such as a test that is qualitative in nature, UKAS M3003 [37] states “there will be uncertainties associated with the underlying test conditions and these should be subject to the same type of evaluation as is required for quantitative test results”. ILAC G17 [38] suggests that with qualitative testing or examinations, an estimation of the probability for false positive or false negative test results may be relevant.

30.1.3 The impact that uncertainty may have on the findings shall be included in both factual and evaluative reports to the CJS where it is relevant.

30.1.4 When a procedure is modified, in addition to any validation or verification, forensic units should also review the measurement uncertainty.

---

[73] The forensic unit may undertake testing as part of incident scene investigation. ILAC-G19 [3] includes, but does not limit such testing to, quantitative measurements and presumptive or screening tests. Inspection activity that contains testing is expected to meet the relevant requirements of ISO 17025 [1], this includes but is not limited to estimation of uncertainty of measurement (see also ILAC-G27 [84]).

30.1.5 Guidance on the estimation of uncertainty of measurement is contained in Appendix N of the UKAS M3003 publication ‘The Expression of Uncertainty and Confidence in Measurement’. [37] [74]

30.1.6 The Criminal Practice Directions V (19A.5c) [25] that supplements Part 19 of the Criminal Procedure Rules [34] include several factors which ought to be considered. However, the following direction that the court may take into account in determining admissibility is particularly relevant:

“19A.5c “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, affecting the accuracy or reliability of those results.”

31. Control of Electronic Data

31.1 General

31.1.1 The forensic unit shall have procedures within its management system to ensure that all necessary information is recorded accurately, maintained so that its authenticity and integrity is not compromised, and is retained and destroyed in accordance with the forensic unit’s retention and destruction policy. [39] [40] [41] This applies to all networks and systems used by the forensic unit, including closed/restricted networks (i.e. digital units) unless specifically indicated in the clause (some clauses do not apply to test items/exhibits/evidence).

31.1.2 This section focuses on information held in an electronic form, more general requirements that also apply for physical items are set out in this Code in sections 21 Document Control, 25 Control of Records, 28 Accommodation and Environmental Conditions, and in section 35 Handling of Items.

31.1.3 The unit shall as part of its risk assessment identify key data and critical control points (i.e. places where data is entered, transferred, stored or processed in a

74 Guidance has also been issued by Eurachem. [116]

manner where it may be vulnerable to corruption, errors, media loss, unauthorised manipulation etc.). [75]

31.1.4 The assessment of critical control points shall include all test items related to the forensic activity, either scene or lab based, including technology operated by the forensic unit such as mobile phones, satellite navigation systems, laptops, cameras etc. [76]

31.1.5 In case of nationally provided and managed services that are outside the control of the organisation, the organisation shall consider, and document, the risk to the organisation and any mitigation introduced to control that risk.

31.1.6 The unit shall identify protection steps to:

a. Minimise the risk of data loss;

b. Minimise the risk of data corruption (deliberate, degraded, actual or suspected);

c. Demonstrate that the results are reliable and analytically sound; and

d. Maintain continuity and prevent unauthorised access to and/or amendment of all electronic records identified by assessment of the critical control points of key data.

31.1.7 Protection steps shall be tested by sampling of key data. [77]

31.1.8 Whilst these clauses indicate the forensic units, this may require some liaison with the organisations Information Security/IT departments or otherwise should be escalated directly via the Senior Accountable Individual.

---

75 This critical control point approach is a risk analysis advocated in guidance issued by the Regulator for assessing the risk of cognitive bias as a result of information flow as well as for assessing contamination and therefore the process mapping may be used for assessment of these and other risks in the process. Should it be required, and relevant, more detailed guidance can be obtained from BS ISO/IEC 27001:2013 Information technology – Security techniques – Information security management [43] systems – Requirements and BS ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management. [44]

76 Critical control points include the data transfer off exhibits, but here also technology operated by the forensic unit which may contain data.

77 Assessment of what is key data should be risk based, and process mapping to look at data flow through each process and identify critical control points would be an appropriate assessment of what stages in the process require specific protection steps to prevent loss, corruption and unauthorised access.

31.2 Electronic Information Capture, Storage, Transfer, Retrieval and Disposal [78]

31.2.1 The forensic unit shall establish procedures for the capture and retrieval of electronic information appropriate for the process or method. If the capture or transformation process does involve any loss or change, this should have been assessed and acceptance criteria stated (e.g. as defined in the method’s end-user requirements, specification or in the procedure itself).

31.2.2 Where scanning technology is used, the forensic unit shall establish procedures and quality control for the scanning of documents in paper form, microforms and other forms of information, as appropriate, to ensure that any potential information loss as a result of the scanning is within acceptable limits. [79]

31.2.3 Appropriate to the associated method or process, the procedure and policies should ensure that where key information is extracted from image files the original images are retained and linked with the captured information, including metadata.

31.2.4 Where a document has, for example embedded files or hyperlinks, all elements of the document shall be stored in line with the forensic unit’s retention policy along with their content.

31.2.5 Critical information should be accessible throughout its period of retention.

31.2.6 When data is migrated to alternative storage media, the forensic unit shall establish procedures to ensure that all digital objects [80] have been successfully migrated. The digital object and file format of the migrated digital objects should not have changed, or that the changes are known, have been audited, and meet requirements.

---

78 Further information and guidance can be found in BS 10008:2014, Evidential weight and legal admissibility of electronic information – Specification. [121]

79 Further information and guidance can be found in ISO 12653-1:2000, Electronic imaging - Test target for the black-and-white scanning of office documents - Part 1: Characteristics. [119]

80 See glossary.

31.2.7 If replacement software (e.g. an operating system or application software) is implemented, the forensic unit shall ensure that procedures are established to retain access to any critical data reliant on that software.

31.2.8 Where information is compressed during the storage and transfer processes (e.g. in order to reduce stored file size), the compression method used shall not affect the authenticity and integrity of the data.

31.2.9 Information shall be retained according to retention and destruction policy until such time as that policy determines it should be destroyed. Destruction or disposal of the information, including the method by which that is achieved should be recorded within the audit trail for that information..

31.3 Electronic Information Security [42]

31.3.1 The forensic unit shall have an information security policy which explains how the unit meets its responsibilities outlined in section 31.1.1 herein. [43] [44] [45] The information security policy shall describe the procedures, based on business and security requirements, as assessed by the forensic unit, for the management of its electronic information. The forensic unit shall ensure procedures are subject to regular testing, audit and review. [81]

31.3.2 The forensic unit’s information security policy shall have processes for the following.

Access Control to Electronic Information

31.3.3 The access control procedures shall include the identification, authentication, and authorisation of users. Users shall have defined privileges which limit, as far as practical, access to only the information and key operational services they require to perform their roles.

31.3.4 When users leave their role or the organisation, the forensic unit shall ensure access is removed. Reviews should take place at least every 6 months to

[81] The testing may be conducted by the forensic unit’s IT provider, however the responsibility to ensure it occurs and provide evidence of the testing resides with the forensic unit.

ensure access rights are still needed - if access rights are no longer needed, they shall be removed.

31.3.5 Users with administrative rights shall use second factor authentication [82] where this is technically possible.

31.3.6 Accounts with administrative rights shall only be used to perform defined administrative duties [83], and not be used for routine access to e-mail or the Internet. The administrative duty may include periodic access to emails/or internet to download software patches or perform a software update, however the risks of this open access should be controlled.

31.3.7 Authentication failures should be throttled to 10 attempts in 5 minutes and locked out where this is practicable and under the control of the forensic unit or the larger organisation the forensic unit may be part of e.g. not a nationally delivered system. Access control mechanisms shall be protected to prevent unauthorised system-wide access. [46] [47]

The Selection, Use and Management of Passwords

31.3.8 Procedures for the selection, use and management of passwords should be formulated to help users to generate better passwords. The procedures shall include the following.

a. Passwords should be of an appropriate level of complexity. Consideration may be given to using:

   i. the 'three random words’ [48] technique for generating suitably complex and memorable passphrases; or

   ii. machine generated passwords with appropriate facilities to store them such as password managers. [49]

b. Passwords shall be a minimum of 8 characters and have no maximum length. Regular password expiry should not be enforced, but users shall

---

82 Second factor authentication or two-factor authentication (often shortened to 2FA) is something that the user (and only the user) can access, such as a code that is sent by text message, or that is created by an application or dongle. [85]

83 With the exception of evidence handling software applications which require administrative rights for normal operation.

change their password when it is known (or suspected) that it has been compromised.

c. Users should be directed to use different passwords for their:

   i. Personal and any work accounts; and

   ii. General work account and any work accounts they may have with administrative rights.

d. Users should be prevented from reusing passwords where technically possible.

e. Users should be directed to not select easily guessed or commonly used passwords [50] and should be prevented from doing so where technically possible.

f. Password should be protected in transit and at rest using appropriate encryption and hashing techniques. [47] [51] [52]

g. All default administrative passwords for applications, network equipment and computers shall be changed [47]to meet the requirements identified above.

Protection Against Malware

31.3.9 With the exception of evidence handling where the detection, removal or treatment of malware may have an actual or potential impact on the results of examinations or analysis, the procedures for the protection against malware shall include detection and removal of malware using anti-malware software.

31.3.10 Anti-malware software shall be updated when new definitions become available. Anti-malware updates should be included in the forensic unit's change procedures to manage any potential impact to the forensic examination process.

31.3.11 Anti-malware software shall be installed on all compatible computers and hardware, unless specified operational requirements dictate otherwise. The forensic unit should implement additional anti-malware procedures such as application/executable allow listing. [53]

31.3.12 The forensic unit shall have, or ensure that its IT provider has, procedures in place to protect from website and email-borne malware for all devices that access the Internet, caused by drive-by download and phishing attacks.

31.3.13 The forensic unit shall access the Internet via a proxy service which blocks malware. The forensic unit shall have procedures for filtering or blocking phishing emails or messages, before they reach users.

31.3.14 The forensic unit shall have procedures to update (patch) software and firmware in a timely manner and included in the forensic unit's change procedures to manage any potential impact to the forensic examination process. 'Critical' and 'High' severity patches for Internet-enabled systems shall be installed promptly. Where this is not possible, then other mitigations (such as physical or logical separation) shall be applied.

31.3.15 Software and firmware that is no longer supported by vendors, should be replaced unless there is a technical or CJS justification for its continued use recorded in the procedure. [84]

31.3.16 All removable storage media shall be scanned using anti-malware software before use/issue.

31.3.17 The forensic unit should securely configure computers by following the End User Device security principles. [54]

31.3.18 The forensic unit shall have access to backup data so that it can recover from any malware. [55] [56]

Management of Removable Storage Media [85]

31.3.19 Procedures for management of removable storage media used by the forensic unit to transfer data (e.g. memory cards, SD cards or flash cards, micro SD) shall include controls related to issue and there use. These procedures shall include wiping/re-formatting of the storage media.

---

84 For example, legacy software is sometimes required to access old media or for revisiting the analysis of old cases.

85 This procedure is for the general transfer of electronic information, it does not relate to exhibit and evidence handling.

31.3.20 Removable storage media shall only be issued to users whose role requires it. Only the minimum interfaces necessary for the use of removable storage media should be enabled on computers and those users to who those computers are issued should be made aware of the permitted interfaces.

31.3.21 Personal removable storage media shall not be used for the transfer of electronic information - only officially issued removeable storage media shall be used which:

a. Shall be physically secured when not in use;

b. Should not be used to take data offsite unless its contents are secured using appropriate encryption techniques [57]; [86] and

c. Should be subject to accountability with the aim of tracking use and managing loss. [46] [58]

The Segregation of Forensic Networks

31.3.22 The forensic unit shall have procedures for the segregation of systems used for forensic science activities from other networks. Systems and data that do not need to communicate or interact with each other should be separated into different network segments, and only allow users to access a segment where needed.[87] Segregation can be achieved physically or ‘logically’. Logical separation can include access control lists, network and computer virtualisation, firewalling, and network encryption such as Internet Protocol Security (IPSec). [59] [60]

Backups, Recovery and Business Continuity

31.3.23 The forensic unit shall have procedures for business continuity with an incident management plan including backup and retrieval of data, to recover from incidents such as ransomware, theft, fire or hardware failure, whilst ensuring the business can continue to function.

---

86 Memory cards used for cameras are excluded from encryption.

87 Systems used for different forensic science work may need segregation from each other; for example, internet intelligence and investigation workstations and systems from other digital forensics activities.

31.3.24 The forensic unit shall identify what electronic information is essential to keeping operations running and make regular backup copies, or where that infrastructure is provided by the larger organisation (e.g. police force) seek assurance the backup is adequate.

31.3.25 The forensic unit shall identify its critical systems and have redundancy arrangements in place. The forensic unit shall test that backups are working to ensure it can restore the electronic information from them in the event of an incident. Offline backups shall be created and stored for as long as necessary to meet the requirements of the CJS.

31.3.26 Where digital data is the evidence, the procedure should be risk-based, balancing consideration of the time between creation of the extracted material, retention of the evidential device and any identified off-site back-up requirement.

31.3.27 Offline backups should be stored at a separate and secure location. [88] [61] [62] The forensic unit may use appropriate cloud services for this back-up of electronic information; ‘offline’ here means digitally disconnected or fully protected from any malware risk when not in use and/or designed and tested to remain unaffected should any incident impact the live environment through robust protection from malware. [63]

31.3.28 The forensic unit shall have an incident management plan [89] which helps staff identify, respond to, and recover from, incidents as well as continue to run the business. The incident management plan should include a communication strategy (which includes appropriate escalation to the Regulator and, if accredited, UKAS), roles and responsibilities of staff and third parties such as service providers and authorities, as well as contact details for those involved.

---

88 Ensuring the back-up is adequately protected from the same physical incident that may affect the primary data store such as fire, explosion or theft may be achieved by this being in a separate building not merely a separate room. However, the risk assessment may detail alternative mitigation to be included in, and tested with, the business continuity/incident management procedure. Sole traders may enter into reciprocal storage agreements if they choose to.

89 This may be part of the overall business continuity procedure or a separate IT incident management plan.

31.3.29 The forensic unit shall test business continuity procedure annually (see 18.1.4 herein). The incident management plan shall be tested also, whether it is part of the overall procedure or separate, to ensure that its electronic information and critical systems can be recovered in the event of an incident.

31.3.30 Revisions to the incident management plan should include lessons learnt to minimise the risk of disruption to the business occurring in the same way again. [46] [58] [64]

Network Security and Mobile Working

31.3.31 The network security and mobile working procedures shall include the management of the network perimeter by using firewalls to create a 'buffer zone' between the Internet (and other untrusted networks) and the networks used by the business.

31.3.32 The forensic unit shall have procedures to protect its internal networks by ensuring there is no direct routing between internal and external networks (especially the Internet). The forensic unit shall have procedures for securing wireless access to its networks. All wireless access points shall be secured using Wi-Fi Protected Access 2 (WPA2) or WPA3, and only allow known devices to connect to corporate Wi-Fi services.

31.3.33 Where mobile working is required, the forensic unit shall have procedures for ensuring that connections are identified, authenticated (preferably using multiple factors) and authorised. All electronic information which transits the Internet (and other untrusted networks) shall be protected from eavesdropping and alteration using appropriate encryption such as IPSec and Transport Layer Security (TLS). [51] [52]

31.3.34 All mobile devices shall only have the necessary applications and electronic information to fulfil the business activity that is being delivered outside the normal office environment. If the mobile device supports it, data shall be encrypted at rest. The forensic unit should ensure there are adequate procedures for monitoring network traffic for unusual incoming and outgoing activity that could be indicative of an attack. The forensic unit shall have procedures for testing the security of its networks. [46]

The Use of Cloud-Based Services

31.3.35 The process for the use of cloud-based services shall include procedures to:

a. Determine the business need and end-user requirements;

b. Identify what data will be transported, stored and processed, and understand the associated risks;

c. Evaluate the security of the service offered; and

d. Understand the residual risks and how these will be managed.

31.3.36 The forensic unit should use cloud providers which meet the National Cyber Security Centre’s (NCSC) cloud security principles. [63] The forensic unit should include within the contract with the cloud-based provider that storage and processing of evidential data and information using cloud-based services should only be performed from data centres physically located in the UK. The forensic unit should periodically review whether the cloud-based services still meet its business and security needs.

Security Monitoring and Situational Awareness

31.3.37 The forensic unit's security monitoring and situational awareness procedures shall include the generation, capture, retention, storage and analysis of records from its computers and network equipment. The forensic unit's security monitoring procedures shall:

a. Provide visibility of communication between their network and other networks (i.e. the Internet or 3rd party suppliers);

b. Capture authentication and access attempts; and

c. Provide asset and configuration information. All records shall be stored securely so they are safe from tampering and unauthorised access. All records should be stored for a minimum of 6 months so that they can be used to support incident management. [65] [66]

32. Reference Collections and Databases (Not National Forensic Databases

32.1.1 Forensic units shall maintain a list of all reference collections and databases used to make inferences and interpretation; this includes, but is not limited to, those internally developed, commercially developed or remotely accessed.

32.1.2 Forensic units shall have a process for determining the requirements of the CJS for internally developed reference collections and databases used to make inferences and interpretations, e.g. through reference to case law.

32.1.3 Information included in all reference collections and databases used to make inferences and interpretations shall be capable of authentication through documentation to its original source, meet a minimum quality standard specified by the owner of the collection or database, be validated for accuracy of transcription on entry to the database, and be auditable for corruption.

32.1.4 Any programs or script for data manipulation employed within databases to make inferences and interpretations shall be validated, either separately or as part of the process or method they are used in as laid out in this Code, e.g. with reference to the impact of any uncertainty of measurement and the risk of false positives/negatives.

32.1.5 All reference collections and databases used to make inferences and interpretations shall be covered by documentation specifying, as a minimum:

a. Their purpose;

b. Their location and identification;

c. Their scope and content;

d. The origin of the data;

e. Any known significant limitations or restrictions;

f. The person responsible for management of the database;

g. The authorisation and competence requirements of organisations/practitioners contributing to the database;

h. The arrangements and format for data collection and submission;

i. The process for authentication or validation of the data;

j. The arrangements and format for data storage;

k. The process for making updates and amendments, and maintaining audit trails;

l. The protocols for access to the database and its interrogation and use;

m. The quality assurance requirements, including those for data integrity, transfer, inconsistency and error checking;

n. The confidentiality and security requirements;

o. The format and content of results and reports from interrogation of the database, including the provision of any caveats relating to any limitations with the results provided;

p. The projected shelf life of the data;

q. The arrangements for review of relevance, use and effectiveness; and

r. All relevant legal, commercial and ethical requirements covering their registration, data content, retention, accessibility or use.

32.1.6 Forensic units should collate the above information on existing as well as new reference collections and databases (used to make inferences and interpretations) and assess if any persisting gaps will affect critical findings and/or admissibility.

33. Equipment

33.1 Computers and Automated Equipment

33.1.1 The forensic unit shall ensure that any software used on computers or automated equipment is assessed for its impact on results and is documented in sufficient detail based on that assessment. This includes any software developed, configured or modified by the forensic unit, or by other outside agencies working on the forensic unit’s equipment.

33.1.2 Commercial off-the-shelf software and software tools whose operation has an impact in obtaining results will require validation, or any existing validation to be verified, as laid out in section 29.3 - Validation of Methods.

33.1.3 User acceptance testing shall be performed prior to software and/or related equipment being placed in service, e.g. when returning from calibration/maintenance or following a move.

33.1.4 Other commercial off-the-shelf software (e.g. Microsoft ® Word and Excel) that does not directly contribute to results obtained shall be considered suitably validated for general use. However, calculations embedded in spreadsheets that do not form part of a validated electronic process shall be included in the required systematic checks.

33.1.5 The forensic unit shall maintain records of software products installed on computer systems critical to the production of analytical results, and shall ensure configuration control so that only specified versions of software, settings and firmware, if applicable, are used. [90] The forensic unit shall have documented procedures for configuration management to ensure that all changes to software/hardware are controlled, and that all individual software installations are known and are periodically checked that the correct version is installed and no unauthorised modifications have occurred, e.g. by service engineers.

33.1.6 The forensic unit shall have a policy for all test items of equipment containing sensitive data to ensure the data:

a. Are secure during any maintenance visit;

b. Remain secure while off-site (e.g. for servicing); or

c. Have been removed or securely overwritten prior to removal from site or disposal.

34. Measurement Traceability - Intermediate Checks

34.1.1 Reference standards/materials and reagents shall not be used beyond the expiry date, where provided, unless it is verified that they remain fit for purpose beyond that date.

---

90 Older versions of software may be needed for compatibility with work being undertaken related to older products, or to maintain the validated systems’ configuration.

35. Handling of Items

35.1 General

35.1.1 Any actions prior to the forensic unit taking control of the scene of incident and/or items are outside of the control of the forensic unit. The forensic unit shall have processes to capture any observations about the scene or received test items that might have an impact on the examination or subsequent analysis.

35.2 Items at the Scene of Incident

35.2.1 Before items are recovered from the scene of incident, the practitioner shall consider the on-site conditions to ensure that the items can be recovered and documented in line with the forensic strategy.

35.2.2 If doubts remain about whether the items can be properly recovered in the prevailing circumstances, the commissioning party should be consulted (before proceeding) about whether and how the available resources should be used. For example, are additional ‘specialist’ examiners or technical resources required to conduct the examination or testing in situ.

35.2.3 The forensic unit shall ensure that its scene examiners are provided with and implement the relevant procedures to minimise the risk of cross-contamination between different scenes, items, suspects, witnesses and victims. [3]

35.2.4 The forensic unit shall have documented procedures to ensure that items or samples recovered from the scene for subsequent examination or testing are, as appropriate:

a. Labelled;

b. Protected/packaged;

c. Preserved

d. Listed on a schedule of recovered items;

e. Transported;

f. Stored;

g. Transferred for analysis/examination; and

h. Retained, returned or disposed of in compliance with agreed and documented procedures.

35.2.5 The forensic unit shall ensure that anti-contamination measures appropriate to the FSA, the analyte of interest and the risk of contamination are employed for any vehicles and equipment used for scene examination purposes or the transport of items and personnel.

35.2.6 Where a large quantity of potentially evidential material is available and a representative sample needs to be taken for analysis/examination, including for presumptive or triage testing, the practitioner should consider the sampling strategy should the sample taken need to be a representative of the whole rather than simply for presumptive testing or triaging submission.

35.2.7 The forensic unit shall preserve the test items during internal processing and delivery to the intended destination, through handling, packaging, storage and protection, and ensure that practitioners who may subsequently examine or analyse the test items are aware of anything that may have potentially compromised the items’ integrity.

35.2.8 The forensic unit shall ensure that recovered items are clearly and uniquely identified within the organisation rather than simply within the case. Initials and number and/or date is not considered unique and although would not devalue or invalidate the item if properly handled, it does add a risk which should be avoided. Where applicable, the identity and location of the item within the scene shall be documented or characterized using plans, measurements, diagrams, photography, photogrammetry, etc.

35.2.9 The forensic unit shall be able to demonstrate that the items recovered from the scene and, where appropriate, submitted for examination or testing, are those subsequently reported on. For this purpose, a ‘chain of custody’ record shall be maintained detailing the location of the item at all times from acquisition of items which details each person who takes possession of the item and when, or the location of the item (e.g. if in storage). The chain of custody record shall include details of when the items are destroyed or the circumstances under which they are released and to whom.

35.2.10 The forensic unit shall also ensure that the identification details provided with each exhibit, on the exhibit label and accompanying submission form, remain with the exhibit throughout its life, so as to ensure that, using a combination of the case number and item identification, no items can be confused physically or when referred to in records or other documents.

35.2.11 All items and associated documentation generated during scene examination shall be independently checked to ensure compliance with the requirements for acceptance set by the forensic unit prior to storage or submission for further examination/analysis.

35.3 Receipt of Cases and Items at the Forensic Unit

35.3.1 The forensic unit shall have procedures for the transportation, receipt [91], handling, protection, storage, retention, and/or disposal of all test items. This shall include a documented risk-based case acceptance procedure [92] for the handling of recoverable irregularities or rejection of an item for examination arising from, but not limited to:

a. Not being able to legally hold any material (e.g. not possessing necessary licences);

b. Having health and safety concerns about the submission or the ability to handle the material safely;

c. Not having the appropriate quality standards to do the examination requested;

d. A missing item label;

e. An unacceptably low level of agreement between the details on an item label and those on the accompanying submission documentation;

---

91 This should include procedures for checking and booking in items, that consider the risk of opening sealed containers without obtaining an immediate inventory i.e. particularly important for cases involving controlled substances/items, but relevant in any area where exhibit loss could be a consideration.

92 Whilst the non-FSA work of commissioning parties is outside the scope of this Code it is good practice for such parties to have procedures for receipt of cases and checking exhibits being returned from the forensic unit.

f. Inconsistency between the details on an item label and/or accompanying submission documentation and what the item actually is;

g. Illegibility in any information on an item label;

h. There being more than one label on an item;

i. Appropriate control samples not being submitted;

j. Repeat of the same identification details on different item labels;

k. Inadequate or untimely packaging or sealing of an item that could prejudice its integrity;

l. Previous handling, storage or evidence of tampering with an item that could prejudice its integrity; and

m. Insufficient material being available for meaningful examination or analysis.

35.3.2 If the forensic unit is unable to accept the submission the reasons for rejection shall be recorded.

35.3.3 Any apparent evidence of tampering with an item shall be investigated. If the outcome of the investigation indicates a deliberate attempt has been made to influence the results of the examination, the Senior Accountable Individual shall be informed to decide the appropriate escalation (which may include involvement of the police), which shall include notifying the Regulator.

35.3.4 The case acceptance procedure shall also specifically address the handling and receipt or rejection of potentially hazardous items that might pose a risk to the health or safety of staff, [93] potentially compromise other work carried out at the laboratory, [94] or which may not be lawfully retained or handled if accepted by the laboratory. [95]

---

93 For example, when handling hypodermic syringe needles or blood samples.

94 For example, firearms, bulk drugs seizures or explosives, where the forensic unit also carries out gunshot residue analysis or trace drugs or explosives analysis, unless separate reception arrangements and accommodation are provided for these.

95 For example, cases involving human tissues, drugs, firearms or explosives, for which there may be specific health and safety legislation requirements or specific licensing required.

35.4 Case Assessment and Prioritisation

General

35.4.1 Prior to commencing work the forensic unit shall, in consultation with the commissioning party, identify the issue(s) in the case, develop an appropriate examination strategy and agree the timescale for the delivery of the results. This may be in an overarching SLA/contract for more routine casework.

35.4.2 In developing the examination strategy, as appropriate and as far as is practicable the practitioner shall:

a. Ensure the relevant requirements of the criminal investigation and/or the instructing solicitor and associated forensic strategy are understood;

b. Ensure that either all the necessary information (including on any previous examinations), and items required for an effective examination strategy are provided or that any resultant limitations to the scope of the examination are discussed with the commissioning party and made clear to the CJS;

c. Establish all relevant details of the incident, what items have been recovered for examination, the circumstances relating to the location and recovery of the items, and any examinations of the test items for potential contamination or loss of integrity of the items prior to them coming into the practitioner’s possession; and

d. Select and prioritise the examinations according to the needs of the criminal investigation, the instructing solicitor, and the CJS, with consideration to the items available.

Evaluative Opinions

35.4.3 Where the forensic unit is commissioned to provide evaluative opinions, the following provisions apply.

35.4.4 The expert needs sufficient case-specific information to determine appropriate propositions, select appropriate analyses and to interpret the observations from those analyses. Other than that information, the expert does not need, and should not see, any more case-specific information (such as information on

previous convictions, reasons unrelated to the scientific analysis why investigators have identified a suspect and any other extraneous information not relevant to the scientist's task). [67]

35.4.5 The expert shall:

a. Consider the questions being asked by the commissioning party in the case and identify the issue(s) their analysis can address;

b. Consider all available, relevant case-specific information and, where necessary, request additional information; and

c. Discuss the issues to be addressed and potential propositions with the relevant instructing party (e.g. police, defence, prosecuting authority) and where possible the other party. [96]

35.4.6 On the basis of the case circumstances and any agreed key issue(s), the following shall be identified.

a. The prosecution proposition(s).

b. The defence proposition(s).

35.4.7 There may be more than two propositions, but the assessment will, in general, consider the propositions in pairs; each pair shall be mutually exclusive.

35.5 Item Handling, Protection and Storage

35.5.1 The forensic unit shall ensure that item handling policies and procedures address continuity requirements including, but not limited to that:

a. The item recovered or sub-sample can, at all times when in the possession or control of the forensic unit, be uniquely identified;

b. The item can be conclusively shown to be the item submitted to the forensic unit;

---

[96] It is recognised that this may not be routinely possible in volume crime case work.

c. Any material recovered from or derived from an item or sub-sample of an item can be conclusively linked to the item or sub-sample from which it came;

d. Any result can be conclusively linked back to the item or sub-sample from which it came, or the key equipment used to create the result;

e. The forensic unit can show whether the item was retained, returned to the organisation that submitted it, or destroyed; and

f. The measures to secure items/derived material that have to be left unattended, to ensure that they cannot be tampered with or otherwise compromised.

35.5.2 The forensic unit shall, as far as possible, preserve the item, or part of the item, in its original form to allow for independent re-examination or testing. If an insufficient quantity of the item remains for independent re-examination or testing, or the form of the item is altered, the forensic unit shall ensure that details of the item in its original form are recorded in sufficient detail for an independent examiner to be able to check that correct procedures and techniques have been used and that the results obtained appear valid.

35.6 Item Return and Disposal

35.6.1 The forensic unit shall have an agreement with its commissioning party for the return or disposal of items, and evidential material recovered from items, once the examination has been completed. [97]

35.6.2 Forensic units may deal with material that is subject to legal control or prohibition on possession, production or use. Policies covering such items should reflect any legal control or prohibition covering retention, the return to the organisation that submitted the items, or destruction. Examples of such items include, but are not limited to:

[97] Any specific clauses or controls stipulated shall be communicated to any subcontractors or external providers who are authorised to handle the exhibits.

a. Human tissue; [98]

b. Drugs;

c. Firearms; and

d. Indecent images of children.

35.6.3 If items are to be returned to the commissioning party, or provided for use in court, the forensic unit shall ensure that the commissioning party or court is made aware of any potential health and safety issues relating to the item, or its handling, and take appropriate steps to minimise the risk to the commissioning party or court.

35.6.4 Biohazardous items should be destroyed by the forensic unit in accordance with health and safety legislation, health and safety regulations and Home Office guidelines. [99] The requirements for retention, agreed with the commissioning party, shall also be adhered to.

36. Assuring the Quality of Test Results

36.1 Inter-Laboratory Comparisons (Proficiency Tests and Collaborative Exercises)

98 In England and Wales and Northern Ireland see the Human Tissue Act 2004 [97] or in Scotland the Human Tissue (Scotland) Act 2006 [98].

99 See HOC 40/73: Handling and disposal of blood samples in criminal cases (other than those brought under the Road Traffic Act 1972) [92] this recommends to Chief Police Officers that on completion of examination the sample should be retained at the laboratory and the defence notified that it will be destroyed after 21 days unless they request otherwise. However, if the sample is exhibited, it should not be destroyed without the permission of the committing court. HOC 41/73 [93] provides similar recommendations to HOC 40/73, but to the courts. HOC 125/76 [90] extends the arrangements of HOC 40/73 and 41/73 to the handling and disposal of saliva samples. HOC 74/82 [94]: Disposal of blood samples, saliva samples and swabs stained with body fluid: handling of exhibits: extends the arrangements of HOCs 40/73 41/73 and 125/76 to the disposal of swabs stained with body fluid. HOC 25/87 [91] extends the provisions of HOC 74/82 to cover the disposal of urine and any other body samples not previously covered.

36.1.1 The forensic unit shall review the availability and appropriateness of schemes for inter-laboratory comparisons that are relevant to its Forensic Science Activities and where relevant its scope of accreditation. [100] [101] [102]

36.1.2 Annex C of ISO/IEC 17043:2010 [68] provides useful information to assist in selection or design of schemes whether the examinations or tests are quantitative, qualitative or interpretive in nature and annex A of the Eurchem publication on proficiency test (PT) schemes [69] includes a checklist which includes consideration of the following.

a. Whether the parameters included in the scheme are similar to those of items encountered in the everyday practice of the forensic unit.

b. Whether the strategies for data collection and analysis applied by the PT provider suitable for the needs of the laboratory.

c. Whether the method used for assessing the participants’ performance is clearly described by the PT provider and understood by the laboratory.

d. The competence of a PT provider, for example:

    i. Compliance with the requirements of ISO/IEC 17043:2010, e.g. accreditation; [103]

    ii. Track record in delivering such schemes;

    iii. Reliability of the assigned values; and

    iv. Fitness for purpose of criteria for proficiency assessment.

---

[100] Forensic units may refer to the European Proficiency Testing Information System [86] or the European Network of Forensic Science Institutes (ENFSI) [87] websites for the availability of proficiency testing (PT) schemes.

[101] ISO 17025 [1] requires laboratories to ensure only suitable externally provided products and services that affect laboratory activities are used. This includes proficiency testing services. ISO/IEC 17043:2010 [68] contains recommendations and guidance on the requirements for the operation of PT schemes. These documents should be used as a basis for such an evaluation.

[102] UKAS accredits PT providers to ISO/IEC 17043:2010; a list of accredited schemes/providers is available. [70]

[103] UKAS recommends the use of an accredited scheme where one exists. [88]

36.1.3 The forensic unit shall participate in appropriate schemes, in order to monitor the validity of its examinations or tests, and its performance, both against its own requirements and against the performance of peer forensic units. [70]

36.1.4 When participating in inter-laboratory comparison schemes, the forensic unit’s own documented methods and procedures shall be used.

36.1.5 Proficiency testing records should include [3]:

a. Full details of the examinations/tests undertaken;

b. Results and conclusions obtained;

c. An indication that performance has been reviewed;

d. Details of the corrective action undertaken, where necessary.

36.1.6 Unexpected performance in inter-laboratory comparisons shall be handled as non-conforming testing (See Control of Non-Conforming Testing).

37. Reporting the Results

37.1 General [33]

General

37.1.1 The forensic unit shall detail lines of communication in a procedure that assigns roles and responsibilities to ensure the appropriate exchange of information and authorisations where relevant. This should cover communication of reports and evaluative statements with the police and prosecuting authorities, both nationally and locally, or with the instructing solicitor, as appropriate, within agreed timescales in accordance with the requirements and needs of each specific case and the known key dates in the criminal justice process.

37.1.2 The forensic unit shall provide early warning of any operational or scientific issues that could unavoidably affect the timeliness of service delivery to the commissioning party. [104]

---

[104] See Criminal Procedure Rules [34] 19.2(1)(b)(ii) where warning the court of any significant failure to act as required by a direction includes warning of any substantial delay in the preparation of a report.

37.1.3 The reporting practitioner shall be competent and comply with all pertinent parts of the Criminal Procedure Rules [34], Criminal Practice Directions [25], other requirements for expert evidence [71] and the applicable obligations on expert witnesses. [33] Reports shall comply with applicable legal provisions.

37.1.4 Full records shall be kept of work done and the results obtained in line with other retention policies, even if the commissioning party does not require a detailed report (including any statement). [105]

Duty to Court

37.1.5 Expert witnesses act as independent advisors to the court and this role creates obligations, to the court, which override any duty to the commissioning party (or anyone else). [33] Expert witnesses owe a duty of candour to the court.

37.1.6 Persons acting as an expert witness shall not do anything which is contrary to their obligations to the court or fail to do something which is required by that duty.

Declarations of Compliance and Non-Compliance with Required Standards [106] [71] [72]

General

37.1.7 All practitioners shall disclose in statements/reports intended for use as evidence, their compliance, or non-compliance, with the Standards of Conduct. [107] [108] The Standards of Conduct require compliance with the quality standards

---

105 Documentation of work underpinning reports and statements may be kept separate where it is traceable to the correct reports and statements.

106 Non-compliance is considered to be information that could significantly detract from the credibility of a witness and may have a bearing on reliability. In England and Wales, disclosure of such matters is not restricted to experts (see the Criminal Procedure and Investigations Act 1996 [96], R v. Ward [1993] 1 W.L.R. 619 and Kumar v. General Medical Council [2012] EWHC 2688 (Admin), or to the prosecution (see Criminal Practice Directions [25] V 19B (1) 13 and Criminal Procedure Rules [34] 19.3(3)(c)). Similar requirements are in place in other UK jurisdictions e.g. Criminal Justice and Licensing (Scotland) Act 2010 [99].

107 This does not apply to a Streamlined Forensic Report 1 (SFR1) as that is not intended to be used as evidence. However, a SFR1 does require a declaration about accreditation; see sub-section Types of report in the CJS.

108 See Criminal Practice Directions [25] V 19B (1) 13 “I confirm that I have acted in accordance with the code of practice or conduct for experts of my discipline, namely [identify the code]”.

set out by the Regulator in this Code (see the definitions of FSA in the appendices).

37.1.8 The Standards of Conduct cross references to the FSA definitions so a practitioner will be compliant with the Standards of Conduct only if they also comply with requirements for their discipline set out in the relevant FSA definition (e.g. accreditation to ISO 17025 [1] and this Code or to an appendix to this Code). [109]

37.1.9 All practitioners shall declare/disclose in statements/reports intended for use as evidence in the following terms, or in terms substantially the same: [110]

a. ‘I confirm that, to the best of my knowledge and belief, I have acted in accordance with the Standards of Conduct published by the Forensic Science Regulator [insert issue]’; or

b. ‘I confirm that, to the best of my knowledge and belief, I have acted in accordance with the Standards of Conduct published by the Forensic Science Regulator [insert issue] for infrequently used methods or new methods. As this method is not within the schedule of accreditation, annex [x] details the steps taken to comply with the specific requirements to control risk’; or

c. ‘I confirm that, to the best of my knowledge and belief, I have acted in accordance with the Standards of Conduct published by the Forensic Science Regulator [insert issue] in all aspects that relate to my personal conduct. However, my organisation is not yet compliant with the required standard (insert standard not met) for (insert discipline/sub-discipline or FSA relevant to the present case). Annex [x] details the steps taken to mitigate the risks associated with this aspect of non-compliance’; or

d. ‘I have not fully complied with the Standards of Conduct published by the Forensic Science Regulator [insert issue]. The nature of this non-compliance, to the best of my knowledge and belief, is that I am not/my

---

109 If the set requirement is accreditation to ISO 17025 [1] and this Code, but the practitioner’s forensic unit only holds accreditation to ISO 17025 [1] without including this Code then it is not fully compliant and the practitioner must disclose this.

organisation is not (delete as applicable) yet compliant with clause [insert clause from the Standards of Conduct] and the required standard for (insert discipline/sub-discipline or FSA relevant to the present case). Annex [x] details the steps taken to mitigate the risks associated with this non-compliance.’

Section 4 2021 Act

37.1.10 Section 4 of the 2021 Act [10] establishes that compliance or non-compliance with the provisions of this Code (as applicable to the work being carried out) is a relevant issue in relation to any matter to be determined by the court. This includes decisions on the admissibility of evidence.

37.1.11 As a consequence, non-compliance with relevant aspects of this Code shall be made clear in reports issued by forensic units.

37.2 Types of Report in the CJS

37.2.1 Forensic units, or persons working in forensic units, may be required to supply technical or expert advice to support the investigative process and factual or opinion evidence to support the judicial process which are all covered by the requirements in this Code including the provision of the following.

a. Interim progress reports [110] to support criminal investigations. These are initial forensic reports used for an assessment of the test items that may help an enquiry, interview or strategy. This report is non-evidential but may be disclosable as unused material and does not require a statement of compliance with the Standards of Conduct (see 37.1.7 et seq - Declarations of Compliance and Non-Compliance with Required Standards).

b. Streamlined Forensic Reports (SFR) [73]. These have been introduced for certain evidence types for use in the case management process to establish the level of agreement between the defence and the prosecution.

[110] ILAC G19 [3] section 4.9 includes oral reports, including the requirement to record the information conveyed.

i. The SFR1 is a summary of the evidence served to determine whether there is any agreement of the evidence, or to ascertain whether there are any issues in dispute. It is deliberately not presented in an admissible format as it is not intended to be presented at trial other than as agreed fact and it does not need to comply with Criminal Procedure Rules 19.4 [34] or Criminal Practice Directions V 19B [25]. It does however require a statement of whether the results are from a method which requires accreditation and if so, if the method is within the forensic unit’s schedule of accreditation. [111] [112]

ii. The SFR2 is produced to answer the issue(s) raised by the defence in response to the SFR1, it is intended to be presented in evidence, unless a full evaluative report is required instead. Therefore an SFR2 does require a statement of compliance with the Standards of Conduct (see section 15) and if it is providing expert opinion it requires an expert’s declaration under Criminal Procedure Rules 19.4 [34].

c. Reports (a statement is a type of report) for use in court proceedings.

i. Factual reports require a statement of compliance with the Standards of Conduct.

ii. Expert reports including opinion evidence require a declaration under Criminal Procedure Rules 19.4(j) [34] and 19B of the Criminal Practice Directions V [25] which should include a statement of compliance with the Standards of Conduct (see section 15) as part of

---

111 The Crown Prosecution Service (CPS) has stated that, in England and Wales, “Statements and Streamlined Forensic Reports (SFR1 and SFR2) should state whether the organisation or laboratory concerned is accredited, whether the forensic evidence relates to DNA and fingerprint evidence or other forensic disciplines.” This position is to facilitate the policy described in the CPS Internet section on expert evidence. [123]

112 In cases where those preparing the SFR1 are aware of further information that might meet the test for common-law disclosure set out above, that information should be communicated to the investigator and by the investigator to the prosecutor using form MG6 (or its equivalent).

the declaration required by 19B of the Criminal Practice Directions V [25].

iii. The court may extend a number of the requirements applicable to expert evidence of opinion to expert evidence of fact (See Part 19 Criminal Procedure Rules [34]).

d. Certificates (e.g. issued under provisions of the Road Traffic Offenders Act 1988) [74].

i. The content of a certificate must comply with the provisions of the statute which created the right to use the certificate and should include statement of compliance with the Standards of Conduct (see section 15).

37.3 Retention, Recording, Revelation and Disclosure

37.3.1 All practitioners, and forensic units, shall comply with legal obligations on retention of evidence, revelation to the instructing party and disclosure. [33]

37.3.2 If a practitioner has carried out a test, or if such a test has been carried out at their laboratory, which casts doubt on a particular proposition they must bring this to the attention of those instructing them.

37.3.3 Forensic units instructed by the prosecution must support the disclosure process and provide access to the defence to material identified as relevant by the prosecution. [24]

37.3.4 All documents, test items and evidential material recovered from test items that are retained by forensic units shall be archived in secure storage, in conditions to prevent damage or deterioration, and indexed so as to facilitate orderly storage and retrieval. [113]

[113] The cost of archiving documents relating to the forensic unit’s testing and examinations is a business cost to be borne by the forensic unit. Reimbursement of the costs for archiving exhibits and evidential material recovered from exhibits is a business matter to be agreed between the forensic unit instructed by the prosecution and the commissioning party (e.g. police).

37.3.5 Only personnel authorised by management shall have access to the retained materials. Movement of material in and out of the archives shall be properly recorded.

37.4 Defence Examinations

37.4.1 The forensic unit instructed by the defence shall ensure that any tests or examinations they conduct, or are conducted on their behalf by someone other than the original forensic unit, are carried out in accordance with the requirements set out in this Code, and that they also comply with any conditions attached by the prosecutor to the release of the test items, or parts of test items, or evidential material recovered from them.

37.4.2 The forensic unit appointed by the prosecution shall have defined policies and procedures to facilitate access by defence examiners to carry out a review of work already completed by the forensic unit, which is deemed by the prosecutor or court to be relevant, in the case.

37.4.3 The policies and procedures shall ensure the security and integrity of the test items and records requested for review, but must also ensure the confidentiality of other work in progress or previously undertaken by the forensic unit instructed by the prosecution, to which access has not been granted.

37.4.4 A forensic unit appointed by the defence seeking pre-trial access to any case material shall first obtain approval for access to these from the prosecutor (or coroner if the prosecuting authority is not involved at that stage).

37.4.5 The forensic unit appointed by the prosecution shall make available to the defence’s forensic unit only what has been deemed by the prosecutor or court to be relevant. Copies of such case file records, documents and supporting information, etc. that have been reasonably requested by the forensic unit appointed by the defence and been deemed relevant may then be provided in hard copy or secure electronic form [114] and be taken into their possession for

---

[114] The Legal Aid Agency’s position on charges levied upon the defence by prosecution forensic science laboratories is available in their publication ‘Guidance on forensic science laboratory charges in criminal matters’. [89]

examination away from the premises of the forensic unit appointed by the prosecution.

37.4.6 The forensic unit instructed by the defence shall retain the notes and records it has created in line with this Code. Material supplied by the prosecution forensic unit shall only be used for the specific case(s) for which the material was provided. [115]

37.4.7 Material supplied by the prosecution is subject to the Data Protection Act 2018 [75] and may be subject to Police and Criminal Evidence Act 1984 [76] as amended by the Protection of Freedoms Act 2012 (e.g. fingerprints and DNA) [77]. [116]

37.4.8 The forensic unit instructed by the prosecution shall only release test items (or evidential material recovered from them) to the defence for examination or testing away from the premises of the forensic unit instructed by the prosecution on receipt of written instructions from the prosecutor and/or the court. Where the examinations or testing might affect their condition, the forensic unit instructed by the prosecution shall ensure that the prosecutor and/or the court is made aware of this before they are released and that this is recorded.

37.4.9 The forensic unit instructed by the prosecution shall ensure that all examinations and tests carried out on the forensic unit’s premises by the defence are adequately supervised, to ensure that they are carried out in accordance with the instructions given by the prosecutor and that nothing is altered, damaged or destroyed without the prior permission of the prosecutor.

37.4.10 The forensic unit instructed by the prosecution shall ensure that all test items (or parts of test items, or evidential material recovered from them) that are to be released to the defence are recorded, securely packaged, labelled and any conditions that apply to handling and retention are made in writing (e.g. from the

---

115 The forensic unit appointed by the prosecution may require, if it chooses to, that supporting supplementary material (e.g. manuals, SOPs) is returned by the defence’s forensic unit or that the supplied copies are destroyed, as appropriate, once the case is concluded.

116 The Protection of Freedoms Act 2012 [77] modified the Police and Criminal Evidence Act 1984 [76] to have specific controls for the destruction, retention and use of biometric data which means certain requirements may be stipulated as a condition of access to any third party which is authorised to handle material.

court, prosecution, commissioning party). The forensic unit appointed by the prosecution shall also retain a signed record of the transfers for continuity purposes.

37.4.11 The forensic unit instructed by the prosecution shall check the integrity and continuity records of the returned test items, or parts of test items, or evidential material for compliance with any conditions of release. Any deficiency in these respects shall be communicated immediately to the prosecutor and the commissioning party, e.g. the police.

37.5 Opinions and Interpretations

General

37.5.1 Where this is to be included in a forensic unit’s schedule of accreditation, the forensic unit will need to ensure that it is, if accredited by UKAS, in compliance with the UKAS publication LAB 13 [78] and ILAC-G19 [3] section 4.9. If the forensic unit is accredited by an accreditation body other than UKAS it shall be in compliance with ILAC-G19 [3] and the requirements of that body in relation for opinions and interpretation.

Evaluative Opinions

37.5.2 A forensic unit providing evaluative opinion evidence shall meet the following requirements.

a. The policies and procedure for case assessment and interpretation shall be part of the quality management system.

b. The policies and procedures for making reports of evaluative opinion shall be part of the quality management system. [117]

c. The method for evaluation shall be validated according to this Code.

---

[117] This is a requirement of LAB 13 section 6.4. [78]

d. The policies and procedures shall ensure there is clarity in any report as to the source(s) of data used in forming the evaluative opinion. [118] [119]

e. The experts providing evaluative opinion shall be demonstrably competent to do so (see also 27.3.7).[120]

f. Any statistical models and assumptions involved in the evaluation shall be clear to the CJS and shall be valid.[121] [122]

g. Processes for the peer review of evaluation shall be part of the quality management system. [123]

37.6 Regulator’s Concerns

37.6.1 As discussed in section 24.3 herein the Regulator may deal with concerns about the work of a forensic unit as part of routine monitoring, by means of a Regulator’s investigation or compliance action.

37.6.2 The forensic unit shall consider whether any activity by the Regulator, as described above, creates an obligation to disclose in reports issued by the forensic unit or its practitioners.

38. Demonstration of Compliance

38.1 General

38.1.1 The Regulator requires, for certain FSA, that forensic units shall demonstrate compliance with this Code in a particular manner.

38.1.2 Where the Regulator has established such a requirement it is set out in section 9 herein and in the appendix relevant to the FSA.

---

118 This is a requirement of LAB 13 section 6.21. [78]

119 This is a requirement of Part 19 CrimPR. [3]

120 This is a requirement of LAB 13 sections 6.6, 6.13 and 6.14 [77]. It is also a requirement of ILAC G19 4.8.3. [3]

121 This is a requirement of LAB13 section 6.10. [78]

122 The validity of the model employed should be addressed as part of the validation of the method (see Methods and Method Validation 29.3.18 and 29.3.67 herein).

123 This is a requirement of ILAC G19 section 4.8.2. [3]

38.2 Accreditation

General

38.2.1 For any FSA the Regulator may require a forensic unit carrying on the FSA to achieve and maintain any combination of the following

a. Accreditation to an appropriate international standard. [124]

b. The accreditation includes adherence to the requirements of this Code.

38.2.2 All forensic units carrying on an FSA which is subject to this Code are bound by this Code (including any appendices) to the extent set out in the appendices. The method of demonstrating compliance with this Code for most of the analytical disciplines, with only a few explicit exceptions [125], is through accreditation to ISO 17025 [1], ISO 17020 [2] and/or ISO 15189 [18] with adherence to this Code recorded in the schedule of accreditation.

38.2.3 The appropriate international standard, or standards, for FSA subject to an accreditation requirement is provided at section 9 herein and in the relevant appendices.

38.2.4 The requirement for accreditation may incorporate the application of documents the Regulator considers to be relevant (e.g. ILAC-G19 [3]). Such documents will be listed in section 12.3 herein - Normative References.

38.2.5 Accreditation to an international standard will only be considered to have met the requirement if:

a. The schedule of accreditation covers the FSA; and

b. The forensic unit has signed a waiver of confidentiality to allow the accreditation body to share information with the Regulator.

38.2.6 It is recognised a new method may require a period of time from introduction to obtain suitable data to demonstrate the operation of the process or procedure satisfactorily for an accreditation body to include this method within the forensic

---

124 A standard published by the International Organization for Standardization.

125 Exceptions are included in the Forensic Science Activities definitions (see the appendices).

unit’s schedule of accreditation. Forensic units intending to introduce such methods should consider the applicability of the provisions around infrequently used methods set out in section 29.3.48 herein and/or discuss options with the accreditation body. [126]

38.2.7 Where accreditation is required, and exigent circumstances mean that a method other than that as detailed in the schedule of accreditation needs to be used and there is no legal impediment, [127] this should be made clear to the commissioning party and the fact that accreditation should apply and was not held should be declared in any statements or reports. Section 37.1.7 et seq Declarations of Compliance and Non-Compliance with Required Standards details some options for declarations. The expectation is that, where any required standard is not met fully, in addition to the declaration a separate annex [128] to the statement or report is also produced which details how the risk is mitigated.

Accreditation Bodies

General

38.2.8 Any requirement for accreditation will only be achieved if the accreditation is issued by an accreditation body recognised by the Regulator.

38.2.9 An accreditation body will only be recognised by the Regulator if the following conditions are met.

a. The body is recognised as an accreditation body by the Government of the country/territory in which it operates;

---

126 Certain parallel or duplication of processing may be used within the same organisation to satisfy this requirement, provided splitting casework does not render the sample suboptimal or introduce significant limitations.

127 See also The Accreditation of Forensic Service Providers Regulations 2018 [95], The Accreditation of Forensic Service Providers (Amendment) Regulations 2019 [100] and European Union (Future Relationship) Act 2020 [101].

128 Producing an annex dealing with issues arising from partial or non-compliance allows the complex issue to be dealt with in the statement/report and could allow forensic units to produce standard lines to take for certain methods. Further detail on the content of the annex is available in the Regulator’s publications on reports and statements. [71]

b. It is, or is seeking to, provide accreditation in a country/territory where it is legal for it to do so;

c. It will only accredit forensic units against this Code where the unit has signed a confidentiality waiver as required by section 38.2.5 herein;

d. It incorporated accreditation to this Code in the Schedule of accreditation;

e. The requirements of ILAC G19 [3] are incorporated into the accreditation process; and

f. It has entered, and operates in accordance with, a data sharing agreement with the Regulator which addresses the issues in section 38.2.10 herein.

38.2.10 The data sharing agreement mentioned in section 38.2.9 herein must achieve the following.

a. The accreditation body must be able to share any concerns about a forensic unit to the Regulator.

b. The Regulator must be able to share any concerns about a forensic unit to the accreditation bodies.

c. The accreditation body must be able to provide the Regulator with general information about the number of bodies accredited etc.

38.2.11 The Regulator will publish, and amend as appropriate, a list of recognised accreditation bodies.

Data Sharing

38.2.12 The Regulator may share information related to any quality concerns about a forensic unit with the appropriate accreditation body or accreditation bodies.

UKAS

38.2.13 UKAS will, at least in non-scene based FSAs where this Code requires accreditation, assess forensic units, in England and Wales, undertaking FSAs against ISO 17025 [1] or ISO 15189 [18] [129] utilising any of the relevant UKAS laboratory publications [79], ILAC-G19 [3] and the supplementary requirements

[129] Where accreditation is the requirement in the definition of the Forensic Science Activity.

of this Code, and will, if the forensic unit has achieved the requisite standards, include compliance with this Code in the Schedule of Accreditation. [130] UKAS can assess forensic units providing forensic science activities at scenes of incidents [131] against ISO 17020 [2], ISO 17025 [1], ILAC-G19 [3], ILAC-P15 [16], this Code, and the inspection recommendation and guidance publication UKAS-RG 201 [17].

Accreditation Issues

38.2.14 The Regulator has based the accreditation requirements in this Code on the use of the international standards ISO 17020 [2] and ISO 17025 [1].

38.2.15 Accreditation to ISO 15189 [18] is a suitable alternative to ISO 17025 [1] for undertaking certain FSA, provided that ‘Forensic Testing/Analysis’ is clearly indicated in the scope of accreditation; this means that the forensic unit has been assessed in accordance with ISO 15189 [18] taking into account ILAC-G19 [3]. The FSA for which accreditation to ISO 15189 [18] is appropriate are set out in the FSA definitions.

38.2.16 Other standards used for certification of organisations that provide scientific services – e.g. Good Laboratory Practice (GLP) [80] regulations and Good Manufacturing Practice (GMP) [81] are not alternatives to ISO 17020 [2], ISO 17025 [1] or ISO 15189 [18], although they do overlap to some extent and provide compatible guidance on good practice.

38.2.17 This Code will be updated to reflect relevant changes in the requirements of ISO 17025 [1], ISO 17020 [2], ISO 15189 [18], ILAC-G19 [3], ILAC-P15 [16] and the CJS.

---

130 The Regulator has a Memorandum of Understanding with the national accreditation body UKAS, agreements with other national accreditation bodies may be entered into if required.

131 The term scenes of incident, includes scenes prior to establishing whether a criminal or illegal action has taken place and relevant locations, for example where a body is found.

Part F - General Provisions

39. References

[1] International Organization for Standardization, “BS EN ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories”.

[2] International Organization for Standardization, “BS EN ISO/IEC 17020:2012, General criteria for the operation of various types of bodies performing inspection”.

[3] International Laboratory Accreditation Cooperation, “ILAC-G19:08/2014, Modules in a Forensic Science Process,” [Online]. Available: https://ilac.org/latest_ilac_news/ilac-g19082014-published/. [Accessed 12 09 2021].

[4] Forensic Science Regulator, “Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System,” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 18 09 2021].

[5] House of Commons Select Committee on Science and Technology, “Forensic Science Service,” 2011.

[6] House of Commons Select Committee on Science and Technology, “The work of the Biometrics Commissioner and the Forensic Science Regulator,” 2019.

[7] House of Commons Select Committee on Science and Technology, “Biometrics Strategy and Forensic Services,” 2018.

[8] House of Lords Select Committee on Science and Technology, “Forensic Science and the Criminal Justice System: A Blueprint for Change,” 2019.

[9] Darren Jones MP, “Forensic Science Regulator and Biometrics Strategy Bill,” [Online]. Available: https://bills.parliament.uk/bills/2616/publications. [Accessed 18 09 2021].

[10] “The Forensic Science Regulator Act 2021,” [Online]. Available: www.legislation.gov.uk/ukpga/2021/14/contents. [Accessed 05 09 2021].

[11] House of Lords, “Official Report - 29 April 2021,” [Online]. Available: https://hansard.parliament.uk/lords/2021-04-29. [Accessed 12 09 2021].

[12] House of Commons, “Official Report - 12 July 2007,” [Online]. Available: https://hansard.parliament.uk/commons/2007-07-12. [Accessed 13 09 2021].

[13] House of Commons, “Forensic Science Regulator and Biometric Strategy Bill - Explanatory Notes,” [Online]. Available: https://bills.parliament.uk/bills/2616/publications. [Accessed 25 09 2021].

[14] “Employment Rights Act 1996,” [Online]. Available: www.legislation.gov.uk/ukpga/1996/18/contents. [Accessed 11 09 2021].

[15] “The Interpretation Act 1978,” [Online]. Available: www.legislation.gov.uk/ukpga/1978/30/contents. [Accessed 05 09 2021].

[16] International Laboratory Accreditation Cooperation, “ILAC-P15:07/2016, Application of ISO/IEC 17020:2012 for the Accreditation of Inspection Bodies,” [Online]. Available: https://ilac.org/publications-and-resources/ilac-policy-series/. [Accessed 12 09 2021].

[17] United Kingdom Accreditation Service, “UKAS-RG 201:2015, Accreditation of Bodies Carrying Out Scene of Crime Examination (Edition 2),” [Online]. Available: https://www.ukas.com/wp-content/uploads/schedule_uploads/6456/RG-201-Accreditation-of-Bodies-Carrying-out-Scene-of-Crime-Examination.pdf. [Accessed 12 09 2021].

[18] International Organization for Standardization, “BS EN ISO 15189:2012, Medical laboratories. Requirements for quality and competence”.

[19] International Organization for Standardization, “BS EN ISO/IEC 17000:2020, Conformity assessment. Vocabulary and general principles”.

[20] “The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018,” [Online]. Available: www.legislation.gov.uk/uksi/2018/952/contents/made. [Accessed 17 10 2021].

[21] National Police Chiefs' Council, “Retention, Storage and Destruction of Materials and Records Relating to Forensic Examinations,” 2021. [Online]. Available: www.fcn.police.uk/sites/default/files/2021-08/NPCC%20Forensic%20Retention%20Guidance%20v1.0.pdf. [Accessed 04 09 2021].

[22] Forensic Science Regulator, “Marker Reference - Policy on Investigations and Complience,” [Online].

[23] “Government Security Classifications,” [Online]. Available: www.gov.uk/government/publications/government-security-classifications. [Accessed 11 09 2021].

[24] Crown Prosecution Service, “CPS Guidance for Experts on Disclosure, Unused Material and Case Management,” [Online]. Available: www.cps.gov.uk/legal-guidance/cps-guidance-experts-disclosure-unused-material-and-case-management. [Accessed 17 11 2020].

[25] “Criminal Practice Directions (Practice Direction (CA(Crim Div); Criminal Proceedings: General Matters) [2015] EWCA Crim 1567,” [Online]. Available: www.gov.uk/guidance/rules-and-practice-directions-2020. [Accessed 05 09 2021].

[26] I. W. Evett, “The Logical Foundation of Forensic Science: Towards Reliable Knowledge,” *Phil. Trans. R. Soc. B,* p. 370, 2015.

[27] D. Rogers and B. Found, “The initial profiling trial of a program to characterize forensic handwriting examiners’ skill,” *Journal of American Society of Questioned Document Examiners,* no. 6, pp. 72-81, 2003.

[28] Forensic Science Regulator, “FSR-G-208, Laboratory DNA: anti-contamination guidance,” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 17 11 2020].

[29] Forensic Science Regulator, “FSR-G-206, Crime Scene DNA: Anti-contamination guidance,” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 17 11 2020].

[30] Forensic Science Regulator, “FSR-G-207, Sexual assault referral centres and custodial facilities: DNA anti-contamination,” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 17 11 2020].

[31] Forensic Science Regulator, “FSR-G-201, Validation,” [Online]. Available: www.gov.uk/government/publications/forensic-science-providers-validation. [Accessed 17 11 2020].

[32] Forensic Science Regulator, “FSR-G-218, Guidance: Method Validation in Digital Forensics.,” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 17 11 2020].

[33] Forensic Science Regulator, “FSR-I-400, Legal Obligations,” [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance.

[34] “Criminal Procedure Rules 2020,” [Online]. Available: www.gov.uk/guidance/rules-and-practice-directions-2020. [Accessed 05 09 2021].

[35] Forensic Science Regulator, “FSR-P-300, Protocol: using casework material for validation purposes,” [Online]. Available: www.gov.uk/government/collections/forensic-science-regulator-technical-guidance. [Accessed 17 11 2020].

[36] United Kingdom Accreditation Service, “TPS 68: UKAS Policy on Accreditation of Infrequently Performed Conformity Assessment Activities,” [Online]. Available: www.ukas.com/download/publications/Technical%20Policy%20Statements/TPS-68-Infrequently-Performed-Activities-Edition-2-June-2020.pdf. [Accessed 17 11 2020].

[37] United Kingdom Accreditation Service, “M3003, The Expression of Uncertainty and Confidence in Measurement,” [Online]. Available: www.ukas.com/download/publications/publications-relating-to-laboratory-accreditation/M3003-Expression-of-Uncertainty-and-Confidence-in-Measurement-Edition-4-October-2019.pdf. [Accessed 17 11 2020].

[38] International Laboratory Accreditation Cooperation, “ILAC G17: 01/2021 Guidelines for Measurement Uncertainty in Testing,” [Online]. Available: https://ilac.org/publications-and-resources/ilac-guidance-series/. [Accessed 16 11 2021].

[39] The National Cyber Security Centre, “Secure Sanitisation of Storage Media,” 2016. [Online]. Available: www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media. [Accessed 24 6 2020].

[40] The Centre for the Protection of National Infrastructure, “Secure Destruction,” 2019. [Online]. Available: www.cpni.gov.uk/secure-destruction. [Accessed 24 6 2020].

[41] The National Cyber Security Centre, “Acquiring, managing, and disposing of network devices,” 2016. [Online]. Available: www.ncsc.gov.uk/guidance/acquiring-managing-and-disposing-network-devices. [Accessed 24 6 2020].

[42] Cabinet Office, “Minimum Cyber Security Standard,” 2018. [Online]. Available: www.gov.uk/government/publications/the-minimum-cyber-security-standard. [Accessed 24 June 2020].

[43] International Organization for Standardization, “BS ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements”.

[44] International Organization for Standardization, “BS ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management”.

[45] Cabinet Office, “Minimum Cyber Security Standard,” [Online]. Available: www.gov.uk/government/publications/the-minimum-cyber-security-standard. [Accessed 17 11 2020].

[46] The National Cyber Security Centre,, “10 Steps to cyber security,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps. [Accessed 24 6 2020].

[47] The National Cyber Security Centre, “Password administration for system owners,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/passwords/updating-your-approach. [Accessed 24 6 2020].

[48] The National Cyber Security Centre, “Three random words or #thinkrandom,” 2016. [Online]. Available: www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0. [Accessed 24 6 2020].

[49] The National Cyber Security Centre, “Password manager buyers guide,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/passwords/password-manager-buyers-guide. [Accessed 24 6 2020].

[50] The National Cyber Security Centre, “Passwords, passwords everywhere,” 2019. [Online]. Available: www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere. [Accessed 24 6 2020].

[51] The National Cyber Security Centre, “Using TLS to protect data 2017,” 2017. [Online]. Available: www.ncsc.gov.uk/guidance/tls-external-facing-services. [Accessed 24 6 2020].

[52] The National Cyber Security Centre, “Using IPSec protect data,” 2016. [Online]. Available: www.ncsc.gov.uk/guidance/using-ipsec-protect-data. [Accessed 24 6 2020].

[53] The National Cyber Security Centre, “The National Cyber Security Centre,” 30 April 2020. [Online]. Available: www.ncsc.gov.uk/blog-post/terminology-its-not-black-and-white. [Accessed 30 6 2020].

[54] The National Cyber Security Centre, “End user device (EUD) security guidance,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles. [Accessed 24 6 2020].

[55] The National Cyber Security Centre, “Mitigation malware,” 2018. [Online]. Available: www.ncsc.gov.uk/guidance/mitigating-malware. [Accessed 24 6 2020].

[56] The National Cyber Security Centre, “Phishing attacks: defending your organisation,” 2018. [Online]. Available: www.ncsc.gov.uk/guidance/phishing. [Accessed 24 6 2020].

[57] The National Cyber Security Centre, “Products & Services,” 2020. [Online]. Available: www.ncsc.gov.uk/section/products-services/all-products-services-categories?&start=0&rows=20. [Accessed 24 6 2020].

[58] The National Cyber Security Centre, “Small Business Guide: Response and Recovery,” 2019. [Online]. Available: www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery. [Accessed 24 6 2020].

[59] The National Cyber Security Centre, “Preventing lateral movement,” 2018. [Online]. Available: www.ncsc.gov.uk/guidance/preventing-lateral-movement. [Accessed 24 6 2020].

[60] The Australian Cyber Security Centre, “Implementing Network Segmentation and Segregation,” 2019. [Online]. Available: www.cyber.gov.au/publications/implementing-network-segmentation-and-segregation. [Accessed 24 6 2020].

[61] The National Cyber Security Centre, “Offline backups in an online world,” 2019. [Online]. Available: www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world. [Accessed 24 6 2020].

[62] The National Cyber Security Centre, “Mitigation malware and ransomware attacks,” 2020. [Online]. Available: www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks. [Accessed 24 6 2020].

[63] The National Cyber Security Centre, “Cloud Security Guidance Implementing the Cloud Security Principles,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles. [Accessed 24 6 2020].

[64] The National Cyber Security Centre, “Incident Management,” 2019. [Online]. Available: www.ncsc.gov.uk/collection/incident-management. [Accessed 24 6 2020].

[65] The National Cyber Security Centre, “Introduction to logging for security purposes,” 2018. [Online]. Available: www.ncsc.gov.uk/guidance/introduction-logging-security-purposes. [Accessed 24 6 2020].

[66] The National Cyber Security Centre, “Logging made easy (LME),” 2019. [Online]. Available: www.ncsc.gov.uk/blog-post/logging-made-easy. [Accessed 24 June 2020].

[67] Forensic Science Regulator, Cognitive Bias Effects Relevant to Forensic Science Examinations FSR-G-217, Forensic Science Regulator.

[68] International Organization for Standardization, “ISO/IEC 17043:2010, Conformity assessment — General requirements for proficiency testing”.

[69] Eurochem, “Selection, Use and Interpretation of Proficiency Testing (PT) Schemes by Laboratories,” 2021. [Online]. Available: www.eurachem.org/index.php/publications/guides/usingpt. [Accessed 2021 11 24].

[70] United Kingdom Accreditation Service, “UKAS Policy on Participation in Proficiency Testing,” [Online]. Available: www.ukas.com/download/publications/Technical%20Policy%20Statements/TPS-47-Participation-in-PT-Edition-4-February-2020.pdf. [Accessed 17 11 2020].

[71] Forensic Science Regulator, “FSR-G-200, Expert Report Guidance,” [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance. [Accessed 17 11 2020].

[72] Forensic Science Regulator, “FSR-G-225, Non-Expert Technical Statement Guidance,” [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance. [Accessed 17 11 2020].

[73] Forensic Capability Network, “Streamlined Forensic Reporting (SFR),” [Online]. Available: www.fcn.police.uk/services/science/streamlined-forensic-reporting-sfr. [Accessed 12 09 2021].

[74] “Road Traffic Offenders Act 1988,” [Online]. Available: www.legislation.gov.uk/ukpga/1988/53/contents. [Accessed 11 09 2021].

[75] “Data Protection Act 2018,” [Online]. Available: www.legislation.gov.uk/ukpga/2018/12/contents. [Accessed 11 09 2021].

[76] “Police and Criminal Evidence Act 1984,” [Online]. Available: www.legislation.gov.uk/ukpga/1984/60/contents. [Accessed 11 09 2021].

[77] “Protection of Freedoms Act 2021,” [Online]. Available: www.legislation.gov.uk/ukpga/2012/9/contents. [Accessed 11 09 2021].

[78] United Kingdom Accreditation Service, “UKAS LAB 13 Guidance on the Application of ISO/IEC 17025 Dealing with Expressions of Opinions and Interpretations,” [Online]. Available: www.ukas.com/download/publications/publications-relating-to-laboratory-accreditation/LAB-13-Edition-3-April-2019.pdf. [Accessed 17 11 2020].

[79] United Kingdom Accreditation Service, “Publications relating to accreditation of Laboratories,” [Online]. Available: www.ukas.com/technical-services/publications/publications-relating-to-laboratories/. [Accessed 17 11 2020].

[80] “The Good Laboratory Practice Regulations 1999,” [Online]. Available: www.legislation.gov.uk/uksi/1999/3106/contents. [Accessed 12 09 2021].

[81] Medicines and Healthcare Products Regulatory Agency, “Good manufacturing practice and good distribution practice,” [Online]. Available: www.gov.uk/guidance/good-manufacturing-practice-and-good-distribution-practice. [Accessed 17 11 2020].

[82] Criminal Procedure Rule Committee, “Criminal Procedure Rules 2020,” 2020. [Online]. Available: www.gov.uk/guidance/rules-and-practice-directions-2020. [Accessed 17 11 2020].

[83] Crown Prosecution Service, “Forensic Science: Core Foundation Principles for Forensic Science Providers,” [Online]. Available: www.cps.gov.uk/legal-guidance/forensic-science-core-foundation-principles-forensic-science-providers. [Accessed 17 11 2020].

[84] International Laboratory Accreditation Cooperation, “ILAC G27:07/2019 Guidance on measurements performed as part of an inspection process,” [Online]. Available: https://ilac.org/publications-and-resources/ilac-guidance-series/. [Accessed 17 11 2020].

[85] The National Cyber Security Centre, “Setting up two-factor authentication (2FA),” [Online]. Available: www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa. [Accessed 17 11 2020].

[86] European Proficiency Testing Information System , “About EPTIS,” [Online]. Available: www.eptis.bam.de/en/index.htm. [Accessed 17 11 2020].

[87] European Network of Forensic Science Institutes, “Welcome to ENFSI!,” [Online]. Available: https://enfsi.eu/. [Accessed 17 11 2020].

[88] United Kingdom Accreditation Service, “Find Accredited Organisations: Proficiency Testing Providers (PTP),” [Online]. Available: www.ukas.com/browse-accredited-organisations/?org_type=13. [Accessed 17 11 2020].

[89] Legal Aid Agency, “Guidance on forensic science laboratory charges in criminal matters,” [Online]. Available: www.gov.uk/guidance/expert-witnesses-in-legal-aid-cases#forensic-science-laboratory-charges-in-criminal-matters. [Accessed 17 11 2020].

[90] Home Office, “Circular 125/1976: Handling and disposal of saliva samples”.

[91] Home Office, “Circular 25/1987: I. Agreement for the use of the Police National Computer, II. Disposal of body samples”.

[92] Home Office, “Circular 40/1973: Handling and disposal of blood samples in criminal cases (other than those brought under the Road Traffic Act 1972)”.

[93] Home Office, “Circular 41/1973: Handling and disposal of blood samples”.

[94] Home Office, “Circular 74/1982: Disposal of blood samples, saliva samples and swabs stained with body fluid: handling of exhibits”.

[95] “The Accreditation of Forensic Service Providers Regulations 2018,” [Online]. Available: www.legislation.gov.uk/uksi/2018/1276/contents. [Accessed 05 09 2021].

[96] “Criminal Procedure and Investigations Act 1996,” [Online]. Available: www.legislation.gov.uk/ukpga/1996/25/contents. [Accessed 05 09 2021].

[97] “Human Tissue Act 2004,” [Online]. Available: www.legislation.gov.uk/ukpga/2004/30/contents. [Accessed 10 09 2021].

[98] “Human Tissue (Scotland) Act 2006,” [Online]. Available: www.legislation.gov.uk/asp/2006/4/contents. [Accessed 11 09 2021].

[99] “Criminal Justice and Licensing (Scotland) Act 2010,” [Online]. Available: www.legislation.gov.uk/asp/2010/13/contents. [Accessed 11 09 2021].

[100] “The Accreditation of Forensic Service Providers (Amendment) Regulations 2019,” [Online]. Available: www.legislation.gov.uk/uksi/2019/1384/contents/made. [Accessed 11 09 2021].

[101] “European Union (Future Relationship) Act 2020,” [Online]. Available: www.legislation.gov.uk/ukpga/2020/29/contents. [Accessed 11 09 2021].

[102] “The Criminal Justice Act 1967,” [Online]. Available: www.legislation.gov.uk/ukpga/1967/80/contents. [Accessed 11 09 2021].

[103] “Contempt of Court Act 1981,” [Online]. Available: www.legislation.gov.uk/ukpga/1981/49/contents. [Accessed 12 09 2021].

[104] British Standards Institution, “Publicly Available Specification (PAS) 377:2012 Specification for consumables used in the collection, preservation and processing of material for forensic analysis - Requirements for product, manufacturing and forensic kit assembly,” 2012.

[105] House of Commons, “Official Report - 5 February 2020,” [Online]. Available: https://hansard.parliament.uk/commons/2020-02-05. [Accessed 12 09 2021].

[106] House of Commons, “Official Report - 25 September 2020,” [Online]. Available: https://hansard.parliament.uk/commons/2020-09-25. [Accessed 12 09 2021].

[107] House of Commons, “Official Report - 11 November 2020,” [Online]. Available: https://hansard.parliament.uk/commons/2020-11-11#undefined. [Accessed 12 09 2021].

[108] House of Commons, “Official Report - 12 March 2021,” [Online]. Available: https://hansard.parliament.uk/commons/2021-03-12. [Accessed 12 09 2021].

[109] House of Commons, “Official Report - 10 November 2020,” [Online]. Available: https://hansard.parliament.uk/commons/2020-11-10. [Accessed 12 09 2021].

[110] House of Lords, “Official Report - 12 March 2021,” [Online]. Available: https://hansard.parliament.uk/lords/2021-03-12. [Accessed 12 09 2021].

[111] House of Lords, “Official Report - 19 March 2021,” [Online]. Available: https://hansard.parliament.uk/lords/2021-03-19. [Accessed 12 09 2021].

[112] House of Lords, “Official Report - 15 April 2021,” [Online]. Available: https://hansard.parliament.uk/lords/2021-04-15. [Accessed 12 09 2021].

[113] House of Lords, “Official Report - 22 April 2021,” [Online]. Available: https://hansard.parliament.uk/lords/2021-04-22. [Accessed 12 09 2021].

[114] “United Kingdom Security Vetting,” [Online]. Available: www.gov.uk/government/organisations/united-kingdom-security-vetting. [Accessed 13 09 2021].

[115] Warwickshire Police, “Vettting Process,” [Online]. Available: www.warwickshire.police.uk/police-forces/warwickshire-police/areas/warwickshire-police/about-us/about-us/national-contractors-vetting-scheme/vetting-process/. [Accessed 13 09 2021].

[116] EuraChem, “Quantifying Uncertainty in Analytical Measurement, 3rd Edition (2012),” [Online]. Available: www.eurachem.org/index.php/publications/guides/quam. [Accessed 24 09 2021].

[117] International Organization for Standardization, “BS EN ISO 9001:2015, Quality management systems. Requirements”.

[118] International Organization for Standardization, “BS ISO 18385:2016 Minimising the risk of human DNA contamination in products used to collect, store and analyse biological material for forensic purposes - Requirements”.

[119] International Organization for Standardization, “ISO 12653-1, Electronic imaging — Test target for the black-and-white scanning of office documents — Part 1: Characteristics”.

[120] International Organization for Standardization, “ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301”.

[121] British Standards Institution, “BS 10008:2014, Evidential weight and legal admissibility of electronic information. Specification”.

[122] International Organization for Standardization, “ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements”.

[123] Crown Prosecution Service, “Expert Evidence,” [Online]. Available: www.cps.gov.uk/legal-guidance/expert-evidence. [Accessed 27 10 2021].

[124] UKAS, “Guidance on the Application of ISO/IEC 17025:2017 Dealing with Expressions of Opinions and Interpretations,” LAB 13. [Online]. Available: https://www.ukas.com/wp-content/uploads/filebase/publications/publications-relating-to-laboratory-accreditation/LAB-13-Edition-3-April-2019.pdf.

40. Acronyms and Abbreviations

Text to be developed.

41. Glossary

Text to be developed

42. Correlation with Key Clauses in the Normative References [132]

		Code of Practice and Conduct: Issue 7	ISO 17025	ISO 15189	ILAC-G19	ISO 17020	UKAS-RG 201
27.2	Code of Conduct		-		3.4	-	6.1.10
12.2	Scope	3	1	1	1	1	1
12.3	Normative references	4	2	2	-	2	-
12.4	Terms and definitions	5	3	3	2	3	-
17	Management requirements	6	8	4, 4.1. 4.2	-	5.1, 5.2, A1	5, 6
18	Business continuity	7	-	-	-	-	-
19	Independence, impartiality and integrity	8	3.1, 4.1	4.1.1.3	2.12, 3.4, 4.8.1	4.1, 5.2.1	4.1, 6.1.10
20	Confidentiality	9	4.2	4.1.1.3, 5.1.5, 5.2.2	3.4	4.2	4.2
21	Document control	10	8.2 (option A)	4.3	3.1	8.3	8.3

[132] Cross references some of the key clauses that appear in the normative references, clauses in other documents may also be relevant (e.g. ILAC-P15) [16].

		Code of Practice and Conduct: Issue 7	ISO 17025	ISO 15189	ILAC-G19	ISO 17020	UKAS-RG 201
22	Review of requests, tenders and contracts	11	6.4, 6.5, 6.4.1, 6.6, 7.3.3, 7.6.2,7.7.1, 7.10	4.4, 4.7	3.2	7.5, 7.6	7.5, 7.6
23.1	Subcontracting	12	6.6	4.6	4.1.3	6.3	-
23.2	Packaging and general chemicals and materials	13	6.4, 6.5, 6.4.1, 6.6, 7.3.3, 7.6.2, 7.7, 7.10	5.3	3.12	6.1, 6.2, 7.1	6.2
24.2	Complaints	14	7.9	4.8	3.2	7.5, 7.6	7.5, 7.6
24.1	Control of non-conforming testing	15	7.1	4.9	3.9	8.7, 5.2	8.7
25	Control of records	16	6.6.2,7.1., 7.2.1.5, 7.2.2.4, 7.3.3, 7.4.2, 7.5, 7.8.1.2, 7.10.2, 8.4	4.13	3.5	7.1, 7.2, 7.3, 8.4	7.3, 8.4
25.3	Checking and review	16.3	7.8.1.1	4.14	4.7.5, 4.8.2	4.1, 7.3	15.3, 25
26	Internal audits	17	8.8 (option A), 8.9 (option A)	4.14	3.7	6.1, 8.6	8.6

		Code of Practice and Conduct: Issue 7	ISO 17025	ISO 15189	ILAC-G19	ISO 17020	UKAS-RG 201
	Technical requirements	18	6.1	5.5, 5.5.1	6.2	6.1	6.1
27	Competence	19	6.2	4.4, 5.1	3.3	6.1	6.1
28	Accommodation and environmental conditions	20	6.3, 7.8.3.1, 7.8.5	5.2	3.11, 4.2.3	6.2, 7.2, 7.3	6.3
29	Test methods and method validation	21	7.2	4.4, 5.4.2, 5.5	3.1	7.1	6.2.2, 7.1
30	Estimation of uncertainty	22	7.6	5.5.1.4, 5.5.2	3.10, 4.9	6.1.3, 7.1.2	
31	Control of data	23	6.4, 6.5, 6.4.1, 6.6, 7.3.3, 7.6.2,7.7.1, 7.10	4.13, 5.10, 5.10.1, 5.10.2, 5.10.3, Annex B	3.12	6.1, 6.2, 7.1	8.3, 8.3
33	Equipment	24	6.4, 6.5, 6.4.1, 6.6, 7.3.3, 7.6.2,7.7.1, 7.10	5.2.5, 5.3	3.12	6.1, 6.2, 7.1	6.2, 7.2
34	Measurement traceability - Intermediate checks	25	6.4.10, 7.7.1	5.3.1.4	4.3	6.2.9	6.2.9
35	Handling of test items	26	7.3, 7.4	5.25, 5.4.3, 5.4.4.3,	4.3.3	7.2	7.2

		Code of Practice and Conduct: Issue 7	ISO 17025	ISO 15189	ILAC-G19	ISO 17020	UKAS-RG 201
				5.4.5, 5.4.6, 5.4.7			
36	Assuring the quality of test results	27	7.7	5.6	4.7.7.2	7.1, 7.2	
37	Reporting the results	28	7.8	5.7, 5.8, 5.9	4.9	4.2, 6.1,7, 7.4	7.4

Part G – Appendices

G# – Standards of Conduct

43. Standards of Conduct

43.1.1 As a person performing an FSA you shall:

1. Recognise your overriding duty is to the court and to the administration of justice. [33]
2. Act with honesty, integrity, objectivity and impartiality.
3. Comply with the legal obligations imposed on practitioners (and specifically expert witnesses) in the jurisdiction(s) in which you practice. [33]
4. Declare, at the earliest opportunity, any personal, business, financial and/or other interest that could be perceived as a potential conflict of interest.
5. Act, and in particular provide expert advice and evidence, only within the limits of your professional competence.
6. Take all reasonable steps to maintain and develop your professional competence, taking account of material research and developments within the relevant field.
7. Inform those instructing you, in writing, of any information which may reasonably be considered to undermine your credibility as a practitioner or the reliability of the material you produce and include this information with/within any written report provided to those instructing you.
8. Establish the integrity and continuity of items as they come into your possession and ensure these are maintained whilst in your possession.

9. Seek access to exhibits/productions/information that may have a significant impact on the output from your work [133] and record both the request for material and the result of that request.

10. Conduct casework using methods of demonstrable validity and comply with the quality standards established by the Regulator, under the provisions of s2 2021 Act , applicable to the FSAs which are being carried out.

11. Be prepared to review any casework if any new information or developments are identified that would significantly impact on the output from your work. [134]

12. Ensure that the relevant instructing party is informed where you have good grounds for believing a situation may result in a miscarriage of justice, either by (a) invoking the appropriate organisational processes for addressing potential miscarriages of justice or (where you do not operate as part of an organisation or the organisation does not have appropriate procedures) (b) by informing the party directly.

13. Preserve confidentiality unless the law obliges, a court/tribunal orders, or a commissioning party explicitly authorises disclosure.

---

133 Particularly conclusions reported in any report or in testimony.

134 Particularly conclusions reported in any report or in testimony.

G# - Infrequently Commissioned Experts

44. Infrequently Commissioned Experts

44.1 Scope

44.1.1 It is recognised that experts from outside the forensic science profession will be called to give evidence, in relation to an FSA, from time to time. These shall be referred to as Infrequently Commissioned Experts (ICE). Where ICE provide advice/evidence in relation to an FSA which is subject to this Code it is impractical to require (a) compliance with all provisions of this Code or (b) compliance with the means of demonstrating compliance (e.g. accreditation).

44.1.2 An individual shall only fall within the definition of an ICE if the following conditions are met in relation to both the practitioner and the evidence provided.

44.1.3 The practitioner, subject to the provisions of section 44.1.4 herein, shall:

a. Not be a member of staff of a forensic unit providing services to the CJS in England and Wales;

b. Not represent themselves as a forensic scientist operating within the CJS in England and Wales; and

c. Not have been involved in any case in an advisory or expert capacity in the CJS in England and Wales in the previous 12 months.

44.1.4 The provision with regard to the frequency of involvement in the CJS in England and Wales do not apply to a practitioner who has provided evidence to a different justice system (e.g. the Family Justice System) and that evidence is subsequently relied on in the CJS.

44.1.5 The evidence provided by an ICE shall not be of a type which can routinely be obtained from a forensic unit.

44.2 Requirements

44.2.1 ICE shall comply with the following requirements.

a. The general obligations of expert witnesses [33] including the requirements of the Criminal Justice System as contained in the Criminal Procedure Rules [82] (and Criminal Practice Directions V, in particular 19A.5 and 19B [25]);

b. The requirements for contents of reports [135], including but not limited to, those prescribed in the Criminal Procedure Rules 19.4 [34] and Criminal Practice Directions V 19B [25];

c. Retention, recording, revelation and prosecution disclosure obligations;

d. The requirements pertaining to the use of reference collections and databases should they rely on them;

e. The requirement to use validated methods or procedures based on sound scientific principles and methodology;

f. The need to demonstrate competence in using these methods or procedures, and evaluating the results obtained objectively and impartially, and according to established scientific and statistical methodology; and

g. The need to consider the impact that confirmation/cognitive bias can have at different stages and consider the use of avoidance strategies.

h. The declaration required in the Criminal Practice Directions V 19B [25] and the Regulator’s requirement for the positive declaration to be in the following terms: [136]

> “I confirm that, to the best of my knowledge and belief, I have acted in accordance with the Standards of Conduct published by the Forensic Science Regulator [insert issue] as it pertains to experts from other professions. Annex [x] details the steps taken to comply with the specific requirements set for experts from other professions.”

---

135 A statement is one form of a report. It is formatted to comply with the provisions of s9 Criminal Justice Act 1967 [102].

136 Experts will need to produce a different declaration if there are other non-compliances, whether inability to comply with specific clauses in the Standards of Conduct, or that accreditation is required.

G#- FSA Definitions – General Provisions

45. General

45.1.1 To avoid considerable repetition in the definitions of FSA, in the FSA specific appendices below, this section addresses conditions which apply generally and provisions which apply generally.

46. General Requirements

46.1 Purpose

46.1.1 The definitions of FSA will only apply to the extent that the activity is undertaken for a purpose specified in s11(2) of the 2021 Act [10]. To achieve this requirement the following general requirements will apply to all FSA definitions.

46.2 Commissioning – Detection and/or Investigation of Crime

46.2.1 To fall within the purpose in s11(2)(a) 2021 Act [10] the following conditions apply.

46.2.2 The activity must have been commissioned by, or undertaken by (or on behalf of), one of the following persons/bodies with the aim that the output should be used for the detection and/or investigation of crime.

a. A law enforcement agency.

b. A prosecuting authority.

c. A suspect, accused or convicted person (in relation to the offence for which they are suspected, accused or convicted) where the relevant criminal investigation and/or prosecution was by a body listed in the sub-clauses above.

d. A legal representative of a person within the description in section c above.

e. A body with legal authority to investigate potential miscarriages of justice.

46.2.3 The detection and/or investigation of crime means.

a. Establishing whether a crime has occurred, has been attempted or is planned.

b. Establishing whether information related to the investigation of crime is accurate and eliminating the innocent from criminal investigations.

c. Establishing by whom, for what purpose, by what means and generally in what circumstances any crime was, or may have been, committed.

d. Obtaining and recording such information as may be needed in the criminal investigation and prosecution of any offence.

e. The apprehension of the person by whom any crime was committed.

46.2.4 Law enforcement agency means any of the following bodies.

a. The forty three territorial police forces in England and Wales.

b. The limited territorial forces listed below.

i. Kew Constabulary.

ii. Mersey Tunnels Police.

iii. Port of Bristol Police.

iv. Port of Dover Police.

v. Port of Felixstowe Police.

vi. Port of Liverpool Police.

vii. Port of Tilbury Police.

viii. Tees and Hartlepool Harbour Police.

c. The non-territorial police forces listed below (in relation to their work in England and Wales).

i. British Transport Police.

ii. Civil Nuclear Constabulary.

iii. Ministry of Defence Police.

d. The military law enforcement bodies set out below (in relation to their work in England and Wales).

i. Royal Air Force Police.

ii. Royal Marines Police.

iii. Royal Military Police.

iv. Royal Naval Police.

e. The National Crime Agency (in relation to its work in England and Wales).

f. The Serious Fraud Office.

g. HM Revenue and Customs (in relation to its work in England and Wales).

h. The Home Office (in relation to its work in England and Wales).

i. The Independent Office for Police Conduct.

j. The security and intelligence agencies listed below when involved in the investigation of crime (in relation to their work in England and Wales).

i. The Government Communications Headquarters.

ii. The Secret Intelligence Service.

iii. The Security Service.

46.2.5 A prosecuting authority means:

a. HM Attorney General;

b. The Director of Public Prosecutions;

c. The Crown Prosecution Service; and

d. The Serious Fraud Office.

46.3 Commissioning - Preparation, Analysis or Presentation of Evidence

46.3.1 To fall within the purpose in s11(2)(b) 2021 Act [10] the following conditions apply.

46.3.2 The activity must have been commissioned by one of the following persons/bodies with the aim that the output should be used for the with the intention that the output is used in criminal proceedings.

a. A law enforcement agency.

b. A prosecuting authority.

c. A suspect, accused or convicted person (in relation to the offence for which they are suspected, accused or convicted) where the relevant criminal investigation and/or prosecution was by a body listed in the sub-clauses above.

d. A legal representative of a person within the description in section c above.

e. A body with legal authority to investigate potential miscarriages of justice.

46.3.3 The term criminal proceedings means, subject to sections 46.3.4 and 46.3.5, any proceeding covered by the following provisions.

a. Section 51 of the Criminal Justice Act 2003.

b. Section 14 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012.

46.3.4 The following proceedings shall not be considered ‘criminal proceedings’ for the purpose of this Code.

a. Proceedings for dealing with an individual under the Extradition Act 2003.

b. Proceedings for binding an individual over to keep the peace or to be of good behaviour under section 115 of the Magistrates' Courts Act 1980 and for dealing with an individual who fails to comply with an order under that section.

c. Proceedings for contempt committed, or alleged to have been committed, by an individual in the face of a court.

d. Proceedings before the Judicial Committee of the Privy Council.

46.3.5 The term ‘criminal proceedings’ shall not cover any activities related to the imposition or management of a sentence imposed on a convicted person.

46.3.6 Where any activity is commissioned for purposes other than those described in s11 2021 Act (and therefore falling within he provisions set out above) generates material which is subsequently of relevance to the CJS the initial work is not an FSA. Any work (e.g. any additional work, the production of

reports or the presentation of evidence) commissioned for CJS use will be an FSA if it falls within the definitions in this Code.

46.4 Modification of Limits

46.4.1 The requirements stated above limit the scope of FSA to a subset of what the 2021 Act [10] states are FSA. The Regulator has determined that at the point of introduction of this Code this is appropriate but future versions of the Code may revise the requirements above and, as a consequence, extend the scope of the FSA.

47. Contingency Capacity/Facility

47.1.1 This section applies where a forensic unit establishes a facility, or capability, which is

a. Only to be used in the event of a potential future event;

b. Not performing any casework which would amount to an FSA; and

c. The work which would be undertaken, if the capacity/facility was brought into use, would amount to an FSA.

47.1.2 In these cases, the preparation and maintenance of the capacity/facility will itself be considered to be carrying on the FSA relevant to the work to be undertaken in the facility/capacity.

48. General Provisions

48.1 General Activities

48.1.1 In all FSA definitions below, the following activities shall be assumed to be part of the definition unless the contrary is clearly stated in the definition.

a. The following aspects of the handling and continuity monitoring of any item or material relevant to the activities listed in the section.

i. The packaging.

ii. The labelling.

iii. The transportation (covering all transportation from the point the item is seized until it is returned to the owner or disposed of).

iv. The storage.

v. The security and continuity.

vi. The destruction.

b. The provisions set out in clause (a) shall also apply to any item, material or information taken from, created from or derived from any item or material relevant to the criminal investigation.

c. The provision of any advice, to a person or body listed in section 6.5.2a, related to the use, potential use or the potential benefits of the activities set out in the definition to the criminal investigation of a specific matter.

d. In relation to the activities set out in the definition any of the following aspects of assessment, interpretation and/or reporting.

i. The case assessment process (see FSR-C-118).

ii. The determination of the examination strategy (see FSR-C-118).

iii. The interpretation of the findings to assess/determine the significance to the criminal investigation (see FSR-C-118).

iv. The reporting of the results of any activities and any assessment of interpretation to the commissioning party of the Criminal Justice System.

v. The provision of evidence (whether evidence of fact or opinion) in relation to the activities (whether the activities were undertaken by or on behalf of the person providing the evidence).

vi. The provision of expert evidence as to the significance of the findings produced by the activities in the context of the case.

vii. The provision of any expert advice or evidence in relation to any activities listed in sections i to vi above.

48.2 Supporting Activities

48.2.1 It must be recognised that all work necessary to provide, or support the provision of, the FSA listed in each definition form part of that FSA and are subject to the applicable standards.

48.2.2 The activities which are necessary for, or support the provision of, the FSA covered in the definition include, but are not limited to, the following.

a. Ensuring all work is undertaken in a suitable environment.

   i. That the accommodation is constructed and maintained in an appropriate way.

   ii. That cleanliness is maintained at a level suitable for the work undertaken.

   iii. That appropriate anti-contamination processes are employed.

   iv. That, where relevant, suitable environmental monitoring is undertaken.

   v. The appropriate security is maintained.

b. Ensuring all equipment employed is fit for purpose.

   i. That suitable equipment is procured.

   ii. That all equipment is subject to appropriate maintenance at pre-determined intervals.

   iii. That all equipment is suitably calibrated.

c. That appropriate provisions are in place in relation to the following.

   i. The physical security of the accommodation.

   ii. The security of all IT systems.

   iii. The security of information.

   iv. The integrity and security clearance of personnel.

d. Ensuring that all methods employed have been appropriately validated for use.

e. Ensuring all persons undertaking work are competent.

   i. That all persons undertaking work have sufficient training, qualifications and experience and have satisfactorily demonstrated that they are able to carry out the work proficiently.

ii. That the ability of all persons to carry out the work to the relevant standards (i.e. proficiently) is maintained and regularly assessed.

f. Ensuring all reagents and consumables are fit for the purpose for which they are being used.

g. That all collections of information or material (e.g. reference databases) used to assist in the examination, analysis of items or the assessment/interpretation of results are fit for purpose.

49. General Exclusions

49.1 Knowledge

49.1.1 The forensic unit commissioned to perform the activity must, at the time the work is commissioned, be aware that the output was to be used for a purpose in s11 of the 2021 Act [10].

49.2 Use of Animals

49.2.1 Any method which is based on the use of non-human animals (e.g. dogs) shall not be considered to form any part of an FSA.

49.3 Type Approval

49.3.1 Where any statute provides the Secretary of State the power to approve any item, or method, for use in circumstances which might fall within the scope of s11 2021 Act. [10] The following shall not be part of any FSA.

a. The process by which the Secretary of State determines whether to grant approval;

b. The process by which the Secretary of State determines whether to continue, suspend or withdraw an existing approval; or

c. Any work undertaken by, on behalf of or commissioned by the Secretary of State to assist in the process of granting, suspending, continuing or withdrawing an approval.

Published by:

The Forensic Science Regulator
c/o Home Office Science
Long Corridor
14th Floor
Lunar House
40 Wellesley Road
Croydon
CR9 2BY

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