Forensic Science Regulator

Overseeing Quality

Codes of Practice and Conduct

For Forensic Science Providers and Practitioners in the Criminal Justice System

FSR-C-100

Issue 7

(Issued as a correction to Issue 6)

Foreword

These Codes detail standards and norms of practice and should be adhered to by all forensic science practitioners, irrespective of the sector in which they are employed and whether their work has been commissioned by prosecution or defence. Some have equated the current lack of statutory enforcement powers for the Regulator with an assumption that compliance is voluntary. That is not the case and any non-compliance with the Code of Conduct must be declared in statements.

This is the final version of the Codes that I will issue as Regulator. There are several reasons why this update is required, in particular:

1. To include provisions in relation to data security, which were recommended by the National Cybersecurity Centre and were published in Regulatory Notice 02/2020.
2. To respond to the increasing impacts of the COVID-19 pandemic on the timescales for achieving compliance with the required quality standards.

It is important that the time extensions set out in the Statement of Standards and Accreditation Requirements are used wisely, to improve the implementation of quality systems and the readiness for assessment. This will ensure that when they restart, as many initial assessments as possible are successful without the need for further visits.

Each organisation should seek to implement the quality standards in a way that actively helps to promote improvement in practice; every practitioner and every leader has a role to play in bringing about improvement. As ever, I urge you all to adapt and improve your quality management system over time, to increase its effectiveness and efficiency. In general, accreditation is the mechanism by which compliance with the requirements needs to be demonstrated, but it is not an end in itself: quality improvement is always the goal.

Dr Gillian Tully CBE
The Forensic Science Regulator

Postscript: Issue 7 is published as a correction to Issue 6; issue 6 omitted subsection 23.4 in error and that is now restored on page 74.

Preface - Statement of Standards and Accreditation Requirements: For All Forensic Units Providing Forensic Science Services

The Forensic Science Regulator expects the following activities wherever performed to be conducted to the standards set out in these Codes [1], irrespective of whether the provider is public, police or commercial. Table 1 specifies standards and any independent assurance mechanisms required to ensure that the standards have been met. Unless otherwise stated, the standard commencement dates for regulation of 6 April and 1 October apply.

Table 1: Standards/requirements for forensic science activity [2]

	Accreditation to ISO 17020/ 17025/15189	Accreditation schedule to include the Codes	Appendix/ Guidance	Notes
Incident scene examination [3] (ISO 17020) [4]	October 2022 [1]	October 2022	UKAS RG201 [2]	Covers all aspects of incident scene investigations including but not limited to assessment, search, identification, recovery and recording (e.g. photography). See also digital forensics.
Forensic collision investigations (ISO 17020)	October 2022	October 2022	UKAS RG201	The scope is road traffic collisions; accreditation is required to cover all aspects of an entity's forensic science activity e.g. scene recording, speed estimation,

1 Except where alternative codes of practice are specified in Table 1.

2 Appendices to these Codes are available from: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct [Accessed 17/11/2020]

3 Where specialists such as crime scene investigators (however named) are deployed.

4 If the activity is limited to testing at scene, the accreditation body may deem ISO 17025 to be more applicable and may be substituted for ISO 17020.

	Accreditation to ISO 17020/ 17025/15189	Accreditation schedule to include the Codes	Appendix/ Guidance	Notes
				vehicle system analysis. Any legal entity conducting collision investigation must gain accreditation by October 2022 for at least the lead region, with the remaining regions/sites becoming accredited by October 2023.
Fire scene examination (ISO 17020)	October 2023	October 2023	UKAS RG201	Including recovery, and inspection, of items from fire scenes. Excludes accelerant analysis, to which ISO 17025 applies. The following interim requirements apply. Interim requirement 1: By October 2021 the Quality Management System shall be established, the Quality Manual drafted, and quality personnel appointed. A skills, training and competency requirements framework shall be set, and standard operating procedures developed. Interim requirement 2: By April 2022 the validation/verification of methods and processes shall be complete, and staff competency evidenced against final procedures.
Visual screening, examination, recovery, or sampling for biological material away from a scene [5] (ISO 17025)	October 2013	October 2017	-	Screening of items to the standards expected in the Criminal Justice System includes competence in low power microscopy and a presumptive blood test.

[5] These Codes do not set out the application of The Accreditation of Forensic Service Providers Regulations 2018, or their effect on admissibility.

	Accreditation to ISO 17020/ 17025/15189	Accreditation schedule to include the Codes	Appendix/ Guidance	Notes
Processing recovered biological samples/material to obtain a DNA profile away from a scene [5] (ISO 17025)	April 2012	October 2017	FSR-C-108 [3]	
Enhancement, development, imaging, recording and/or recovery of visible/latent finger marks [5] (ISO 17025)	October 2015	October 2017	FSR-C-127 [4]	
Fingerprint comparison [5] [6] (ISO 17025)	October 2018	October 2018	FSR-C-128 [5]	
Digital forensics	For fixed site activities, ISO 17025 applies from October 2017. For scene activities, ISO 17020 applies from October 2022.	See definition and sub categories for details.	As applicable UKAS RG201 FSR-C-107 [6] FSR-C-119 [7] FSR-C-134 [8] FSR-C-135 [9]	Digital forensics is the process by which information is extracted from any digital system or data storage media, rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings. The scope below includes aspects such as remote storage and systems associated with computing, imaging, image comparison, video processing and enhancement (including CCTV), audio analysis, satellite navigation, communications. The definition is intentionally wide, and any exclusions will be explicit. The following should be conducted by competent staff using methods approved by the organisation, but are excluded from the ISO 17025 digital forensics.

[6] Fingerprints includes marks and palm comparison conducted away from the scene.

	Accreditation to ISO 17020/ 17025/15189	Accreditation schedule to include the Codes	Appendix/ Guidance	Notes
				accreditation requirement: automatic number plate recognition, manual classification of indecent images of children, eFit, recovery from a working CCTV system in situ, recovery of footage from body worn video and production of clips to support an officer's statement, CCTV replay for viewing with no further analysis (acknowledging that there may be quality limitations to the material viewed). Extraction of data from cameras used at incident scenes is not included in this scope; when performed, it is part of incident scene recording.
Digital forensics - Incident scene activity (ISO 17020) [7]	October 2022	October 2022	UKAS RG201 FSR-C-107	Screening, capture and preservation or analysis of data from a device conducted at scene (including but not limited to routers).
Digital forensics - Capture and preservation from digital media (ISO 17025)	October 2017	October 2017	FSR-C-107 As applicable FSR-C-119 FSR-C-134	The process of creating a copy of the digital data in whole or in part from digital storage media and storing the copy in a manner that allows subsequent processing and analysis to take place in accordance with the relevant validated method being applied. This may be logical or physical.
Digital forensics - Processing of data from digital media (ISO 17025)	October 2017	October 2017	FSR-C-107 As applicable FSR-C-119 FSR-C-134	The process of converting (e.g. extraction, organising of data) digital data to produce meaningful information either by a manual or automated process to allow subsequent analysis to take place.

[7] If the activity is limited to testing at scene, the accreditation body may deem ISO 17025 to be more applicable and may be substituted for ISO 17020.

	Accreditation to ISO 17020/ 17025/15189	Accreditation schedule to include the Codes	Appendix/ Guidance	Notes
Digital forensics - Analysis of data from digital media (ISO 17025)	October 2017	October 2017	FSR-C-107 As applicable FSR-C-119 FSR-C-134	The process of targeting and/or evaluating digital data via application of a predefined forensic strategy (either on a case by case basis or in a service level agreement). a. Narrowing/filtering (i.e. findings from validated digital forensics methods) and comparing them with other types of data e.g. communications data to support reasonable lines of enquiry. b. Using forensic analysis and technical explanation of the data (using validated digital forensic methods) to deliver a defined forensic strategy. c. Expert interpretation of digital forensic findings, including but not limited to comparisons and evaluation of the findings as they relate to hypotheses or propositions. Methods shall be validated.
Digital forensics - Screening or recovery of data from a device using an off the shelf tool for factual reporting (ISO 17025)	October 2017	October 2017	-	The use of tools and methods by frontline non-practitioners is permitted but the organisation needs to hold accreditation for at least one deployment. Further deployments of the method under central control may be permitted outside the scope of accreditation provided that the method chosen can be demonstrated to have adequate configuration control (e.g. locked down data recovery methods and control) and that staff are competent. Fully mobile deployments with no fixed site are considered to be incident scene deployments and so the deadline has been deferred from October 2020. [7]

	Accreditation to ISO 17020/ 17025/15189	Accreditation schedule to include the Codes	Appendix/ Guidance	Notes
				Configuration control and records that the staff are competent are still required in the intervening period.
Digital forensics - Network capture and/or analysis	-	-	FSR-C-107	The Codes and requirements in FSR-C-107 apply, however the formal accreditation date is still to be determined.
Digital forensics - Internet intelligence and investigation (inc. open source intelligence from the internet)	-	-	-	The Codes apply, however the compliance mechanism is still to be determined. It should be performed by competent staff, using valid methods, working to a written forensic/investigative strategy, and actions taken recorded in sufficient detail that a similarly competent practitioner can understand how information captured was derived.
Digital forensics - Cell site analysis and communications data	-	-	FSR-C-135	The Codes and requirements in appendix Cell Site Analysis FSR-C-135 apply, however the formal accreditation date is still to be determined.
Toxicology (ISO 17025)	October 2017	October 2017	FSR-C-133 for s5a of the Road Traffic Act 1988 [10]	Presumptive toxicology testing (using Home Office type approved equipment) is permissible outside of the ISO 17025 standards framework. For evidential purposes, all compounds for which the laboratory routinely tests as part of a toxicology service shall be within its scope of accreditation (either by being named in the scope or as a result of flexible scope [11]) and new compounds, as they become more common, will be brought within the scope in a timely fashion. The laboratory must have a procedure setting out how it analyses compounds that are new or rarely tested for and are not in scope of accreditation, covering how the laboratory assures the quality of such analyses. Analysis in relation to section

	Accreditation to ISO 17020/ 17025/15189	Accreditation schedule to include the Codes	Appendix/ Guidance	Notes
				5a of Road Traffic Act 1988 is subject to specific requirements set out in FSR-C-133. Provided the accreditation takes into account ILAC-G19:08/2014 Modules in a Forensic Science Process and therefore has Forensic Testing/Analysis clearly indicated in the scope of accreditation, ISO 15189 is a suitable alternative to ISO 17025. Due regard should be given to the laboratory guidance issued by the UK and Ireland Association of Forensic Toxicologists. [12]
Firearms triage	-	-	-	Triage is permitted to be performed by competent individuals outside the scope of accreditation, where it is to decide whether further action is warranted, such as an examination by an accredited provider. Preliminary classifications are only permitted without accreditation to enable a charge or remand decision to be made only where such a decision cannot, for reasons of operational risk, be deferred until a report has been provided by an accredited organisation. In such instances the following apply. [13] a. The remand statement must be clearly caveated that it contains findings only. b. The prosecutor shall ensure that there has been a proper completion of Form MGFSP for submission identifying the forensic issues that need to be addressed, the classification of the weapon and the timescale required.

	Accreditation to ISO 17020/ 17025/15189	Accreditation schedule to include the Codes	Appendix/ Guidance	Notes
				c. A report shall be obtained from an accredited provider within the specified timescale.
Firearms classification, firing marks, ballistics etc. (ISO 17025)	April 2012	October 2017	-	Accreditation is required for examinations intended to result in a statement/report to be used in evidence for all firearms classification.
Firearm Discharge Residue (ISO 17025)	April 2012	October 2017	-	
Drug analysis to evidential standards (ISO 17025)	April 2012	October 2017	-	Presumptive drug testing (for example under Evidential Drug Identification Testing (EDIT) guidance or HOC 15/2012 [14]) is currently permissible outside of the ISO 17025 standards framework. For evidential purposes, all drugs for which the forensic unit routinely tests (in relation to the Misuse of Drugs Act 1971 and/or Psychoactive Substances Act 2016) shall be within its scope of accreditation (either by being named in the scope or as a result of flexible scope) and new drugs, as they become more common, shall be brought within the scope in a timely fashion. The forensic unit shall have a procedure setting out how it analyses drugs that are new or rarely tested for and are not in scope of accreditation, covering how the laboratory assures the quality of such analyses.
Blood pattern analysis (ISO 17025)	April 2012	October 2017	FSR-C-102 [15]	
Toolmark impression comparison (ISO 17025)	April 2012	October 2017	-	

	Accreditation to ISO 17020/ 17025/15189	Accreditation schedule to include the Codes	Appendix/ Guidance	Notes
Bare or socked footprints and wear features of footwear	A separate code of practice(s) is being considered.	-	-	
Archaeology	-	-	-	A separate standard and guidance applies from December 2014. [16]
Forensic gait analysis	-	-		A separate code of practice applies, applies from December 2019. [17]
Evidence recovery during the forensic medical examination of complainants of alleged sexual assault e.g. at Sexual Assault Referral Centres (ISO 15189 with forensic analysis on the schedule).	October 2023	October 2023	FSR-C-116 [18]	Accreditation of the activity is required by October 2023; there are interim requirements detailed in FSR-C-116, reproduced below. Interim requirement 1: By October 2020 the Quality Management System shall be created, a Quality Manual drafted, and quality personnel appointed/identified. Interim requirement 2: By October 2021, the job roles, skill and training and competency requirements framework and procedures shall be developed. Interim requirement 3: By April 2022, the validation/verification of methods and processes and staff competency evidenced against final procedures shall be complete. Interim requirement 4: By April 2022, internal audit, improvement implementation and management review shall be in place and initial assessment shall be scheduled.

	Accreditation to ISO 17020/ 17025/15189	Accreditation schedule to include the Codes	Appendix/ Guidance	Notes
Footwear impressions - Screening and/or coding for the purpose of making a decision on whether or not to submit for further comparison	-	-	-	Conducted by competent staff using validated methods approved by the organisation, but accreditation to ISO 17025 is optional.
Footwear impressions - Screening [8] for the purpose of producing an intelligence report	-	-	-	Conducted by competent staff using validated methods approved by the organisation, but accreditation to ISO 17025 is optional unless the report is intended to support a charge. If reports are intended to support a charge the unit shall be either accredited to ISO 17025 by October 2017, or the output must be verified through an accredited forensic unit prior to being used to support a charge, or the item shall be submitted for accredited footwear impression comparison.
Footwear impressions Comparison to evidential standards (ISO 17025)	April 2012	Oct 2017	-	
Anthropology	-	-	-	A separate code of practice applies, applicable from April 2018. [19]
Forensic Casework Review	-	-	-	Casework review that involves no testing or scene examination (which are covered by other categories) is under consideration.

[8] Whether through coding, auto coding or manual comparison.

	Accreditation to ISO 17020/ 17025/15189	Accreditation schedule to include the Codes	Appendix/ Guidance	Notes
Forensic Pathology	-	-	-	A separate code of practice and performance standards applies. [20]
National DNA Database ®	-	-	-	ISO 9001 [21] TickITplus [22] ISO 17043 [23]
Experts from other professions called to give evidence	-	-	-	This may include experts from overseas or from other fields, called infrequently to provide evidence in the Criminal Justice System, who should be directed by those instructing them to adhere to section 3. Scope for general requirements and section 3.1.6 in particular.
Laboratory activity including, but not limited to, handling, developing, analysing and/or interpreting scientific evidence not listed separately in this table. (ISO 17025)	October 2013	October 2017	-	

Contents

Code of Conduct for Forensic Science Practitioners

The Forensic Science Regulator (the Regulator) sets out for all practitioners, whether instructed by the prosecution or defence, the values and ideals the profession stands for. [9] This Code of Conduct provides a clear statement to customers and the public of what they have a right to expect.

As a practitioner you shall:

1. Recognise your overriding duty is to the court and to the administration of justice.
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.
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 [10] and record both the request for material and the result of that request.

---

9 Developed from work by the Council for the Registration of Forensic Practitioners.

10 Particularly conclusions reported in any report or in testimony.

10. Conduct casework using methods of demonstrable validity and comply with the quality standards set by the Regulator [11] relevant to the area in which you work.

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. [9]

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 customer explicitly authorises disclosure.

[11] As set out in the Statement of Standards and Accreditation within the Forensic Science Regulator's Codes of Practice and Conduct.

Code of Practice for Forensic Units Providing Forensic Science Services

1. Introduction

1.1.1 The Code of Practice is aimed at all those providing forensic science services to the Criminal Justice System (CJS), whether individual practitioners, academics, public or private sector forensic science providers, and refers to all as forensic units in line with the terminology used in ILAC-G19:08/2014. These can be small teams in larger organisations, sole practitioners or large providers and can be instructed by the prosecution or the defence.

1.1.2 The Code of Practice is not intended to be a substitute for the complete version of the international standards (e.g. BS EN ISO/IEC 17025:2017 and BS EN ISO/IEC 17020:2012 [12]). Section 32 of this Code of Practice cross references to some of the key clauses that appear in the normative references and other clauses may also be relevant. Forensic units applying for accreditation to one of the international standards remain responsible for ensuring they are aware of all relevant requirements.

1.1.3 The Code of Practice specifies the requirements for a management system for forensic units providing forensic science services to demonstrate their ability to deliver products and services that consistently meet the requirements of their customers in the CJS.

1.1.4 The United Kingdom Accreditation Service (UKAS ®) [13] will assess forensic units providing forensic science services against ISO 17025 [14] utilising any of the relevant UKAS laboratory publications [24], ILAC-G19 and the supplementary requirements of this Code of Practice, and will include

---

12 Standards will be referred to in full the first time they appear in the body of this document and then, with the exception of the 4. Normative References section, in a shortened form (e.g. ISO 17025, ISO 17020) from that point onwards unless specific cross references to clauses in that year's version are made.

13 UKAS is a registered trademark of the United Kingdom Accreditation Service which is the national accreditation body for the United Kingdom.

14 Where accreditation is the requirement in the Statement of Standards and Accreditation Requirements.

compliance with this Code of Practice in the Schedule of Accreditation. [15] UKAS can assess forensic units providing forensic science services at scenes of incidents [16] against ISO 17020, ILAC-G19, ILAC-P15:07/2016, this Code of Practice, and the inspection recommendation and guidance publication UKAS-RG 201:2015.

1.1.5 Forensic units required to be assessed by an accreditation body as detailed in the preface to this document the Statement of Standards and Accreditation Requirements, shall sign a confidentiality disclosure waiver to allow the accreditation body (e.g. UKAS) to disclose significant quality-related issues to the Regulator.

1.1.6 The word 'shall' has been used in this document where the clause is a requirement; the word 'should' has been used to indicate the clause is a recommendation based on generally accepted practice in the forensic science profession.

1.1.7 Appendices [17] complementary to the Code are included in the index of this document and when they come into effect are to be read as part of the Code, expanding and interpreting it, where necessary, for specific activities, processes or evidence types. In between issues of the Code, Regulatory Notices may be issued and may either signal the intention to add provisions to the Code or include clarifications intended for the next issue.

1.1.8 Although not part of the Code, the Regulator may issue Lessons Learnt documents which should be considered, for instance, when reviewing the operation of quality assurance measures.

---

15 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.

16 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.

17 Appendices to these Codes (included in the index) are available from: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct [Accessed 25/02/2021].

1.1.9 The Code of Practice also incorporates, where applicable, any specific requirements determined by the CJS in England and Wales. [18]

1.1.10 Compliance with this Code of Practice is intended to provide the CJS and the public with confidence in the reliability of forensic science and to enhance customer satisfaction through the effective application of the management system.

1.1.11 Accreditation to BS EN ISO 15189 is a suitable alternative to ISO 17025 for the provision of certain medical laboratory services, provided that Forensic Testing/Analysis is clearly indicated in the scope of accreditation; this means that the laboratory has been assessed in accordance with ISO15189 taking into account ILAC-G19.

1.1.12 Other standards used for certification of organisations that provide scientific services – e.g. Good Laboratory Practice (GLP) [25] regulations and Good Manufacturing Practice (GMP) [26] are not alternatives to ISO 17025, although they do overlap to some extent and provide compatible guidance on good practice.

1.1.13 The Code and any subsequent appendices will be updated to reflect relevant changes in the requirements of ISO 17025, ISO 17020, ISO 15189, ILAC-G19, ILAC-P15 and the CJS. The updated version will be made available to all interested parties.

1.1.14 All practitioners shall comply with the principles contained in the Code of Conduct at the beginning of this document and shall declare this compliance (or otherwise) as set out in section 28.2.

1.1.15 The Code of Conduct, the Code of Practice and Statement of Standards and Accreditation Requirements for all forensic units providing forensic science services are referred to collectively from this point forward as the Codes.

---

[18] The Codes can be extended or adopted by other jurisdictions with approval of the appropriate Ministers, governing bodies and prosecuting authorities.

2. Modification

2.1.1 This is the seventh issue of the Codes; it is issued to reinstate section 23.4 omitted in error from issue six. It is effective from 22nd March 2021 and replaces all previously issued versions. [19]

2.1.2 Significant changes from the last issue are highlighted in grey, significant deletions are marked as "[deleted text]". Where sections are inserted, moved or renumbered, the subsequent renumbering of sections that follow is not generally marked. [20]

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

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

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

2.1.6 This document is subject to review at regular intervals. If you have any comments please send them to the address or email set out at: www.gov.uk/government/organisations/forensic-science-regulator.

---

19 Organisations are expected to phase in changes into their quality management systems within 3 months of publication.

20 Due to the regulations for accessibility for web publishing, significant changes are also listed here and include: 2.1.1, 23.4 (whole section – reinstated from Issue 5)
Footnotes are marked up as changed: 20, 95.

3. Scope

3.1.1 The Codes are for all forensic units supplying forensic science services to the CJS. Forensic science is taken to include the sciences performed by the police service, the fire and rescue services, the public and private sector forensic units and, to a lesser extent, academia. They are intended to be able to cover sciences with scene and/or laboratory-based elements and are not intended for disciplines such as forensic accountancy or psychiatry. The Codes have been extended to cover forensic medicine in so far as it applies to the examination of complainants of alleged sexual assault, by issuance of an appendix. [21] The Codes currently cover forensic units that include the:

a. Initial examination of complainants or forensic science activity at the incident scene;

b. Strategy for the examination of complainants, suspects or incident scenes;

c. Recovery, preservation, transport and storage of exhibits;

d. Screening tests for use in the field;

e. Assessment, selection, examination, sampling, testing and/or analysis of exhibits;

f. Testing activities using laboratory-based methods;

g. Recording of actions taken;

h. Assessment/review of examination and test results;

i. Reporting and presentation of results; and

j. Interpretations and opinions. [22]

3.1.2 The Codes initially specify the general requirements for competence for laboratory activities including sampling, laboratory examinations and tests and

---

21 The Codes and associated appendices may be used to provide guidance on certain suspect and victim sampling activities, however, when issued, the Forensic Medical Examination Standard FSR-C-116, will set the standards required for the forensic medical examination of complainants of alleged sexual assault.

22 Where this is to be included in a provider's schedule of accreditation, they will need to ensure that they are in compliance with the UKAS publication LAB 13. [94]

the provision of expert testimony. Where relevant, appropriate legal, regulatory and information security is included.

3.1.3 All forensic units [23] offering forensic science services to the CJS are bound by these Codes. The method of demonstrating compliance with the Codes for most of the scientific disciplines, with only a few explicit exceptions [24], is through accreditation to ISO 17025, ISO 17020 or ISO 15189.

3.1.4 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 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 21.2.45 and/or discuss options with the accreditation body. [25]

3.1.5 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, [26] this should be made clear to the instructing party and the fact that accreditation should apply and was not held should be declared in any statements or reports. Section 28.2 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 [27] to the statement or report is also produced which details how the risk is mitigated.

---

23 See glossary definition, this includes all providers of forensic science services to the CJS including sole practitioners, whether instructed by the prosecution or defence.

24 Exceptions are included in the Statement of Standards and Accreditation Requirements.

25 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.

26 See also The Accreditation of Forensic Service Providers Regulations 2018, The Accreditation of Forensic Service Providers (Amendment) Regulations 2019 and European Union (Future Relationship) Act 2020.

27 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. [74]

3.1.6 It is also recognised that experts from other professions will be called to give evidence from time to time. The customer shall ensure that such experts are bound by the Code of Conduct and should make them aware of:

a. The general obligations of expert witnesses including the requirements of the Criminal Justice System as contained in the Criminal Procedure Rules [27] (and Criminal Practice Directions V, in particular 19A.5 and 19B);

b. The requirements for contents of reports [28], including but not limited to, those prescribed in the Criminal Procedure Rules 19.4 and Criminal Practice Directions V 19B;

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 and the Regulator's requirement for the positive declaration to be in the following terms: [29]

> "I confirm that, to the best of my knowledge and belief, I have acted in accordance with the Code of Conduct published by the Forensic Science Regulator [insert issue] as it pertains to experts from other

---

28 A statement is one form of a report. It is formatted to comply with the provisions of s9 Criminal Justice Act 1967.

29 Experts will need to produce a different declaration if there are other non-compliances, whether inability to comply with specific clauses in the Codes of Conduct, or that accreditation is required.

professions. Annex [x] details the steps taken to comply with the specific requirements set for experts from other professions."

4. Normative References

4.1.1 The following normative references are included in section 29. References:

a. BS EN ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories; [28]

b. ILAC-G19:08/2014, Modules in a Forensic Science Process; [29]

c. BS EN ISO/IEC 17020:2012, General criteria for the operation of various types of bodies performing inspection; [30]

d. ILAC-P15:07/2016, Application of ISO/IEC 17020:2012 for the Accreditation of Inspection Bodies; [31]

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

f. BS EN ISO 15189:2012, Medical laboratories. Requirements for quality and competence; [32] and

g. BS EN ISO/IEC 17000:2004, Conformity assessment. Vocabulary and general principles. [33]

5. Terms and Definitions

5.1.1 For the purposes of these Codes, the definitions of terms are given in section 31. Glossary.

5.1.2 The meanings of abbreviations are given in section 30. Acronyms and Abbreviations.

6. Management Requirements

6.1.1 Where the Statement of Standards and Accreditation Requirements specifies accreditation, the forensic unit shall have a Schedule of Accreditation covering compliance with the standards identified in that statement and the supplementary requirements of these Codes for the methods, products and services it is routinely providing.

6.1.2 Where top management is referred to in the standard, this would usually be at Chief Officer or board level.

7. Business Continuity

7.1.1 The forensic unit shall develop procedures to be implemented following interruption to, or failure of, business critical processes, to maintain or restore operations and ensure continuous availability, confidentiality and integrity of information. [30] [31] [32] See also section 23. Control of Data (e.g. Backups, Recovery and Business Continuity).

7.1.2 Forensic units should ensure that their business continuity plans include provision to preserve and/or recover any material transferred to a subcontractor's facility should that subcontractor go out of business with no legal successor (e.g. through stipulation in a contract with the subcontractor to assist receivership disputes).

7.1.3 Business continuity plans shall be tested on an annual basis and the results documented. [33] Any identified need for action to modify the plans shall be implemented and the plans re-tested.

8. Independence, Impartiality and Integrity

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

---

30 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. [77]

31 Customers 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.

32 The Regulator expects all forensic units to consider what additional supporting information would be required to support case files in such a circumstance (e.g. validation reports, calibration records) and make provisions for an appropriate body to retain access to it should it be required.

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

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

a. Being coerced or having the perception of being coerced, openly or secretively;

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

c. Being the sole reviewer of their critical findings;

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

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

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

g. Having a close/significant personal or financial relationship with a party likely to be affected by the outcome;

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

i. Acting in self-interest.

8.1.3 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.

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

8.1.5 The required policies and procedures shall not only 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.

9. Confidentiality

9.1.1 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.

10. Document Control

10.1.1 The forensic unit shall ensure that document/version control procedures are applied to the following where they are integral to the forensic process, including:

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.

10.1.2 The retention period for obsolete/superseded documents should be defined and should take into account customer, regulatory and legal requirements. [34]

11. Review of Requests, Tenders and Contracts

11.1.1 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. These may include, but not be limited to:

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

---

[34] 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.

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

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

d. Outcomes from case conferences; and

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

11.1.2 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 26.4 exhibit return and disposal).

11.1.3 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.

12. Subcontracting

12.1.1 A forensic unit may need to subcontract work or use external services which affect the quality of forensic unit's activities. In all such cases, the customer shall be informed in writing and approval is required. The original forensic unit shall ensure that the forensic unit any work is being subcontracted to, meets the

requirements of these Codes and shall ensure all continuity, security and recording requirements are met. The original forensic unit remains responsible for the overall quality of the work, including that of any subcontracted element.

12.1.2 Forensic unit shall have a procedure and retain records for: [35]

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

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

c. Ensuring that subcontractors and providers of external services conform to relevant requirements of these Codes.

12.1.3 Where applicable, the original forensic unit shall include in its business continuity plan the arrangements that have been made to preserve retained material [36] should their subcontractor forensic unit or its contracted storage facility cease business and have no legal successor.

12.1.4 If other necessary approvals are required by rules or convention, such as work connected to firearms examination, child exploitation, drug analysis or for inclusion on the National DNA Database ® [37], the subcontracted forensic unit must also be appropriately approved or licensed.

13. Packaging and General Chemicals and Materials

13.1.1 Customers and forensic units shall ensure that any swabs, consumables sampling/collection kits, packaging and/or chemicals they use are fit for purpose. [38]

---

35 Forensic units conducting activities which require accreditation to ISO 17025:2017 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.

36 Including relevant data, reports and records.

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

38 This can be demonstrated by 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 [93] and/or BS ISO 18385:2016

14. Complaints

14.1.1 The forensic unit shall have policies and procedures for dealing with complaints. These procedures shall define what constitutes a complaint [39] in relation to the work undertaken by the forensic unit and shall ensure that appropriately scaled investigations are instigated on receipt of any complaints.

14.1.2 The Regulator shall be informed at the earliest opportunity about any complaint or non-conforming testing/inspection if it has significantly disaffected the customer such that it could attract adverse public comment, be against the public interest or lead to a miscarriage of justice. [40] The policies and procedures relating to complaints shall also indicate the escalation criteria and the individual/role holder responsible for notifying the Regulator.

14.1.3 Complaint investigations shall include examination of the potential impact on any work that has already been undertaken by the forensic unit. In the event that it is shown that there could have been an impact on any work this should be dealt with through the non-conforming work process (see 15. Control of non-conforming testing).

14.1.4 Records shall be retained of all complaints and of the subsequent investigations and outcomes in line with the case file retention period. Where the complaint has been referred to the Regulator, a copy of the investigation report shall be provided to the Regulator when requested.

14.1.5 Complaints may be received from many sources including customers, persons reporting 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).

Minimising the risk of human DNA contamination in products used to collect, store and analyse biological material for forensic purposes. [92] Demonstration of fitness for purpose of chemicals (e.g. reagents) is through initial validation and appropriate quality control of chemicals used in the method.

39 A commonly accepted definition is any expression of negative feedback.

40 This may include where it has been identified there was a wrongful acquittal or a failure to detect the offender.

15. Control of Non-Conforming Testing

15.1.1 Examples of non-conforming testing that [41] could require escalation to the Regulator include, but are not limited to, significant instances of:

a. Unexpected performance in proficiency testing/inter-laboratory comparison;

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. Loss of security clearance by staff;

i. Contamination incidents;

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

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.

15.1.2 The Regulator shall be informed about any non-conforming test if it has potential to significantly disaffect the customer 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 investigation report when requested.

---

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

15.1.3 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 investigation reports;

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

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

16. Control of Records

16.1 General

16.1.1 The forensic unit shall establish retention times that satisfy the requirements of legislation, its accrediting body and its customers, as appropriate. [34]

16.1.2 Records should be stored and subsequently disposed of in a manner appropriate to their sensitivity and/or protective marking (e.g. incinerated or shredded to specified standards).

16.1.3 If information is required under the disclosure rules, [35] protective marking does not provide an exclusion to disclosure.

16.1.4 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 23 Control of Data).

16.2 Technical Records

16.2.1 As a minimum, the technical records [42] shall contain all relevant information relating to the following.

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

---

[42] Technical records are accumulations of data and information that result from carrying out tests, which should contain sufficient information to establish an audit trail and enable the repetition of the activity under conditions as close to the original as possible.

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

iv. The means by which the material was received or passed from/to another party (see 26. 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 exhibits, and materials recovered from exhibits, 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.

16.2.2 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.

16.2.3 Whenever practicable, technical records shall be produced contemporaneously. The practitioner shall normally begin making records from the time instructions are received and shall continue making records throughout their involvement in the case, although, in some circumstances, it may be appropriate to start making records prior to any formal instructions from the customer.

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

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

16.2.6 It should be possible to associate all changes to critical data with the person having made those changes. [43] [44] Reasons for the changes shall be recorded.

16.2.7 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. [45] Each page of every document in the case record shall be traceable to the analyst or examiner responsible for the sampling and/or performance of each examination or test, to a uniquely identified case and uniquely identified exhibit. [46] 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. Alterations or comments in the records shall be clear and be signed, or otherwise be attributable to the individual who made them, and dated.

16.3 Checking and Review

16.3.1 The forensic unit shall have a procedure for checking and review. For methods that require calculations [47] and/or critical data transfers that are not part of a validated electronic process, the procedure shall include a requirement for effective checks to be carried out.

---

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

44 Changes to critical data are expected to be traceable, however it is accepted that systems may not always readily assist this, and any residual risks should be recorded and managed accordingly. It is expected that forensic units strive to implement systems which increase traceability of all technical records.

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

46 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.

47 Including those embedded in spreadsheets.

16.3.2 The forensic unit shall have a procedure for carrying out checks on critical findings and designate competent individuals authorised to carry out such checks. [48] [49] 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 non-conforming results or findings.

16.3.3 Where the forensic unit has deemed [50] the procedure requires an independent check, the organisation should define this level of independence [51] and records should be kept to demonstrate this.

16.3.4 The forensic unit shall have documented policies and procedures and authorised staff 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.

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

16.3.6 The checks and reviews shall be recorded as entries against each finding or on a summary of findings or on a report, as appropriate. If the checker/reviewer

---

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

49 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.

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

51 Note ILAC-G19 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.

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.

17. Internal Audits

17.1.1 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 23.3 Electronic Information Security).

17.1.2 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. [52]

17.1.3 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.

17.1.4 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.

17.1.5 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.

---

[52] 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.

18. Technical Requirements

18.1 Personnel

18.1.1 The forensic unit shall ensure appropriate background verification 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. [53]

18.1.2 The contracts for all staff, permanent and temporary, shall contain confidentiality agreements, [54] their own and the forensic unit's responsibility for information security, and details of their expected conduct.

18.2 Code of Conduct

18.2.1 The forensic unit shall have a Code of Conduct compatible with the Forensic Science Regulator's; staff 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.

18.3 Training

18.3.1 The forensic unit and/or individual members of staff, including sub-contracted staff, shall maintain and keep readily available appropriate records of education, training, skills and experience in sufficient detail to provide evidence of proper training and formal assessment. [55] These records shall include, but not be limited to:

a. Academic and/or professional qualifications;

b. Internal/external courses attended;

---

[53] The required level of clearance for prolonged or unsupervised access to case material is normally Security Check (SC) or Non-Police Personnel Vetting (NPPV) level 3, or equivalent. The clearance level required may however be varied in writing by the controller of the data or exhibit.

[54] 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.

[55] This may include records of Continuous Professional Development.

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;

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.

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

19. Competence

19.1.1 The competence of staff shall be routinely assessed at defined intervals to ensure that it has been maintained and is up to date.

19.1.2 Policies and procedures for on-going competency should consider any adverse judicial comments and complaints that may undermine an individual's credibility.

19.1.3 The forensic unit shall have policies and procedures for taking remedial action when competence is found to have lapsed. See also 15. Control of non-conforming testing.

19.1.4 The forensic unit shall determine the appropriate competence framework for technical roles. [56]

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

20. Accommodation and Environmental Conditions

20.1 Laboratory/Examination Facilities

20.1.1 The laboratory/examination facilities shall include, as appropriate:

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 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/exhibits both 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.

20.1.2 The access and use of 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.

20.1.3 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.

20.2 Contamination Avoidance, Monitoring and Detection [36] [37] [38]

20.2.1 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.

20.2.2 The steps in establishing procedures relevant to contamination control in new methods [57] for trace evidence shall include, [58] 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 points in the process where contamination events could occur (e.g. consumable selection, transfers, etc.);

c. Establishing acceptable control limits at each point or stage of the method;

d. Establishing monitoring requirements (e.g. frequency);

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

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

g. Establishing requirements for record keeping; and

h. Establishing procedures for verifying that the contamination control system remains fit for purpose.

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

a. Limiting and recording access by internal and external visitors, taking into account any recent activities relevant to casework including, but not limited to:

---

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

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

i. Incident scene attendance;

ii. Medical examination of complainant or suspect (for the purposes of taking samples);

iii. Prisoner handling; and

iv. Firearm and drug handling.

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

i. Un-amplified and amplified DNA;

ii. High and low-level drugs work;

iii. Examination of firearms and firearm discharge residues;

iv. Examination of accelerant and fire scene debris; and

v. Examination of exhibits from suspects, complainants and scenes. [59]

c. Use of disposable equipment e.g. gloves, face masks and mop caps.

d. Testing and record keeping of batches of consumables and reagents in all areas of the examination/analytical processes and, where appropriate, for contaminants that could interfere with the success or interpretation of the examination or test.

e. Good working practices, such as:

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

ii. Not introducing contaminated spatulas/pipettes into stock bottles of solvent, standard or reagent;

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

iv. Frequent changing of solvent used for rinsing equipment.

---

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

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

i. Methods for both routine and deep cleaning/decontamination including:

   i. The nature of contaminants significant to the operation of the laboratory;

   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. The governance and oversight by senior management.

20.2.4 The policies and procedures shall ensure access to laboratory areas is restricted to authorised individuals. Where appropriate these individuals shall be covered by relevant elimination databases (e.g. DNA, fingerprints) and any results found in casework screened against them as detailed in policies and procedures. These databases may be locally or remotely maintained.

20.2.5 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.

21. Test Methods and Method Validation

21.1 Selection of Methods

21.1.1 The general requirement is that all technical methods and procedures used by a forensic unit shall be validated. This section details the principles of the requirement for validated methods, the next section, 21.2 Validation of Methods, details the required processes.

21.1.2 Forensic units with methods already [60] 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 detailed in 21.2.57. [61]

21.1.3 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 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.

---

60 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.

61 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.

21.1.4 If a method is required to use portable equipment 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 applications, see UKAS-RG 201:2015 section Process Requirements 7.1.1 (including but not limited to temperature, humidity, surfaces, cross reactivity, lighting, cross contamination control, handling controls).

21.1.5 For novel [62] techniques, non-routine or infrequently used activities the forensic unit should have validated the method, product or service in accordance with the requirements of these Codes and/or should ensure that the status of the validation, product, method or service is clearly understood by the customer prior to commissioning any such work. If these activities are to become part of the routine activities of the forensic unit, accreditation should always be sought.

21.2 Validation of Methods

21.2.1 Validation should be conducted prior to implementation of the method. This may be performed by the forensic unit, manufacturer or another forensic unit, but the forensic unit implementing the method will need to review the validation data to determine if the validation is adequate, reliable and relevant to the purpose it intends for the method.

21.2.2 Except where the method has been validated for incident scene use (see UKAS-RG 201:2015), if the validation has not been conducted at the site that will be using the method the forensic unit must still verify the scope of the validation with the required steps in 21.2.5. 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 competent staff shall demonstrate

62 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.

such adopted methods perform reliably at the given location following the validation process. [63] [29] [39] [40]

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

21.2.4 To ensure validation studies are conducted on the final method, there should be a clear boundary between development and validation. This should include consideration of how to prevent inadvertent re-entering of the development process once validation has started.

21.2.5 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.

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

---

63 See ILAC-G19:08/2014 (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 21.2.57.

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

21.2.7 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 end-user, the requirements of all intermediate users of a method through to the expectations of the court (e.g. Criminal Practice Directions V 19A.5, relevant case law) need to be determined.

21.2.8 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.

21.2.9 The Criminal Practice Directions V (e.g. 19A.5) that supplement Part 19 of the Criminal Procedure Rules should be considered as providing an insight as to the expectations of the CJS end-user. [27]

21.2.10 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;

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.

21.2.11 End-user 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.

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

Determining the Specification

21.2.13 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 requirement document or a separate document.

21.2.14 The specification adds detail to the requirements captured in end-user requirement from the range of users (e.g. analysts, reporting officers) as well as drawing 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.

21.2.15 At this stage the list contained in the ILAC-G19:08/2014 (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

21.2.16 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.

21.2.17 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.

21.2.18 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.

21.2.19 Where exhibits 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 for their use and include their use in the risk assessment. [41]

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

Review of the End-Users' Requirements

21.2.21 The forensic unit shall review the end-user's requirement 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 specifying the requirement (e.g. analysts, reporting officers) may be involved in this review process.

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

21.2.23 Any subsequent changes to the specification shall then be made formally and only following further review and acceptance of the impact of the changes by the intended end-user.

21.2.24 The forensic unit shall ensure that all staff 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

21.2.25 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.

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

The Validation Plan

21.2.27 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.

21.2.28 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.

21.2.29 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. [64]

21.2.30 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.

21.2.31 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.

21.2.32 Particularly where this is a plan for the validation of a new method rather than an adopted method (see 21.2.7), it is accepted additional individuals may be needed to provide the breadth of technical knowledge to evaluate the plan. [65] In such cases these individuals shall be listed and their role in supporting the person responsible for sign-off should be recorded.

Validation of Measurement-Based Methods

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

a. Using 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

---

64 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. [41]

65 Good experimental design ensures the study tests the features required and can reduce the overall experimental effort.

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

21.2.34 The functional and performance requirements, and the relevant parameters and characteristics for measurement-based methods [66] that shall be considered include the:

a. Competence requirements of the analyst/user;

b. Environmental constraints;

c. Exhibit/sample size;

d. Exhibit/sample handling;

e. Exhibit/sample homogeneity;

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

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;

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

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

---

66 The applicability of the parameter should be considered against the aim and the nature of the test. Determining a limit of quantification (j) may be evaluated as not applicable in an entirely qualitative test, but there may still be a requirement to estimate the uncertainty (see 22. Estimation of Uncertainty).

n. Limitations of applicability.

Validation of Interpretive Methods [67]

21.2.35 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. [68] They concentrate on the competence requirements for the staff involved and how the staff shall demonstrate that they can provide consistent, reproducible, valid and reliable results that are compatible with the results of other competent staff. 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);

c. External recognition with a recognised and relevant professional body; and

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

21.2.36 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

21.2.37 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.

21.2.38 Where the validation has not been conducted at the site [69] that will be using the method, the forensic unit must verify the scope of the validation with the study

---

67 Examples of interpretive methods may include the comparison of marks, handwriting or microscopic comparisons.

68 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.

69 See UKAS RG 201 for methods intended for incident scene use. [2]

scaled up or down according to the adequacy and relevance of the available existing validation study.

21.2.39 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 of the forensic unit's staff with the techniques, equipment and facilities involved.

21.2.40 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.

21.2.41 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 not be overlooked.

21.2.42 The 'validation' report shall have as a minimum a summary of the experimental work/review, results, staff training/competence requirement and assessment plans. The required validation library and statement of validation completion shall be produced.

Minor Changes in Methods

21.2.43 Replacing like-for-like equipment [70] 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.

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

Infrequently Used Methods

21.2.45 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, or if not included

---

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

on the schedule of accreditation re-verified in accordance with the requirements of these Codes prior to each use in casework. [42] If these activities are to become part of the routine activities of the forensic unit, accreditation should always be sought.

21.2.46 All methods the forensic unit intends using, including infrequently used methods, shall have been validated in line with these Codes and the forensic unit shall demonstrate competence to perform the method. The validation, verification or re-verification shall include the steps in 21.2.5, and as with all methods, a validation library is required. [71]

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

a. How staff competence will be maintained or is demonstrated;

b. The definition of infrequently performed examinations/test;

c. Responsibility for the validation or verification;

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

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

Validation Outcomes

21.2.48 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 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;

---

[71] 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 21.2.5, even if these are brief.

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. [72]

Assessment of Acceptance Criteria Compliance

21.2.49 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.

21.2.50 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. [73]

21.2.51 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.

21.2.52 Should the forensic unit 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.

---

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

[73] 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.

Validation Report [74]

21.2.53 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. It 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.

21.2.54 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 applicable:

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;

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;

---

[74] Forensic units with methods already within the schedule of accreditation will often only be required to compile the validation library, 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.

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.

21.2.55 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.

21.2.56 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, which will normally be kept for 30 years following its last use in casework. [75]

A Statement of Validation Completion

21.2.57 The aim of this statement is to provide those making decisions on the use of the results 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. [76]

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

21.2.59 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;

---

[75] 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, as amended.

[76] See also the CPS Core Foundation Principles for Forensic Science Providers [78] and the list of questions in direction 19A.5 contained in the Criminal Practice Directions. [27]

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

21.2.60 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; [77]

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.

21.2.61 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.

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

---

[77] 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.

21.2.63 The information in the library shall be disclosable [78] and should be prepared with that requirement in mind.

Implementation Plan and Any Constraints

21.2.64 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 customer;

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;

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;

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 special health and safety, environmental protection, data protection and information security arrangements;

---

78 Commercial-in-confidence does not override the disclosure requirements of the Criminal Procedure and Investigations Act 1996 as amended and may prevent methods, products or services being used.

m. The communication plan; and

n. The schedule for post-implementation review.

22. Estimation of Uncertainty

22.1.1 Guidance on the estimation of uncertainty of measurement is contained in Appendix N of the UKAS M 3003 publication 'The Expression of Uncertainty and Confidence in Measurement'.

22.1.2 A forensic unit performing testing [79] is required to evaluate measurement uncertainty, even where the test method precludes rigorous evaluation of measurement such as a test that is qualitative in nature. UKAS M 3003 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". [43]

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

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

22.1.5 The Criminal Practice Directions V (19A.5c) that supplements Part 19 of the Criminal Procedure Rules include several factors which ought to be considered. However, the following direction that the court may take into account in accessing 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."

[79] The forensic unit may undertake testing as part of incident scene investigation. ILAC-G19 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, this includes but is not limited to estimation of uncertainty of measurement (see also ILAC-G27 [79]).

23. Control of Data

23.1 General

23.1.1 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. [44] [45] [46]

23.1.2 The unit shall identify key data and critical control points (i.e. places where data is entered, transferred, stored or processed in a manner where it may be vulnerable to corruption, errors, unauthorised manipulation etc.). [80]

23.1.3 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.

23.1.4 Protection steps shall be tested by sampling of key data. [81]

23.2 Electronic Information Capture, Storage, Transfer, Retrieval and Disposal [82]

23.2.1 The forensic unit shall establish procedures for the capture and retrieval of electronic information appropriate for the process or method to ensure that all

---

80 This critical control point approach is 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.

81 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.

82 Further information and guidance can be found in BS 10008:2014, Evidential weight and legal admissibility of electronic information – Specification. [80]

the necessary information is captured without change, and that any information lost as a result of the capture process is at an acceptable level. [83]

23.2.2 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. [84]

23.2.3 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.

23.2.4 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.

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

23.2.6 When information is migrated to alternative storage media, the forensic unit shall establish procedures to ensure that all digital objects [85] have been successfully migrated and the digital object and file format of the migrated digital objects have not changed, or that the changes are known, have been audited, and meet requirements.

23.2.7 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 the data.

23.2.8 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.

---

83 Acceptable may be defined in the method's end-user requirements or specifications.

84 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. [81]

85 A digital object is a discrete digital structure that contains meaningful data (e.g. a text file, call record or image), metadata (e.g. details of the data format, ownership or relationship to other data) and a unique identifier.

23.2.9 Information shall be retained in audit trails, or using other appropriate processes, which record the disposal of information as specified by the retention and disposal policy.

23.3 Electronic Information Security [47]

23.3.1 The forensic unit shall have an information security policy which explains how the unit meets its responsibilities outlined in section 23.1.1. [48] [49] [50] The information security policy shall describe the procedures, based on assessed business and security requirements, for the management of electronic information. The forensic unit shall ensure procedures are subject to regular testing, audit and review. [86]

23.3.2 The forensic unit's information security policy shall have processes for the following.

Access Control to Electronic Information

23.3.3 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 needed and the key operational services they require to perform their roles.

23.3.4 Access shall be removed when users leave their role or the organisation. Reviews should take place at least every 6 months to ensure access rights are still needed - if access rights are no longer needed, they shall be removed.

23.3.5 Users with administrative rights shall be authenticated using a second factor [87] where this is technically possible.

---

86 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.

87 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. [82]

23.3.6 Accounts with administrative rights shall only be used to perform administrative duties [88] and shall not be used to access e-mail or the Internet - separate accounts shall be provided for this.

23.3.7 Authentication failures should be throttled to 10 attempts in 5 minutes or locked out where this is practically possible as per industry norms. Access control mechanisms shall be protected to prevent unauthorised system-wide access. [51] [52]

The Selection, Use and Management of Passwords

23.3.8 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. Users should use machine-generated passwords and have appropriate facilities to store them.

b. Password managers [53] for the secure storage of passwords should be used where appropriate. Alternatively, users should adopt the 'three random words' [54] technique for generating suitably complex and memorable passphrases.

c. Passwords shall be a minimum of 8 characters and have no maximum length. Regular password expiry should not be enforced, users shall change their password when it is known (or suspected) that it has been compromised.

d. Users should be educated to not use the same passwords for personal and work accounts.

e. Passwords shall not be reused for accounts with administrative rights.

f. Users should be prevented from selecting easily guessed or commonly used passwords. [55]

---

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

g. Password should be protected in transit and at rest using appropriate encryption and hashing techniques. [52] [56] [57]

h. All default administrative passwords for applications, network equipment and computers shall be changed [52], and meet the requirements identified above.

Protection Against Malware

23.3.9 With the exception of evidence handling where the detection or removal 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.

23.3.10 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.

23.3.11 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. [58]

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

23.3.13 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.

23.3.14 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.

23.3.15 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. [89] '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.

23.3.16 All removable storage media shall be scanned using anti-malware software before use.

23.3.17 The forensic unit should securely configure computers by following the End User Device security principles. [59]

23.3.18 The forensic unit shall have access to offline backups of electronic information so that it can recover from a ransomware attack. [60] [61]

Management of Removable Storage Media

23.3.19 Procedures for management of removable storage media shall include controls related to issue and use. [90]

23.3.20 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.

23.3.21 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 [62]; [91] and

c. Should be subject to accounting with the aim of tracking use and managing loss. [51] [63]

---

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

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

91 Memory cards used for cameras are excluded from encryption.

The Segregation of Forensic Networks

23.3.22 The forensic unit shall have procedures for the segregation of systems used for forensic science work 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.[92] 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). [64] [65]

Backups, Recovery and Business Continuity

23.3.23 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 or hardware failure, whilst ensuring the business can continue to function.

23.3.24 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.

23.3.25 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.

23.3.26 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 Criminal Justice System.

---

92 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.

23.3.27 Offline backups should be stored at a separate and secure location. [93] [66] [67] The forensic unit may use appropriate cloud services for this back-up of electronic information; 'offline' here means digitally disconnected when not in use and designed to remain unaffected should any incident impact the live environment. [68]

23.3.28 The forensic unit shall have an incident management plan [94] 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, roles and responsibilities of staff and third parties such as service providers and authorities, as well as contact details for those involved.

23.3.29 The forensic unit shall periodically test the incident management plan to ensure that its electronic information and critical systems can be recovered in the event of an incident, whilst ensuring that the business can continue to operate. Revisions to the incident management plan should include lessons learnt to ensure the same event cannot occur in the same way again. [51] [63] [69]

Network Security and Mobile Working

23.3.30 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.

23.3.31 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.

---

93 Separate location means a separate building not merely a separate room. Exceptions to this requirement will be rare, but may include forensic units with specific high security requirements. Back-ups also need to be secured from potential malware or ransomware attacks so offline backup is expected. Sole traders may enter into reciprocal storage agreements if they choose to.

94 This may be part of the overall business continuity and disaster recovery plan or a separate IT incident management plan.

23.3.32 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). [56] [57]

23.3.33 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. [51]

The Use of Cloud-Based Services

23.3.34 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 and information will be transported, stored and processed, and understand the associated risks;

c. Evaluate the security of the offering; and

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

23.3.35 The forensic unit should use cloud providers which meet the NCSC's cloud security principles. [68] The 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 their business and security needs.

Security Monitoring and Situational Awareness

23.3.36 The forensic unit's security monitoring and situational awareness procedures shall include the generation, capture, retention, storage and analysis of logs 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 logs shall be stored securely so they are safe from tampering and unauthorised access. All logs should be stored for a minimum of 6 months so that they can be used to support incident management. [70] [71]

23.4 Reference Collections and Databases [95]

23.4.1 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.

23.4.2 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.

23.4.3 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 database, be validated for accuracy of transcription on entry to the database, and be auditable for corruption.

23.4.4 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 these Codes, e.g. with reference to the impact of any uncertainty of measurement and the risk of false positives/negatives.

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

a. Their purpose;

---

95 This subsection was omitted in error from Issue 6, Issue 7 corrects this omission.

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.

23.4.6 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.

24. Equipment

24.1 Computers and Automated Equipment

24.1.1 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.

24.1.2 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 21.2 Validation of Methods.

24.1.3 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.

24.1.4 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.

24.1.5 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. [96] 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.

---

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

24.1.6 The forensic unit shall have a policy for all 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.

25. Measurement Traceability - Intermediate Checks

25.1.1 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.

26. Handling of Test Items

26.1 Receipt of Cases and Exhibits at the Laboratory

26.1.1 The forensic unit shall have procedures for the transportation, receipt [97], handling, protection, storage, retention, and/or disposal of all test items. This shall include a documented risk-based case acceptance procedure [98] for the handling of recoverable irregularities or rejection of an item for examination arising from, but not limited to:

a. A missing exhibit label;

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

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

---

97 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.

98 Customers should consider having a procedure for receipt of cases and checking exhibits being returned from the forensic unit.

d. Illegibility in the name, identification number or any other information on an exhibit label;

e. There being more than one label on an exhibit;

f. Appropriate control samples not submitted;

g. Repeat of the same identification details on different exhibit labels;

h. Inadequate or untimely packaging or sealing of an exhibit that could prejudice its integrity;

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

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

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

26.1.3 Any apparent evidence of tampering with an exhibit shall be investigated. If the outcome of the investigation indicates a deliberate attempt has been made to influence the results of the examination, the forensic unit's top management shall be informed to decide the appropriate escalation, which shall include notifying the Regulator.

26.1.4 The case acceptance procedure shall also specifically address the handling and receipt or rejection of potentially hazardous exhibits that might pose a risk to the health or safety of staff, [99] potentially compromise other work carried out at the laboratory, [100] or which may not be lawfully retained or handled if accepted by the laboratory. [101]

---

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

100 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.

101 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.

26.2 Case Assessment and Prioritisation

26.2.1 Prior to commencing work the forensic unit shall, in consultation with the customer, 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.

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

a. Ensure the relevant requirements of the police 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 exhibits required for an effective examination strategy are provided or that any resultant limitations to the scope of the examination are discussed with the customer and made clear to the CJS;

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

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

26.3 Exhibit Handling, Protection and Storage

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

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

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

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

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

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

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

26.3.2 The forensic unit shall, as far as possible, preserve the exhibit, or part of the exhibit, in its original form to allow for independent re-examination or testing. If an insufficient quantity of the exhibit remains for independent re-examination or testing, or the form of the exhibit is altered, the forensic unit shall ensure that details of the exhibit 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.

26.4 Exhibit Return and Disposal

26.4.1 The forensic unit shall have an agreement with its customers for the return or disposal of exhibits, and evidential material recovered from exhibits, once the examination has been completed. [102]

26.4.2 The nature of forensic science is such that forensic units will deal with material that is subject to legal control or prohibition on possession, production or use. Policies covering such exhibits should reflect any legal control or prohibition covering retention, the return to the organisation that submitted it, or destruction. Examples of such exhibits include, but are not limited to:

a. Human tissue; [103]

b. Drugs;

c. Firearms; and

---

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

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

d. Indecent images of children.

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

26.4.4 Biohazardous exhibits shall be destroyed by the forensic unit in accordance with health and safety legislation, regulations and Home Office guidelines. [104]

27. Assuring the Quality of Test Results

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

27.1.1 The forensic unit shall investigate the availability and appropriateness of schemes for inter-laboratory comparisons that are relevant to their scope of accreditation. [105] [106] [107]

27.1.2 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. [72]

---

104 See HOC 40/73: Handling and disposal of blood samples in criminal cases (other than those brought under the Road Traffic Act 1972) [83] 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 [84] provides similar recommendations to HOC 40/73, but to the courts. HOC 125/76 [85] extends the arrangements of HOC 40/73 and 41/73 to the handling and disposal of saliva samples. HOC 74/82 [86]: 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 [87] extends the provisions of HOC 74/82 to cover the disposal of urine and any other body samples not previously covered.

105 Forensic units may refer to the [88] or the European Network of Forensic Science Institutes (ENFSI) [89] websites for the availability of proficiency testing (PT) schemes.

106 BS EN ISO/IEC 17025:2017 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 [23] 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.

107 UKAS accredits PT providers to ISO/IEC 17043:2010; a list of accredited schemes/providers is available; UKAS recommends the use of an accredited scheme where one exists. [90]

27.1.3 When participating in inter-laboratory comparison schemes, the forensic unit's own documented methods and procedures shall be used.

27.1.4 Unexpected performance in inter-laboratory comparisons shall be handled as non-conforming testing (15. Control of non-conforming testing).

28. Reporting the Results

28.1 General [73]

28.1.1 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.

28.1.2 The forensic unit shall provide early warning of any operational or scientific issues that could unavoidably affect the timeliness of service delivery to the customer. [108]

28.1.3 The reporting practitioner shall be competent and comply with all pertinent parts of the Criminal Procedure Rules, Criminal Practice Directions as well as other requirements. [74]

28.1.4 Full records shall be kept of work done and the results obtained in line with other retention policies, even if the customer does not require a detailed report or statement. [109]

---

[108] See Criminal Procedure Rules 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.

[109] Documentation of work underpinning reports and statements may be kept separate where it is traceable to the correct reports and statements.

28.2 Declarations of Compliance and Non-Compliance with Required Standards [110] [74] [75]

28.2.1 All practitioners shall disclose in statements/reports intended for use as evidence, their compliance, or non-compliance, with the Code of Conduct. [111] [112] [113] The Code of Conduct requires compliance with the quality standards set out by the Regulator in the Statement of Standards and Accreditation Requirements.

28.2.2 The Code of Conduct cross references to the Statement of Standards and Accreditation Requirements so a practitioner will be compliant with the Code of Conduct only if they also comply with requirements for their discipline set out in the Statement of Standards and Accreditation Requirements (e.g. accreditation to ISO 17025 and the Codes or to a standalone code of practice). [114]

28.2.3 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 Code of Conduct published by the Forensic Science Regulator [insert issue]'; [115] or

---

110 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, 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 V 19B (1) 13 and Criminal Procedure Rules 19.3 (3)(c)). Similar requirements are in place in other UK jurisdictions e.g. Criminal Justice and Licensing (Scotland) Act 2010.

111 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.

112 See Criminal Practice Directions 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]".

113 In England and Wales.

114 If the set requirement is accreditation to ISO 17025 and the Codes, but the practitioner's forensic unit only holds accreditation to ISO 17025 without including the Codes then they are not fully compliant and must declare so. If no firm requirement has been set for an area of work (e.g. case review), then the requirement is for practitioners to be compliant with the Code of Conduct, but not the entirety of the Codes or any specific accreditation.

115 This will be the issue of the Code of Conduct that was in force on the date of the statement. If the analytical work was conducted to the standards required at the time it was performed, it will be deemed to be compliant, even if the statement is produced later when a future Code of Conduct applies. Should the practitioner feel the that time gap between the analytical work and the statement

b. ‘I confirm that, to the best of my knowledge and belief, I have acted in accordance with the Code 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 Code 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 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 Code 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 organisation is not (delete as applicable) yet compliant with clause [insert clause from the Code of Conduct] and the required standard for (insert discipline/sub-discipline relevant to the present case). Annex [x] details the steps taken to mitigate the risks associated with this non-compliance.’

28.3 Types of Report in the CJS [116]

28.3.1 Forensic units can be required to supply technical or expert advice to support the investigative process and factual or expert evidence to support the judicial process which are all covered by the requirements in the Code including the provision of the following.

a. Interim progress reports [117] to support investigations. These are initial forensic investigation reports used for an assessment of the forensic exhibits that may help an enquiry, interview or strategy. This report is non-

might mislead, they may wish to add “and the standards required at the time of the analytical work” to this declaration.

116 For England and Wales.

117 ILAC G19 section 4.9 includes oral reports, including the requirement to record the information conveyed.

evidential but may be disclosable as unused material and does not require a statement of compliance with the Code of Conduct (see 28.2 Declarations of Compliance and Non-Compliance with Required Standards).

b. Streamlined Forensic Reports (SFR) [76]. 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.

   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 or Criminal Practice Directions V 19B. 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. [118] [119]

   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 Code of Conduct (see section 28.2) and if it is providing expert opinion it requires an expert's declaration under Criminal Procedure Rules 19.4.

c. Reports (a statement is a type of report) for use in court proceedings.

---

[118] The Crown Prosecution Service 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."

[119] 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).

i. Factual reports require a statement of compliance with the Code of Conduct.

ii. Expert reports require a declaration under Criminal Procedure Rules 19.4(j) and 19B of the Criminal Practice Directions V which should include a statement of compliance with the Code of Conduct (see section 28.2) as part of the declaration required by 19B of the Criminal Practice Directions V.

d. Certificates (e.g. issued under provisions of the Road Traffic Offenders Act 1988).

e. 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 Code of Conduct.

28.4 Reporting Competencies

28.4.1 Forensic units shall ensure that all staff 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. That assumptions they have relied upon are reasonable; and

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

28.4.2 Forensic units shall ensure that all staff who provide expert evidence have a sufficient level of experience, knowledge, standing in the peer group 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.

28.4.3 Forensic units shall ensure that all staff who provide expert evidence based on their practical experience and/or their professional knowledge are additionally able to provide: [120]

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 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); [35] [121] 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 28.2.3 and Criminal Practice Directions v 19b.1.13).

---

120 Also see the list included in the Criminal Practice Directions V (19A.5c).

121 Note the Criminal Procedure Rules 19.3-(3c) 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 providing reports for either the defence or prosecution team.

28.5 Retention, Recording, Revelation and Prosecution Disclosure

28.5.1 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.

28.5.2 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. [35]

28.5.3 All documents, exhibits and evidential material recovered from exhibits 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. [122]

28.5.4 Only personnel authorised by management shall have access to the archives. Movement of material in and out of the archives shall be properly recorded.

28.6 Defence Examinations

28.6.1 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 these Codes, and that they also comply with any conditions attached by the prosecutor to the release of the exhibits, or parts of exhibits, or evidential material recovered from them.

28.6.2 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.

28.6.3 The policies and procedures shall be based on appropriate guidance.

28.6.4 The policies and procedures shall ensure the security and integrity of the exhibits and records requested for review, but must also ensure the

---

[122] 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 customer (e.g. police).

confidentiality of other work in progress or previously undertaken by the forensic unit instructed by the prosecution, to which access has not been granted.

28.6.5 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).

28.6.6 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 [123] and be taken into their possession for examination away from the premises of the forensic unit appointed by the prosecution.

28.6.7 The defence forensic unit must use material supplied by the prosecution forensic unit only for the specific case(s) for which the material was provided. [124] Material supplied by the prosecution is subject to the Data Protection Act 2018 and may be subject to Police and Criminal Evidence Act 1984 as amended by the Protection of Freedoms Act 2012 (e.g. fingerprints, DNA). [125] The defence's forensic unit shall retain the notes and records it has created in line with these Codes.

28.6.8 The forensic unit appointed by the prosecution shall only release exhibits (or evidential material recovered from them) to the defence for examination or testing away from the premises of the forensic unit appointed by the prosecution on receipt of written instructions from the prosecutor and/or the court. Where

---

123 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'. [91]

124 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.

125 The Protection of Freedoms Act 2012 modified the Police and Criminal Evidence Act 1984 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.

the examinations or testing might affect their condition, the forensic unit appointed 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.

28.6.9 The forensic unit appointed 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.

28.6.10 The forensic unit shall ensure that all exhibits (or parts of exhibits, 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 court, prosecution, customer). The forensic unit appointed by the prosecution shall also retain a signed record of the transfers for continuity purposes.

28.6.11 The forensic unit appointed by the prosecution shall check the integrity and continuity records of the returned exhibits, or parts of exhibits, or evidential material for compliance with any conditions of release. Any deficiency in these respects shall be communicated immediately to the prosecutor and the customer, e.g. the police.

28.7 Opinions and Interpretations

28.7.1 Where this is to be included in a forensic unit's schedule of accreditation, the forensic unit will need to ensure that they are in compliance with the UKAS publication LAB 13 and ILAC-G19:08/2014 section 4.9.

29. References

[1] Forensic Science Regulator, “Regulatory Notice 03/2020: Deadline for accreditation of incident scene investigation” 2020. [Online]. Available: www.gov.uk/government/publications/regulatory-notice-032020-deadline-for-accreditation-of-incident-scene-investigation. [Accessed 03 02 2021].

[2] UKAS-RG 201:2015, “Accreditation of Bodies Carrying Out Scene of Crime Examination (Edition 2) ” [Online]. Available: www.ukas.com/wp-content/uploads/schedule_uploads/6456/RG-201-Accreditation-of-Bodies-Carrying-out-Scene-of-Crime-Examination.pdf [Accessed 03 02 2021]

[3] Forensic Science Regulator, “DNA Analysis, FSR-C-108” [Online]. Available: www.gov.uk/government/publications/dna-analysis-codes-of-practice-and-conduct. [Accessed 03 02 2021].

[4] Forensic Science Regulator, “Friction Ridge Detail (Fingermark) Visualisation and Imaging, FSR-C-127” [Online]. Available: www.gov.uk/government/publications/fingermark-visualisation-and-imaging. [Accessed 03 02 2021].

[5] Forensic Science Regulator, “Friction Ridge Detail (Fingerprint) Comparison, FSR-C-128” [Online]. Available: www.gov.uk/government/publications/fingerprint-comparison. [Accessed 03 02 2021].

[6] Forensic Science Regulator, “Digital Forensic Services, FSR-C-107” [Online]. Available: www.gov.uk/government/publications/digital-forensic-services-codes-of-practice-for-forensic-service-providers. [Accessed 03 02 2021].

[7] Forensic Science Regulator, “Digital Forensics - Video Analysis, FSR-C-119” [Online]. Available: www.gov.uk/government/publications/video-analysis-codes-of-practice-for-forensic-service-providers. [Accessed 03 02 2021].

[8] Forensic Science Regulator, “Speech and Audio Forensic Services, FSR-C-134” [Online]. Available: www.gov.uk/government/publications/speech-and-audio-forensic-services. [Accessed 03 02 2021].

[9] Forensic Science Regulator, “Digital Forensics – Cell Site Analysis, FSR-C135” [Online]. Available: www.gov.uk/government/publications/cell-site-analysis. [Accessed 03 02 2021].

[10] Forensic Science Regulator, “The Analysis and Reporting of Forensic Specimens in Relation to s5A Road Traffic Act 1988, FSR-C-133”.

[11] UKAS LAB 39: 2004: UKAS Guidance on the Implementation and Management of Flexible Scopes of Accreditation within Laboratories..

[12] S.P. Elliott , D.W.S. Stephen and S. Paterson “The United Kingdom and Ireland association of forensic toxicologists forensic toxicology laboratory guidelines (2018)” Sceince and Justice, vol. 58, pp. 335-345, 2018. Available: www.ukiaft.co.uk/publications.html [Accessed 03 02 2021].

[13] Crown Prosecution Service, “Firearms,” [Online]. Available: www.cps.gov.uk/legal-guidance/firearms. [Accessed 03 02 2021].

[14] HOC 15/2012: The testing of substances suspected to be drugs controlled under the Misuse of Drugs Act 1971.

[15] Forensic Science Regulator, “Bloodstain Pattern Analysis, FSR-C-102” [Online]. Available: www.gov.uk/government/publications/bloodstain-pattern-analysis-codes-of-practice. [Accessed 03 02 2021].

[16] Chartered Institute for, “Standard and guidance for forensic archaeologists,” [Online]. Available: www.archaeologists.net/sites/default/files/CIfAS&GForensics_2.pdf. [Accessed 03 02 2021].

[17] Chartered Society of Forensic Sciences and College of Podiatry, “Forensic gait analysis: code of practice,” [Online]. Available: www.gov.uk/government/publications/forensic-gait-analysis-code-of-practice. [Accessed 03 02 2021].

[18] Forensic Science Regulator, “Sexual Assault Examination: Requirements for the assessment, collection and recording of forensic science related evidence, FSR-C-116” [Online]. Available: www.gov.uk/government/publications/sexual-assault-examination-requirements-for-forensic-science-related-evidence. [Accessed 03 02 2021].

[19] Royal Anthropological Institute, “Code of Practice for forensic anthropology,” [Online]. Available: www.therai.org.uk/forensic-anthropology. [Accessed 17 11 2020].

[20] The Royal College of Pathologists, “Code of practice and performance standards for forensic pathology in England, Wales and Northern Ireland,” [Online]. Available: www.rcpath.org/uploads/assets/5617496b-cd1a-4ce3-9ec8eabfb0db8f3a/Code-of-practice-and-performance-standards-for-forensic-pathology-in-England-Wales-and-Northern-Ireland.pdf. [Accessed 03 02 2021].

[21] BS EN ISO 9001:2015, Quality management systems. Requirements.

[22] “Introduction - TickITplus,” [Online]. Available: www.tickitplus.org/en/information/the-tickit-plus-scheme.html. [Accessed 03 02 2021].

[23] ISO/IEC 17043:2010, Conformity assessment — General requirements for proficiency testing.

[24] United Kingdom Accreditation Service, “Publications relating to accreditation of Laboratories,” [Online]. Available: www.ukas.com/resources/publications/laboratory-accreditation/. [Accessed 03 02 2021].

[25] Statutory Instrument 1999 No. 3106: The Good Laboratory Practice Regulations 1999.

[26] 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 03 02 2021].

[27] Criminal Procedure Rule Committee, “Criminal Procedure Rules and Practice Directions 2020,” 2020. [Online]. Available: www.gov.uk/guidance/rules-and-practice-directions-2020. [Accessed 03 02 2021].

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

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

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

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

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

[33] BS EN ISO/IEC 17000:2004, Conformity assessment. Vocabulary and general principles.

[34] National Police Chiefs' Council, “Storage, retention and destruction of records and materials seized for forensic examination,” [Online]. Available: www.gov.uk/government/publications/storage-retention-and-destruction-of-records-and-materials-seized-for-forensic-examination/storage-retention-and-destruction-of-records-and-materials-seized-for-forensic-examination-accessible-version. [Accessed 03 02 2021].

[35] 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 03 02 2021].

[36] Forensic Science Regulator, “Laboratory DNA: anti-contamination guidance, FSR-G-208” [Online]. Available:

www.gov.uk/government/publications/laboratory-dna-anti-contamination-guidance. [Accessed 03 02 2021].

[37] Forensic Science Regulator, “Crime scene DNA: anti-contamination guidance, FSR-G-206” [Online]. Available: www.gov.uk/government/publications/crime-scene-dna-anti-contamination-guidance. [Accessed 03 02 2021].

[38] Forensic Science Regulator, “The Control and Avoidance of Contamination in Forensic Medical Examinations, FSR-G-207” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 03 02 2021].

[39] Forensic Science Regulator, “Guidance: Validation. FSR-G-201. Birmingham: Forensic Science Regulator,” [Online]. Available: www.gov.uk/government/publications/forensic-science-providers-validation. [Accessed 03 02 2021].

[40] Forensic Science Regulator, “Guidance: Method Validation in Digital Forensics, FSR-G-218” [Online]. Available: www.gov.uk/government/publications/method-validation-in-digital-forensics. [Accessed 03 02 2021].

[41] Forensic Science Regulator, “Protocol: using casework material for validation purposes. FSR-P-300,” [Online]. Available: www.gov.uk/government/publications/protocol-using-casework-material-for-validation-purposes. [Accessed 03 02 2021].

[42] United Kingdom Accreditation Service, “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 03 02 2021].

[43] 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 03 02 2021].

[44] The National Cyber Security Centre, “Secure Sanitisation of Storage Media,” 2016. [Online]. Available: www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media. [Accessed 03 02 2021].

[45] The Centre for the Protection of National Infrastructure, “Secure Destruction,” 2019. [Online]. Available: www.cpni.gov.uk/secure-destruction-0. [Accessed 03 02 2021].

[46] 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 03 02 2021].

[47] Cabinet Office, “Minimum Cyber Security Standard,” 2018. [Online]. Available: www.gov.uk/government/publications/the-minimum-cyber-security-standard. [Accessed 03 02 2021].

[48] BS ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.

[49] BS ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management.

[50] Cabinet Office, “Minimum Cyber Security Standard,” [Online]. Available: www.gov.uk/government/publications/the-minimum-cyber-security-standard. [Accessed 03 02 2021].

[51] 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 03 02 2021].

[52] The National Cyber Security Centre, “Password administration for system owners,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/passwords/updating-your-approach. [Accessed 03 02 2021].

[53] The National Cyber Security Centre, “Password manager buyers guide,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/passwords/password-manager-buyers-guide. [Accessed 03 02 2021].

[54] 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 03 02 2021].

[55] The National Cyber Security Centre, “Passwords, passwords everywhere,” 2019. [Online]. Available: www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere. [Accessed 03 02 2021].

[56] The National Cyber Security Centre, “Using TLS to protect data 2017,” 2017. [Online]. Available: www.ncsc.gov.uk/guidance/tls-external-facing-services. [Accessed 03 02 2021].

[57] The National Cyber Security Centre, “Using IPSec protect data,” 2016. [Online]. Available: www.ncsc.gov.uk/guidance/using-ipsec-protect-data. [Accessed 03 02 2021].

[58] The National Cyber Security Centre, “Terminology: it's not black and white” 30 April 2020. [Online]. Available: www.ncsc.gov.uk/blog-post/terminology-its-not-black-and-white. [Accessed 30 June 2020].

[59] The National Cyber Security Centre, “End user device (EUD) security guidance”. [Online]. Available: www.ncsc.gov.uk/collection/end-user-

device-security/eud-overview/eud-security-principles. [Accessed 03 02 2021].

[60] The National Cyber Security Centre, “Mitigation malware”. [Online]. Available: www.ncsc.gov.uk/guidance/mitigating-malware. [Accessed 03 02 2021].

[61] The National Cyber Security Centre, “Phishing attacks: defending your organisation,” 2018. [Online]. Available: www.ncsc.gov.uk/guidance/phishing. [Accessed 03 02 2021].

[62] 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 03 02 2021].

[63] 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 03 02 2021].

[64] The National Cyber Security Centre, “Preventing lateral movement,” 2018. [Online]. Available: www.ncsc.gov.uk/guidance/preventing-lateral-movement. [Accessed 03 02 2021].

[65] The Australian Cyber Security Centre, “Implementing Network Segmentation and Segregation,” 2020. [Online]. Available: www.cyber.gov.au/acsc/view-all-content/publications/implementing-network-segmentation-and-segregation. [Accessed 03 02 2021].

[66] 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 03 02 2021].

[67] The National Cyber Security Centre,, “Mitigation malware and ransomware attacks,” 2020. [Online]. Available: www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks. [Accessed 03 02 2021].

[68] 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 03 02 2021].

[69] The National Cyber Security Centre, “Incident Management,” 2019. [Online]. Available: www.ncsc.gov.uk/collection/incident-management. [Accessed 03 02 2021].

[70] The National Cyber Security Centre, “Introduction to logging for security purposes,” 2018. [Online]. Available: www.ncsc.gov.uk/guidance/introduction-logging-security-purposes. [Accessed 03 02 2021].

[71] The National Cyber Security Centre, “Logging made easy (LME),” 2019. [Online]. Available: www.ncsc.gov.uk/blog-post/logging-made-easy. [Accessed 03 02 2021].

[72] United Kingdom Accreditation Service, “UKAS Policy on Participation in Proficiency Testing,” [Online]. Available: www.ukas.com/wp-content/uploads/schedule_uploads/759162/TPS-47-UKAS-Policy-on-Participation-in-Proficiency-Testing.pdf. [Accessed 03 02 2021].

[73] Forensic Science Regulator, “Legal Obligations, FSR-I-400” [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance. [Accessed 03 02 2021].

[74] Forensic Science Regulator, “Expert Report Guidance, FSR-G-200,” [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance. [Accessed 03 02 2021].

[75] Forensic Science Regulator, “Non-Expert Technical Statement Guidance, FSR-G-225” [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance [Accessed 03 02 2021].

[76] Crown Prosecution Service, “Streamlined Forensic Reporting Guidance and Toolkit,” [Online]. Available: www.cps.gov.uk/legal-guidance/streamlined-forensic-reporting-guidance-and-toolkit. [Accessed 03 02 2021].

[77] ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301.

[78] 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 03 02 2021].

[79] 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 03 02 2021].

[80] BS 10008:2014, Evidential weight and legal admissibility of electronic information. Specification.

[81] ISO 12653-1, Electronic imaging — Test target for the black-and-white scanning of office documents — Part 1: Characteristics.

[82] The National Cyber Security Centre, “Setting up two-factor authentication (2FA),” [Online]. Available: www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa. [Accessed 03 02 2021].

[83] HOC 40/73: Handling and disposal of blood samples in criminal cases (other than those brought under the Road Traffic Act 1972).

[84] HOC 41/73: Handling and disposal of blood samples.

[85] HOC 125/76: Handling and disposal of saliva samples.

[86] HOC 74/82: Disposal of blood samples, saliva samples and swabs stained with body fluid: handling of exhibits.

[87] HOC 25/87: I. Agreement for the use of the Police National Computer, II. Disposal of body samples.

[88] European Proficiency Testing Information System , “About EPTIS,” [Online]. Available: www.eptis.bam.de/en/index.htm. [Accessed 03 02 2021].

[89] European Network of Forensic Science Institutes, “Welcome to ENFSI!,” [Online]. Available: https://enfsi.eu/. [Accessed 03 02 2021].

[90] United Kingdom Accreditation Service, “Find Accredited Organisations: Proficiency Testing Providers (PTP),” [Online]. Available: www.ukas.com/find-an-organisation/?q=&type%5B%5D=281. [Accessed 03 02 2021].

[91] 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 03 02 2021].

[92] 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.

[93] 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.

[94] 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 03 02 2021].

30. Acronyms and Abbreviations

Abbreviation	Meaning
BS	British Standard
CCTV	Closed-circuit Television
CJS	Criminal Justice System
CPS	Crown Prosecution Service
DNA	Deoxyribonucleic acid
EDIT	Evidential Drug Identification Testing
EN	European Norm
ENFSI	European Network of Forensic Science Institutes
EPTIS	European Proficiency Testing Information System
EU	European Union
EWHC	High Court of England and Wales
GLP	Good Laboratory Practice Regulations 1999
GMP	Good Manufacturing Practice
HOC	Home Office Circular
IEC	International Electrotechnical Commission
ILAC	International Laboratory Accreditation Cooperation
ISO	International Organisation for Standardisation
NPPV	Non-Police Personnel Vetting
OIC	Officer in charge
PAS	Publicly Available Specification
PT	Proficiency testing
SASR	South Australian State Reports
SC	Security Check
SFR	Streamlined Forensic Report
SLA	Service Level Agreement
SOP	Standard Operating Procedure
UK	United Kingdom of Great Britain and Northern Ireland
UKAS	United Kingdom Accreditation Service

31. Glossary

Accreditation

Third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks. In the UK the sole national accreditation body recognised by the Government to assess UK organisations that provide certification, testing, inspection and calibration services is UKAS.

Accuracy

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

Analyte

Substance to be identified or measured; in digital forensic science it may be taken to include data as the focus of the analysis.

Audit

A systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which specified criteria are fulfilled.

Internal audit:

sometimes called a first-party audit, conducted by, or on behalf of, the organisation itself for internal purposes.

External audit:

includes what are generally termed a ‘second-’ or ‘third-party’ audit. Second-party audits are conducted by parties having an interest in the organisation, such as customers, or by other persons on their behalf. Third-party audits are conducted by external independent organisations. Such organisations provide certification or registration of conformity with requirements such as those of ISO 9001.

Blank

A sample containing none of the analyte of interest, used in analysis for detecting the background level of the analyte in the matrix or contamination.

Calibration

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

Collaborative exercise

An inter-laboratory exercise to determine the performance characteristics of a method or procedure, to establish the effectiveness and comparability of new tests or measurement methods, or to assign values to reference materials and assess their suitability for use in specific test or measurement procedures. Collaborative exercises do not require known expected outcomes.

Competence

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

Complainant

A person who makes a complaint or allegation of having been the victim of a criminal offence or in relation to whom such an allegation is made.

Contamination

The undesirable introduction of substances or trace materials.

Control sample

A matrix-matched standard used to determine the linearity and stability of a quantitative test or determination over time, prepared from a reference material (weighed or measured separately from the calibrators), purchased or obtained from a pool of previously analysed samples.

A positive control contains the analyte at a concentration above a specified limit.

A negative control contains the analyte at a concentration below a specified limit.

The term is used in the forensic science context to refer to a sample obtained from a known source against which material from an unknown source (recovered sample) is to be compared to consider the strength of the evidence in support of a common origin.

Critical findings

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

a. They have a significant impact on the conclusion reached and the interpretation and opinion provided;

b. They cannot be repeated or checked in the absence of the exhibit or sample;

c. They could be interpreted differently.

Customer

Whether internal or external, it is the organisation or a person that receives a product or service (e.g. the consumer, end-user, retailer, beneficiary or purchaser).

Databases

Collections of information designed to provide information rather than for archive, which are stored systematically in hard copy or electronic format and are, e.g. used for:

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

b. Providing statistical information.

Also see the “Reference collection” entry.

End user

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

Expert (witness)

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

Firmware

A term sometimes used to denote the mainly fixed, usually rather small, programs that internally control various electronic devices (e.g. mobile phones, digital cameras, calculators, hard disks, keyboards, memory cards). There are no strict, or well defined, boundaries between firmware and software, but firmware is typically involved with very basic low-level operations in a device, without which the device would be completely non-functional.

Forensic Unit

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

Infrequently Used Methods

Methods that are not routinely performed in a particular forensic unit, these require to be validated and usually require specific procedures to ensure the forensic unit remains competent to perform them.

Integrity: Data/Results

The maintenance of, and the assurance of the accuracy, consistency and completeness of, data over its entire life-cycle. This applies to electronic and manual records.

Integrity: Personal

The quality of being honest and having strong moral principles.

Investigating body

A relevant law-enforcement body as defined in s63A(1A) and (1B) of the Police and Criminal Evidence Act 1984, as amended.

Logical (Data Capture)

The capture of extant files, records, and returned values from a communication with a digital storage device. See for contrast the entry for Physical (Data Capture).

Measurand

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

Method

A logical sequence of operations, described generically for analysis (e.g. for the identification and/or quantification of drugs or explosives, or the determination of a DNA profile) or for comparison of items to establish their origin or authenticity (e.g. fingerprint/footwear mark/toolmark examination; microscopic identifications).

Non-conformity

The non-fulfilment of a requirement, either within the organisation’s policies, procedures or in the specification of the customer.

Organisation

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

Physical (data capture)

The production of a bit for bit copy of the targeted digital data. See for contrast the entry for “Logical (Data Capture)”.

Practitioner

An individual providing a forensic science service at any level or stage in the criminal investigation and trial process.

Product

A product is a discrete manufactured item used in the application of a method (e.g. a sampling kit or a piece of software). Its contents and performance will have defined characteristics, normally provided as a product specification.

Proficiency tests

Exercise to evaluate the competence of analysts and the quality performance of a laboratory.

Open or declared proficiency test:

a test in which the analysts are aware that they are being tested.

Blind or undeclared proficiency test:

a test in which the analysts are not aware that they are being tested.

External proficiency test:

a test conducted by an agency independent of the analysts or laboratory being tested.

Precision

Precision is synonymous with reproducibility or repeatability, whereas accuracy is about obtaining the true or correct value for the quantity measured. An incorrectly calibrated device may be capable of giving reproducibly precise readings even though data generated are not accurate.

Provider

The term is used to include all providers of forensic science, whether commercial, public sector or internal to the police service (e.g. scenes of crime, fingerprint bureau).

Quality

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

Quality manual

A document specifying the management system of an organisation.

Recovered sample

A term used in the forensic science context to refer to a sample obtained from an unknown source against which material from a known source (control sample) is to be compared to consider the strength of the evidence in support of a common origin.

Reference collection

A collection maintained for the purpose of study and authentication, also see database.

Reference material

A quality control material or substance, traceable to its source, one or more of whose property values are sufficiently homogeneous and well established to be used for the calibration of an apparatus, the assessment of a measurement method, the correct functioning of reagents, or for assigning values to materials.

Reference standard

A standard, generally of the highest quality available at a given location, from which measurements made at that location are derived.

Requirement

The need or expectation that is stated, generally implied or obligatory.

Risk

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

Robustness

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

Ruggedness

The capacity of an analytical procedure to withstand small uncontrolled or unintentional changes in its operating conditions.

Sample

A representative portion of the whole material to be tested.

Scene

A person, vehicle or location associated with an incident, on or at which may be found evidence to indicate what has happened, when and how, who was involved, and whether a criminal offence may have been committed.

Schedule of accreditation

A document issued by the national accreditation organisation specifying the examinations or tests the organisation has been accredited for, and for which it could issue certificates or reports bearing the testing mark.

Scope of accreditation

The range of examinations or tests for which the organisation has been accredited by the national accreditation organisation.

Selectivity (or specificity)

The ability of a method to determine accurately and specifically the analyte of interest in the presence of other components in a sample matrix under the stated conditions of the test.

Standard operating procedure

A written procedure that describes how to perform certain examination or test activities.

Subcontractor

A person or organisation contracted to do work for the forensic unit within the subcontractor's own legal entity and under the subcontractor's own quality system.

Supplier

An organisation or person that provides a product (e.g. a producer, distributor, retailer or vendor of a product, or forensic unit of a service or information).

Uncertainty of measurement

This based upon the principle that all measurements are subject to uncertainty and that a value is incomplete without a statement of accuracy. Sources of uncertainty can include unrepresentative samples, rounding errors, approximations and inadequate knowledge of the effect of external factors.

Validation

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

Verification

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. The forensic unit must demonstrate the reliability of the procedure in-house against any documented performance characteristics of that procedure.

32. Correlation with Key Clauses in the Normative References [126]

		ISO/IEC 17025:2017	ILAC-G19: 08/2014	ISO/IEC 17020:2012	UKAS RG 201
	Code of Conduct	-	3.4	-	6.1.10
3	Scope	1	1	1	1
4	Normative references	2	-	2	-
5	Terms and definitions	3	2	3	-
6	Management requirements	8	-	5.1, 5.2, A1	5, 6
7	Business continuity	-	-	-	-
8	Independence, impartiality and integrity	3.1, 4.1	2.12, 3.4, 4.8.1	4.1, 5.2.1	4.1, 6.1.10
9	Confidentiality	4.2	3.4	4.2	4.2
10	Document control	8.2 (option A)	3.1	8.3	8.3
11	Review of requests, tenders and contracts	6.4, 6.5, 6.4.1, 6.6, 7.3.3, 7.6.2,7.7.1, 7.10	3.2	7.5, 7.6	7.5, 7.6
12	Subcontracting	6.6	4.1.3	6.3	-

[126] 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).

		ISO/IEC 17025:2017	ILAC-G19: 08/2014	ISO/IEC 17020:2012	UKAS RG 201
13	Packaging and general chemicals and materials	6.4, 6.5, 6.4.1, 6.6, 7.3.3, 7.6.2, 7.7, 7.10	3.12	6.1, 6.2, 7.1	6.2
14	Complaints	7.9	3.2	7.5, 7.6	7.5, 7.6
15	Control of non-conforming testing	7.1	3.9	8.7, 5.2	8.7
16	Control of records	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	3.5	7.1, 7.2, 7.3, 8.4	7.3, 8.4
16.3	Checking and review	7.8.1.1	4.7.5, 4.8.2	4.1, 7.3	15.3, 25
17	Internal audits	8.8 (option A), 8.9 (option A)	3.7	6.1, 8.6	8.6
18	Technical requirements	6.1	6.2	6.1	6.1
19	Competence	6.2	3.3	6.1	6.1
20	Accommodation and environmental conditions	6.3, 7.8.3.1, 7.8.5	3.11, 4.2.3	6.2, 7.2, 7.3	6.3
21	Test methods and method validation	7.2	3.1	7.1	6.2.2, 7.1
22	Estimation of uncertainty	7.6	3.10, 4.9	6.1.3, 7.1.2	
23	Control of data	6.4, 6.5, 6.4.1, 6.6, 7.3.3, 7.6.2,7.7.1, 7.10	3.12	6.1, 6.2, 7.1	8.3, 8.3

		ISO/IEC 17025:2017	ILAC-G19: 08/2014	ISO/IEC 17020:2012	UKAS RG 201
24	Equipment	6.4, 6.5, 6.4.1, 6.6, 7.3.3, 7.6.2,7.7.1, 7.10	3.12	6.1, 6.2, 7.1	6.2, 7.2
25	Measurement traceability - Intermediate checks	6.4.10, 7.7.1	4.3	6.2.9	6.2.9
26	Handling of test items	7.3, 7.4	4.3.3	7.2	7.2
27	Assuring the quality of test results	7.7	4.7.7.2	7.1, 7.2	
28	Reporting the results	7.8	4.9	4.2, 6.1,7, 7.4	7.4

Appendices to the Codes

(Appendices are available from www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct) [Accessed 09/02/2021].

33. **Blood Pattern Analysis - FSR-C-102**

34. **Digital - FSR-C-107**

35. **DNA - FSR-C-108**

36. **Sexual Assault Examination: Requirements For The Assessment, Collection And Recording Of Forensic Science Related Evidence - FSR-C-116**

37. **Video Analysis - FSR-C-119**

38. **Fingerprint Examination - Terminology, Definitions and Acronyms - FSR-C-126**

39. **Friction Ridge Detail (Fingermark) Visualisation and Imaging - FSR-C-127**

40. **Fingerprint Comparison - FSR-C-128**

41. **The Analysis and Reporting of Forensic Specimens in Relation to S5a Road Traffic Act 1988 - FSR-C-133**

42. **Speech and Audio Forensic Services - FSR-C-134**

43. **Cell Site Analysis - FSR-C-135**

44. **Development of Evaluative Opinions - FSR-C-118**

Published by:

The Forensic Science Regulator
5 St Philip's Place
Colmore Row
Birmingham
B3 2PW

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