Paper to lie before both Houses of Parliament until approved by a resolution of each House

Home Office

Forensic Science Regulator

Draft Code of Practice 2025 (Version 2)

March 2025

Paper to lie before both Houses of Parliament until approved by a resolution of each House

Forensic Science Regulator

Draft Code of Practice 2025 (Version 2)

Presented to Parliament pursuant to section 3(3)(b) of the Forensic Science Regulator Act 2021

March 2025

© Office of the Forensic Science Regulator copyright 2025.

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at FSREnquiries@forensicscienceregulator.gov.uk

ISBN 978-1-5286-5516-3

E03313596 03/25

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

This Code of Practice comes into force on 00:01 on the 2nd of October 2025, when it replaces version 1.

Table of Contents

Table of Contents 4

Introduction 8

1. Introduction 8
2. Normative references 13
3. Demonstration of compliance 14
4. Future obligations 18
5. Modification 18

Part A: General Requirements 20

6. Senior Accountable Individual (SAI) 20
7. Regulator's consideration of quality issues 21
8. Quality issues 24
9. Specialists from outside the forensic science profession 28

Part B – Technical Requirements 31

10. Overview of part B of the Code 31
11. Management requirements 31
12. Business continuity 31
13. Independence, impartiality and integrity 32
14. Confidentiality 34
15. Document control 34
16. Review of requests, tenders and/or contracts 35
17. Developing an examination strategy 36
18. Externally provided products and services 38
19. Control of records 41
20. Checking and review 44
21. Personnel requirements 49
22. Competence 50
23. Environment 54
24. Methods and method validation 61
25. Measurement uncertainty 80
26. Control of data 81
27. Reference collections and databases 92

28. Equipment 94
29. Handling of items/exhibits 96
30. Assuring the quality of results 102
31. Reporting the results 104
32. Obligations for defence examinations 110
33. Retention, recording, revelation and disclosure 111

Part C – Standards of conduct 114

34. Standards of conduct 114

Part D – FSA definitions 115

35. FSA definitions – general provisions 115
36. General inclusions 117
37. General exclusions 120
38. Secretary of State approval 120

D1 – FSAs to which the Code applies 122

39. FSA – INC 100 – Incident scene examination 122
40. FSA – BIO 100 – Forensic medical examination of complainants 124
41. FSA – BIO 200 – Human biological material examination and testing 126
42. FSA – BIO 201 – Human biological material distribution and interpretation 128
43. FSA – BIO 202 – Human DNA analysis 129
44. FSA – BIO 203 – Human kinship analysis 130
45. FSA – BIO 301 – Non-human biological examination and analysis: vertebrates 131
46. FSA – BIO 500 – Taggant analysis 133
47. FSA – DTN 100 – Toxicology: analysis for drug(s), alcohol and/or noxious substances 134
48. FSA – DTN 101 – Toxicology: analysis for drugs and/or alcohol under the Road Traffic Act 1988, Transport and Works Act 1992, and Railways and Transport Safety Act 2003 136
49. FSA – DTN 102 – Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988 138
50. FSA – DTN 103 – Examination and analysis to identify and quantify controlled drugs and/or associated materials 140
51. FSA – DTN 200 – Examination and analysis of corrosives and/or noxious substances 143
52. FSA – DTN 300 – Examination and analysis of residues of lubricants used in sexual offences, including oils, greases and lubricants 144
53. FSA – DTN 400 – Examination and analysis of ignitable liquids and their residues 146
54. FSA – DTN 500 – Examination and analysis of chemical and/or biological agents and associated materials 147

55. FSA – DTN 501 – Examination and analysis of explosives, explosives precursors and explosive residues 150
56. FSA – MTP 100 – Friction ridge detail: visualisation and enhancement 152
57. FSA – MTP 101 – Friction ridge detail: comparison 153
58. FSA – MTP 200 – Footwear: coding 155
59. FSA – MTP 201 – Footwear: screening 157
60. FSA – MTP 202 – Footwear mark comparisons 158
61. FSA – MTP 300 – Marks visualisation and enhancement 160
62. FSA – MTP 301 – Marks comparison 161
63. FSA – MTP 400 – Damage and physical fit 163
64. FSA – MTP 500 – Examination and analysis of particulate trace materials 165
65. FSA – MTP 600 – Examination and analysis of gunshot residue (GSR) 167
66. FSA – MTP 601 – Examination, analysis and classification of firearms, ammunition and associated materials 168
67. FSA – MTP 602 – Firearms: ballistics 172
68. FSA – MTP 700 – Document handwriting 174
69. FSA – MTP 701 – Document authenticity and origin 176
70. FSA – DIG 100 – Data capture, processing and analysis from digital storage devices 179
71. FSA – DIG 200 – Cell site analysis for geolocation 183
72. FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) 185
73. FSA - DIG 301 - Specialist video multimedia, recovery, processing and analysis 189
74. FSA – DIG 400 – Audio acquisition, conversion and processing 193

D2 – FSAs to which the Code does not apply 196

75. FSA – INC 101 – Collision investigation 196
76. FSA – INC 102 – Examination of fire scenes 198
77. FSA – INC 103 – Examination of explosion scenes 200
78. FSA – INC 200 – Forensic examination of witnesses/complainants/suspects 202
79. FSA – INC 201 – Forensic examination of deceased individuals 203
80. FSA – BIO 302 – Non-human biological examination and analysis: plants, fungi, diatoms, microbes, and invertebrates 204
81. FSA – DTN 104 – Toxicology: alcohol technical calculations 205
82. FSA – DTN 105 – Examination and analysis relating to the preparation and production of controlled drugs and/or psychoactive substances 207
83. FSA – DTN 502 – Examination and analysis of radioactive material 209
84. FSA – DTN 503 – Examination and analysis of suspected explosive devices and associated material 211

85. FSA – DIG 101 – Analysis of communications network data 213
86. FSA – DIG 102 – Digital network capture and analysis 215
87. FSA – DIG 401 – Speech and audio analysis 216
88. FSA – CDM 100 – Case review 218
89. FSA – CDM 200 – Control and management of a forensic database service 220

D3 – FSA specific requirements 222

90. Incident scene examination 222
91. Forensic medical examination of sexual offence complainants - assessment, collection and recording of forensic science related evidence 232
92. Human DNA examination and analysis 243
93. Bloodstain pattern analysis 254
94. Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988 258
95. Friction ridge detail: visualisation and enhancement 270
96. Friction ridge detail: comparison 278
97. Digital forensics 289
98. Video processing and analysis 295
99. Cell site analysis for geolocation 321

Part E – General information 340

100. Scope of Forensic Science Activities (FSAs) 340
101. References 346
102. Acronyms and abbreviations 355
103. Glossary 359
104. Highlighted changes 386

Introduction

1. Introduction

1.1 General

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

1.1.2 The model for regulation of forensic science in England and Wales is based on each forensic unit (a legal entity or a defined part of a legal entity that performs any part of a forensic science activity) implementing and operating effective quality management that meets the requirements specified in the Code of Practice. This will provide control of processes and minimise the risk of quality failure.

1.1.3 Effective quality management allows forensic units to understand and manage the risk of quality failure and recover from quality failure. The key elements of quality management include:

a. valid methods;

b. defining, demonstrating and testing the initial and ongoing competence of personnel;

c. having documented and controlled procedures, and an internal audit process to ensure they are effective and being followed;

d. commitment from senior leadership, including making available sufficient resources; and

e. enabling continual improvement.

1.1.4 The establishment of an effective quality management system (QMS) provides the basis for forensic units to produce reliable results and to understand and manage the risk of a quality failure.

1.1.5 The provisions establishing the Forensic Science Regulator (the 'Regulator') under the Forensic Science Regulator Act 2021 were commenced on 25 July 2022 [1]

1.2 Section references in the Code of Practice

1.2.1 Throughout the Code of Practice, the Forensic Science Regulator Act 2021 is referred to as 'the Act' and any references to it are shown as follows - section 4(1) of the Act, or s4(1) of the Act. The subsection number is in brackets. Where reference is made to provisions from other legislation, the full title of the relevant legislation will be set out.

1.2.2 The Code of Practice is referred to as 'the Code'.

1.2.3 References to section numbers that are not followed by 'of the Act' or the title of a piece of legislation refer to sections within the Code itself.

1.3 The Forensic Science Regulator Act 2021

1.3.1 The Act placed the Regulator on a statutory basis (as a new legal entity) and provides the Regulator with legal powers. The Act was commenced in full on the 2 October 2023.

1.3.2 The statutory powers conferred on the Regulator include the following:

a. Prepare and issue a Code of Practice (s2 of the Act).

b. Conduct investigations (s5 of the Act).

c. Issue compliance notices or bring proceedings for an injunction - including an interim injunction (s6 of the Act).

d. Issue completion certificates (s7 of the Act).

e. Issue guidance and/or advice (s9 of the Act).

1.3.3 The Regulator sets the quality standards and requirements through issuing a statutory Code of Practice which must be complied with by those undertaking

FSAs to which the Code applies in England and Wales. The Code was developed in consultation with representatives of, but not limited to, those who are likely to be carrying out activities to which the Code applies, those who commission the work, and those who are affected by the Code.

1.3.4 The Regulator may also provide guidance in relation to undertaking FSAs (whether covered by this Code or not) in England and Wales. The guidance may advise forensic units on how to achieve and maintain the requirements set out in the Code. Non-compliance with the guidance does not, by itself, establish non-compliance with the Code, but any forensic unit which does not comply with guidance (e.g. chooses another approach to achieving requirements) shall be capable of showing how the requirements of the Code have been met.

1.3.5 The Regulator, under the provisions of s10 of the Act, may disclose to any other public authority any information received by the Regulator, in connection with any of the Regulator's functions if the disclosure is made for the purpose of enabling or assisting the other public authority to discharge any of its functions.

1.3.6 The Act introduced powers for the Regulator to intervene where they have reason to believe that a person may be undertaking an FSA to which this Code applies in a way that creates a substantial risk of:

a. adversely affecting any investigation; or

b. impeding or prejudicing the course of justice in any proceedings.

1.3.7 In determining substantial risk, the Regulator will take into account the facts of each case and, where the Regulator considers that there is a risk which is more than theoretical or remote, the Regulator may exercise the powers in s5 and s6 of the Act.

1.3.8 The Act makes provision for the Regulator to require persons to provide copies of documents and other information in the persons' possession or control as part of a Regulator's investigation.

1.4 The Code

1.4.1 This Code builds on the forensic science regulatory model in place prior to the introduction of the Act in England and Wales. It requires each forensic unit to operate an effective QMS and, where stated, achieve and maintain

accreditation to a suitable international standard, and include compliance with this Code in the schedule of accreditation.

1.4.2 This Code is not intended to be a substitute for the complete versions of the international standards referenced. Forensic units applying for, or holding, accreditation to one or more of the international standards remain responsible for ensuring they are aware of all relevant requirements within, or related to, those standards.

1.4.3 The Code applies to all those undertaking FSAs. Unless explicitly excluded in the FSA definition, it also applies to the related activities as set out in section 36. In the Code, forensic unit is the term used to refer to a legal entity or part of a legal entity that performs any part of an FSA; it can be a team, a unit or a single practitioner. A practitioner is any individual who is directly involved in undertaking an FSA. The undertaking of an FSA is not limited by or to the title of the role or unit (i.e. does not require the word forensic or similar), and for example would include police officers or staff in a police organisation undertaking an FSA.

1.4.4 This version of the Code applies to FSAs undertaken for matters related to the Criminal Justice System (CJS) in England and Wales. Future versions of the Code may be applied to other purposes by order of the Secretary of State (s11(2)(c) of the Act).

1.4.5 This Code defines activities that are FSAs and these are divided into those FSAs to which the Code applies (Part D1) and those to which this version of the Code does not apply (Part D2).

1.4.6 It is inevitable that there will be circumstances where the work on an individual case will occur over a timescale in which more than one version of the Code is in force. All work should be performed in accordance with the version of the Code which is in force at the time the work was performed. There is no requirement to revisit work which has already been completed if the Code changes, except where a quality issue has been reported.

1.4.7 From the date this version of the Code comes into force, it replaces the Code version 1 dated March 2023 [2].

1.5 Structure

1.5.1 The Code is formed of several parts as set out below.

- Introduction
- Part A – General requirements.
- Part B – Technical requirements.
- Part C – Standards of conduct.
- Part D – Forensic science activities.
    - General inclusions for the majority of FSAs.
    - D1 - Definitions of FSAs including the means of demonstrating compliance with this Code relevant to a specific FSA or group of FSAs.
    - D2 - Definition of FSAs to which the Code does not apply.
    - D3 – FSA specific requirements that are relevant to an FSA or groups of FSAs.
- Part E – General information.
    - Scope of Forensic Science Activities.
    - References.
    - Acronyms and abbreviations.
    - Glossary.

1.6 Terms and definitions

1.6.1 For the purposes of this Code, the definitions of terms are provided in the Glossary.

1.6.2 The meanings of abbreviations and acronyms are given in section 102 – Acronyms and abbreviations.

1.6.3 The word ‘shall’ is used in this Code where the clause is a requirement.

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

1.7 Application of standards

The Code

1.7.1 Forensic units carrying on FSAs to which the Code applies, shall comply with the requirements set out in the FSA definition, including any relevant FSA specific requirements (i.e. section D3).

1.7.2 The requirements in the Code apply from the date the Code comes into force. All forensic units must comply with the provisions of the Code from the date the Code comes into force as set out on page 3.

1.7.3 The Code sets requirements for some FSAs which apply from the date specified in the Code for that particular FSA, rather than from the date the Code comes into force. Forensic units should aim to meet the requirement before the date specified.

Non-Code documents

1.7.4 The Regulator may issue other documents (e.g. guidance documents) under s9 of the Act. These do not form part of the Code issued under s2 of the Act.

2. Normative references

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

a. BS EN ISO/IEC 17025:2017: General requirements for the competence of testing and calibration laboratories [3];

b. BS EN ISO/IEC 17020:2012: General criteria for the operation of various types of bodies performing inspection [4];

c. BS EN ISO 15189:2022: Medical laboratories – Requirements for quality and competence [5]; and

d. ILAC-G19:06/2022: Modules in a Forensic Science Process [6].

2.1.2 The Code sets requirements within the FSA definitions, for the FSAs to which the Code applies - this can include a requirement to achieve accreditation to specific ISO standards and take account of guidance documents produced by ILAC or UKAS that support the achievement of accreditation. The Regulator will

determine the ISO standards, other requirements and guidance documents that will apply to forensic science activities that are subject to the Code.

2.1.3 Where accreditation is the requirement, the Code, through the general provisions and FSA specific requirements, will provide an interpretation of ISO standards or guidance documents that are used to support accreditation for FSAs that are subject to the Code, and will be the primary basis on which compliance with the Code will be declared (section 31.3). In the event that an interpretation of ISO standards or guidance for FSAs that are subject to the Code requires definition or clarification the Regulator will provide the interpretation by issuing guidance under s9 of the Act, and where appropriate make changes to the Code following the procedure set out in s3 of the Act.

3. Demonstration of compliance

3.1 General

3.1.1 The Regulator requires that forensic units carrying on FSAs that the Code applies to demonstrate compliance with the requirements set out in the relevant FSA definition in the Code.

3.1.2 The Regulator may suspend the compliance requirements set, including any requirement for accreditation, and may reinstate any suspended requirements; the Regulator will notify forensic units that undertake the FSA and the CJS through a report issued under s9 of the Act.

3.1.3 The compliance set for each FSA broadly fall into one of the following categories.

a. Compliance with all relevant sections in the Code, with accreditation to a specified international standard as the assurance method.

b. Compliance with:

   i. the FSA definitions in part D1;

   ii. general governance requirements in part A of the Code;

   iii. an FSA specific requirement in part D3 of the Code and/or a specified framework;

c. No compliance required, the Code does not yet apply (i.e. part D2).

3.2 Compliance with all relevant sections in the Code and accreditation

3.2.1 Where the requirements are compliance with the Code and an international standard, compliance is demonstrated by having accreditation to the standard, the Code and the sub-activities of the FSA that the organisation undertakes, on the schedule of accreditation.

3.2.2 Forensic units shall sign a waiver of confidentiality to allow the accreditation body to share with the Regulator any information that is relevant to the role and functions of the Regulator as set out in the Act.

3.2.3 Any requirement for accreditation shall only be achieved if the accreditation is granted by an accreditation body recognised by the Regulator.

3.2.4 The Regulator recognises that the UK government takes a position that there is a single national accreditation body for the UK, and that UKAS is appointed as the sole UK national accreditation body.

3.2.5 Where the Code requires accreditation, UKAS will assess forensic units undertaking FSAs against ISO/IEC 17025:2017 [3], ISO/IEC 17020:2012 [4] or BS EN ISO 15189:2022 [5].

3.2.6 All practitioners are required to declare their compliance to the Code via a declaration in their reports (section 31.2 details the types of report and section 31.3 covers the declarations for this compliance requirement).

3.3 Compliance to the Code part A and a framework

3.3.1 The general requirements in part A of the Code set requirements for governance, and reporting issues to the Regulator. Adherence to the requirements in part A is to ensure that should non-conformances and/or substantial risks be identified, they are escalated to the Regulator.

3.3.2 The technical requirements set out in part B of the Code do not apply where a framework is used to declare compliance with requirements set in the Code. The requirement to adhere to a framework, including technical requirements, where specified in the Code, is intended to be proportionate to the understood risks. FSAs with this assurance route may have prescribed methods, but many of the controls set out in the Code will not have been applied, or, if they have,

they will have been applied differently and/or their implementation may not require them to be externally assessed.

3.3.3 The Regulator will keep the operation of all such frameworks under review and reserves the right to terminate the use of a framework if risks are not being controlled as expected or if compliance levels to the framework are not satisfactory. The Regulator will seek updates on the level of compliance from the framework owner, as well as relevant SAIs.

3.3.4 As the technical requirements in part B of the Code do not apply in this category, the FSA definition typically requires a declaration of compliance to the framework the Code sets as a requirement rather that the Code as a whole. This is set out in any FSA definition and/or specific requirements where a framework is permitted.

3.4 Summary of FSAs

3.4.1 The following table summarises the high-level compliance and assurance requirements set out in the full FSA definitions in Part D.

Table 1: Summary list of FSAs (a super script 1 denotes an alternative to full Code compliance may also apply for a limited scope – see the FSA definition for full details)

		Name	Code applies
		Incident examination	
INC	100	Incident scene examination	✓
INC	101	Collision investigation	×
INC	102	Examination of fire scenes	×
INC	103	Examination to establish the origin and cause of an explosion	×
INC	200	Forensic examination of witnesses, complainants and suspects	×
INC	201	Forensic examination of deceased individuals	×
		Biology	
BIO	100	Forensic medical examination of complainants	✓
BIO	200	Human biological material examination and testing	✓
BIO	201	Human biological material distribution and interpretation	✓
BIO	202	Human DNA analysis	✓
BIO	203	Human kinship analysis	✓
BIO	301	Non-human biological examination and analysis: vertebrates	✓
BIO	302	Non-human biological examination and analysis: plants, fungi, diatoms, microbes and invertebrates	×

		Name	Code applies
BIO	500	Taggant analysis	✓
		Drugs, toxicology and noxious materials	
DTN	100	Toxicology: analysis for drug(s), alcohol and/or noxious substances	✓
DTN	101	Toxicology: analysis for drugs and alcohol under the Road Traffic Act 1988, Transport and Works Act 1992, and Railways and Transport Safety Act 2003	✓
DTN	102	Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988	✓
DTN	103	Examination and analysis to identify and quantify controlled drugs and/or associated materials	✓
DTN	104	Toxicology: alcohol technical calculations	×
DTN	105	Examination and analysis relating to the preparation and production of drugs and/or psychoactive substances	×
DTN	200	Examination and analysis of corrosives and/or noxious substances	✓
DTN	300	Examination and analysis of residues of lubricants used in sexual offences, including oils, greases and lubricants	✓
DTN	400	Examination and analysis of ignitable liquids and their residues	✓
DTN	500	Examination and analysis of chemical and/or biological agents and associated materials	✓
DTN	501	Examination and analysis of explosives, explosives precursors and explosive residues	✓
DTN	502	Examination and analysis of radioactive material	×
DTN	503	Examination and analysis of suspected explosive devices and associated material	×
		Marks, traces and pattern	
MTP	100	Friction ridge detail: visualisation and enhancement	✓
MTP	101	Friction ridge detail: comparison	✓
MTP	200	Footwear: coding	✓[1]
MTP	201	Footwear: screening	✓
MTP	202	Footwear mark comparisons	✓
MTP	300	Marks visualisation and enhancement	✓
MTP	301	Marks comparison	✓
MTP	400	Damage and physical fit	✓
MTP	500	Examination and analysis of particulate trace materials	✓
MTP	600	Examination and analysis of gunshot residue (GSR)	✓
MTP	601	Examination, analysis and classification of firearms, ammunition and associated materials	✓
MTP	602	Firearms: ballistics	✓
MTP	700	Document handwriting	✓
MTP	701	Document authenticity and origin	✓
		Digital	
DIG	100	Data capture, processing and analysis from digital storage devices	✓
DIG	101	Analysis of communications network data	×

		Name	Code applies
DIG	102	Digital network capture and analysis	×
DIG	200	Cell site analysis for geolocation	✓
DIG	300	Recovery and processing of footage from closed-circuit television (CCTV) /video surveillance systems (VSS)	✓[1]
DIG	301	Specialist video multimedia, recovery, processing and analysis	✓
DIG	400	Audio acquisition, conversion and processing	✓[1]
DIG	401	Speech and audio analysis	×
		Case and data management	
CDM	100	Case review	×
CDM	200	Control and management of a forensic database service	×

4. Future obligations

4.1.1 Where HM Government has determined that the United Kingdom (or any part thereof) should comply with international agreements or treaties which relate to the quality of forensic science, these may be reflected in future versions of the Code.

4.1.2 **Dealing with Changes to References**

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

a. The legislation as amended.

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

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

5. Modification

5.1 General

5.1.1 This Code may be published in alternative formats (e.g. in a different language or addressing specific accessibility issues). All versions are intended to be consistent in content. Should any discrepancy be identified between different formats in which the Code is published then this should be considered an error and the published PDF version of the Code should be considered the definitive version. Should any issues arise as to the interpretation between versions of the Code published in different languages then the English language version shall be deemed the definitive version.

5.1.2 This is version 2 of the Code.

5.2 Approach

5.2.1 The Regulator will, under normal circumstances, modify this Code in the following manner:

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

b. The Regulator shall publish the Code following approval under the provisions of s3 of the Act.

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

5.3 Online publication

5.3.1 The Code is published online in both portable document format (PDF) and Hyper Text Markup Language (HTML) formats.

5.4 Tracking

5.4.1 Subsequent versions of the Code will adopt the following approach:

5.4.2 Significant changes from the previous version will be highlighted in grey; to comply with the Regulations on accessibility [7], highlighted changes are set out in section 104.

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

5.4.4 **Review**

5.4.5 This document is subject to review. Comments should be sent to FSREnquiries@forensicscienceregulator.gov.uk or to the address provided at www.gov.uk/government/organisations/forensic-science-regulator.

Part A: General Requirements

6. Senior Accountable Individual (SAI)

6.1 Appointment

6.1.1 Where a forensic unit is comprised of two or more practitioners, it shall appoint a senior manager (that being at the level of director, partner, board, chief officer or equivalent level of strategic leadership) to be the unit's SAI.

6.1.2 Where a forensic unit is comprised of only one practitioner that practitioner shall be the SAI.

6.2 Role

6.2.1 The SAI shall be accountable for the strategic leadership of the forensic unit's compliance with this Code and be accountable for risks related to any FSA to which the Code applies undertaken by, or under the control of, the forensic unit from the date the Code comes into force. There should be particular focus on monitoring and mitigation of the risk of quality failures which could adversely affect an investigation or impede or prejudice the course of justice in any proceedings.

6.2.2 The SAI shall be accountable, on behalf of the forensic unit, in relation to any investigation or compliance action by the Regulator (section 7).

6.2.3 The SAI shall have the authority to make decisions and deploy resources to address quality matters in the forensic unit.

6.2.4 The name and contact details of the SAI shall be notified to the Regulator. The SAI shall be the route through which any communications related to action under sections 5 and/or 6 of the Act will be addressed. The role of the SAI does not require that all communications between a forensic unit and the Regulator go through that individual.

6.2.5 The forensic unit shall promptly (and in any event within 30 days) notify the Regulator of any change in the information provided about the SAI.

6.3 Requirements

6.3.1 Each forensic unit shall have a document setting out the following for the SAI:

a. The name of the SAI.

b. The date of appointment of the SAI.

c. The responsibilities of the SAI in relation to the Act.

6.3.2 The document which sets out the SAI's role and responsibilities shall be endorsed by the SAI within 30 days of taking up their responsibilities.

7. Regulator's consideration of quality issues

7.1 General

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

a. Self-referral: notification of non-conformances in the delivery of FSAs at the forensic unit referencing itself, and/or complaints received about that forensic unit, under the provisions of section 8.1.7 and/or section 18.2.9.

b. Third party referral: notification by a party other than the forensic unit.

c. Indirect referral: information in the public domain (e.g. a court judgment or media reports).

7.1.2 The Regulator's response to such quality issues depends on the nature of the issue(s) and their potential impact on the CJS. The options include, but are not limited to, the following:

a. To work with the forensic unit as part of the normal quality monitoring process to determine the nature of the issue(s) and the appropriate response.

b. To initiate an investigation under the powers given to the Regulator by s5 of the Act.

c. To initiate compliance action under the powers given to the Regulator by s6 of the Act.

7.1.3 The manner in which the Regulator deals with quality issues is set out in the Regulator's policy on enforcement action [8].

7.1.4 The Regulator may publish a general notification to alert the CJS to risks and enforcement action taken by the Regulator.

7.2 Monitoring of quality

7.2.1 Where the Regulator is considering a potential quality issue in a forensic unit, once the forensic unit is notified of this, the forensic unit shall cooperate with the Regulator to the maximum extent possible including providing, as far as permitted by law, all information sought by the Regulator or potentially relevant to the Regulator's consideration. The forensic unit shall also ensure sufficient resources are employed to address the issue in an agreed timescale.

7.3 Regulator's investigations [s5 of the Act]

General

7.3.1 Where it is appropriate to initiate an investigation into any aspect of the work of a forensic unit, the forensic unit shall (when notified), in addition to the requirements set out in section 7.2:

a. familiarise itself with the provisions of s5 of the Act; and

b. ensure that all nominated personnel involved in the Regulator's investigation are:

   i. aware of the provisions of s5 of the Act; and

   ii. aware of the potential consequences of non-compliance with requests for information issued under s5 of the Act.

7.3.2 An investigation under s5 of the Act, involves information gathering to establish if a person may be carrying on an FSA to which the Code applies in a way that creates a substantial risk of adversely affecting any investigation, or impeding or prejudicing the course of justice in any proceedings. It is a formal process, but does not of itself constitute an adverse finding by the Regulator. If a request for information issued under s5 is not complied with, the Regulator may bring proceedings for an injunction (including an interim injunction), and/or issue a compliance notice under s6 of the Act.

Reporting

7.3.3 Unless the Regulator states otherwise to a forensic unit under investigation under s5 of the Act, there is no requirement for practitioners of that forensic unit to refer to the investigation in their declaration in their report.

7.4 Compliance action [s6-8 of the Act]

General

7.4.1 Where the Regulator initiates compliance action in relation to any aspect of the work of a forensic unit, that unit shall (when notified), in addition to the requirements set out in section 8 and/or section 9:

a. familiarise itself with the provisions of sections 6–8 of the Act; and

b. ensure all nominated personnel involved in the Regulator's compliance action are:

   i. aware of the provisions of sections 6–8 of the Act; and

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

Reporting

7.4.2 Any compliance action taken by the Regulator shall be declared (section 31.1.7) unless a completion certificate has been issued in respect of that compliance notice. Compliance actions include, but are not limited to the:

a. issue of a compliance notice;

b. application for and/or granting of an injunction; and

c. initiation of contempt proceedings or finding of contempt.

7.4.3 Being issued with a compliance notice by the Regulator amounts to an adverse finding which shall be disclosed by whoever it is served upon, as required by the Criminal Procedure and Investigations Act 1996 [9] and/or the Criminal Practice Directions 2023 section 7.1.4(e).

8. Quality issues

8.1 Control of non-conforming FSA related work

8.1.1 Non-conformance refers to the forensic unit's work that does not meet the requirements set out in the forensic unit's policies, procedures, commissioning party requirements, or the Code.

8.1.2 The forensic unit shall have policies and procedures to

a. identify and manage non-conformances; and

b. mitigate the risk of such non-conformances being repeated.

8.1.3 The forensic unit carrying on an FSA to which the code applies shall inform the Regulator about non-conforming work if it has potential to:

a. adversely affect any investigation;

b. impede or prejudice the course of justice in any proceedings;

c. create adverse public comment; or

d. be against the public interest.

8.1.4 The forensic unit shall notify the Regulator at the earliest opportunity, rather than after a potentially prolonged review, once an issue related to non-conforming work has been confirmed as a quality failure.

8.1.5 Basic information on the non-conforming work and likely timescale for the review may be sufficient at the notification stage, although as much information as possible should be provided (section 8.1.6 below for the type of information sought). The forensic unit may risk assess the non-conformity as part of their escalation process. However, any assessment to determine the level of risk in respect to provisions in the Act is for the Regulator alone.

8.1.6 The forensic unit shall provide the Regulator with a report on the review of the non-conformity, which should detail the following.

a. Forensic unit impacted.

b. The FSA the non-conformity arose in.

c. Date of non-conformity.

d. Summary of the non-conformity.

e. How the non-conformity was identified.

f. Date of detection.

g. Immediate containment actions taken.

h. Impact – single case/multiple cases.

i. Root cause(s) – as identified.

j. Mitigations to prevent recurrence.

k. Close out report completed or date for close out report.

8.1.7 Examples of non-conformances, or circumstances that indicate non-conformance may have occurred, include, but are not limited to:

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

b. a method being found to be producing erroneous results;

c. missing or compromised items/exhibits and/or case files;

d. equipment not receiving timely calibration or maintenance;

e. personnel not following procedures or norms of integrity that impact on quality;

f. any fault identified in standards/reference materials, equipment or reagents;

g. contamination incidents which may have an adverse impact on the CJS (those identified through the use of quality controls within the method do not usually warrant notification to the Regulator; however, any identified trends should be reported);

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

i. unauthorised access to restricted areas or information;

j. potential criminal activity by personnel;

k. withdrawal of security clearance from personnel;

l. judicial criticism; or

m. any significant issue identified by an external body such as accreditation body.

8.1.8 The forensic unit shall maintain a record of non-conformances which:

a. is capable of being used to identify trends;

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

c. includes any review reports (e.g. root cause analysis);

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

e. details reviews of opportunities where similar non-conformances may occur and the preventative actions taken;

f. records any evaluation of the corrective action; and

g. is retained for at least as long as the case file retention period.

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

8.2 Complaints received by the forensic unit

8.2.1 A complaint means any expression of negative feedback. Complaints may be received from many sources, including the commissioning party, persons professing to be victims of crime, police forces, other departments within the same forensic unit, and the judicial system (including adverse court decisions pertinent to the work).

8.2.2 The forensic unit shall have policies and procedures for dealing with complaints. These procedures shall define what constitutes a complaint in relation to the FSAs undertaken, by the forensic unit, that are subject to the Code, and shall ensure that proportionate reviews are instigated on receipt of any complaints.

8.2.3 The forensic unit shall inform the Regulator via FSREnquiries@forensicscienceregulator.gov.uk or the address given at www.gov.uk/government/organisations/forensic-science-regulator at the earliest

opportunity about any complaint in respect of the carrying on of FSAs to which the Code applies if it has potential to:

a. adversely affect any investigation;

b. impede or prejudice the course of justice in any proceedings;

c. create adverse public comment; or

d. be against the public interest.

8.3 Reporting changes to accreditation status and action taken by an accreditation body

8.3.1 Forensic units shall promptly, and as soon as practicable, report to the Regulator any suspension, withdrawal, or change in their accreditation status (and/or the accreditation status of any external forensic unit sub-contracted to provide FSAs to the forensic unit) where the suspension, withdrawal or change in accreditation means that the forensic unit is no longer compliant with the Code.

8.3.2 If such a situation arises, the forensic unit shall take the following steps:

a. Identify all cases affected by the change in accreditation status, including considering if the reason for suspension/withdrawal was likely to apply to completed cases.

b. Set out in its report to the Regulator:

   i. the basis and reasons for the suspension, withdrawal or change in accreditation;

   ii. any action that has been taken to deal with issues that have led to suspension, withdrawal or change in accreditation; and

   iii. the impact of any suspension, withdrawal or change in accreditation on the results or opinions that have been made in any statements or reports.

c. Use appropriate and risk-based strategies to consider remedial actions such as issuing a further witness statement as a result of changes to accreditation status or compliance with requirements set out the Code.

The Regulator may advise the forensic unit in determining what further information is appropriate and any other remedial actions.

d. Inform the commissioning party of cases identified as affected by the change in accreditation status and proposed remedial actions to be put in place. This should be with specific reference to s4 of the Act and noting that any work reported in statements or reports for such affected cases may not have been compliant with the Code at the time of examination/analysis/reporting.

9. Specialists from outside the forensic science profession

9.1 Scope

9.1.1 Specialists from outside the forensic science profession may, from time to time, be commissioned to give expert evidence of a technical nature in relation to an FSA which is subject to this Code. This could, for instance, include technologists and material scientists from manufacturing industry (e.g. glass, textiles, building materials, vehicle manufacturers). Where specialists from outside the forensic science profession provide advice/evidence in relation to an FSA which is subject to this Code, it is impractical to require compliance with all provisions of this Code or with the means of demonstrating compliance (e.g. accreditation).

9.1.2 An individual shall only fall within the definition of a specialist from outside the forensic science profession if the conditions in section 9.1.3 are met in relation to both the practitioner and the evidence provided.

9.1.3 The practitioner, subject to the provisions of section 9.1.2, shall:

a. not be a member of staff of a unit providing forensic science services to the CJS in England and Wales;

b. not represent themselves as a forensic practitioner operating within the CJS in England and Wales; and/or

c. not have been specifically commissioned, in an advisory or expert capacity, in any case in the CJS in England and Wales in the previous 12 months.

9.1.4 Specialists from outside the forensic science profession are responsible for informing the commissioning party of any previous provision of evidence to the CJS.

9.1.5 The commissioning party is responsible for ensuring that specialists from outside the forensic science profession are aware of the requirements set out in this section of the Code.

9.1.6 Provision of evidence to a different justice system (e.g. Family Justice System) is not deemed to contribute to the frequency with which an expert has any involvement in the CJS and so does not have any bearing on the status of specialists from outside the forensic science profession.

9.1.7 The evidence provided by any specialists from outside the forensic science profession shall not be of a type which can ordinarily be obtained from a forensic unit.

9.2 Requirements

9.2.1 Specialists from outside the forensic science profession shall comply with the following requirements:

a. The general obligations of expert witnesses [10], including the requirements of the CJS as contained in the Criminal Procedure Rules [11] (and Criminal Practice Directions 2023, in particular directions 7.1.2 and 7.2).

b. The requirements for contents of reports including, but not limited to, those prescribed in the Criminal Procedure Rules Part 19.4 and Criminal Practice Directions 2023.

c. Retention, recording, revelation and disclosure obligations.

d. The requirement to declare in their report if reference collections and databases have been used.

e. The requirement to use validated methods or procedures based on sound scientific principles and methodology.

f. The requirement 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.

g. The requirement to consider the impact that confirmation/cognitive bias can have at different stages and use appropriate avoidance strategies.

h. The requirement to include the declaration required in the Criminal Practice Directions 2023 direction 7.2 and the Regulator's requirement for the positive declaration to be in the following terms:

> 'I confirm that, to the best of my knowledge and belief, I have acted in accordance with requirements of part A of the Code of Practice [insert version] published by the Forensic Science Regulator as it pertains to specialists from outside the forensic science profession. Annex [x] details the steps taken to comply with the specific requirements set for experts from outside the forensic science profession.'

Part B – Technical Requirements

10. Overview of part B of the Code

10.1.1 This part of the Code sets out the technical requirements that apply to the undertaking of FSAs, all applicable sections apply unless FSA's definition explicitly specifies that part B they do not.

11. Management requirements

11.1.1 Where the Code specifies accreditation for an FSA, the forensic unit shall have a schedule of accreditation covering compliance with the applicable international standard(s) identified for the FSA and this Code. Provisions in the Code vary this requirement with regard to specialists from outside the forensic science community (section 9) and/or where the provisions for infrequently used methods apply (section 24.2.8-24-2.16, and what follows).

11.1.2 The forensic unit shall define all roles within the forensic unit that have a direct influence on the carrying on of an FSA or part thereof undertaken, and detail any specific requirements for these roles (section 22).

11.1.3 Where a role is supporting the delivery of the FSA within a forensic unit, but not directly undertaking the FSA (personnel with access to examination areas e.g. cleaning or equipment and building maintenance), role-specific awareness training (e.g. security, confidentiality, integrity, contamination control) shall be given and documented.

12. Business continuity

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

12.1.2 The business continuity procedures shall include:

a. consideration of information required to support case file data (e.g. validation reports, calibration records);

b. consideration of the risk from a provider going out of business with no legal successor, to ensure retained material, case files and associated records are 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; and

c. an IT incident management plan for retrieval of critical data (section 26).

12.1.3 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 [12].

12.1.4 A forensic unit may need to use externally provided services in the undertaking of all, or any part, of an FSA (section 18.2). The commissioning forensic unit should ensure that its business continuity procedures include provision to preserve and/or recover any material transferred to, or generated by, the provider commissioned to perform the work.

12.1.5 Where externally provided services are performed by a separate legal entity, these business continuity procedures should include safeguards in the event that legal entity were to go out of business with no legal successor (e.g. through stipulation in a contract with the legal entity in question to assist in receivership disputes).

12.1.6 The business continuity procedures shall be tested, for each area of work and/or site, at a frequency in proportion to risk (at least once in an accreditation cycle) and the results documented. In some circumstances a desktop exercise may be justifiable. Any identified need for action to modify the plans shall be implemented and the plans retested.

13. Independence, impartiality and integrity

13.1.1 The forensic unit shall ensure that all of its practitioners are made aware of, and adhere to, the standards of conduct in respect of their independence, impartiality and integrity (see section 34). The organisational structure, management, policies and procedures shall support this.

13.1.2 The forensic unit shall have policies and procedures to record potential conflicts of interest and this record shall be regularly reviewed and updated.

13.1.3 The required policies and procedures should seek to control internal and external influence on the results of the FSA performed. Policies and procedures which reward practitioners shall stipulate that any such award be independent of the outcome of the case.

13.1.4 The policy and procedures should require, in the event of a conflict of interest, the commissioning party being made aware and other actions taken to manage risk.

13.1.5 The process map required to assure data integrity (section 26.1.3) should be used in the development of the procedure for the FSA. The process map should assess the risk of cognitive bias. If identified as a risk, non task-relevant information should be held back until completion of the stage(s) which may be influenced by such information.

13.1.6 The required policies and procedures should also cover the 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 (section 31).

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

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

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

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

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

e. having not sought independent review of their critical findings;

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

g. being overfamiliar with, or trusting, another person instead of relying on objective evidence;

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

   i. the practitioner's work; and/or

   ii. the case;

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

j. acting in self-interest.

13.1.8 Practitioners giving an evaluative opinion should interpret the evidence in light of the propositions set out by all parties and provide evidence in a balanced manner.

14. Confidentiality

14.1.1 The forensic unit shall have documented policies and procedures detailing confidentiality requirements (or equivalents, such as statutory restrictions on the use of information), including any disclosure requirements, and shall ensure that those requirements are applied to any externally provided services. The procedures shall address the following:

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

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

c. The potential legal liability for breach of confidentiality.

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

15. Document control

15.1.1 The forensic unit shall have a process for controlling documentation, where this is integral to the undertaking of an FSA, including but not limited to:

a. Procedures – technical and quality.

b. Software;

c. Technical methods;

d. Forms;

e. Locally held copies of key external documents.

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

15.1.2 The retention period for obsolete/superseded documents should be defined, taking into account requirements from the commissioning party, the Criminal Procedure and Investigations Act 1996 [9] and legal requirements. Retention for 30 years from the last time the technique the documents refer to was used and/or reported, may be required.

16. Review of requests, tenders and/or contracts

16.1.1 This terminology is used in various standards to cover the process of agreeing and recording the commissioning party's and forensic unit's interaction when requesting or tasking. Typically, where the commissioning party is external to the forensic unit, as well as any wider organisation of which the forensic unit is part, a commercial arrangement is entered into. This Code does not seek to govern how commercial arrangements are entered into, only how work is controlled, and instructions are captured which may involve a service level agreement (SLA) in more routine casework.

16.1.2 Requirements made on the external forensic unit should also be applied to any externally provided services that a forensic unit engages where those external providers are delivering any part of the FSA.

16.1.3 Where the commissioning party and the forensic unit are part of the same organisation, a request may be managed through an internal work order control system.

16.1.4 The processes surrounding the review of requests, tenders and/or contracts may occur at several different levels and at several key stages through the processing of forensic work. Any review taking place at whatever level shall be documented.

16.1.5 The issues to be addressed shall include how the following will apply before the work commences:

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

b. Whether the forensic unit has sufficient resource (amount and competence) to manage work and meet the requirements of the CJS.

c. Whether the forensic unit meets the standards required for the work and can demonstrate compliance with the requirements set out in the Code.

d. Whether the practitioners have the level of background checks (e.g. security checks) the commissioning party requires for the work (section 21).

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

16.1.6 The forensic unit shall have a policy to record all instances when work requirements are discussed and reviewed such that a demonstrable audit trail, including justifications and authorisations, is available for each piece of work undertaken.

17. Developing an examination strategy

17.1.1 The purpose of an examination strategy is to ensure that the FSA, or suite of FSAs, being applied is appropriate to the investigative questions or evaluative opinion (section 31.4.6-31.4.9) to be addressed. These can include, but are not limited to:

a. identifying whether a crime has been committed;

b. identifying or eliminating a suspect;

c. investigating the accounts of suspects, complainants or witnesses; and/or

d. establishing the sequence of events.

17.1.2 The forensic unit shall have a policy that enables it, prior to commencing work, to:

a. identify the issue(s) in the case;

b. develop an appropriate examination strategy;

c. indicate the FSAs being proposed;

d. determine the sequence of sampling and/or examination; and

e. agree the timescale for the delivery of the results.

17.1.3 This policy may be included in an overarching SLA/contract for more routine case work/examination or developed in consultation with the commissioning party.

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

a. ensure the relevant requirements of the commissioning party are captured;

b. request that all the task-relevant information (including information from any previous examinations), and/or information about secondary scenes and/or items/exhibits required for an effective examination strategy, are provided;

c. consider phased disclosure of information not related to the task in the strategy;

d. highlight any limitations to the scope of the examination with the commissioning party and make them clear to the CJS;

e. establish all task-relevant details of the incident, including:

i. the incident type and how this influences the scale of the examination; and

ii. what items/exhibits will be or have been recovered for examination, and the circumstances relating to the location and recovery of the items/exhibits.

f. determine the facilities and techniques/equipment required;

g. select and prioritise the examinations according to the needs of the investigation, the commissioning party, and/or the CJS, with consideration to the scenes and/or items/exhibits available; and

h. determine the sequence of examinations and/or sampling of the items/exhibits in order to obtain the most effective evidence with reference to the following:

i. recognition and prioritisation of the evidence types most likely to address assumed reasonable alternative versions of events in the case;

ii. the potential cross contamination of scenes or items/exhibits;

iii. the risk of loss of integrity of the items/exhibits; and

iv. whether access to non-task-relevant information might require phased disclosure.

i. consider how to proceed should other evidence types be revealed when performing this examination revising the strategy and sequence where necessary (e.g. visualising footwear marks when conducting the FSA for friction ridge enhancement).

18. Externally provided products and services

18.1 Externally provided products

18.1.1 Forensic units shall ensure that any consumables, such as sampling/collection kits, packaging, and/or chemicals they use are fit for purpose. The manner in which this can be demonstrated may include procuring consumables from manufacturers and kit assemblers whose products meet the requirements set out in:

a. Publicly Available Specification (PAS) 377:2023 [13]. Consumables used in the collection, preservation and processing of material for forensic analysis – Product, manufacturing and forensic kit assembly – Specification [13]; and/or

b. BS ISO 18385:2016, Minimising the risk of human DNA contamination in products used to collect, store and analyse biological material for forensic purposes [14].

18.1.2 Demonstration of fitness for purpose of externally provided materials is through initial validation and/or appropriate quality assurance of materials used in the method. For DNA consumables supplied as 'Forensic DNA Grade' (i.e. compliant with PAS 377:2023 [13] or BS ISO 18385:2016 [14]) there is no requirement for end user batch testing (see also 92.2.3).

18.1.3 Forensic units shall have in place a process for the ongoing review of the suitability of consumables and other externally provided products.

18.2 Externally provided services

18.2.1 A forensic unit may obtain services from outside the forensic unit (externally provided services) as part of the undertaking of all, or any part, of an FSA. Services can be obtained through any model (contractual or otherwise), including subcontracts. Any services so provided will be subject to this Code.

18.2.2 A forensic unit may also obtain services from outside the forensic unit for activities directly related to the delivery of an FSA, but which are not explicitly part of the FSA and delivered in a manner where application of all Parts of the Code could not reasonably apply. A related service may be a courier service for recovered items or a mobile phone repair or password recovery service. Setting requirements for such services is covered in 18.2.3.

18.2.3 The forensic unit commissioning the work shall have policy(s) and procedure(s), and retain records, for:

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

b. seeking and recording agreement from the commissioning party for the use of externally provided FSA services (in part or whole);

c. specifying the requirements of the services to be obtained from the external provider; and

d. ensuring that externally provided services conform to the forensic unit's requirements set out in section 18.2.3a.

18.2.4 The records should include what aspects of compliance are deemed relevant, how assurance was achieved and may also include a record of any specific relevant key competencies any key personnel providing the service were identified to hold to support the decision.

18.2.5 Forensic units conducting activities which require accreditation to ISO/IEC 17025:2017 [3] 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.

18.2.6 The forensic unit commissioning the work shall ensure that:

a. all FSA related work meets the requirements set out in the FSA definition;

b. all FSA general inclusions are met; and

c. the provider of the external services has all required licences and/or approvals to perform the work (such as work connected to firearms examination, child exploitation, drug analysis or for inclusion on the National DNA Database®).

18.2.7 The forensic unit obtaining the externally provided services as part of an FSA they are delivering and reporting remains responsible for the overall quality of the work, including that of any external element. If the externally provided service is an FSA to which the Code applies, the external provider will also be subject to the Code.

18.2.8 Forensic units intending to obtain external services related to the undertaking of any FSA, or part of an FSA, shall include in its business continuity procedure the arrangements that have been made to preserve retained material (including relevant data, reports and records) should their external provider or its contracted storage facility cease business and have no legal successor.

18.2.9 The forensic unit commissioning the work shall have policies and procedures relating to complaints involving external provided service and shall also indicate the escalation criteria and the individual/role holder responsible for notifying the Regulator.

18.2.10 Reviews by the forensic unit commissioning the work prompted by complaints shall include examination of the potential impact on any work that has already been completed by the forensic unit. In the event that it is shown that there could have been an impact on any previous work, this should be dealt with through the non-conforming work process (section 8.1).

18.2.11 The forensic unit commissioning the work shall retain records of all complaints and of the subsequent reviews and outcomes in line with the case file retention policy. If the externally provided service is an FSA to which the Code applies, the external provider will also be subject to the Code, including but not limited to the control of conforming work and retention of records. Where the complaint has been referred to the Regulator, a copy of the report on the finding of the review shall be provided to the Regulator.

19. Control of records

19.1 General

19.1.1 The forensic unit shall establish retention times that satisfy the requirements of legislation (see the Criminal Procedure and Investigations Act 1996 [9]), its accrediting body, the party commissioning the work [15] and the Code. The forensic unit must also be aware of compliance with other legislations with regard to the retention and disposal of information including the data protection legislation.

19.1.2 Records shall be stored and subsequently disposed of in a manner appropriate to their format (e.g. electronic or physical), sensitivity and/or protective marking (e.g. incinerated or shredded to a specified standard which has been agreed with the commissioning party).

19.1.3 Protective marking (e.g. with a Government Security Classification [16]) does not, by itself, provide an exemption to disclosure obligations [17].

19.1.4 Where records are distributed across different 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 section 26).

19.2 Technical records

19.2.1 Technical records shall be made with sufficient information to allow subsequent interpretation to be effective in meeting the objectives of the commissioned work.

19.2.2 To achieve this, as a minimum, the forensic unit shall maintain technical records that contain all relevant information relating to the following:

a. The collection and movement of material (physical items/exhibits, data and records e.g. taking a case file to court), including:

   i. date (and time/ time range when critical) on which the material was recovered or received in the forensic unit;

   ii. date (and time when critical) of 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 (section 29) or data was transferred, shared or accessed.

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

i. the written method or standard operating procedure used (including the version);

ii. a specific instrument;

iii. the instrument configuration, e.g. software version or, if relevant, firmware;

iv. the operator of the instrument; and

v. the date of the examination/analysis.

c. The examination of items/exhibits, and examination/analysis of materials recovered from items/exhibits.

d. Verbal and other communications, including reports.

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

f. E-mails and other electronic transmissions (e.g. images) sent or received.

19.2.3 The records, in whatever form, shall be clear and comprehensive, and expressed in such a manner 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:

a. re-examination (e.g. at scenes) is not possible;

b. there is an insufficient quantity of the items/exhibits remaining for independent re-examination or testing; or

c. the form of the items/exhibits is altered.

19.2.4 Technical records should be produced contemporaneously or for incident scenes, at the first practical opportunity. The practitioner shall begin making

records from the time a commission is received and shall continue making records throughout their involvement in the case. If there is any discussion between the practitioner and the commissioning party about the case, or advice on tasking or submission was sought, prior to or during contract review, the practitioner should, where it is practical to do so, record such discussions before receiving formal instructions from the commissioning party.

19.2.5 Image capture may be used as part of contemporaneous notes. There shall be a procedure in place for image use, which shall draw distinction between general image records and images taken at high resolution and/or to scale for downstream examination/analysis, comparison and interpretation.

19.2.6 When a request for an examination is rejected, an item is rejected at submission, or a test result or report is rejected by the forensic unit, the reasons for the original rejection shall be recorded, even when a report is to be replaced.

19.2.7 For the period of record retention, traceability shall be maintained for all names, initials and/or identifiers of anyone who had any part in progressing the case. These should be legible and understandable.

19.2.8 All changes to data shall be traceable to the individual who made those changes. Reasons for the changes shall be recorded. It is acceptable for the critical data and changes to be located in different electronic systems or locations if this can be demonstrated to achieve the required traceability.

19.2.9 Completeness of any hard-copy record shall be demonstrable, e.g. through pagination using a page numbering system which indicates the total number of pages or an index sheet with this information (see ILAC-G19 section 3.5 [6]):

a. Each page of every document in the case record shall be traceable to the practitioner responsible for the sampling and/or performance of each examination or test, to a uniquely identified case and uniquely identified item/exhibit (section 19.2.7).

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

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

19.2.10 Assurance of completeness for electronic records should also be demonstrated.

20. Checking and review

20.1 General

20.1.1 The forensic unit shall have a procedure for carrying out appropriate checking and review.

20.1.2 For methods that require calculations, including those embedded in spreadsheets, and/or critical data transfers that are not part of a validated electronic process, the procedure shall include a requirement for effective checks of those calculations and/or critical data transfers to be carried out.

20.1.3 Each check or review shall be carried out by someone who has been deemed competent to do so by the forensic unit. The competence should reflect the nature of the activity being checked or reviewed.

20.1.4 Different types of check and their expected applications are as follows:

a. Examination strategy review to assess whether the commissioning party's requirements can be met;

b. Critical finding check, including the manner of initiating the check, with the correct level of independence:

   i. with full sight of the original practitioner's findings (i.e. open); or

   ii. with no sight of the original practitioner's findings (i.e. blind); or

   iii. with no sight of certain aspects of the original practitioner's experience-based findings (see also section 20.2.5).

c. Peer review, an assessment of:

   i. whether the requirements set out by the commissioning party have been met:

   ii. whether the forensic unit's policies and processes have been followed: and

   iii. the logic of the thought processes in the examination, analysis and interpretation of findings and any conclusions made.

d. Administrative checks.

20.2 Critical finding check

20.2.1 A critical finding is an output from a test and/or analysis of an item/exhibit that:

a. has a significant impact on the opinion provided; and

b. cannot be repeated to confirm the finding; and/or

c. a different opinion could be reached by a suitably qualified practitioner in the FSA under consideration.

20.2.2 Generally tests or examinations that do not result in an opinion, such as extraction of data and recovery of suspected forensic traces including body fluids, friction ridge detail and incident scenes, are not critical findings, however the results of tests or examinations that significantly contribute to an opinion are considered critical findings, such as analysis of recovered data, body fluid distribution analysis and comparison of friction ridge detail.

20.2.3 The forensic unit shall have a procedure for carrying out critical findings checks. These may be carried out by suitably qualified individuals who are external to the forensic unit carrying out the work.

20.2.4 Where critical findings checks are carried out, the records shall indicate:

a. the critical finding that has been checked;

b. whether the finding was agreed or not;

c. the name of the checker; and

d. when the checks were performed.

20.2.5 Where an independent check is required, the unit should define and record this level of independence. The requirement for such a check may, for instance, be determined at the identification of end user requirements in the validation study.

20.2.6 The procedure shall ensure that check stages are clear, and whether the check was open or blind.

Open and blind checking

20.2.7 Where findings are fully supported by objective data then the critical finding check may proceed as an open check, i.e. it can be carried out with knowledge of the original finding.

20.2.8 Findings which have a blind check involve a second practitioner providing an independent assessment of the findings in isolation from the original finding to be checked. Checks shall be performed blind when:

a. the critical finding check is the only substantive quality control procedure for checking that finding; and/or

b. the finding or opinion to be checked is based on the experience of the practitioner rather than direct objective data.

20.2.9 Blind checking may require the checker to be aware of contextualisation without the introduction of biasing information. In such a circumstance, the degree of independence of the check carried out shall be identifiable from the records.

20.2.10 The procedure shall detail how casework is identified for blind checking and/or how individual aspects will be presented for checking.

20.3 Peer review

20.3.1 Peer review is an assessment of whether or not the requirements set out by the commissioning party have been met, and the forensic unit's policies and processes have been followed. Peer review is part of the originally commissioned work by the forensic unit.

20.3.2 The forensic unit shall have documented policies and procedures and authorised practitioners for the peer review of case records, including the interpretation and opinions expressed in reports.

20.3.3 If the forensic unit has correctly implemented steps to safeguard against contextual bias with discrete aspects pared off for checking, it may be possible for the same individual to perform both a critical findings check and peer review.

20.3.4 The review shall establish from the case notes, and discussion with the practitioner who carried out the original work, whether or not the work carried out addresses the request made, and the question(s) asked, by the commissioning party and is:

a. appropriate to the requirements of the case;

b. within the competence and experience of the practitioner;

c. fully documented in the case notes, with appropriate checks on critical findings, calculations and other data, including data transfers;

d. in compliance with the forensic unit's documented policies and procedures; and

e. consistent with the contents of the report, including any interpretation or opinions expressed in the report, with any and all limitations declared.

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

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

20.4 Difference resolution

20.4.1 The checking and review process may lead to a difference of opinion between the original and reviewing practitioner.

20.4.2 The forensic unit shall have a documented procedure for resolving that difference and reaching a conclusion in such cases. This could typically involve seeking an independent view from another suitably competent practitioner.

20.4.3 The procedure shall include steps to ensure the obligations in relation to disclosure to the CJS are discharged. This procedure shall include steps to revisit critical findings which safeguard against contextual bias, e.g. blind, as well as the conclusion in the context of the task-relevant information.

20.4.4 Any disagreement shall be recorded and, when possible, a consensus conclusion agreed upon, with reasons declared.

20.4.5 The forensic unit shall have a process in place to resolve differing opinions for the circumstance in which no such consensus can be reached, including how the issue is raised in the expert's report.

20.4.6 The procedure shall include a feedback mechanism for the practitioners involved.

20.4.7 A difference of opinion should not be confused with an error. When an error has been established, either technical or administrative, a non-conformance shall be raised.

20.4.8 **Administrative checks**

20.4.9 The forensic unit shall have documented policies and procedures for the administrative check of case records, including reports.

20.4.10 The administrative check shall establish that the records/reports comply with the forensic unit's policies with regard to administrative content and structure of such records.

20.4.11 The administrative check may be carried out as part of a peer review, or may be carried out separately, prior to delivery to the commissioning party.

20.5 Internal audits

20.5.1 Internal audits are conducted by, or on behalf of, the forensics unit itself for internal purposes, but may be used to give assurance to external bodies. The audit programme shall cover all aspects of the management system. This shall include, but not be limited to:

a. implementation of the management system, including the implementation of methods used in FSAs;

b. records of individual case files; and

c. security and integrity of information and data (sections 26.2.9 and 26.3).

20.5.2 Where the forensic unit undertakes to make statements of opinions and interpretations, the audits shall also include:

a. a review of the process by which these are made; and

b. the competence requirements of the personnel authorised to make such statements.

20.5.3 A risk-assessment based approach should be taken to determine the frequency of the audit schedule, and this should be documented. In any event, methods shall be audited at least once every four-year cycle. The frequency of audits should take account of:

a. the stability of the QMS;

b. the length of time the QMS has been in place;

c. the size of the forensic unit;

d. the complexity of the work being audited;

e. the frequency of use of specific technical methods or procedures; and

f. the potential consequences of non-compliance with the requirements.

20.5.4 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 that support or are utilised in the carrying on of the FSAs that are delivered from that site.

20.5.5 When the results of the audit cast doubt on the effectiveness of examinations or analyses, or the correctness of the forensic unit's results to the extent that

misleading information may have been reported, the forensic unit shall treat the audit result as non-conforming work.

21. Personnel requirements

21.1 General

21.1.1 The forensic unit shall ensure background checks have been completed on all candidates for employment and other personnel in accordance with relevant laws and regulations. These checks shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. The forensic unit shall ensure appropriate security clearance is maintained by all personnel and contractors.

21.1.2 The clearance level required should be defined by the commissioning party, the controller of the data, or the SAI of the commissioning party (where the party and the forensic unit are part of the same organisation) and may be varied in writing. The level of vetting required for prolonged or unsupervised access to case material will be dependent upon the environment. Within policing, for police personnel, a minimum of Recruitment Vetting (RV) will be required as other checks are included. For external personnel who require access to police premises, information or other assets, a minimum of Non-Police Personnel Vetting level 2 full (NPPV2 full) [18] will be required. Outside of policing, those who require prolonged or unsupervised access to case material will normally be expected to be cleared to the National Security Vetting level of Security Check (SC) [19].

21.1.3 The forensic unit shall agree with the commissioning parties the level of background checks required for personnel during the review of requests, tenders and contracts (section 19).

21.1.4 The terms and conditions of employment for all personnel, permanent and temporary, shall contain confidentiality agreements, setting out their own and the forensic unit's responsibility for information security, and details of their expected conduct. 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.

21.2 Standards of conduct

21.2.1 The forensic unit shall have a code of conduct compatible with the standards of conduct provided in part C of the Code. Practitioners shall be made aware how the code of conduct relates to their role in the administration of justice and details of how this was achieved shall be recorded.

21.2.2 Personnel not directly conducting any aspect of an FSA or supporting the delivery of FSAs should be made aware of issues relevant to their role, including access permissions, security, continuity, contamination control, and the information security and confidentiality requirements set out in section 21.1.4. However, there is no requirement for them to be bound by a code of conduct compatible with the standards of conduct.

22. Competence

22.1 General

22.1.1 Competence is defined by the Regulator as the skills, knowledge and understanding required to carry out a role evidenced consistently over time through performance in the workplace. It is the ability to apply knowledge and skills to achieve intended results.

22.1.2 The forensic unit shall determine and document the requirements for achieving initial competence and demonstrating ongoing competence for each role including the competencies required for reporting findings.

22.1.3 The forensic unit shall determine the appropriate competence framework for each role; this should include consideration of the following:

a. education;

b. qualification;

c. training, including statement/report writing and courtroom skills;

d. technical knowledge;

e. skills and experience;

f. an understanding of the requirements for compliance with the Code, the implications of non-compliance, and any mitigations necessary to address non-compliance;

g. the nature of the competence assessment;

h. the frequency of reassessment of competence

i. whether observation of any testing or examinations are required, and if so, the frequency of this; and

j. including material, where relevant to give awareness of:

i. relevant policies and agreements (such as an SLA);

ii. potential threats to confidentially (e.g. security of notes at scenes) and the actions to take to preserve confidentiality;

iii. the distinction between evidence of opinion and evidence of fact; and

iv. issues around cognitive bias and conflict of interest and how to mitigate these and/or how the SOPs seek to control them.

22.1.4 The forensic unit shall have processes in place to address the following:

a. Remedial actions when competence has lapsed or not been demonstrated.

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

i. judicial criticism;

ii. complaints;

iii. criticism by a professional body; and

iv. criticism by the Regulator.

22.2 Competence required for reporting

22.2.1 The forensic unit shall clearly define the competence requirements for carrying on FSAs, and parts of FSAs, including reporting. Where reporting requires interpretations and expressions of opinions, only practitioners authorised by, or on behalf of, the SAI should present such evidence.

22.2.2 Forensic units shall ensure that all practitioners who report factual evidence based on the validated scientific methodology are aware of the following:

a. Whether there is any relevant specialist literature relating to the field.

b. That the scientific principles and methods they have relied on are valid.

c. Where factual reporting in the FSA ends, and where evidence of opinion begins.

d. That they need to be able to demonstrate that any assumptions they have relied upon are reasonable.

e. The impact of the uncertainty of measurement associated with the application of a given method.

22.2.3 Forensic units shall ensure that all practitioners who provide reports have a sufficient level of skill, experience, knowledge 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. Practitioners shall also ensure that they are able to explain their methodology and reasoning, in a way that is comprehensible to a lay person and not be misleading. Such explanations should be concise.

22.2.4 The forensic unit shall consider whether any issues, other than performance against the criteria listed in section 22.2.3, would call into question the credibility of a competent practitioner and take appropriate action. Relevant issues include, but are not limited to, the following:

a. adverse judicial comments;

b. an active compliance notice issued under section 6 of the Act (i.e. one which has not been discharged through a completion certificate relating to any step or steps raised in the compliance notice);

c. adverse findings by the Regulator issued by a route other than by a compliance notice under section 6 of the Act (e.g. issued as section 9 guidance to Crown Bodies); and

d. adverse findings by professional, or other regulatory bodies.

22.2.5 Forensic units shall ensure that all practitioners who provide evidence, including opinion based on their practical experience and/or their professional knowledge, are additionally able to provide, where available (also see the list included in the Criminal Practice Directions 2023 (direction 7.1.2) [11]):

a. an explanation of their methodology and reasoning;

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

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

d. a demonstration that their methodology, assumptions and reasoning have been considered by other practitioners 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 other practitioners, 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) [17]; and

g. the statement of understanding and truth in expert reports for the CJS in England and Wales, as required in the Criminal Practice Directions 2023 (direction 7.2) [11].

22.2.6 The broad range of case circumstances encountered in any discipline of forensic science means that a particular practitioner will have more relevant skill, experience, and expertise in some cases than in others. In order to demonstrate the competence of experts, a system shall be in place that addresses the following:

a. The competence of each expert in each discipline in which they claim expertise, which is thereafter monitored at appropriate intervals.

b. complying with their obligations under Criminal Procedure Rules Part 19.4 (b) and (f) [11]: experts should remain up to date with their knowledge of the scientific literature relevant to their field.

c. Experts should participate in regular evaluation of their expertise [20] [21] through, for example, proficiency tests that are representative of the complexity encountered in casework.

22.3 Competence records

22.3.1 The manner in which competence is developed, achieved, demonstrated and maintained shall be documented, and the forensic unit shall have a policy for retention of training materials, training, and competence assessment records in line with the policy for retention of case files.

22.3.2 If continuous professional development is to be used as part of formal competence assessment, then adequate records shall be kept to evidence that.

22.3.3 Competence records shall be kept in sufficient detail to provide evidence of suitable training and formal competence assessment. These records shall include, but not be limited to:

a. academic and/or professional qualifications;

b. internal/external courses attended;

c. relevant training/retraining received from the forensic unit;

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

e. any substantive accolades or commendations pertinent to skills and experience;

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

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

h. date(s) on which competence and authorisation lapsed or were removed.

23. Environment

23.1 Examination facilities

23.1.1 An examination facility is one where appropriate environmental conditions can be achieved and maintained for the optimum performance of a given technique. Such a facility is not necessarily at a fixed location and may include dedicated

mobile facilities. Incident scenes, vehicle recovery facilities, and ad-hoc examination areas are not considered to be examination facilities in this context (section 90.9).

23.1.2 The examination facilities shall include, as appropriate to the work being undertaken:

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

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

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

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

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

23.1.3 Policies and procedures shall ensure that access to controlled areas, such as item/exhibit storage areas, server rooms, and controlled examination facilities where FSAs or related activities are undertaken, is restricted to authorised personnel.

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

23.2 Non-dedicated work areas

23.2.1 The forensic unit may authorise an FSA or parts of an FSA, including general activities (e.g. report writing, strategy setting) to be performed in a place that is

not dedicated or primarily designed for that purpose (e.g. home/remote working). Activities that form part of the end-to-end process of incident scene examination may be performed at a location other than the incident scene and these are not considered to be non-dedicated work areas, see sections 90.9.2 and 90.9.4.

23.2.2 Prior to authorising implementation, the forensic unit shall consider and record the types of location where the activity is to be conducted and how the security of the information and the integrity and identity of documents, records, and test items/exhibits is maintained before, during, and after examinations or tests have been performed.

23.2.3 A contamination risk assessment (section 23.3.6) shall be used to identify the critical control points and the controls to be maintained and may be used in the authorisation process.

23.2.4 The forensic unit shall document the controls being used for working in non-dedicated work areas, such as clear desk policies, restricting the amount of information held off site, and any mitigation steps the practitioner may need in order to protect information. The forensic unit shall identify how it will assure compliance and/or include within its internal audit [22].

23.3 Contamination risk management

General

23.3.1 Personnel shall receive training in the risks of contamination, how the controls aim to manage risks and their role in contamination risk management.

23.3.2 The forensic unit shall identify activities, including scenes, where personnel are required to provide samples, for inclusion on contamination elimination databases relevant to the nature of the work undertaken in areas they access (e.g. biological material/DNA recovery and analysis, friction ridge detail recovery) and for any results found in casework to be screened against. These databases may be locally or remotely maintained.

23.3.3 Policies and procedures for elimination databases of personnel, 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 forensic units);

h. agreements/consents; and

i. release forms.

Examination facilities

23.3.4 The following requirements relate to contamination controls in controlled examination facilities as defined at 23.1.1.

23.3.5 The forensic unit shall have procedures relevant to the nature of the FSAs undertaken for the prevention, monitoring and detection of contamination that could interfere with testing for the analyte(s) of interest.

23.3.6 The steps in establishing contamination control procedures can combine consideration of controls for trace evidence and data contamination (section 26.1.3). With new methods involving data or digital media, steps in establishing procedures relevant to data contamination control shall include steps a, b and e below, although trace evidence analysis should be conducted first, or all these issues may still apply. For trace material the steps shall include, but not be limited to:

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

b. identifying critical control points in the process where contamination events could occur (e.g. consumable/equipment storage and selection, equipment reuse, transport of items/exhibits, etc.) and for these critical control points:

i. establish acceptable contamination controls at each point;

ii. establish the type and frequency of monitoring; and

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

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

d. establishing requirements for record keeping; and

e. establishing procedures to include acceptance criteria for verifying that the contamination control process remains fit for purpose.

23.3.7 The processes and procedures for the management of contamination for trace material (i.e. not digital data) shall also include, but not be limited to, consideration of the following:

a. Limiting and recording, and if required, preventing access to any areas where FSAs are undertaken where any recent activity by that individual could have an adverse effect on that FSA. Such activity could include, but not be limited to:

i. attendance at related incident scenes;

ii. examination of complainant and/or suspect(s) (e.g. for the purposes of taking samples) in the same case;

iii. processing, management of the movement and transfer of suspects/detainees; and

iv. handling of, or exposure to, relevant materials (e.g. firearms and drugs).

b. Effective separation of incompatible activities to prevent contamination. The extent of physical separation will dictate if objective evidence is needed to demonstrate effectiveness. However, if separation in time is the intention, then the effectiveness of the approach should be demonstrated. Incompatible activities include, but are not limited to, the handling of:

i. unamplified and amplified DNA;

ii. bulk and low-level (trace) drugs activities;

iii. examination of toxicology biological fluid samples and reference drugs, alcohol or noxious substances;

iv. examination of firearms and firearm discharge residues; and

v. examination of accelerant and fire scene debris.

c. Effective separation of the examination of items/exhibits from suspects, complainants and scenes associated with one case or linked cases (for forensic medical examinations see sections 91.6.6 to 91.6.8) .

d. Use of disposable equipment in specified areas and/or performing specific FSAs (e.g. gloves, face masks, mop caps and scalpels).

e. Ensuring equipment is stored in a manner that reduces risk of contamination with analytes relevant to the FSA it is intended for, or likely subsequent FSAs (e.g. DNA, gunshot residue, ignitable liquid residue).

f. Testing and record keeping of consumables and chemicals in all stages of the examination/analytical processes and, where appropriate, testing for specific contaminants that could interfere with the success or interpretation of the examination or test (see also section 29.2.3).

g. Good working practices, such as:

i. protecting items/exhibits in wrapping/containers when not being worked on or used;

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

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

iv. frequent changing of solvent used for rinsing equipment.

h. Good housekeeping practices.

i. Selection and analysis of blank controls.

j. 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.

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

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

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

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

   iv. appropriate training and competence of personnel deployed in cleaning/decontamination processes; and

   v. governance and oversight by senior management.

Incident scenes

23.3.8 The forensic unit shall have policies and procedures to actively manage the risk of contamination occurring at incident scenes such as, but not limited to, management of the risk of contamination from DNA, footwear, particulate trace material, friction ridge detail, and ignitable liquid residues.

23.3.9 In developing appropriate contamination risk management methods for incident scene examination the forensic unit shall;

a. carry out, and document, a risk assessment of the end-to-end process, identifying the critical control points at which there is a contamination risk, such as entering an incident scene or at the point of sampling;
b. identify appropriate measures to manage the risks of contamination occurring at these points, noting that management measures may not be the same at all critical control points or at all incident types/circumstances;
c. define, and document, the contamination management measures, allowing for measures to reflect the contaminant type and the incident type/circumstance; and
d. ensure that policies and procedures include appropriate mechanisms to ensure that contamination control measures are effective at managing the risk (see clause below).

23.3.10 The guidance document on DNA contamination controls at incident scenes, FSR-GUI-0016, contains some examples of how this risk assessment can be

undertaken. The risk assessment of the end-to-end process shall include, but not be limited to:

a. Contamination of/from equipment and consumables;
b. Cross-contamination within and between scenes; and
c. Contamination from practitioners at scenes.

23.3.11 At incident scenes, practitioners shall actively manage the risk of contamination relevant to the examination activities being undertaken and implement contamination control measures that are proportionate to the incident and/or examinations being undertaken and take into account investigative requirements.

23.3.12 Contamination control measures taken shall be documented for all scenes examined.

24. Methods and method validation

24.1 General

24.1.1 All methods for examinations/tests used by a forensic unit shall be fit for purpose; this requires validation data, or verification of existing validation data against the forensic unit's end user requirement and that the unit is competent to perform the examination/test.

24.1.2 Validation is defined here as the process of providing objective evidence that a method or procedure is fit for the specific purpose intended. Validation involves establishing that the method operates in a manner that fulfils the acceptance criteria derived from the end user requirements, that the limitations of the method are properly understood, that the planned use of the method is appropriate, and that the approach to reporting is logical. Validation studies will draw on the existing body of knowledge and scientific research that underpins the test or examination being undertaken.

24.1.3 Verification is defined here as confirmation, through the documented assessment of existing objective evidence or through experiment, that a method is fit (or remains fit) for the specific purpose intended (i.e. the end user requirements).

24.1.4 Confirmation that a method is fit for purpose includes a documented understanding of the risks involved in the use of a method (section 24.6).

24.1.5 Section 11 requires all roles within the forensic unit that have a direct influence on the carrying on an FSA to be defined, this includes competencies specified for method development, validation and verification. Personnel will often be practitioners (i.e. perform the FSA), but may be other personnel who are deemed competent.

24.1.6 The SAI is accountable for the strategic leadership of the forensic unit's compliance with this Code including, but not limited, to approving methods as fit for purpose (section 6). The SAI may delegate authority for signing off the validation or perform the function themselves.

24.2 Selection of methods

24.2.1 This section details the principles of the requirement for methods that are fit for purpose; section 24.3 details the required processes.

24.2.2 Methods shall be documented and controlled, typically as a standard operating procedure or instructions for use.

24.2.3 Even where a method is considered standard and is in widespread use, scientific validity still needs to be demonstrated. If a method validation has not been conducted by the forensic unit, and validation data is available, the forensic unit should follow the adopted methods procedure to demonstrate the method works in its hands.

24.2.4 If a method requires the use of portable equipment (i.e. equipment intended to be used at different locations), the validation study shall include testing any additional quality controls as well as assessing any additional aspects that may impact on the tests or results obtained.

24.2.5 If the implementation plan requires pilot testing of the method in a live environment after the validation study but prior to routine use in casework (e.g. for novel methods), any use by the forensic unit prior to this piloting being completed, i.e. the status of the validation or implementation, shall be declared to the commissioning party and the forensic unit shall disclose this status in any reports. Some restrictions may apply (e.g. see [23]).

24.2.6 External developers or testers of methods or tools are encouraged to conduct their validation exercises in a comparable manner to the requirements set out in this Code, as well as making the SOP and data available, which the forensic unit can review to ensure fitness for purpose as part of the verification to demonstrate suitability when deployed within forensic units' own system (section 24.9 – Plan to demonstrate the validity of a method).

24.2.7 Major breakthroughs, novel uses of existing science or significant changes might warrant wider stakeholder consultations. In these cases, the Regulator should be notified and may advise on the most expedient method of ensuring that the CJS requirements are understood.

Infrequently used methods

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

24.2.9 Methods used no more than once in every three-month period across a forensic unit in separate cases are considered to be infrequently used.

24.2.10 The Regulator may determine that this section on 'Infrequently used methods' will not apply where the risk profile and impact of the work undertaken (for example, in critical national forensic provision) is such that compliance with the relevant sections of the Code for that FSA will apply. In such instances, the Regulator will inform the relevant forensic unit.

24.2.11 All methods used by the forensic unit, including infrequently used methods, shall have been shown to be valid in line with the Code and the practitioner shall demonstrate competence to perform the method prior to implementation or use. The validation, verification, or re-verification shall include the steps in 24.3.8, or review of these steps and, as with all methods, a validation/verification library (section 24.14) is required.

24.2.12 Forensic units shall have a procedure to manage infrequently used methods and their maintenance or use, including the following:

a. How to determine if new methods would be infrequently used and how established methods changing from frequently used to infrequently used will be identified, such as via competency records;

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

c. How competence will be maintained or is demonstrated, either by;

i. regular use of control samples or mock scenes even when casework samples/live scenes are not being analysed or examined; or

ii. re-verification before the examination/analysis in question is performed on a casework sample involving at least the use of an appropriate reference material, followed by replicate examination/testing of the real sample [6].

d. The sign-off procedure for use in casework, including the role of the SAI, or delegate, in the sign-off and justification of method choice.

e. How the status of the method will be described in reports.

24.2.13 If the infrequently used method is accredited, forensic units should discuss with the accreditation body any specific requirements for maintaining accreditation. For example, UKAS requires each aspect of the FSA included in the schedule of accreditation to be assessed at least once within the four-year accreditation cycle. UKAS details its requirements in its policy on accreditation of infrequently performed conformity assessment activities [24].

24.2.14 If the method is not included on the schedule of accreditation, the method shall be re-verified in accordance with the requirements of the Code or (section 24.9.11-24.9.17 as well as ILAC-G19 [6]) should any of the following apply:

a. its last use was more than twelve months ago;

b. any of its component parts have changed.

24.2.15 Provided the forensic unit is acting in accordance with all other relevant sections of the Code and the method not used more frequently than is set out in section 24.2.9, the declaration for infrequently used methods (section 31.3.2b) should be used and the risk mitigation annex should explain why the method remains reliable. If the other aspects of non-compliance against requirements in the Code should also be declared, then the declaration in section 31.3.2c may be more appropriate.

24.2.16 If these activities are to become part of the routine activities of the forensic unit (i.e. used more frequently than once every three months), and the FSA requires it, accreditation shall be sought and declarations shall reflect any non-compliance.

24.3 Demonstrating methods for examination/testing are valid

24.3.1 Methods should be shown to be fit for purpose prior to implementation. This may be performed in its entirety by the forensic unit, or using data provided by the manufacturer or another forensic unit or a third party. The intention is that whether producing objective evidence that the method is fit for purpose or valid, or the forensic unit is verifying data from another source against its end-user requirements, that the documentation addresses all aspects in the validation (i.e. in the validation/verification library).

24.3.2 If the data is provided by a manufacturer, another forensic unit or third-party, then the forensic unit implementing the method shall review the data to determine the adequacy, reliability and relevance to the intended use and the end user requirements (section 24.4).

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

24.3.4 To ensure validation studies relate to the method that will be implemented, there should be a clear boundary between method development and validation. It is important that any significant outcomes indicating any of the acceptance criteria are not met are not corrected for in the method during validation, but that the method is declared to have failed validation. Following such a failure either:

a. the method shall be abandoned; or

b. the method shall be amended (if that is possible while maintaining the required standards), and the validation study evaluated and repeated.

24.3.5 Evaluation of the change may mean the entire validation study needs to be repeated, or that elements of the original study remain suitable to provide objective evidence depending on the nature or, more importantly, the stage of the method that is changed.

24.3.6 If validation needs to be repeated, it should be considered whether using the same dataset or item would risk optimising the method to the validation sample set itself.

24.3.7 If a method is amended during validation, then the validation is invalid. The procedure should include consideration of how to prevent inadvertent re-entering of the development process once validation has started.

24.3.8 Where relevant, the procedure for showing a method is valid shall include, but is not limited to:

a. determining the end user requirements;

b. determining the specification;

c. risk assessment of the method;

d. a review of the end user requirements and specification;

e. setting the acceptance criteria;

f. the plan to demonstrate the method is valid;

g. the outcomes of the validation exercise;

h. assessment of acceptance criteria compliance;

i. report on method validity;

j. statement that the method is valid; and

k. implementation plan.

24.3.9 In certain circumstances an implemented validated method will require a new validation study, such as when:

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

b. deficiencies have become apparent after the method has been implemented; or

c. the end user identifies a change in requirement.

24.4 Determining the end user requirements

24.4.1 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. If the forensic

unit developed the method in-house or is verifying an existing validated method then there may already be end-user requirements to consider. The likely requirements of all end users (e.g. other practitioners, investigators, prosecutors and the CJS) should be considered. To meet the needs of the CJS and the expectations of the court (e.g. Criminal Practice Directions [11]), relevant case law [10] need to be determined.

24.4.2 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.

24.4.3 The Criminal Practice Directions 2023 that supplement Part 19 of the Criminal Procedure Rules [11] should be considered as providing an insight as to the expectations of the CJS end user. These expectations apply regardless of whether the result is evidence of fact or opinion.

24.4.4 The end user requirements shall take account of, as appropriate, the following:

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

b. What the method is intended to deliver to the end user.

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

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

e. What level of quality performance is expected.

f. By what date the method is required for implementation.

24.4.5 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 method will do, not how it will do it.

d. Each requirement specifies in its wording whether it is essential, or desirable and therefore not essential.

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

24.4.6 Where the method is part of a service to be provided to a specified commissioning party, the forensic unit shall inform the commissioning party of the specific method used.

24.5 Determining the specification

24.5.1 A detailed specification shall be written for the method and shall include, where relevant, the technical quality standards (e.g. limits of detection, thresholds for negative and positive controls, quantitation curves/scores). It may be an extension of the end user requirements document or a separate document.

24.5.2 The specification translates the end user requirement from the range of users, drawing in other technical requirements, into what is to be tested in the validation study. It encapsulates what this method is to do, the configuration, and what the method can and cannot be used for.

24.5.3 The list contained in ILAC-G19 (3.10) [6] 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.

24.6 Risk assessment of the method

24.6.1 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 method may be put, the possible impact on the CJS of any errors in the method, associated materials or procedures; and

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

24.6.2 The forensic unit should define the risk assessment method it will use. The methodology recommended in both is based upon process mapping and

identifying the critical control points for the risks or failure modes (e.g. Failure Mode Effect Analysis) at those stages. One process map may be used to cover the whole method against different risks, and may be used to evaluate, or at least identify, potential contributions to uncertainty.

24.6.3 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.

24.6.4 In light of the assessment there may be recommendations for modification of the specification, specific studies to be included in the validation exercise, further evidence to be sought in verification, or additional procedures and/or safeguards that should be implemented. Examples include, but are not 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.

24.6.5 Where items/exhibits provided by an end user, or data derived from these (such as recordings of scenes), are required for the development work or validation, the forensic unit shall obtain prior permission, from those with responsibility for the items/exhibits, scene, and/or data (e.g. the commissioning party or prosecuting authority) for their use and include their use in the risk assessment. Given the risks involved in the use of casework items/exhibits and/or data, the SAI for the forensic unit as the owner of the risk on behalf of the organisation shall be informed of the proposed use and of the risk assessment.

24.6.6 The risk assessment shall be subject to version control and should feed into the statement that the method is valid.

24.7 Review of the end user requirements

24.7.1 The forensic unit shall review the requirements collated to ensure that requirements considered essential/mandatory have been translated correctly

into the specification. Where appropriate or practical, the original contributor of a specific end user requirement may be involved in this review process.

24.7.2 When a review identifies that there are risks, or that there are compatibility, legality, or ethical issues, the forensic unit shall produce a revised end user requirement and/or specification.

24.7.3 The specification shall be subject to change control policies and procedures. Any proposed changes affecting end user requirements shall be subject to review, acceptance and change control of the end user requirements' documentation. Any proposed changes affecting the specification shall be reviewed and accepted before amendment of the specification.

24.7.4 The forensic unit shall ensure that all personnel involved in the development and validation/verification of the method are informed of any agreed changes to the end user requirements or specification so the correct version proceeds to the next stage.

24.8 Acceptance criteria

24.8.1 The acceptance criteria shall be established in advance of the experimental part of the validation study or the review of validation data as part of a verification activity being commenced, and should be:

a. clearly stated; and

b. based upon the specification, the risk analysis and any strategies put in place to control identified risks.

24.8.2 The acceptance criteria shall be used to demonstrate the meeting of the formally accepted specification based on the end user requirements, within measurable and set tolerances, and including any control strategy.

24.9 Plan to demonstrate the validity of a method

24.9.1 The validation or verification of existing validation data against the end-user requirements shall be carried out according to a documented plan. The plan shall be based on the formally accepted specification based on the end user requirements. It shall identify and define:

a. the functional and performance requirements;

b. the relevant parameters and characteristics to be studied or reviewed; and

c. the acceptance criteria for the experimental or review outputs obtained to confirm that the specified requirements for the method or service have been met.

24.9.2 Where indicated by the specification, the 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 or review of existing data is required whether the method is to be used routinely or infrequently (section 24.2.8 - 24.2.16).

24.9.3 Where a validation study is required, or the review of existing validation data prompts additional tests, the study/tests shall be carried out using simulated casework material or mock scenes in the first instance. Subsequently, where possible, permitted and appropriate, this may be with actual casework material or live scenes to confirm its robustness. Legal advice may be required for the use of casework material or use at live scenes where the exemption in relevant legislation 'for law enforcement purposes' may not apply.

24.9.4 The plan should be tailored depending on whether, for example, it is intended for:

a. Validation of measurement-based methods.

b. Validation of interpretive methods.

c. Verification of the validation of adopted methods.

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

24.9.5 A member of personnel with sufficient knowledge of the relevant field under study, and independence from the development of the method, should be responsible for the sign off of the validation plan.

24.9.6 Where this is a plan for the validation of a new method rather than an adopted method (section 24.9.7 – 24.9.17), it is accepted that additional personnel may be needed to provide the required breadth of technical knowledge to evaluate the plan. In such cases these personnel shall be listed in the validation/verification report and their role in supporting the decision for sign-off should be recorded.

Validation of measurement-based methods

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

a. by personnel competent in the field of work under study, who have sufficient knowledge of the work to be able to make appropriate decisions from the findings as the study progresses; and

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

24.9.8 The functional and performance requirements, and the relevant parameters and characteristics for measurement-based methods that shall be considered, include the following:

a. Competence requirements of the practitioner.

b. Environmental conditions.

c. Item/exhibit and/or sample size, and/or size of area to be tested.

d. Item/exhibit and/or sample handling.

e. Consistent, reliable, accurate and robust results, with an uncertainty of measurement.

f. Compatibility with results obtained by other practitioners using different equipment and different methods.

g. Item/exhibit and/or sample homogeneity and/or homogeneity within or between scenes.

h. Ability of the sampling process to provide a representative sample of the item/exhibit and/or area to be tested.

i. Efficiency of recovery of the substance(s) to be identified/measured (i.e. analyte).

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

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

l. Minimum amount of each analyte that can be accurately quantified (if the method is not a qualitative test).

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

Validation of interpretive methods

24.9.9 Though the functional and performance requirements for interpretive methods (such as comparison of marks, handwriting, microscopic comparisons, bloodstain pattern analysis) are less prescriptive than for measurement-based methods, the methods should include testing against representative ground truth data. The validation of interpretive methods concentrates on the competence requirements for the practitioners involved and how the practitioners shall demonstrate that they can provide consistent, reproducible, valid and reliable results that are compatible with the results of other practitioners. This may be achieved by a combination of:

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

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

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

24.9.10 An interpretive method shall require the relevant subset of the parameters and characteristics for measurement-based methods to be determined (section 24.9.8).

Verification of the validation of adopted methods

24.9.11 Verification is defined here as confirmation, through the assessment of existing objective evidence or through experiment, that a method is fit (or remains fit) for the specific purpose intended (i.e. the end user requirements).

24.9.12 Each of the steps of the validation process are to be completed (i.e. as detailed in 24.3.8), whether personnel are producing the objective evidence for relevance, reliability and completeness themselves or objectively reviewing data produced by others.

24.9.13 The end user requirements and specification define the fitness of purpose the verification is intended to be against. If a specification is being adopted from elsewhere, this should be assessed for suitability against the end user requirements and adapted if needed.

24.9.14 The assessment to identify likely risks, or potential risks, to the CJS related to the use of the method or amendment to the method should be included.

24.9.15 If an existing validation study was not conducted by the forensic unit, the forensic unit may verify the validation data against its own end user requirements (see 24.4.4). If the method is to be used in a different way to the original validation study additional evidence may be required to support the validity of the method.

24.9.16 Portable methods, excluding those intended for use at incident scenes, and methods validated to be part of an agreed deployment (sections 97.4.13 – 97.4.15) require a review of the validation study for each location in which the method will be used. The aim of this review is to assess whether the method remains fit for purpose in the new location(s). This is the case even if the validation study was performed by the same forensic unit but the validation was not conducted at the location where the method will be used.

24.9.17 The validation/verification library (section 24.14) shall have, as a minimum, a summary of:

a. the experimental work/review;

b. results;

c. end user requirements and specification used in the review;

d. the risk assessment;

e. practitioner training/competence requirement;

f. assessment plans; and

g. the statement of validation completion.

Verification of the impact of minor changes in methods

24.9.18 Replacing like-for-like equipment or minor changes to a validated method in use by the forensic unit may not always require a full revalidation exercise.

However, the impact of the change shall be risk assessed, verified against the original validation and authorised in line with other validation studies. Replacing the same make and model of equipment may still need some assessment, as minor modifications, including software and firmware, might affect the operation.

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

24.10 Validation outcomes

24.10.1 A summary of the outcome of the exercise to demonstrate the method was valid shall be included in the validation/verification report, which shall be retained for 30 years after the last use of the method (section 11.2 of the National Police Chiefs' Council's (NPCC's) Guidance on Retention, Storage and Destruction of Materials and Records relating to Forensic Examination [15]). A full record of the exercise will usually 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 plan and any subsequent changes to the plan, with justifications and authorisations for the changes;

b. all critical experimental results from the exercise or assessed during the exercise;

c. a detailed comparison of the data generated/reviewed against the specified end-user requirements and specification;

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

e. independent approval and sign off of the method as valid (independent evaluation (point d above), approval and sign off can be carried out by the same member of personnel if competent to do so).

24.11 Assessment of acceptance criteria compliance

24.11.1 The independent evaluation of compliance of the experimental results with specified requirements shall be carried out by personnel not involved in the development of the method or conducting the validation process.

24.11.2 The personnel carrying out the evaluation shall have demonstrated they have sufficient knowledge of the issues involved to be able to identify and assess the significance of any deficiencies. The personnel 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 would need to be able to demonstrate the appropriate level of independence.

24.11.3 The independent evaluation shall typically establish whether the validation work is adequate and has fully demonstrated compliance of the method with the acceptance criteria for the agreed specification and end user requirements.

24.12 Report on method validity

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

24.12.2 The content of the report will depend on the type of work undertaken but as a general guide it should include or make reference to, as appropriate:

a. a title and unique identifier;

b. the end user requirements and the specification;

c. the name, version number and manufacturer of any equipment used;

d. the name(s) and signature(s) of personnel assigned for the development of the validation processes, or when verifying existing validation data the details of the organisation that originally validated the method;

e. the final plan to demonstrate the method is valid;

f. the risk assessment;

g. a summary of the experimental work produced or assessed and outcomes in sufficient detail to ensure that the tests could be independently replicated by competent personnel;

h. details of any review reports produced;

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

j. any limitations/constraints applicable;

k. any related published papers and similar methods in use by the forensic unit;

l. any recommendations relating to the implementation of the method, product or service; and

m. the date of the report.

24.12.3 The forensic unit shall submit the report for review by personnel who are suitably qualified and independent of the validation/verification process; any issues arising should be dealt with expeditiously.

24.12.4 All the records relating to the development and validation of the method shall be archived, together with the means of accessing the records, and retained for 30 years after the last use of the method (section 11.2 of the National Police Chiefs' Council's (NPCC's) Guidance on Retention, Storage and Destruction of Materials and Records relating to Forensic Examination [15]).

24.13 Statement that the method is valid

24.13.1 The forensic unit shall prepare a 'statement of validation/verification completion' on the successful completion of the exercise to demonstrate the method is valid. The aim of the statement of validation completion is to provide a short executive summary of the validation steps performed and key issues identified in the validation, including strengths, weaknesses, and limitations. The intention is that the statement should be no more than two sides of A4 paper in plain language.

24.13.2 The SAI may delegate authority for approving and signing off the method as validated or perform the function themselves. Either way, the scope of the validation being signed off as approved shall be clear.

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

a. caveats about the use of the method;

b. the approved uses of the method, which could be by case type or item/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.

24.14 Validation/verification library

24.14.1 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/verification report, the content of this library shall include, but not be limited to:

a. the specification for the method approved (section 24.5);

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. The literature review also ensures the body of knowledge requirement as outlined in R v Bonython [25] can be demonstrated as well as supporting the application of direction 7.1.2e of the Criminal Practice Directions 2023 [11];

c. the risk assessment for the method approved;

d. the validation plan for the method approved;

e. the report on method validity;

f. the record of approval; and

g. the statement that the method is valid.

24.14.2 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.

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

24.14.4 The information in the library may be disclosable in criminal proceedings and should be prepared with that possibility in mind. ‘Commercial-in-confidence’ does not override disclosure requirements, including those of the Criminal

Procedure and Investigations Act 1996 [9], and a refusal to disclose may prevent methods being used.

24.15 Implementation plan and any constraints

24.15.1 The forensic unit shall have a plan for implementation of methods new to the forensic unit. Where relevant, this plan shall address:

a. whether the new method can provide new analytical opportunities relevant to revisiting old cases. If so, the forensic unit should determine if any action is warranted, such as communicating the benefits and risks to previous commissioning parties (this may be a general communication on the new capability);

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

c. requirements for practitioner training, competence assessment, and ongoing monitoring of practitioner competence;

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

e. the steps required to include the method in the scope of accreditation (if needed);

f. the monitoring mechanisms to be used to demonstrate that the method remains under satisfactory control during its use. The forensic unit will also assist with any post-implementation review, including:

   i. managing planned increases in volume (i.e. any ramp up from validation studies levels), whether through a phased approach or piloting of the validated method using casework;

   ii. controlling changes in workflow.

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 item/exhibit handling/approach at scene and management of contamination risk;

k. the accommodation plan;

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

m. the communication plan; and

n. the schedule for post-implementation review.

25. Measurement uncertainty

25.1.1 A forensic unit performing testing is required to evaluate measurement uncertainty, and where practicable, the effect of components of uncertainty should be minimised.

25.1.2 The forensic unit may undertake testing as part of incident scene examination. ILAC G19:06/2022 [6] includes, but does not limit such testing to, quantitative measurements and presumptive or screening tests [6]. FSAs that involve testing are expected to meet the relevant requirements of ISO/IEC 17025:2017 [3] and/or BS ISO 15189:2022 [5]; this includes, but is not limited to, estimation of uncertainty of measurement (see also ILAC G27 [26]).

25.1.3 Qualitative testing may be for the presence or absence of a defined analyte but there will be uncertainty associated with the underlying test conditions. Where the test method precludes rigorous evaluation of measurement, such as a test that is qualitative in nature, The UKAS M3003 publication ‘The Expression of Uncertainty and Confidence in Measurement’ (appendix N.1.5) [27], states, “Many tests involve some form of examination (or inspection) where the outcome of the test is a nominal property (e.g., colour, shape, species, sequence of markers…). In the case of these ‘qualitative’ tests the concept of measurement uncertainty does not readily apply. But that is not to say that measurement uncertainty doesn't play a role in such tests…in fact, in most cases, such tests are performed under defined conditions that are themselves subject to measurement.”. ILAC G17 [28] indicates that with qualitative testing or examinations, an estimation of the probability for false positive or false negative test results may be relevant. A method of evaluating contributions to

uncertainty may include the method used for risk assessment during the validation of the method (section 24.6.2).

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

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

25.1.6 Guidance on the estimation of uncertainty of measurement is contained in Appendix N of the UKAS M3003 publication 'The Expression of Uncertainty and Confidence in Measurement' [27] and EURACHEM's guide Quantifying Uncertainty in Analytical Measurement [29].

25.1.7 The Criminal Practice Directions 2023 (direction 7.1.2), which supplements Part 19 of the Criminal Procedure Rules [11], include several factors which should be considered in determining the reliability of expert opinion, and especially of expert scientific opinion. However, the following factor that the court may take into account in determining admissibility is particularly relevant:

"7.1.2d 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."

26. Control of data

26.1 General

26.1.1 The forensic unit shall have procedures within its QMS to ensure that information is:

a. recorded accurately;

b. maintained so that its authenticity and integrity is not compromised; and

c. retained and destroyed in accordance with the forensic unit's retention and destruction policy (section 33.1.8) [15] [30] [31] [32].

26.1.2 These procedures should apply within all environments where the FSA is performed or output from it is stored, including remote sites such as authorised home-based working environments.

26.1.3 The forensic unit shall perform a risk assessment around the control of data that should include process mapping to identify critical control stages requiring specific protection steps to prevent loss, degradation and unauthorised access. This risk assessment may occur during method development or method validation. It may be combined with risk assessments looking at risk of contamination. Alternatively, it may be standalone looking at data. The steps included in the risk assessment shall include the following:

a. Identify critical data.

b. Identify critical control points (i.e. places where data is entered, transferred, stored or processed).

c. Identify hazards to be controlled at the critical control points (e.g. data corruption, errors, media loss, unauthorised access, unauthorised manipulation or the practitioner having sight of data extraneous to the stage of the activity, i.e. if there is a risk of cognitive bias in a stage of the FSA). Should it be required and relevant, more detailed guidance about the types of risk is available in ISO/IEC 27001:2022 Information technology – Security techniques – Information security management systems – Requirements [33] and ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection [34].

d. Consider all items/exhibits being examined/analysed related to the FSA which are carrying data, or if wider risk assessment is being performed, all items being examined/analysed.

e. Include technology operated by the forensic unit, such as mobile phones, satellite navigation systems, laptops and cameras.

26.1.4 The forensic unit shall identify mitigation based on the risk assessment to:

a. minimise the risk of data loss;

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

c. control extraneous information;

d. demonstrate that the results are reliable and analytically sound; and

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

26.1.5 In the case of nationally provided and managed services (e.g. Police National Computer) that are outside the control of the forensic unit, the forensic unit shall consider, and document, the risk to the forensic unit and any mitigation introduced to control that risk.

26.1.6 Whilst these clauses indicate forensic units, where the forensic unit is within a larger organisation, achieving or demonstrating compliance may require some liaison with the organisation's Information Security/Technology departments. The SAI is responsible for ensuring compliance with this Code and should be senior enough to ensure support services in larger organisations that are outside the forensic unit's control assist with compliance and/or demonstration of compliance if required (section 22).

26.1.7 More general requirements that also apply for physical items/exhibits are set out in this Code in sections 15 – Document control, 19 – Control of records, 23 – Environment, and in section 29 – Handling of items/exhibits.

26.2 Electronic information capture, storage, transfer, retrieval and disposal

26.2.1 The forensic unit shall establish procedures for the capture and retrieval of electronic information appropriate for the process or method. If the capture or transformation process involves any loss of, or change to that information, this should have been assessed during validation and the acceptance criteria stated (e.g. as defined in the method's end user requirements, specification, or in the method itself).

26.2.2 For the scanning of documents in paper forms, microforms and other forms of information, the forensic unit shall establish procedures and quality control to ensure that any potential information loss as a result of the scanning is within acceptable limits (for further information and guidance see ISO 12653-1:2000, Electronic imaging – Test target for the black-and-white scanning of office documents – Part 1: Characteristics [35]).

26.2.3 Appropriate to the associated FSA, the procedure and policies should ensure that where key information is extracted from pictorial image files, the original images are retained and linked with the captured data, including relevant digital metadata.

26.2.4 Where an electronic document has, for example, embedded files or hyperlinks, all relevant parts of the document shall be stored in line with the forensic unit's retention policy, along with their content.

26.2.5 Critical data should be accessible throughout its period of retention.

26.2.6 When data is migrated from storage media owned or controlled by the forensic unit (i.e. not the submitted item/exhibit) to alternative storage media, the forensic unit shall establish procedures to ensure that all digital objects have been successfully migrated. The digital object and file format of the migrated digital objects should remain unchanged unless such changes are known, have been audited and meet end user requirements.

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

26.2.8 Any compression applied to the archival storage of data/information should be fit for purpose so as not to put into question its data integrity or authenticity. For example, for evidential data this may mean that an assessment is made to test that compression is mathematically lossless.

26.2.9 Data shall be retained according to the forensic unit's retention and destruction policy until such time as that policy determines it should be destroyed (section 39). Destruction or disposal of the data, including the method by which that is achieved, should be recorded within the audit trail for that data.

26.3 Electronic information security

26.3.1 The forensic unit shall have an information security policy that explains how the unit meets its responsibilities outlined in section 26.1. The information security policy shall describe the procedures, based on business and security requirements, as assessed by the forensic unit, for the management of its electronic information. The forensic unit shall ensure procedures are subject to regular testing, audit and review. The testing may be conducted by the forensic

unit's IT provider; however, the responsibility to ensure it occurs and to provide evidence of the testing resides with the forensic unit.

26.4 Access control to electronic information

26.4.1 The forensic unit shall have access control procedures which define how the identification, authentication and authorisation of users will be conducted. Users shall have defined privileges which limit, as far as is practicable, access to only the information and key operational services they require to perform their roles.

26.4.2 When users leave their role or the forensic unit, the forensic unit shall ensure access is amended or removed as appropriate.

26.4.3 Reviews should take place at least every six months to determine whether access rights are still needed; if access rights are no longer needed, they shall be removed.

26.4.4 Users with administrative rights shall use multi-factor authentication (such as second factor or two-factor authentication (see [36])) where this is technically possible.

26.4.5 Accounts with administrative rights shall only be used to perform defined administrative duties (with the exception of evidence handling software applications which require administrative rights for normal operation), and shall not be used for routine access to e-mail or the Internet. The administrative duty may include periodic access to e-mails/or the Internet to download software patches or perform a software update and the risks of this open access should be controlled.

26.4.6 Where network access is under the control of the forensic unit (e.g. not a nationally delivered system), authentication failures should be throttled to 10 attempts in five minutes and locked out where this is practicable (i.e. within the influence of the forensic unit). Access control mechanisms shall be protected to prevent unauthorised system-wide access [37] [38].

26.5 Selection, use and management of passwords

26.5.1 The forensic unit shall have procedures for the selection, use and management of passwords which should be formulated to help users to generate better passwords. The procedures shall include the following:

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

   i. the ‘three random words’ [39] technique for generating suitably complex and memorable passphrases; or

   ii. machine-generated passwords with appropriate facilities to store them, such as password managers [40].

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

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

   i. personal and any work accounts; and

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

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

e. Users should, where technically possible, be directed not to select easily guessed or commonly used passwords [41] and should be prevented from doing so.

f. The system should be designed to protect the password in transit and at rest using appropriate encryption and hashing techniques [38] [42] [43].

g. All default administrative passwords for applications, network equipment and computers shall be changed [38] to meet the requirements identified in this section.

26.6 Protection against malware

26.6.1 The provisions of this section do not apply to evidence handling activities where the use of anti-malware processes have the potential to adversely affect the work. In activities where anti-malware processes are not employed, the forensic unit should implement suitable safeguards against the effect of malware.

26.6.2 Subject to the provisions of section 26.6.1 above, the forensic unit shall have procedures for the detection, removal and/or treatment of malware. These procedures may be based on system design and one or more software packages. The procedures should ensure the detection, quarantine, removal and/or mitigation of the impact malware may have.

26.6.3 Software which is part of the anti-malware system shall be updated when new definitions become available. Such software is to give anti-malware functionality; it might be part of an anti-virus software suite. Anti-malware updates should be included in the forensic unit's change procedures to manage any potential impact to the FSA.

26.6.4 The 'anti-malware system' shall cover 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 [44].

26.6.5 For all devices that access the Internet, the forensic unit shall have (or ensure that its IT provider has) procedures in place to protect from website and e-mail-borne malware caused by drive-by download, phishing attacks or other methods.

26.6.6 The forensic unit should access the Internet via a proxy service which blocks malware. The forensic unit shall have procedures for filtering or blocking phishing e-mails or messages before they reach users.

26.6.7 For all devices that access the Internet, the forensic unit shall have procedures to update (patch) malware software and firmware in a timely manner. This shall be included in the forensic unit's change procedures to manage any potential impact to the forensic examination process. Where this is a managed service, the forensic unit shall have access to the procedure for audit purposes.

26.6.8 'Critical' and 'High' severity patches (as defined by the organisation issuing the 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. Logical separation can include access control lists, network and computer virtualisation, firewalling and network encryption such as Internet Protocol Security (IPSec) [45] [46].

26.6.9 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 (e.g. legacy software is sometimes required to access old media or for revisiting the examination/analysis of old cases).

26.6.10 All removable storage media, including that believed to be new, shall be scanned using the anti-malware system or forensically wiped before use/issue. Optical media (e.g. CDs, DVDs etc), digital tapes (e.g. mini DV, DVC Pro, Digi-8 etc) and analogue tapes (VHS, Hi-8 etc) are considered lower risk and a risk-based quality assurance is acceptable, rather than an absolute requirement to scan all these classes of media.

26.6.11 The forensic unit should securely configure computers by following the End User Device security principles [44].

26.6.12 The forensic unit shall have access to backup data to assist recovery from malware [47] [48].

26.7 Management of removable storage media

26.7.1 Procedures for management of removable storage media used by the forensic unit to transfer data (e.g. memory cards, USB drives, optical media) shall include controls related to issue and their use. These procedures shall include wiping/reformatting of the storage media appropriate to the FSA the media is used in (i.e. typically using a defined secure or forensic method). These procedures are for the general transfer of electronic information and do not relate to item/exhibit and evidence handling.

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

26.7.3 Personal removable storage media shall not be used for the transfer of electronic data; 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 off-site unless its contents are secured using appropriate encryption techniques, excluding storage media used for cameras and video systems which are excluded from encryption [49]; and

c. should be subject to accountability with the aim of tracking use and managing loss [37] [50].

26.8 Segregation of forensic networks

26.8.1 The forensic unit shall have procedures for the segregation of networks used for FSA from other networks. Networks 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. Systems used for different activities may need segregation from each other; e.g. internet intelligence and investigation workstations segregated from systems from other digital forensics activities. Segregation can be achieved physically or 'logically'.

26.9 Backups, recovery and business continuity

26.9.1 The forensic unit shall have procedures for business continuity with an incident management plan that includes backup and retrieval of data, to recover from incidents such as malware (section 26.6.12), theft, fire or hardware failure, whilst ensuring the forensic unit can continue to function.

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

26.9.3 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 needed to meet the requirements of the CJS. 'Offline' means digitally disconnected or fully protected from any malware risk when not in use, and/or designed and tested to remain unaffected through robust protection from malware, should any incident impact the live environment [51].

26.9.4 Offline backups should be stored at a separate and secure location [52] [47]. Ensuring the back-up is adequately protected from the same physical incident that may affect the primary data store, such as fire, explosion or theft, may be achieved through the use of a separate building. However, the risk assessment may detail alternative mitigation to be included in, and tested with, the business continuity/incident management procedure. Reciprocal storage agreements are an option for sole traders.

26.9.5 The forensic unit may use appropriate cloud services for this back-up of electronic information.

26.9.6 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 (sections 26.1.3 and 33).

26.9.7 The forensic unit shall have an incident management plan which helps personnel identify, respond to and recover from incidents as well as continue to run the forensic unit. This may be part of the overall business continuity procedure or a separate IT incident management plan. The incident management plan should include a communication strategy (which includes appropriate escalation levels to the SAI, the Regulator and, if accredited, its accreditation body), roles and responsibilities of personnel and third parties such as service providers and authorities, as well as contact details for those involved.

26.9.8 The forensic unit shall test its business continuity procedure at least once in a four-year cycle (section 12.1.6), but may be more frequent. The incident management plan shall also be tested whether it is part of the overall business continuity procedure or separately, to ensure that its electronic information and critical systems can be recovered in the event of an incident.

26.9.9 Revisions to the incident management plan should include lessons learnt to minimise the risk of disruption to the forensic unit occurring in the same way again [37] [50] [51].

26.10 Network security and mobile working (including home working)

26.10.1 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 forensic unit.

26.10.2 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, or the latest protected access method, and only allow known devices to connect to corporate Wi-Fi services.

26.10.3 Where mobile working is required, the forensic unit shall have procedures for ensuring that connections are identified, authenticated (using multi-factor authentication where possible) 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) [42] [53].

26.10.4 All mobile devices used to carry out any part of an FSA should only have the applications and electronic information required 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 [37].

26.11 Use of cloud-based services

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

a. determine the business need and end user requirements;

b. determine and document the boundary of the cloud and the network perimeter (if the cloud-based services are entirely contained within the

forensic units' own network boundary, all the requirements in this section should be considered);

c. identify what data will be transported, stored and processed, and document the associated risks;

d. evaluate the security of the service offered; and

e. understand the residual risks and how these will be managed.

26.11.2 The forensic unit should use cloud providers that meet the National Cyber Security Centre's cloud security principles [54]. The forensic unit should include within the contract with the cloud-based provider that storage and processing of evidential data using cloud-based services should only be performed from data centres physically located in the UK. The forensic unit should periodically review whether the cloud-based services still meet its business and security needs.

26.12 Security monitoring and situational awareness

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

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

b. Capture authentication and access attempts.

c. Provide asset and configuration information.

26.12.2 All records shall be stored securely so they are safe from tampering and unauthorised access. All records should be stored for a minimum of six months so that they can be used to support incident management [55] [56].

27. Reference collections and databases

27.1.1 Forensic units shall maintain a record of all reference collections and databases (including, but not limited to, those internally developed, commercially developed or remotely accessed) used to:

a. make inferences and interpretation;

b. support the validation of search algorithms, training and proficiency testing in-house (i.e. ground truth data); and

c. support the investigation or control of contamination (e.g. staff elimination databases and/or contamination elimination databases).

27.1.2 Forensic units shall have a process for determining the requirements of the CJS for internally developed reference collections and databases used to make inferences and interpretations or for supporting validation.

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

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

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

a. their purpose;

b. their location and identification;

c. their scope and content;

d. the origin of the data;

e. any known significant limitations or restrictions;

f. the personnel responsible for management of the database;

g. the authorisation and competence requirements to contribute to the database;

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

i. the process for authentication or validation of the data appropriate for its use;

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.

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

28. Equipment

28.1 Computers and related automated equipment

28.1.1 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 outside agencies working on the forensic unit's equipment.

28.1.2 Commercial off-the-shelf software and software tools whose operation has an impact on obtaining results will require validation, or any existing validation to be verified, as laid out in section 24.3.

28.1.3 The forensic unit's procedures shall include what testing or verification is required prior to computers and/or related equipment being returned to service, e.g. when returning from calibration/maintenance or following a move.

28.1.4 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.

28.1.5 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. However, older versions of software may be needed for compatibility with work being undertaken related to older products or to maintain the validated systems' configuration. 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 to ensure the correct version is installed and that no unauthorised modifications have occurred, e.g. by service engineers.

28.1.6 The forensic unit shall have a policy for all items/exhibits or 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.

28.2 Measurement traceability – intermediate checks

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

28.2.2 If the output from measuring or recording equipment (including photographic) is used for evidential purposes, then there should be traceable records related to the calibration/suitability of the equipment used.

29. Handling of items/exhibits

29.1 General

29.1.1 Any actions prior to the forensic unit being requested to attend a scene or the forensic unit taking control of items/exhibits are outside the control of the forensic unit. The forensic unit shall have processes to capture any information provided about the scene or submitted items/exhibits that might have an impact on the examination or subsequent analysis.

29.2 Items/exhibits at a scene

29.2.1 Before items/exhibits are recovered from a scene, the practitioner shall assess the scene and consider on-site conditions and whether necessary competencies are held to ensure effective recovery.

29.2.2 The forensic unit shall ensure that its practitioners are provided with and implement the relevant procedures to mitigate the risk of cross-contamination between different scenes, items/exhibits, suspects, witnesses, and complainants [22].

29.2.3 The forensic unit shall have documented procedures to ensure that items/exhibits recovered from the scene are appropriately:

a. labelled;

b. protected/packaged;

c. preserved;

d. listed on a schedule of recovered items/exhibits;

e. transported;

f. stored;

g. transferred for examination/analysis; and

h. retained, returned or destroyed.

29.2.4 Where a large quantity of potentially evidential material is available and a representative sample needs to be taken for examination/analysis, including for presumptive tests (e.g. simple screening tests for a drug), the practitioner should consider this in the sampling strategy.

29.2.5 The forensic unit shall protect the items/exhibits during processing and delivery to the intended destination, through handling, packaging, storage, and protection, and ensure that practitioners who may subsequently examine or analyse the items/exhibits are aware of anything that may have potentially compromised the items'/exhibits' integrity.

29.2.6 The forensic unit shall ensure that recovered items/exhibits are clearly and uniquely identified within the forensic unit rather than simply within the case e.g. more than a combination of practitioner initials, identity number and date.

29.2.7 The description and location of the item/exhibit within the scene shall be documented, including the use of plans, measurements, diagrams, photography and photogrammetry.

29.2.8 A 'chain of custody' record shall be maintained detailing the location of the item/exhibit at any time, from recovery of items/exhibits. The chain of custody shall detail:

a. all personnel who take possession of the item/exhibit;

b. when such possession was taken;

c. the location of the item/exhibit (e.g. shelf and/or bay location if in storage); and

d. details of when and how the items/exhibits are:

   i. destroyed; or

   ii. released, including to whom.

29.2.9 The forensic unit shall ensure that it is possible to correctly identify every item/exhibit and associate it with the correct case at all times and ensure that no items/exhibits can be confused physically or when referred to in records or other documents.

29.2.10 Items/exhibits generated during scene examination shall be checked against examination notes listing items/exhibits recovered, by someone other than the

practitioner who generated them prior to storage or submission for further examination/analysis. The purpose of this check is to prevent rejection of items/exhibits at a store or forensic unit based on the relevant points listed at 29.2.3.

29.2.11 Forensic units should provide suitable advice to any commissioning party that has access to items/exhibits to assist the commissioning party's understanding of their responsibilities in the control and management of exhibits after forensic units transfer the items/exhibits to them.

29.3 Receipt of cases and items/exhibits at the forensic unit

29.3.1 The forensic unit shall have procedures for the transportation, receipt, handling, protection, storage, retention, and/or disposal of items/exhibits, whilst recording the chain of custody throughout. The procedure for checking and booking in items should include consideration of maintenance of the chain of custody in urgent instances. This is particularly important for cases involving controlled substances/items.

29.3.2 These procedures shall include a documented case acceptance policy which should include a risk-based rejection procedure for the handling of an item/exhibit for examination arising from, but not limited to:

a. a low level of agreement between the details on an item/exhibit label and those on the accompanying submission documentation;

b. inconsistency between the details on an item/exhibit label and/or accompanying submission documentation and what the item/exhibit actually is;

c. illegibility in any information on an item/exhibit label;

d. there being conflicting information on the label(s) on an item/exhibit;

e. repeat of the same identification details on different item/exhibit labels;

f. inadequate, improper or untimely packaging or sealing of an item/exhibit that could prejudice its integrity; and

g. previous handling, storage or evidence of tampering with an item/exhibit that could prejudice its integrity.

29.3.3 If the forensic unit is unable to accept the submission, the reasons for rejection shall be recorded and communicated to the commissioning party in such a manner to facilitate changes to the commissioning party's submission process to minimise similar rejections in future.

29.3.4 The process for receipt of items should include identification of items that could be subject to additional safety and/or security provisions.

29.3.5 Any evidence of tampering with an item/exhibit or suggestion that tampering may have occurred or been attempted, shall be investigated (section 8.1.3). The SAI shall decide the appropriate escalation based on the outcome of the investigation (which may include criminal investigation) and shall notify the Regulator of this investigation at its outset.

29.3.6 The case acceptance procedure shall also specifically address the handling and receipt or rejection of potentially hazardous items/exhibits (e.g. sharps), that might pose a risk to the health or safety of personnel, potentially compromise other work carried out at the forensic unit's facility (e.g. incompatible items such as firearms into a GSR testing facility) or which may not be lawfully retained or handled if accepted by the forensic unit (e.g. human tissue).

29.3.7 It may be during the examination assessment that the submission is rejected, due to one or more of the following:

a. insufficient material being available for meaningful examination or analysis;

b. insufficient material being submitted following sampling of a larger quantity prior to submission to the forensic unit;

c. inappropriate sampling of a larger quantity of material prior to submission to the forensic unit, such that the submitted sample is not representative of the larger quantity; or

d. appropriate control samples not being submitted.

29.4 Item/exhibit handling, protection and storage

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

a. the item/exhibit can, at all times when in the possession or control of the forensic unit, be uniquely identified;

b. any specific measures that might apply given the type of item/exhibit should be identified, e.g. alleged controlled substance, alleged firearm;

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

d. any result can be conclusively linked back to the item/exhibit from which it came, or the key equipment used to create the result;

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

f. there are measures to secure items/exhibits and/or derived material to ensure that they cannot be tampered with or otherwise compromised without detection;

g. only personnel authorised by management shall have access to the retained materials; and

h. movement of material in and out of the facility shall be properly recorded (section 29.1).

29.4.2 The forensic unit shall store the item/exhibit in a manner which prevents or minimises deterioration. This shall include any temporary storage, such as in a vehicle, whilst awaiting transfer to a facility. Temporary storage facilities should also be assessed to ensure that the integrity and security of the item/exhibit is not compromised.

29.4.3 The forensic unit shall, as far as possible, preserve the item/exhibit, or part of the item/exhibit, in its original form to allow for independent re-examination/analysis. If an insufficient quantity of the item/exhibit remains for independent re-examination/analysis or the form of the item/exhibit is altered, the forensic unit shall ensure that details of the item/exhibit in its original form are recorded in sufficient detail for an independent practitioner to be able to check whether the correct procedures and techniques have been used and the validity of any the results.

29.5 Item/exhibit return and disposal

29.5.1 The forensic unit shall have an agreement with its commissioning party for the return or disposal of items/exhibits once the examination/analysis has been completed. Any specific clauses or controls stipulated shall be communicated to any subcontractors or external providers who are authorised to handle the items/exhibits.

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

a. human tissue (Human Tissue Act 2004 [57]);

b. drugs;

c. firearms; and

d. indecent images of children.

29.5.3 Human tissue held by the police or a forensic unit as part of the CJS process is, generally, outside the provisions of the Human Tissue Act 2004 [57] (s39 of that Act). However, it is important that such tissue is managed appropriately; the guidance issued by the Human Tissue Authority is of value in determining appropriate processes. When the tissue ceases to be required for CJS purposes it may become subject to the provisions of the Human Tissue Act 2004 [57]. The codes and guidance issued by the Human Tissue Authority should be considered when such situations arise.

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

29.5.5 If items/exhibits are to be destroyed they shall be destroyed in accordance with health and safety legislation, health and safety regulations, and Home Office guidelines. The following Home Office circulars (HOCs) may be useful:

a. HOC 40/73: Handling and disposal of blood samples in criminal cases (other than those brought under the Road Traffic Act 1972) [58] provides recommendations to Chief Police Officers.

b. HOC 41/73 [59]: Provides similar recommendations to HOC 40/73 [58], but to the courts.

c. HOC 125/76 [60]: Extends the arrangements of HOC 40/73 and 41/73 to the handling and disposal of saliva samples.

d. HOC 74/82 [61]: Extends the arrangements of HOCs 40/73, 41/73 and 125/76 to the disposal of swabs stained with body fluid.

e. HOC 25/87 [62]: Extends the provisions of HOC 74/82 to cover the disposal of urine and any other body samples not previously covered.

29.5.6 The requirements for retention, agreed with the commissioning party, shall also be adhered to.

30. Assuring the quality of results

30.1 Proficiency tests, interlaboratory comparisons and collaborative exercises

30.1.1 The forensic unit shall determine the availability and evaluate the appropriateness of schemes for proficiency tests (PT), interlaboratory comparisons (ILC) and collaborative exercises (CE) that are relevant to its FSAs and, where relevant, its scope of accreditation.

30.1.2 PTs are designed to evaluate the participants' performance, usually against pre-established criteria, whereas collaborative exercises may be used for monitoring performance but are more often designed to address specific issues such as troubleshooting, method validation or characterisation of reference materials [63].

30.1.3 ISO 17043:2023 [64] is the accreditation standard for PT providers and the standard contains recommendations and guidance on the requirements for the operation of PT schemes. A list of those accredited by UKAS can be found on the UKAS website. The European Proficiency Testing Information System [65] or the European Network of Forensic Science Institutes (ENFSI) [66] websites also provide information on the availability of PT schemes.

30.1.4 When selecting a PT provider the forensic unit should consider the following:

a. The competence of a PT provider, e.g.:

i. compliance with the requirements of ISO 17043:2023, such as accreditation;

ii. track record in delivering such schemes;

iii. reliability of the assigned values; and

iv. fitness for purpose of criteria for proficiency assessment.

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

c. Whether the strategies for data collection and examination/analysis applied by the PT provider are suitable for the needs of the forensic unit.

d. Whether the method used for assessing the participants' performance is clearly described by the PT provider and understood by the forensic unit.

e. The PT provider allows the identity of participating forensic units covered by this Code to be made known to the Regulator and this condition shall be set out in any agreement between the forensic unit and the PT provider.

30.1.5 The forensic unit shall use its own methods and procedures to participate in appropriate schemes in order to monitor the validity of its examinations/analyses and its performance, both against its own requirements and against the performance of other forensic units.

30.1.6 Records should include:

a. full details of the examinations/analysis undertaken;

b. results obtained and conclusions arrived at;

c. an indication that performance has been reviewed; and

d. details of any corrective action undertaken.

30.1.7 Where no appropriate PT/CE/ILCs are available, or where no distributions/rounds of appropriate PT/CE/ILC are available, other means such as reference materials and replicate testing as part of their quality assurance should be used.

30.1.8 Unsatisfactory performance in proficiency tests or PT/CE/ILCs shall be considered as non-conforming testing (section 8.1).

31. Reporting the results

31.1 General

31.1.1 The forensic unit shall detail in a procedure its roles and responsibilities in ensuring the appropriate exchange of information and authorisations. This should cover communication of reports (including evaluative reports) with the commissioning party (and as needed by other parties in the CJS), 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.

31.1.2 Any forensic unit-specific requirements for using standardised terminology for reporting on examination /analysis shall be defined; deviations and alternative phraseology from the terminology shall be explained in reports.

31.1.3 The forensic unit shall provide prompt warning of any operational or scientific issues that could affect the timeliness (i.e. substantial delay) of service delivery to the commissioning party (see Criminal Procedure Rules [11] Part 19.2(1)(b)(ii)).

31.1.4 The practitioner shall be competent and comply with all relevant sections of the Criminal Procedure Rules and Criminal Practice Directions 2023 [11]. Where evidence including opinion is provided, the practitioner shall comply with the requirements for evidence of opinion [67] and the applicable obligations on expert witnesses [10]. Reports shall comply with applicable legal provisions. Guidance on the legal obligations and expert report writing can be found on the Regulator's website.

31.1.5 Practitioners called as expert witnesses act as independent advisors to the court and this role creates obligations to the court which override any duty to the commissioning party (or anyone else) [10].

31.1.6 Records shall be kept of work done and the results obtained in line with other retention policies, even if the commissioning party does not require a detailed

report. Documentation of work underpinning reports and statements may be stored separately, provided it can be linked to the correct report/ statement.

31.1.7 The forensic unit shall consider and record whether any action by the Regulator as outlined in section 7 creates an obligation to disclose that action in reports issued by the forensic unit or its practitioners., e.g. an enforcement action conducted under s6 of the Act into the forensic unit or its practitioners (section 7.3).

31.1.8 Reports shall make clear which information forms the basis of the conclusion which is communicated in the report. The forensic unit shall have a process in place for re-evaluating findings and revising conclusions on receipt of new information, including at court.

31.2 Types of report in the Criminal Justice System (CJS)

31.2.1 Forensic units, or practitioners working in forensic units, may be required to provide reports such as oral reports, initial forensic reports (e.g. MG22A) to support an enquiry, interview or a strategy in criminal investigations, or 'reporting' by updating internal database systems. Such reports do not require a declaration of compliance or non-compliance or a defined quality check of the 'reporting' prior to being provided to the commissioning party.

31.2.2 All the following reports require a declaration of compliance or non-compliance with the Code, mitigation in cases of non-compliance in an annex to the report (referred to as annex [x] here) and a defined quality check prior to being provided to the commissioning party; this includes, but is not limited to:

a. Streamlined Forensic Reports (SFR) [68]. 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 (see the Forensic Capability Network's (FCN's) guidance on SFRs [68]).

   i. An SFR1 (MG22B) is a summary of the forensic evidence; it is not a witness statement or an expert report to which the Criminal Procedure Rules Part 19 applies [68].

   ii. An SFR2 (MG22C) is produced to answer an issue(s) raised by the defence in response to an SFR1; it is intended to be presented in evidence, unless a full evaluative report is required instead. If the

SFR2 is providing evidence of opinion, it also requires an expert's declaration under the Criminal Procedure Rules Part 19 [11].

b. Factual reports (e.g. MG22D).

c. Expert reports including opinion evidence also require a declaration under the Criminal Procedure Rules Part 19 and section 7.2 of the Criminal Practice Directions 2023.

d. Certificates (e.g. issued under provisions of the Road Traffic Offenders Act 1988 [69]). The content of a certificate shall comply with the provisions of the statute which created the right to use the certificate. A certificate should include a statement of compliance with this Code where the FSA is subject to the Code, unless the statute prohibits this.

31.2.3 If there is a need to provide results prior to the production of peer reviewed final report, then the provisional status of the report shall be made clear to the commissioning party through the use of appropriate caveats.

31.2.4 Where the forensic unit is commissioned by the prosecution, any further information relevant to disclosure (other than the declaration of compliance with the Code) should be communicated to the prosecutor.

31.2.5 In cases where more than one party wants to introduce expert evidence the court may direct experts to produce a joint statement on matters on which they agree and disagree (Criminal Practice Directions 2023 [11]). Such statements are a matter for the courts and their production is not considered an activity covered by the Code.

31.3 Declarations of compliance and non-compliance

31.3.1 The Code incorporates the FSA definitions (section D1 – FSAs to which the Code applies) so a practitioner will be compliant with this Code only if they also comply with requirements set out in the relevant FSA and any associated FSA specific requirements. For example, if the FSA requires accreditation to ISO/IEC 17025:2017 [3] and inclusion of the Code on the schedule of accreditation, but the practitioner's forensic unit only holds accreditation to ISO/IEC 17025:2017 [3] without including the Code, then the forensic unit is not compliant with the Code and the practitioner must declare this.

31.3.2 All practitioners reporting on FSAs requiring compliance with this part of the Code (i.e. Part B), shall declare compliance with the Code in reports listed in 31.2.2 (except in SFR 1 – section 31.3.4) in the following terms, or in terms substantially the same:

a. I confirm that, to the best of my knowledge and belief, I have complied with the Code of Practice [insert version] published by the statutory Forensic Science Regulator; or

b. I confirm that, to the best of my knowledge and belief, I have complied with the Code of Practice [insert version] published by the statutory Forensic Science Regulator 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 have not complied with the Code of Practice [insert version] published by the statutory Forensic Science Regulator. The details of this non-compliance are included to the best of my knowledge and belief in annex [x], with details of the steps taken to mitigate the risks associated with non-compliance.

31.3.3 Details of non-compliance and mitigating steps given in the annex described as annex [x] above shall address the following issues:

a. Competence of the practitioners involved in the work.

b. Validity of the method employed.

c. Documentation of the method employed.

d. Suitability of the equipment employed (including the approach to maintenance and calibration).

e. Suitability of the environment in which the work is undertaken.

31.3.4 An SFR1 is not a witness statement so an organisational declaration is appropriate, the name may be included, however the contact details should be sufficient to be traceable back to the unit such as by role title (e.g. Fingerprint Bureau Manager at FPBureau@*********).

31.3.5 For SFR1 the declaration may be in the following terms, or in terms substantially the same.

a. [The named forensic unit] has complied with the Code of Practice published by the statutory Forensic Science Regulator [insert issue].

b. [The named forensic unit] has not complied with the Code of Practice published by the statutory Forensic Science Regulator [insert issue] annex [x] details the steps taken to comply with the specific requirements to control risk.

31.3.6 The Regulator may issue guidance on making declarations [70].

31.4 Opinions and interpretations

General

31.4.1 Where opinions and interpretations are part of an FSA which requires accreditation to ISO/IEC 17025:2017 compliance with the UKAS publication LAB 13 [71] is also required and the requirements set out in 31.4.2-31.4.5 below apply. This section does not apply to Incident Scene Examination (INC 100), the Regulator will issue guidance on giving investigative opinions in Incident Scene Examination.

31.4.2 The policies and procedure for interpretation and development of opinions shall be part of the QMS.

a. Validation of interpretive methods shall be according to this Code (section 24.9).

b. The policies and procedures shall require that there is clarity in any report as to the source(s) of data used in forming the evaluative opinion (Part 19 of the Criminal Procedure Rules [11]).

c. Experts providing opinion shall be demonstrably competent to do so (see also section 22.2.3 of the Code).

d. The use of statistical models and any assumptions involved in the interpretation and opinion shall be set out in reports.

e. Processes for the peer review of evaluation shall be part of the QMS.

31.4.3 The expert needs sufficient task-relevant information to select appropriate analyses and interpret the findings from those analyses. Other than that information, the expert does not need, and should guard against seeing, any

non task-relevant information. For example, non task-relevant could include information on previous convictions, reasons unrelated to the scientific examination/analysis (such as why investigators have identified a suspect), and any other extraneous information not relevant to the expert's task [72].

31.4.4 In formulating opinions, the expert shall:

a. consider the questions being asked by the commissioning party in the case and identify the issue(s) that can be addressed; and

b. consider all available, task-relevant information and, where needed, request additional information.

31.4.5 All forms of interpretation involve professional judgement, which is defined as the application of professional knowledge and experience to reach a conclusion or recommendation about a situation.

Evaluative Opinion

31.4.6 Specifically for evaluative opinions, the expert also needs sufficient task-relevant information to determine appropriate propositions.

31.4.7 The expert shall discuss the issues to be addressed and potential propositions with the relevant commissioning party and, where applicable, communicate with the representatives of the other party/parties.

31.4.8 On the basis of the case circumstances and any agreed key issue(s), the following, where they have been put forward by the prosecution and defence (or their representatives), shall be identified:

a. The prosecution proposition(s).

b. The defence proposition(s).

31.4.9 There may be more than two propositions, but the evaluation will, in general, consider the propositions in pairs; each pair shall be mutually exclusive. Evaluative opinion should not be confused with professional judgment which can be exercised in the undertaking all FSAs, professional judgement is defined as the application of professional knowledge and experience to reach a conclusion or recommendation about a situation. Professional judgement involves considering the information, the professional standards, the laws and

the ethical principles that are relevant to the situation. Professional judgement also requires an element of decision-making and problem-solving.

32. Obligations for defence examinations

32.1.1 A forensic unit commissioned by the defence seeking access to material not provided to them by the commissioning body (e.g. teams/exhibits, records or equipment etc) shall advise their commissioning party to obtain approval for access to these from the prosecutor (or if a prosecuting authority is not involved at that stage, from a person with authority over the material).

32.1.2 The forensic unit commissioned by the prosecution shall make available to the forensic unit commissioned by the defence only what has been deemed by the court to be relevant. Copies of such case file records, documents, and supporting information that have been reasonably requested by the forensic unit commissioned by the defence and been authorised for release may then be provided in hard copy or secure electronic form and be taken into their possession for examination away from the premises of the forensic unit commissioned by the prosecution.

32.1.3 In line with the Code, the forensic unit commissioned by the defence shall retain the notes and records it has created. Material supplied by the forensic unit commissioned by the prosecution shall only be used for the specific case(s) for which the material was provided. The forensic unit commissioned by the prosecution may require that supplementary material (such as manuals and standard operating procedures) is returned by the forensic unit commissioned by the defence, or that the supplied copies are destroyed once the case is concluded.

32.1.4 Material supplied by the initial forensic unit is subject to the Data Protection Act 2018 [73] and may be subject to the Police and Criminal Evidence Act 1984 [74] as amended by the Protection of Freedoms Act 2012 (e.g. friction ridge detail and DNA) [75] which requires specific controls for the destruction, retention and use of biometric data.

32.1.5 The forensic unit commissioned by the prosecution shall only release items/exhibits (or evidential material recovered from them) to the defence for examination or testing away from the premises of the forensic unit

commissioned by the prosecution on receipt of written instructions from the prosecutor and/or the court. Where the examinations or testing might affect the condition of the items/exhibits, the forensic unit commissioned by the prosecution shall ensure that the prosecutor and/or the court is made aware of this before the items/exhibits are released and that this is recorded.

32.1.6 The forensic unit commissioned by the prosecution shall ensure that all examinations and testing carried out on its premises by the forensic unit commissioned 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.

32.1.7 The forensic unit commissioned by the prosecution shall ensure that all items/exhibits (or parts of items/exhibits or 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 recorded in writing (e.g. from the court, prosecution, commissioning party). The forensic unit commissioned by the prosecution shall also retain a record, signed by personnel acting on behalf of the receiving party, of the transfers for continuity purposes.

32.1.8 The forensic unit commissioned by the prosecution shall check the integrity and continuity records of the returned items/exhibits, or parts of items/exhibits, or records for compliance, with any conditions of release. Any deficiency in these respects upon return shall be communicated promptly to the prosecutor and the party that commissioned the original examination, e.g. the police.

33. Retention, recording, revelation and disclosure

33.1.1 All practitioners and forensic units shall comply with legal obligations on retention of evidence [15], revelation to the commissioning party and disclosure [10] [75].

33.1.2 The forensic unit shall have a retention policy that ensures that retention of records pertinent to the FSA are maintained for at least the minimum period to fulfil the legal obligations on retention of evidence.

33.1.3 The retention period for records shall satisfy the requirements of legislation, the party commissioning the work [15], and the Code. The retention of records policy shall cover the following:

a. Full records shall be kept of work done and the results obtained in line with other retention policies, even if the commissioning party does not require a detailed report (including any statement).

b. Obsolete/superseded documents, taking into account commissioning party [15], regulatory and legal requirements (section 15).

c. Non-conformities or complaints and the subsequent reviews and outcomes, in line with the case file retention period.

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

e. Training material, training and competence assessment records in line with the policy for retention of case files.

33.1.4 The retention policy shall ensure the retention, return or destruction of items/exhibits (section 29.5) meets the legal obligations placed on the forensic unit or assists, or at least does not interfere with, the commissioning party meeting its legal obligations.

33.1.5 Forensic units can be the commissioning party, with external forensic units acting as sub-contractors or external service providers. The retention requirements for items/exhibits and any copies of items/exhibits should be set out in any contractual agreements and SLAs between the commissioning party and forensic unit being commissioned (section 16).

33.1.6 Original items/exhibits collected or seized by, or submitted to, forensic units should be returned to the commissioning party or nominee, normally as soon as possible after the examination/analysis is complete and/or a case report is issued, except where:

a. they fall within the special provisions, such as being a biohazard, or have other controls stipulated by the commissioning party;

b. they are/were submitted to the National Ballistics Intelligence Service (NABIS); and/or

c. agreement is reached for the forensic unit to retain them, or part of them, under any specified storage conditions, for an agreed and lawful purpose.

33.1.7 The Criminal Procedure Rules place requirements on all parties to the legal case who want to introduce evidence of opinion (see rule 19.3). Rule 19.3(d)(i) requires access to "record of any examination, measurement, test or experiment on which the expert's findings and opinion are based" if requested [11]. However, whilst all material is disclosable if the conditions of the Criminal Procedure Rules are met [11], it is not a general right for access to all information the forensic unit is required to retain, e.g. the standard operating procedure for an FSA would not be considered a record on which an expert's opinion is based.

33.1.8 Forensic units commissioned by the prosecution must comply with the disclosure process and provide the defence access to material identified as relevant by the prosecution [17].

33.1.9 All documents, items/exhibits and material recovered from items/exhibits that are retained by forensic units shall be archived in secure storage, in conditions to prevent damage or minimise deterioration, and indexed so as to facilitate orderly storage and retrieval.

33.1.10 Only personnel authorised by the forensic unit shall have access to the retained materials. Movement of material in and out of the archives shall be recorded.

Part C – Standards of conduct

34. Standards of conduct

34.1.1 The Regulator sets out, for all practitioners carrying on any FSA to which this Code applies (and this Code specifies compliance in the FSA definition), the values and ideals the profession stands for. These standards of conduct provide a clear statement to commissioning parties, the CJS and the public of what they have a right to expect.

34.1.2 As a practitioner undertaking an FSA you shall:

a. recognise your overriding duty is to the court and to the administration of justice [10];

b. act with honesty, integrity, objectivity, and impartiality;

c. comply with the legal obligations imposed on practitioners (and specifically expert witnesses) in England and Wales [10];

d. declare, at the earliest opportunity, any personal, business, financial, and/or other interest or situation that could be perceived as a potential conflict of interest;

e. act and, in particular, provide expert advice and evidence, only within the limits of your professional competence;

f. maintain and develop your professional competence, taking account of material research and developments within the relevant field;

g. inform those commissioning 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 commissioning you;

h. establish the integrity and continuity of items/exhibits as they come into your possession and ensure these are maintained whilst the items/exhibits remain in your possession;

i. seek access to items/exhibits/information that may have a significant impact on the output from your work, particularly any conclusions included

in any report of evidence, and record both the request for the items/exhibits/information and the result of that request;

j. conduct casework using demonstrably valid methods;

k. be prepared to review any casework if any new information or developments are identified that would significantly impact on the output from your work, particularly any conclusions included in any report of evidence;

l. where you have grounds for believing a situation may result in a miscarriage of justice, ensure that the relevant commissioning party is informed either by: (i) 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) (ii) by informing the party directly;

m. preserve confidentiality unless the law obliges, a court/tribunal orders, or a commissioning party explicitly authorises disclosure.

Part D – FSA definitions

35. FSA definitions – general provisions

35.1 General

35.1.1 To avoid considerable repetition in the definitions of FSAs in the FSA specific requirements, this section addresses conditions and provisions which apply generally. The FSA definitions cover activity that is undertaken for a purpose specified in s11(2) of the Act. To achieve this requirement the following general requirements apply to all FSA definitions.

35.1.2 FSAs are defined as discrete forensic science activities.

35.1.3 In general, a forensic unit that is carrying on an FSA is not required to deliver every aspect of the description of the FSA.

35.1.4 A forensic unit that undertakes any part of an FSA is undertaking that FSA, including those to which this version of the Code does not apply.

35.1.5 Specifying activities as FSAs allows the delineation of the remit of the Regulator. It is not intended, by itself, to make any comment on the nature or value of any activity (whether defined as an FSA or not).

35.2 FSAs conducted at incident scenes

35.2.1 ISO/IEC 17020:2012 [4] is a standard for inspection activity and applies to incident scenes because there is a need to take a holistic view to interpreting and examining the scene. Where a forensic unit holds ISO/IEC 17025:2017 [3] accreditation for an FSA in a dedicated facility, the unit could extend the scope of its ISO/IEC 17025:2017 [3] accreditation to include testing at scenes and/or at a location away from the dedicated facility.

35.2.2 Forensic units undertaking FSAs other than FSA - INC 100 at incident scenes shall demonstrate awareness of section 90.7 on the co-ordination of others at an incident scene, for example via inclusion in training.

35.3 Modification of scope

35.3.1 The requirements stated in this version of the Code limit the scope of FSAs to a subset of that which the Act states are FSAs, but future versions of the Code may revise the requirements above and, as a consequence, extend the scope of the FSAs.

35.3.2 This version of the Code includes FSAs to which the Code does not yet apply (section D2). The purpose of including these FSAs is to allow those delivering these activities to prepare in readiness to meet the requirements of the Code when the FSAs are included in future versions.

35.4 Contingency capacity/facility

35.4.1 This section applies where a forensic unit establishes and maintains a facility or capability which is:

a. to be used in the circumstance of a potential future event (such as terrorist events or events causing disruption involving existing facilities);

b. not currently performing any casework which would amount to an FSA; and

c. the work which would be undertaken, if the capacity/facility was brought into use, would amount to an FSA.

35.4.2 In these cases, the preparation and maintenance of the capacity/facility will itself be considered to be carrying on the FSA relevant to the work to be undertaken in the facility/capacity.

36. General inclusions

36.1 General activities

36.1.1 The following activities shall be assumed to be part of the FSA definition unless the contrary is clearly stated in the definition:

a. The following aspects of the handling, continuity and monitoring of any item/exhibit or material relevant to the activities listed in the section:

i. packaging;

ii. labelling;

iii. transportation (covering all transportation whilst the forensic unit is in possession of the item/exhibit);

iv. storage;

v. integrity and security;

vi. retention;

vii. destruction; and

viii. receipting.

b. The preservation, recovery, and/or recording of relevant material from an item/exhibit or scene using such methods as are deemed appropriate for the material under consideration.

c. Where downstream DNA processing is required, DNA anti-contamination handling practices and forensic grade consumables shall be used (sections 29.2, 92.2 and 92.4).

d. The provisions set out in clause a shall also apply to any item/exhibit, material or information taken from, created from or derived from any item/exhibit or material relevant to the criminal investigation, as well as the

recording of and note taking (including general photography) relating to any item/exhibit or scene.

e. In relation to the activities set out in the definition, any of the following aspects of assessment, interpretation and/or reporting:

   i. Case assessment process.

   ii. Determination of the examination strategy.

   iii. Interpretation of the findings to assess/determine the significance in light of the case circumstances/information provided.

   iv. Reporting of the findings of any activities and the interpretation to the commissioning party or the CJS.

   v. Provision of evidence (whether evidence of fact or opinion) in relation to the activities (whether the activities were undertaken by or on behalf of the practitioner/expert providing the evidence).

   vi. Provision of evidence of opinion as to the significance of the findings produced by the activities in the context of the case.

   vii. Provision of any expert advice or evidence in relation to any activities listed in sections i to vi above.

f. The critical findings check and review (section 20).

36.1.2 The provision of any advice related to the use, including potential use and potential contribution, of an FSA to the criminal investigation of a specific matter to a person or body listed in sections 100.6 or 100.7.

36.1.3 The forensic unit, in undertaking any FSA, may need to consider whether other evidence types may be of value, and assess the prioritisation of such evidence types and the impact of any examination on other evidence types. This shall be considered part of the examination strategy in section 17.

36.2 Supporting activities

36.2.1 All work to provide or support the provision of the FSA listed in each definition forms part of that FSA and is subject to the standards specified in the Code.

36.2.2 The activities which are needed for, or support the provision of, the FSA covered in the definition include, but are not limited to, the following:

a. Ensuring all work is undertaken in a suitable environment and that:

   i. the accommodation is constructed and maintained in an appropriate way;

   ii. cleanliness is maintained at a level suitable for the work undertaken;

   iii. appropriate anti-contamination processes are employed;

   iv. where relevant, suitable environmental monitoring is undertaken; and

   v. appropriate security is maintained.

b. Ensuring all equipment employed is fit for purpose, i.e.:

   i. suitable equipment is procured;

   ii. all equipment is subject to appropriate maintenance at pre-determined intervals; and

   iii. equipment is suitably calibrated where required.

c. That appropriate provisions are in place in relation to the following:

   i. physical security of the accommodation;

   ii. security of all IT systems;

   iii. security of information; and

   iv. security clearance and integrity of personnel.

d. That the method is documented.

e. Ensuring that all methods employed have been appropriately validated for use.

f. Ensuring all personnel undertaking work are competent, i.e.:

   i. all personnel undertaking work have sufficient training, qualifications and experience, and have satisfactorily demonstrated that they are able to carry out the work competently; and

   ii. the ability of all personnel to carry out the work to the relevant standards (i.e. competently) is maintained and regularly monitored.

g. Ensuring all reagents and consumables are fit for the purpose for which they are being used.

h. That all collections of information or material (e.g. reference databases) used to assist in the examination, analysis of items/exhibits or the assessment/interpretation of results are fit for purpose.

37. General exclusions

37.1 Use of animals

37.1.1 Any method which is based on the use of non-human animals (e.g. dogs) shall not be considered to form any part of an FSA.

37.2 Covert recovery

37.2.1 Recovery or acquisition of material under authority of any specified parts in the following legislation shall not be considered to form any part of an FSA:

a. The Security Service Act 1989 (any Part) [76].

b. The Intelligence Services Act 1984 (any Part) [77].

c. The Regulation of Investigatory Powers Act 2000 (Part 2 only) [78].

d. The Investigatory Powers Act 2016 (any Part) [79].

37.3 Other exclusions

37.3.1 Additional exclusions are included with the individual FSA definitions in Part D1.

38. Secretary of State approval

38.1 Type approval

38.1.1 Where any statute provides the Secretary of State the power to approve any equipment, or method, for use in circumstances which might fall within the scope of s11 of the Act, the following shall not be part of any FSA:

a. The process by which the Secretary of State determines whether to grant approval.

b. The process by which the Secretary of State determines whether to continue, suspend, or withdraw an existing approval.

c. Any work undertaken by, on behalf of, or commissioned by the Secretary of State to assist in the process of granting, suspending, continuing or withdrawing an approval.

D1 – FSAs to which the Code applies

39. FSA – INC 100 – Incident scene examination

39.1 Definition

39.1.1 The controlled management, interpretation and examination of the location of an incident scene, or other related location (see note), for contact traces, biological and physical material, such that any further testing or examination would be subject to another FSA specified by the Code.

39.1.2 This FSA applies to a practitioner who is commissioned to carry out all or part of the sub-activities defined in this FSA or part of this FSA.

39.2 Required compliance

39.2.1 Compliance with the Code, including the FSA specific requirements in section 90 (Incident Examination), is required from the date the Code comes into force for this FSA or the sub-activities of this FSA that the forensic unit undertakes.

39.2.2 From 6 April 2027, compliance is demonstrated by having accreditation to ISO/IEC 17020:2012 [4], that includes the Code and this FSA or sub-activities including the Incident Examination FSA specific requirements (section 90) of this FSA that the forensic unit undertakes on the schedule of accreditation.

39.2.3 This FSA does not distinguish between activities performed at volume and major incident scenes and compliance for activities undertaken at all the incident types relevant to the forensic unit is required.

39.2.4 Where activities performed at an incident scene are specified in another FSA, these may be performed under the accreditation standard required by that FSA, provided it is appropriate for the type and extent of activity performed at the incident scene.

39.2.5 RG 201 ‘UKAS accreditation of bodies carrying out incident scene examination’ does not apply to this FSA.

39.3 Sub-activities

39.3.1 The following sub-activities are considered to constitute 'Incident scene examination':

a. Forensic scene management, including but not limited to:

i. scene assessment and control;

ii. setting of an examination strategy, including joint examination strategies where necessary;

iii. coordination of activities at the incident scene;

iv. management of other practitioners and activities; and

v. interpretation of the incident scene(s).

b. Examination of surfaces and items and recovery of items, such that further testing or examination that is specified as an FSA in the Code can be undertaken.

39.4 Note

39.4.1 In this FSA the term 'location' means the following:

a. a location where an incident is known or suspected to have occurred; and/or

b. a location where an item relevant to the incident is located (e.g. a body or vehicle).

39.4.2 Such locations may be:

a. owned, occupied or under the control of a person of interest (e.g. complainant or suspected/accused person);

b. related to the incident but not the primary location of interest (e.g. a familial address);

c. a vehicle, unless the vehicle was recovered solely for the purpose of collision investigation, in which case FSA – INC 101 – Collision investigation (section 75) applies. Note that a vehicle could also be examined as an exhibit rather than a scene; or

d. a fire or explosion scene, unless the examination of the fire or explosion scene is solely for the purpose of establishing the origin or cause of a fire or explosion, in which case the relevant FSAs apply (FSA – INC 102 – Examination of fire scenes (section 76) and FSA – INC 103 – Examination to establish the origin and cause of an explosion (section 77)).

39.4.3 Where activities that are specified as other FSAs are performed at an incident scene, those FSAs apply, e.g. FSA – DIG 100 - Data capture, processing and analysis from digital storage devices (section 70), FSA – MTP 602 – Firearms: ballistics (section 67) or FSA – BIO 201 – Human biological material distribution and interpretation(section 42).

39.5 Exclusions from this FSA and the Code

39.5.1 The following do not fall within the definition of 'Incident scene examination' and are not covered by the Code:

a. Evidence collection that does not include a wider assessment or interpretation of the scene, e.g. the recovery of identification documents from a location by a police officer or large-scale searching activities by specialist search teams.

b. Activity undertaken to protect/preserve items/exhibits from imminent alteration or destruction by persons not specifically commissioned to carry out an FSA as specified in the Code, e.g. first responders.

40. FSA – BIO 100 – Forensic medical examination of complainants

40.1 Definition

40.1.1 The recovery of items and/or samples believed to be relevant to an alleged sexual offence from a complainant in a dedicated facility.

40.2 Required compliance

40.2.1 Compliance with the Code, including FSA specific requirements in Forensic medical examination of sexual offence complainants undertaken in a Sexual Assault Referral Centre - (section 91), is required.

40.2.2 Compliance is demonstrated by having accreditation to ISO 15189:2022 [5] with the Code and this FSA or the sub-activities of this FSA that the organisation undertakes, on the schedule of accreditation.

40.3 Sub-activities

40.3.1 The following sub-activities are considered to constitute 'Forensic medical examination of sexual offence complainants':

a. Physical examination of an individual for biological and trace material which may be evidence or give rise to evidence in an alleged offence under investigation:

   i. 'Recording of information' may include the use of image capture devices (including colposcopes) for specialist image capture/photo-documentation in general and intimate images, and/or the use of body diagrams/maps to record the presence, location and measurements of injuries and marks, or the apparent absence of injuries and marks.

   ii. Material believed to be biological or non-biological (which includes particulate trace material).

b. Recovery of items. This includes obtaining blood and urine samples, and DNA buccal/hair samples and recording findings and information to enable body fluid distribution analysis and/or interpretation.

Sub-activities not required to be included in accreditation scope

40.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Examinations conducted in a custodial unit (e.g. Custody), off-site examinations (e.g. in emergency departments, residential care homes and mobile units) and in temporary facilities used whilst build or upgrade of a permanent facility is in progress.

b. For these locations the risks and mitigations taken to minimise potential contamination shall be identified and documented.

40.4 Exclusions from this FSA and the Code

40.4.1 The following do not fall within the definition of 'Forensic medical examination of sexual offence complainants' and are not covered by the Code:

a. An examination to determine whether someone is fit to be interviewed and/or examined.

b. The activities of an individual other than the practitioner, who is taking steps to protect/preserve or collect evidence.

c. Clinical assessment, medical diagnosis, prescribing treatments/medicines and the provision of medical care, including treatment of injuries (general and specific, such as injuries sustained by female genital mutilation).

d. Examination of a deceased person.

41. FSA – BIO 200 – Human biological material examination and testing

41.1 Definition

41.1.1 The examination and testing of human biological material.

41.2 Required compliance

41.2.1 Compliance with the Code, including sections 92.3 to 92.5.2– Human DNA examination and analysis, is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and this FSA or sub-activities of this FSA listed in section 41.3 that the organisation undertakes on the schedule of accreditation.

41.3 Sub-activities

41.3.1 The following sub-activities are considered to constitute 'Human biological material examination and testing':

a. Visual examination, including with the use of light sources of an appropriate wavelength, automated devices, and microscopic examination.

b. Presumptive and/or confirmatory testing, including microscopy, for the location and/or identification of biological material.

c. Chemical enhancement of non-visible biological material such as blood.

d. Differentiation of human and animal hairs.

e. Recovery of biological material from items and surfaces for further testing or examination.

f. Assessing the significance of results of examination and testing, including reporting presence or absence of biological material at factual and source-level only (section 41.3.2).

Sub-activities not required to be included in accreditation scope

41.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Attribution of a DNA profile to specific biological material.

b. Examination to determine somatic origin and/or ethnicity of hair.

41.4 Note

41.4.1 Activity level interpretation does not fall within the definition of this FSA and is subject to FSA – BIO 201 - Human biological material distribution and interpretation (section 42).

41.4.2 Where downstream DNA processing is required, DNA anti-contamination handling practices shall be used (sections 18.1, 23.1 and 92 to 92.5.1).

41.4.3 The sub-activities may apply to mixtures of more than one biological material.

41.4.4 Relevant sub-activities may be undertaken under this FSA or FSA – INC 100 - Incident scene examination, as appropriate (section 41.3).

41.4.5 The following do not fall within the definition of 'Human biological material examination and testing' but are the subject of a different FSA definition:

a. FSA – INC 100 – Incident scene examination (section 39).

b. FSA – BIO 201– Human material distribution and interpretation (section 41).

c. FSA – BIO 202 – Human DNA analysis (section 43).

42. FSA – BIO 201 – Human biological material distribution and interpretation

42.1 Definition

42.1.1 The interpretation of biological material with consideration to its appearance, location, size/extent, and/or morphology for the purpose of providing opinion at the activity level.

42.2 Required compliance

42.2.1 Compliance with the Code, including section 93 – Bloodstain pattern analysis for sub-activity 'a', is required.

42.3 Sub-activities

42.3.1 The following activities shall be considered to constitute 'Human biological material distribution and interpretation':

a. Bloodstain pattern analysis.

b. Time since intercourse analysis.

c. Interpretation of the size/extent, location and/or morphology of biological material, such as but not limited to, blood, semen, saliva, vaginal material and cellular material, including with the use of computer-assisted methods.

d. Examination of digital material such as images, video, and/or 3D modelling for the purpose of undertaking human biological material distribution and interpretation.

42.4 Note

42.4.1 Where downstream DNA processing is required, DNA anti-contamination handling practices shall be used (sections 18.1, 23.1 and 92 to 92.5.1).

42.4.2 This FSA includes consideration of issues relating to transfer, persistence, prevalence and recovery.

42.4.3 This FSA applies when the relevant sub-activities are undertaken at an incident scene.

42.4.4 The following do not fall within the definition of ‘Human biological material distribution and interpretation’ but are the subject of a different FSA definition:

a. FSA – INC 100 – Incident scene examination (section 39).

b. FSA – BIO 200 – Human biological material examination and testing (section 41).

c. FSA – BIO 202 – Human DNA analysis (section 43).

43. FSA – BIO 202 – Human DNA analysis

43.1 Definition

43.1.1 The use of DNA methods applicable to human biological material to determine the potential source(s).

43.2 Required compliance

43.2.1 Compliance with the Code, including section 92 – Human DNA examination and analysis, is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3] or ISO 15189:2022 [5], with the Code and this FSA or the sub-activities of this FSA that the organisation undertakes on the schedule of accreditation.

43.3 Sub-activities

43.3.1 The following sub-activities are considered to constitute ‘Human DNA analysis’:

a. Extraction, purification, and, where applicable, quantification of DNA, including the use of PCR and fragment separation (e.g. by electrophoresis). Note that DNA quantification is not required for reference samples (including hairs, liquid blood and buccal swabs).

b. Sequencing of DNA and production of autosomal DNA/haplotype profiles.

c. Profile interpretation, including designation and comparison for single source and DNA mixtures.

d. Statistical analysis up to and including the point of generating a likelihood ratio.

e. Quality assurance checks, including batch contamination checks, checks against DNA elimination databases, profile designation and sample switch checks.

f. Use of reference and population databases (section 27).

g. Submitting permitted profile results to DNA databases.

43.4 Note

43.4.1 The following do not fall within the definition of 'Human DNA analysis' but are the subject of a different FSA definition:

a. FSA – BIO 201 – Human material distribution and interpretation (section 42).

b. FSA – BIO 203 – Human kinship analysis (section 44).

c. FSA – BIO 301 – Non-human biological examination and analysis: vertebrates (section 45).

44. FSA – BIO 203 – Human kinship analysis

44.1 Definition

44.1.1 The use of DNA analysis to determine the biological relationship from within a closed set of individuals.

44.2 Required compliance

44.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3] or ISO 15189:2022 [5], with the Code and this FSA or sub-activities of this FSA that the organisation undertakes on the schedule of accreditation.

44.3 Sub-activities

44.3.1 The following sub-activities are considered to constitute 'Human kinship analysis':

a. Outputs from autosomal, haplotype and/or mitochondrial technologies used to conduct paternity and/or biological relationship analysis.

b. Profile/sequence designation and comparison.

c. Statistical analysis, including the use of population reference databases (section 27).

d. Quality assurance checks, including designation checks, pedigree build, reference data used and calculations.

e. Submitting permitted results to DNA databases.

f. Identification in criminal incidents using DNA kinship analysis.

44.4 Note

44.4.1 The following does not fall within the definition of 'Human kinship analysis' but is the subject of a different FSA definition:

a. FSA – BIO 202 – Human DNA analysis (section 43).

44.5 Exclusions from this FSA and the Code

44.5.1 The following do not fall within the definition of 'Human kinship analysis' and are not covered by the Code:

a. Disaster victim identification (natural disasters).

b. Civil paternity.

45. FSA – BIO 301 – Non-human biological examination and analysis: vertebrates

45.1 Definition

45.1.1 Examination and analysis of non-human vertebrate material to determine the species and/or the potential source of the material.

45.2 Required compliance

45.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code, and the sub-activities of this FSA listed in section 45.1.1 that the organisation undertakes on the schedule of accreditation.

45.3 Sub-activities

45.3.1 The following sub-activities are considered to constitute ‘Non-human biological examination and analysis: vertebrates’:

a. DNA analysis for species identification, individual profiling and pedigree analysis, including:

i. recovery of DNA;

ii. extraction and purification of DNA, including, but not limited to, the use of polymerase chain reaction (PCR) (dependent on the investigative question) and electrophoresis;

iii. processing of a PCR result, including sequencing and genotyping (depending on the test applied); and

iv. comparison and interpretation, including use of reference databases (section 27) and statistical analysis.

Sub-activities not required to be included in accreditation scope

45.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Morphological examination of relevant material to determine species or the potential source of non-human material.

b. Macroscopic, microscopic, and immunological tests to determine the species.

45.4 Note

45.4.1 In this FSA, non-human vertebrate material refers to any part of a vertebrate, including tissue, hair, skin, teeth, bone, scales, feathers and processed products such as traditional medicines.

45.5 Exclusions from this FSA

45.5.1 The following do not fall within the definition of ‘Non-human biological examination: vertebrates’ and are not covered by the Code:

a. Analysis to determine geographical provenance of non-human vertebrate material.

b. The anthropological examination of bone and teeth determine whether material is human or non-human.

c. The activities of an individual other than the practitioner, who is taking steps to protect/preserve or collect material for analysis.

46. FSA – BIO 500 – Taggant analysis

46.1 Definition

46.1.1 The analysis of known reference taggants used to mark items of property, assets, or items marked during the deployment of a taggant marker system, and comparison with taggants from a known deployment or a database to determine where the taggant was deployed.

46.2 Required compliance

46.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and this FSA or sub-activities of this FSA that the organisation undertakes on the schedule of accreditation.

46.3 Sub-activities

46.3.1 The following sub-activities are considered to constitute ‘Taggant analysis’:

a. analysis and identification of the taggant, including use of reference databases (section 36.2.2h); and

b. evaluation of results.

46.4 Exclusions from this FSA and the Code

46.4.1 The following do not fall within the definition of ‘Taggant analysis’ and are not covered by the Code:

a. manufacture and performance of taggants; and

b. locating and recovery of taggants.

47. FSA – DTN 100 – Toxicology: analysis for drug(s), alcohol and/or noxious substances

47.1 Definition

47.1.1 Analysis of human biological material to determine the presence of drug(s), drug metabolites, alcohol, and/or noxious substances (including poisons) or their metabolites, and if relevant, the concentration of the drug, alcohol or noxious substance and/or metabolites.

47.1.2 This section applies whether or not the person was alive at the time the material was separated from the body or body part.

47.2 Required compliance

47.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3] or ISO 15189:2022 [5], with the Code and the sub-activities of this FSA listed in section 47.3 that the organisation undertakes on the schedule of accreditation.

47.2.2 Lab 51 ‘UKAS accreditation of laboratories performing analysis of toxicology samples’ may apply to this FSA.

47.3 Sub-activities

47.3.1 The following sub-activities are considered to constitute ‘Toxicology: analysis for drug(s), alcohol and/or noxious substances’:

a. Analysis (whether qualitative or quantitative) of material believed to originate from a human body (or part thereof) for any drug, alcohol or noxious substance (including poison) or their metabolites.

b. Any analysis which is required in connection with or to assist in understanding of the findings. Examples include, but are not limited to, analysis to determine the concentration of preservatives in any sample.

c. Classification/identification, including use of reference databases as relevant (section 27).

Sub-activities not required to be included in accreditation scope

47.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Consideration of any of the following areas:

i. Effect (or possible effect) in general terms of any drug(s), alcohol or noxious substance(s) (including poisons) on an individual.

ii. Manner in which the concentration of any drug(s), alcohol or noxious substance(s) (including poisons) varies in an individual with respect to absorption, distribution, metabolism, elimination, tolerance and/or degradation.

iii. Interpretation of drug concentrations with respect to abuse/therapeutic/toxic/fatal levels.

47.4 Note

47.4.1 The following do not fall within the definition of 'Toxicology: analysis for drug(s), alcohol, and/or noxious substances' but are the subject of a different FSA definition:

a. FSA – DTN 101 – Toxicology: analysis for drugs and/or alcohol under the Road Traffic Act 1988, Transport and Works Act 1992, and Railways and Transport Safety Act 2003 (section 48).

b. FSA – DTN 102 – Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988 (section 49).

c. FSA – DTN 103 – Examination and analysis to identify and quantify controlled drugs and/or associated materials (section 50).

47.5 Exclusions from this FSA and the Code

47.5.1 The following do not fall within the definition of 'Toxicology: analysis for drug(s), alcohol and/or noxious substances' and are not covered by the Code:

a. Analysis of breath for alcohol for road traffic law purposes by any of the following:

i. a type-approved roadside screening device; or

ii. a type-approved instrument for evidential purposes.

b. Analysis of any bodily material for any drugs (other than alcohol) for road traffic law and transportation safety purposes, as long as the results shall not be used as the primary evidence of the concentration of any drug found in the CJS, by any of the following:

i. a type-approved roadside screening device; or

ii. presumptive drug tests at roadside.

c. Provision of any evidence in relation to whether a particular compound (or group or class of compounds) is a psychoactive substance in relation to the provisions of the Psychoactive Substances Act 2016 [80].

48. FSA – DTN 101 – Toxicology: analysis for drugs and/or alcohol under the Road Traffic Act 1988, Transport and Works Act 1992, and Railways and Transport Safety Act 2003

48.1 Definition

48.1.1 Analysis of blood and/or urine for the detection and quantification of drugs, drug metabolites, and/or alcohol in relation to s4 of the Road Traffic Act 1988 [81], s5 of the Road Traffic Act 1988, s27 of the Transport and Works Act 1992 [82], s28 of the Transport and Works Act 1992, s78 of the Railways and Transport Safety Act 2003 [83], and/or s92 of the Railways and Transport Safety Act 2003.

48.2 Required compliance

48.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3] or ISO 15189:2022 [5], with the Code and the sub-activities of this FSA listed in section 48.3 that the organisation undertakes on the schedule of accreditation.

48.2.2 Lab 51 ‘UKAS accreditation of laboratories performing analysis of toxicology samples’ may apply to this FSA.

48.3 Sub-activities

48.3.1 The following sub-activities are considered to constitute 'Toxicology: analysis for drugs and alcohol under the Road Traffic Act 1988, Transport and Works Act 1992, and Railways and Transport Safety Act 2003':

a. Analysis of a blood or urine sample to determine the presence, and where relevant, the concentration, of any drug (and/or drug metabolite) and/or alcohol with the intention that the results be used in an investigation or prosecution (the use in a prosecution includes use by the defence) under:

   i. s4 of the Road Traffic Act 1988 [81];

   ii. s5 of the Road Traffic Act 1988 [81];

   iii. s27 of the Transport and Works Act 1992 [82];

   iv. s28 of the Transport and Works Act 1992 [82];

   v. s78 of the Railways and Transport Safety Act 2003 [83]; or

   vi. s92 of the Railways and Transport Safety Act 2003 [83].

b. Any analysis which is required in connection with or to assist in understanding of the above.

c. Classification/identification, including use of reference databases (section 27).

d. Consideration of whether, in a given time frame, the concentration of a drug exceeded a legal limit.

Sub-activities not required to be included in accreditation scope

48.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Consideration of whether the drug and/or alcohol may have had an effect on the behaviour or abilities of the individual from whom the sample was taken.

48.4 Note

48.4.1 The following do not fall within the definition of 'Toxicology: analysis for drugs and alcohol under the Road Traffic Act 1988, Transport and Works Act 1992,

and Railways and Transport Safety Act 2003' but are the subject of a different FSA definition:

a. FSA – DTN 100 – Toxicology: analysis for drug(s), alcohol and/or noxious substances (section 47).

b. FSA – DTN 102 – Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988 (section 49).

c. FSA – DTN 103 – Examination and analysis to identify and quantify controlled drugs and/or associated materials (section 50).

d. FSA – DTN 104 – Toxicology: alcohol technical calculations (section 81).

48.5 Exclusions from this FSA and the Code

48.5.1 The following do not fall within the definition of 'Toxicology: analysis for drugs and alcohol under the Road Traffic Act 1988, Transport and Works Act 1992 and Railways and Transport Safety Act 2003' and are not covered by the Code:

a. Testing of a suspect by a police officer using type-approved roadside equipment.

b. Testing of a suspect by a police officer using type-approved evidential breath alcohol equipment.

49. FSA – DTN 102 – Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988

49.1 Definition

49.1.1 Analysis of blood and/or urine for the detection and quantification of drugs in relation to s5A of the Road Traffic Act 1988 [81].

49.2 Required compliance

49.2.1 Compliance with the Code, including the FSA-specific requirements in section 94 – Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988**.** Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3] or ISO 15189:2022 [5] with the Code; this FSA or the sub-activities of this FSA that the organisation undertakes; as well as the FSA-

specific requirements in section 94 (analysis for drugs in relation to s5A of the Road Traffic Act 1988).

49.2.2 Compliance with this FSA and FSA-specific requirements is required by 6 April 2026.

49.2.3 Lab 51 ‘UKAS accreditation of laboratories performing analysis of toxicology samples’ does not apply to this FSA.

49.3 Sub-activities

49.3.1 The following sub-activities are considered to constitute ‘Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988’:

a. Analysis of a blood or urine sample for detection of drugs in relation to offences under s5A of the Road Traffic Act 1988 [81] to determine the presence and/or concentration of any drug subject to a specified limit under The Drug Driving (Specified Limits) (England and Wales) Regulations 2014 (as amended) [84].

b. Analysis to determine whether the concentration of the relevant drug is above the specified legal limit.

c. Consideration of factors that might impact on uncertainty of the results, the potential impact of the uncertainty and the determination of whether the sample was above the specified legal limit.

d. Any analysis which is required in connection with or to assist in understanding of the findings obtained from the work activities above.

e. Classification/identification, including use of reference databases (section 27).

49.4 Note

49.4.1 The analysis of blood and urine samples for s5A of the Road Traffic Act 1988 [81] shall be specifically listed in the scope of accreditation.

49.4.2 A forensic unit should have the drugs it analyses for in relation to s5A [81] listed in the relevant section of its scope: (a) by the date the Code comes into force; or (b) a limit being established for that drug in the jurisdiction within which the laboratory operates. The forensic unit is responsible for ensuring those

commissioning its services in relation to s5A [81] are aware of the drugs which will be analysed for either in general or in any sample where the general provisions are not applicable. The date on which limits were first established for each drug are provided in FSA specific requirements section 94.

49.4.3 The following does not fall within the definition of 'Toxicology: analysis for drugs under s5A of the Road Traffic Act 1988' but is the subject of a different FSA definition:

a. FSA – DTN 101 – Toxicology: analysis for drugs and/or alcohol under the Road Traffic Act 1988, Transport and Works Act 1992, and Railways and Transport Safety Act 2003 (section48).

49.5 Exclusions from this FSA and the Code

49.5.1 The following does not fall within the definition 'Toxicology: analysis for drugs under s5A of the Road Traffic Act 1988' and is not covered by the Code:

a. Testing of a suspect by a police officer with type-approved roadside testing equipment.

50. FSA – DTN 103 – Examination and analysis to identify and quantify controlled drugs and/or associated materials

50.1 Definition

50.1.1 Examination, analysis, quantification and legal classification of controlled drugs, psychoactive substances and/or associated materials.

50.2 Required compliance

50.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and this FSA or sub-activities of this FSA that the organisation undertakes on the schedule of accreditation.

50.3 Sub-activities

50.3.1 The following sub-activities are considered to constitute 'Analysis to identify and quantify drugs and/or associated materials':

a. Separating the item into sub-items based on the uniformity of the contents, as appropriate.

b. Measuring the quantity of the drug/material.

c. Selecting a portion of the submitted drug/material for analysis.

d. Examination and recovery of traces of a relevant substance or associated material.

e. Analysis of any drug/material to determine whether it contains or is a relevant substance or associated material.

f. Classification/identification, including use of reference databases (section 27).

g. Quantification of the proportion of drug/material which is a relevant substance ('purity') where appropriate.

h. Providing the legal classification of any relevant substances according to the Misuse of Drugs Act 1971 (as amended) [85] and/or the Psychoactive Substances Act 2016 [80].

50.4 Note

50.4.1 In this section the term 'relevant substance' means anything falling within the descriptions below:

a. any substance which is listed (by name or under a generic definition due to its chemical structure) in Schedule 2 of the Misuse of Drugs Act 1971 (as amended) [85]; and/or

b. any substance which is a psychoactive substance within the provisions of the Psychoactive Substances Act 2016 [80].

50.4.2 In this section the term 'associated material(s)' includes cutting agents and diluents.

50.4.3 All drugs for which the forensic unit routinely tests (in relation to the Misuse of Drugs Act 1971 [85] and/or Psychoactive Substances Act 2016 [80]) 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 commonly received, shall be brought within the scope.

50.4.4 The following do not fall within the definition of ‘Analysis to identify and quantify drugs and/or associated materials’ but are the subject of a different FSA definition:

a. FSA – DTN 100 – Toxicology: analysis for drug(s), alcohol and/or noxious substances (section 47).

b. FSA – DTN 105 – Examination and analysis relating to the preparation and production of controlled drugs and/or psychoactive substances (section 82).

50.5 Exclusions from this FSA and the Code

50.5.1 The following do not fall within the definition of ‘Analysis to identify and quantify drugs and/or associated materials’ and are not covered by the Code:

a. Testing of any item, or part thereof, to determine whether it is comprised of or contains a relevant substance:

i. with a Home Office-approved kit under the processes permitted by a Home Office Circular (HOC); or

ii. with a Home Office-approved kit under the processes set out in the Evidential Drug Identification Testing (EDIT) programme [86].

b. Identification of cannabis under any process permitted by a HOC or the EDIT programme.

c. Provision of any evidence in relation to the psychoactivity of a particular compound (or group or class of compounds) in relation to the provisions of the Psychoactive Substances Act 2016 [80].

d. Non-contact screening of items for drugs through packaging or at a port.

e. Presumptive drug test for which this FSA is subsequently carried out by a forensic unit that holds relevant accreditation.

f. Weighing of drugs for remand purposes, where weighing is later carried out as part of the full forensic analyses by a forensic unit that is compliant with the Code. The circumstances (such as whether the weight includes packaging) and preliminary nature of the weight must be detailed in the result for the remand.

g. Estimating the street value of drugs.

51. FSA – DTN 200 – Examination and analysis of corrosives and/or noxious substances

51.1 Definition

51.1.1 Examination and analysis of material suspected and/or believed to be noxious, including a lachrymator and/or corrosive which may have the potential to be used or which are suspected of having been used in alleged attacks.

51.2 Required compliance

51.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and this FSA or sub-activities of this FSA that the organisation undertakes on the schedule of accreditation.

51.3 Sub-activities

51.3.1 The following sub-activities are considered to constitute 'Analysis of corrosive and/or noxious substances':

a. Selecting a portion of the material submitted for analysis.

b. Examination and/or analysis (whether qualitative or quantitative) of any item/exhibit to determine whether it comprises, contains or is contaminated with any relevant substance.

c. Identification of corrosive or noxious substances, including use of reference databases (section 27).

d. Analysis to determine the concentration of a relevant substance.

e. Analysis of corrosive or noxious substances pre-cursors (including but not limited to hydrochloric acid and acetone) and poisonous metals (such as mercury).

f. Examination and/or analysis of any item/exhibit or matter to determine the degree of similarity of a sample of relevant material to any reference material or sample of known origin.

51.4 Note

51.4.1 In this section the term ‘relevant substance’ means anything listed (irrespective of their concentrations) in Schedule 1 of the Offensive Weapons Act 2019 [87], and lachrymators.

51.4.2 The following do not fall within the definition of ‘Analysis of corrosive and/or noxious substances’ but are the subject of a different FSA definition:

a. FSA – DTN 100 – Toxicology: analysis for drug(s), alcohol and/or noxious substances (section 47).

b. FSA – DTN 500 – Examination and analysis of chemical and/or biological agents and associated materials (section 54).

52. FSA – DTN 300 – Examination and analysis of residues of lubricants used in sexual offences, including oils, greases and lubricants

52.1 Definition

52.1.1 Examination and analysis of substances used as lubricants in sexual offences, and evaluation of the findings in the context of the alleged circumstances or to inform lines of inquiry.

52.2 Required compliance

52.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3] with the Code and this FSA or sub-activities of this FSA that the organisation undertakes on the schedule of accreditation.

52.3 Sub-activities

52.3.1 The following sub-activities are considered to constitute ‘Analysis of residues of lubricants used in sexual offences, including oils, greases and lubricants’:

a. Visual examination, including microscopy, for the purpose of locating relevant material and residues of relevant material, and comparisons using lighting techniques.

b. Recovery of relevant material and residues of relevant material:

i. Extraction methods for polar and non-polar lubricants (aqueous and organic) are included.

ii. Solvent extraction of previously prepared extracts (body fluid/DNA).

c. Speculative extraction of swabs and targeted areas of items to detect and identify latent residues through chemical analysis, supported by extraction and analysis of appropriate control samples.

d. Identification of the lubricant, including use of reference databases (section 27).

e. Comparison of any relevant material and/or residues of relevant material detected with a suspected source from reference items.

52.4 Note

52.4.1 In this FSA, relevant material means oils, greases and lubricants. Some of the materials identified will be genuine lubricants, but others may not be recognised as such.

52.4.2 The following do not fall within the definition of 'Analysis of residues of lubricants used in sexual offences, including oils, greases and lubricants' but are the subject of a different FSA definition:

a. FSA – INC 100 – Incident scene examination (section 39).

b. FSA – BIO 100 – Forensic medical examination of complainants (section 40).

c. FSA – BIO 202 – Human DNA analysis (section 43).

52.5 Exclusions from this FSA and the Code

52.5.1 The following does not fall within the definition of 'Analysis of residues of lubricants used in sexual offences, including oils, greases and lubricants' and is not covered by the Code:

a. Provision of opinions relating to absorption or interpretation of what may be remaining after application to human skin.

53. FSA – DTN 400 – Examination and analysis of ignitable liquids and their residues

53.1 Definition

53.1.1 Examination and analysis of ignitable liquids and their residues from samples, including fire debris samples and clothing of individuals believed to have been handling ignitable liquids, and materials impregnated with ignitable liquids or their residues.

53.1.2 In this section, the sub-activities may apply to mixtures of ignitable liquids with each other or with other substances (e.g. engine oil).

53.2 Required compliance

53.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 59.3.1 that the organisation undertakes on the schedule of accreditation.

53.3 Sub-activities

53.3.1 The following sub-activities are considered to constitute 'Analysis of ignitable liquids and their residues':

a. Examination to include recovery and extraction.

b. Analysis of ignitable liquids or their residues.

c. Identification of the ignitable liquid/residue, including the use of reference databases (section 27).

d. Comparison of ignitable liquids/ignitable liquid residues recovered from fire debris or other material against reference standards and/or reference samples collected from a location of interest.

Sub-activities not required to be included in accreditation scope

53.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Examination and/or analysis of materials with a view to establishing their explosive effect in relation to being considered a petrol bomb which is

classed as an ‘explosive substance’ under the Explosive Substances Act 1883 [88].

53.4 Note

53.4.1 The following do not fall within the definition of ‘Analysis of ignitable liquids and their residues’ but are the subject of a different FSA definition:

a. FSA – INC 100 – Incident scene examination (section 39).

b. FSA – INC 102 – Examination of fire scenes (section 76).

c. FSA – DTN 501 – Examination and analysis of explosives, explosives precursors and explosive residues (section 55).

53.5 Exclusions from this FSA and the Code

53.5.1 The following do not fall within the definition of ‘Analysis of ignitable liquids and their residues’ and is not covered by the Code:

a. Determination or measure of how flammable, combustible or ignitable a liquid or residue is.

b. Interpretation of use of the ignitable liquid/residue in relation to fire investigation, including (but not limited to) assessment of potential harm.

c. Examination and analysis of gases (such as methane, ethane, propane, butane or hydrogen).

54. FSA – DTN 500 – Examination and analysis of chemical and/or biological agents and associated materials

54.1 Definition

54.1.1 The examination and analysis of chemical and/or biological agents and associated materials.

54.2 Required compliance

54.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and this FSA or sub-activities of this FSA that the organisation undertakes on the schedule of accreditation.

54.3 Sub-activities

54.3.1 The following sub-activities are considered to constitute ‘Examination and analysis of chemical and/or biological agents and associated materials’:

a. Examination and/or analysis of any item/exhibit to determine whether relevant material is present.

b. Recovery of any relevant material or item of the descriptions below:

   i. an item comprised of relevant material; and/or

   ii. an item which has relevant material in or on it.

c. Examination and/or analysis of any item/exhibit or matter to determine the identity and nature of relevant material present.

d. Agent identification, including use of reference databases (section 27).

e. Examination and/or analysis of any item/exhibit or matter to determine any of the following:

   i. potential immediate source (e.g. device or dissemination mechanism) of relevant material;

   ii. degree of similarity of separate samples of relevant material; and/or

   iii. degree of similarity of a sample of relevant material to any reference material or sample of known origin.

54.4 Note

54.4.1 Presumptive testing conducted at incident scenes are included, unless conducted for public safety reasons rather than for directing evidential recovery.

54.4.2 In this FSA ‘relevant material’ means any of the following:

a. A chemical or biological agent produced or held in circumstances where the possession amounts to a criminal offence.

b. A chemical or biological agent which is being produced or held with the intention that it may be used for, or to facilitate, the commission of a criminal offence.

c. Any chemical or biological agent which is being produced or used for, or to facilitate, the commission of a criminal offence.

d. Any chemical or biological agent which has contaminated any person or location as the result of a criminal offence or attempt to commit an offence.

e. Any precursor chemical or material, or breakdown products relevant to any chemical or biological agent.

54.4.3 The definition of the criminal offence need not refer to chemical or biological agents.

54.4.4 The term chemical agent means a chemical weapon as defined in s1 of the Chemical Weapons Act 1996 [89].

54.4.5 The term biological agent means any biological agent, toxin or weapon, or genetically modified forms of any of the above, subject to the provisions of the Biological Weapons Act 1974 [90].

54.4.6 Any reference to a chemical or biological agent shall be taken to include any material produced by or from the agent.

54.4.7 The following does not fall within the definition of 'Examination and analysis of chemical and/or biological agents and associated materials' but is the subject of a different FSA definition:

a. FSA – DTN 100 – Toxicology: analysis for drug(s), alcohol and/or noxious substances (section 47).

54.5 Exclusions from this FSA and the Code

54.5.1 The following do not fall within the definition of 'Examination and analysis of hazardous chemical and biological agents and associated materials' and are not covered by the Code:

a. Clinical or diagnostic testing.

b. Consideration of the potential method of production and/or the geographical origin (i.e. national geographical location or production facility) of any relevant material.

55. FSA – DTN 501 – Examination and analysis of explosives, explosives precursors and explosive residues

55.1 Definition

55.1.1 Examination and analysis of material suspected to be an explosive substance, explosives precursor or explosives residue.

55.2 Required compliance

55.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 55.3.1 that the organisation undertakes on the schedule of accreditation.

55.3 Sub-activities

55.3.1 The following sub-activities are considered to constitute 'Examination and analysis of explosives, explosives precursors and explosives residues':

a. Recovery of:

   i. an item/exhibit comprised of relevant material; and/or

   ii. an item/exhibit which has relevant material in or on it.

b. Examination and/or analysis of any item/exhibit to determine the presence and nature of any relevant material. This includes trace and bulk explosives analysis.

c. Identification of explosive material, including use of reference databases (section 27).

d. Examination and/or analysis of any item/exhibit to determine any of the following:

   i. potential sources of relevant material; and/or

   ii. degree of similarity of individual samples of relevant material and/or a sample of relevant material to any reference material or sample of known origin.

e. Examination and/or analysis of any item/exhibit to determine whether it (or anything produced from it) is capable of producing an explosive substance.

Sub-activities not required to be included in accreditation scope

55.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. The examination and/or analysis of any item/exhibit or matter to determine any of the following:

i. the potential explosives significance of chemical precursors; and/or

ii. the cause and/or circumstances of an explosion.

b. Consideration of whether explosive substances may be produced from any materials, including in cases where no such materials have been recovered (e.g. from a methodology in a written publication or other form of media, such as video).

55.4 Note

55.4.1 Presumptive testing conducted at incident scenes is included, unless conducted for public safety reasons rather than for directing evidential recovery.

55.4.2 Recovery activities conducted at incident scenes are covered by this FSA, excluding recovery from deceased individuals/body parts (see FSA – INC 201 – forensic examination of deceased individuals (section 79).

55.4.3 In this section ‘relevant material’ means any of the following:

a. An explosive substance or explosives precursor held in circumstances where the possession amounts to a criminal offence.

b. An explosives residue that has been recovered from any person, item/exhibit or location as the result of a criminal offence or attempt to commit an offence.

55.4.4 The term ‘explosive substance’ shall cover any substance which would be subject to the provisions of the Explosives Act 1875 [91], the Explosive Substances Act 1883 [88], or the Explosives Regulations 2014 [92].

55.4.5 The following do not fall within the definition of ‘Examination and analysis of explosives, explosives precursors and explosives residues’ but are the subject of a different FSA definition:

a. FSA – DTN 503 – Examination and analysis of suspected explosive devices (section 84).

b. FSA – MTP 601 – Examination, analysis and classification of firearms, ammunition and associated materials (section 66).

c. FSA – DTN 400 – Examination and analysis of ignitable liquids and their residues (section 53).

d. FSA – INC 200 – Forensic examination of witnesses/complainants/suspects (section 78).

e. FSA – INC 201 – Forensic examination of deceased individuals (section 79).

55.5 Exclusions from this FSA and the Code

55.5.1 The following does not fall within the definition of ‘Examination and analysis of explosives, explosives precursors and explosives residues’ and are not covered by the Code:

a. Screening of items/persons for explosives residue at a port.

56. FSA – MTP 100 – Friction ridge detail: visualisation and enhancement

56.1 Definition

56.1.1 Application of methods to suspected areas of friction ridge detail to visualise, enhance and capture marks to improve the level of detail in those marks and to support comparisons that are to be carried out.

56.2 Required compliance

56.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 56.3.1 that the organisation undertakes on the schedule of accreditation.

56.2.2 This FSA should be read in conjunction with the FSA-specific requirements set out in section 95.

56.3 Sub-activities

56.3.1 The following sub-activities are considered to constitute 'Friction ridge detail: visualisation and enhancement':

a. Analysis of an area of friction ridge detail, either latent or visible, to determine a method, or sequence of methods, that could be utilised to most effectively enhance and reveal friction ridge detail within that area.

b. Application of the method(s) determined at a above. Methods can be physical in nature (e.g. light sources or powder application) or chemical.

c. Assessment of the outcome of the application of the applied method(s) to assess whether they have performed as expected and the determination of any remedial action if they have not.

d. Marking up relevant detail.

e. Use of specialist lighting, camera settings, optics and other digital systems to optimise image capture.

f. Capture and recording of the friction ridge detail.

g. When required, digital enhancement to facilitate comparison using post-capture image processing to appropriately compensate for perceived failings in the image.

Sub-activities not required to be included in accreditation scope

56.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Analysis of an area of friction ridge detail to determine the activity that caused the deposition.

57. FSA – MTP 101 – Friction ridge detail: comparison

57.1 Definition

57.1.1 Examination, including search and macroscopic or magnified comparison of two or more areas of friction ridge detail, howsoever made and presented, to

evaluate whether or not they originated from the same source or different sources.

57.2 Required compliance

57.2.1 Compliance with the Code is required, demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and comparison of Friction Ridge Detail on the accreditation schedule. Accreditation schedules issued against Code version 1 are recognised for this purpose.

57.2.2 From 2 October 2026 the sub-activities that the organisation undertakes of this FSA listed in section 57.3.1 are required to be reflected on the schedule of accreditation.

57.2.3 This FSA should be read in conjunction with the FSA specific requirements set out in section Friction ridge detail: comparison (section 96).

57.3 Sub-activities

57.3.1 The following sub-activities describe services provided by bureaux and are considered to constitute ‘Friction ridge detail: comparison’:

a. Search of FRD
    i. Algorithmic process to provide potential candidates to take forward for comparison.
b. Identity check
    i. Equates to comparison of friction ridge detail recorded under controlled conditions for the purpose of identity confirmation;
    ii. Includes living or deceased persons;
c. Scene linking
    i. Equates to mark-to-mark comparison of friction ridge detail;
    ii. Algorithmic or manual.
d. Direct comparisons of persons of interest
    i. Manual process of comparison between FRD from a person of interest and questioned FRD
e. Provision of a report.

Sub-activities not required to be included in accreditation scope

57.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. The consideration of the orientation of an area of friction ridge detail to determine the activity or handling that caused the deposition.

57.4 Note

57.4.1 The sub-activities set out at 57.3.1.a.i and 57.3.1.c.ii involve the interrogation of a database. The control and management of such a database falls under FSA-CDM 200- Control and management of a forensic database service.

58. FSA – MTP 200 – Footwear: coding

58.1 Definition

58.1.1 The provision of information to link incident scenes through the consideration of footwear marks recovered from those scenes.

58.2 Required compliance

58.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 58.3.1 that the organisation undertakes on the schedule of accreditation.

58.2.2 However, as the activity is limited to scene-to-scene linking by coding of marks recovered from scenes, the Regulator will allow such activity to be undertaken in the absence of accreditation provided the forensic unit adheres to the NPCC's Framework for Footwear Coding [93] and demonstrates such adherence. The Framework includes the following requirements:

a. the forensic unit shall have methods approved by the NPCC.

b. the forensic unit shall record and maintain competence of personnel it authorises to conduct this FSA.

c. practitioners adhere to the practices set out in the NPCC's Framework for Footwear Coding.

d. the Regulator can conduct an audit of the process and the forensic unit carrying it out at any time.

e. the organisation will make an appropriate declaration.

f. the Regulator can withdraw this dispensation at any time, defaulting to a requirement for accreditation to ISO/IEC 17025:2017 [3].

g. where reports are produced, a declaration should be included, as follows or in terms substantially the same:

I confirm that, to the best of my knowledge and belief, I have acted in accordance with the NPCC Framework for Footwear Coding [insert issue] as required by the statutory Forensic Science Regulator.

58.3 Sub-activities

58.3.1 The following sub-activities are considered to constitute 'Footwear: coding':

a. Enhancement of footwear marks as is considered appropriate and proportionate to the case in question.

b. Macroscopic examination/analysis of the footwear mark(s) received.

c. Use of a reference database (section 27) to:

i. identify the undersole pattern represented in the mark by reference to an alpha-numeric code which ordinarily indicates manufacturer and style/model of footwear; and/or

ii. identify other occurrences of the undersole pattern at other scenes.

58.4 Note

58.4.1 'Footwear marks' does not include footwear prints taken in custody.

58.4.2 Any sub-activities listed in this FSA shall be included in a forensic unit's accreditation to ISO/IEC 17025:2017 [3] if the forensic unit is intending to use the output to support any activity carried out under the following FSAs which require such accreditation and which should be read in conjunction with this one:

a. FSA – MTP 201 – Footwear: screening.

b. FSA – MTP 202 – Footwear mark comparisons.

59. FSA – MTP 201 – Footwear: screening

59.1 Definition

59.1.1 The analysis of footwear, or prints from known footwear, and marks recovered from one or more scenes, with a view to recommending whether or not a comparison is carried out, under FSA – MTP 202 – Footwear mark comparisons.

59.2 Required compliance

59.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 59.3.1 that that the organisation undertakes on the schedule of accreditation.

59.3 Sub-activities

59.3.1 The following sub-activities are considered to constitute 'Footwear: screening':

a. Examination of one or more seized/surrendered items of footwear pertinent to:

   i. a detainee;

   ii. a person(s) of interest suspected of involvement in crime;

   iii. a location relevant to anyone covered in (i) and (ii) above; and/or

   iv. people who have legitimate access to the scene of incident.

b. Reference to/operation of a database to determine the undersole pattern present on the submitted footwear item/exhibit(s) (section 27).

c. Production of appropriate test-impressions from the footwear in question.

d. Receipt of footwear marks, in whatever format and howsoever produced, from one or more incident scenes. This includes receipt of items recovered from incident scenes which bear footwear marks.

e. Recovery or recording of the submitted mark(s).

f. Enhancement of the submitted marks.

g. Macroscopic examination of the footwear mark(s) received.

h. Provision of a report recommending whether or not an evidential comparison can and/or should be carried out. This could include consideration of apparent size, wear and damage on the sole of the footwear when making the decision to submit for comparison.

59.4 Note

59.4.1 Screening can involve:

a. One or more items of footwear, whether recovered from individuals suspected of involvement in an incident or incidents under investigation, or from locations associated with those individuals.

b. One or more items of footwear or test-impressions taken from the footwear of individuals known to have had legitimate access to the scene.

59.4.2 Screening does not include an assessment of evidential strength.

59.4.3 Screening does not include cursory or preliminary selection of footwear for examination, including premises searches.

59.4.4 Screening submissions may be the result of coding activities such as are described in FSA – MTP 200 – Footwear: coding. That FSA should be read in conjunction with this one.

59.4.5 Screening activities as described in this FSA can lead to comparisons as described in FSA – MTP 202 – Footwear mark comparisons.

60. FSA – MTP 202 – Footwear mark comparisons

60.1 Definition

60.1.1 The analysis and examination of footwear and marks recovered from one or more scenes to determine whether or not those specific items of footwear could have contributed to the recovered marks, and the evaluation of evidential strength

60.2 Required compliance

60.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of

this FSA listed in section 60.3.1 that the organisation undertakes on the schedule of accreditation.

60.3 Sub-activities

60.3.1 The following sub-activities are considered to constitute 'Footwear mark comparison':

a. The examination of one or more items of footwear pertinent to:

   i. a detainee and/or individual(s) suspected of involvement in crime;

   ii. a person with legitimate access, including witnesses, emergency service personnel, and complainants; and/or

   iii. a location relevant to anyone covered in (i) and (ii) above.

b. Reference to/operation of a database (section 27) to determine the undersole pattern present on the submitted footwear item(s).

c. Production of appropriate test-impressions from the submitted footwear.

d. Analysis of footwear marks, in whatever format and howsoever produced, from one or more incident scenes. This includes items recovered from incident scenes which bear footwear marks.

e. Enhancement of the submitted mark(s).

f. Macroscopic and/or magnified examination of the footwear mark(s) received.

g. A macroscopic and/or magnified comparison between the submitted footwear, or test-impressions from the submitted footwear, and marks from incident scenes to determine areas of agreement and difference.

h. Interpretation of the source of the footwear mark.

Sub-activities not required to be included in accreditation scope

60.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Interpretation of the activity leading to the deposition of the footwear mark.

b. Comparison between submitted footwear or test-impressions from submitted footwear and injury marks.

60.4 Note

60.4.1 Comparison can cover:

a. one or more item(s) of footwear, or test-impressions taken from the footwear, whether recovered from individuals suspected of involvement in an incident or incidents under investigation, or from locations associated with those individuals;

b. one or more items of footwear, or test-impressions taken from the footwear, of individuals known to have had legitimate access to the scene of incident; or

c. comparison of footwear and/or test-impressions as described at (a) and (b) above with one or more marks recovered from one or more scenes or injury marks.

60.4.2 Comparison may come about as a direct consequence of an investigation or it may follow on from coding and screening activities such as are described in FSA – MTP 200 – Footwear: coding and FSA – MTP 201 – Footwear: screening respectively. Those FSAs should be read in conjunction with this.

61. FSA – MTP 300 – Marks visualisation and enhancement

61.1 Definition

61.1.1 The application of methods to visualise latent marks on a physical item and/or to improve the level of detail in indistinct marks.

61.2 Required compliance

61.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 61.3.1 that the organisation undertakes on the schedule of accreditation.

61.3 Sub-activities

61.3.1 The following sub-activities are considered to constitute ‘Marks: visualisation and enhancement’:

a. Macroscopic or magnified examination of a relevant area where a mark, either latent or visible, may be present, to determine a method or sequence of methods that could be employed to most effectively reveal further detail within that area.

b. Application of the determined method(s) (e.g. lighting/chemical). This includes image capture methods.

c. Macroscopic or magnified consideration of the outcome of the application of the determined method(s) to assess whether they have performed as expected, and remedial action if they have not.

d. Analysis to identify relevant detail.

e. Use of methods, both physical and digital, to optimise image capture.

f. Recording of the mark(s).

Sub-activities not required to be included in accreditation scope

61.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Consideration of context to determine the activity that caused the deposition.

61.4 Note

61.4.1 This FSA relates to marks other than those due to friction ridge detail.

62. FSA – MTP 301 – Marks comparison

62.1 Definition

62.1.1 The analysis and examination of a mark or a series of marks, and an item/exhibit or items/exhibits suspected of making them, to determine whether or not those specific items/exhibits could have contributed to the recovered marks, and the evaluation of evidential strength.

62.1.2 Such marks may be present on any substrate and in any medium, including substrates that allow for three-dimensional representation of the item responsible.

62.2 Required compliance

62.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 62.3.1 that the organisation undertakes on the schedule of accreditation.

62.3 Sub-activities

62.3.1 The following sub-activities are considered to constitute ‘Marks: comparison’:

a. Macroscopic or magnified comparison of two or more marks, from one or more scenes, to determine whether or not they could have been made by the same item/exhibit, including screening exercises.

b. Macroscopic or magnified examination and/or analysis of a mark, or marks, to determine what may have caused it, either generically or specifically, where appropriate with reference to database material.

c. Operation/interrogation of a database referred to in clause (b) (section 27).

d. Macroscopic or magnified comparison of a mark or marks, howsoever made, with an item/exhibit suspected of making it/them, including screening exercises, to determine areas of agreement and difference.

e. Recording, including the creation of a cast or replica of any mark.

f. Recovery of erased marks and serial numbers.

g. Production of test-impressions from an item/exhibit, or items/exhibits, suspected of having made or contributed to a mark.

h. Interpretation of the source of the mark.

Sub-activities not required to be included in accreditation scope

62.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Macroscopic or magnified examination and/or analysis of a mark (or image of a mark) to determine the activity that may have led to the production of that mark.

b. Any of the above activities when performed on marks on skin.

62.4 Note

62.4.1 This FSA relates to marks other than those due to friction ridge detail or footwear; it relates therefore to toolmarks or miscellaneous marks.

62.5 Exclusions from this FSA and the Code

62.5.1 The following do not fall within the definition of 'Marks: comparison' and are not covered by the Code:

a. Examination of penetrating wounds.

b. Examination of bite marks and odontology.

63. FSA – MTP 400 – Damage and physical fit

63.1 Definition

63.1.1 Analysis and examination of items/exhibits to:

a. determine the cause of damage sustained by the item/exhibit;

b. reconstruct part/whole of an original thing from two or more parts;

c. link implements/individuals to incidents; and/or

d. provide information as to the possible type of implement involved in an incident.

63.2 Required compliance

63.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and this FSA or the sub-activities of this FSA listed in section 63.3.1 that the organisation undertakes on the schedule of accreditation.

63.3 Sub-activities

63.3.1 The following sub-activities are considered to constitute ‘Damage and physical fit’:

a. Macroscopic examination of items/exhibits and/or component parts, noting general condition, damage, and any associated staining:

   i. The sample types that may be assessed include any type of physical material that is susceptible to damage and/or that can be broken.

   ii. The sample may be given as separate items/exhibits or searched for (e.g. stab cuts in fabric).

b. Microscopical examination to identify and document detailed physical features that characterise the nature of damage.

c. Recording and comparison of fracture surfaces.

d. Comparison between two or more items/exhibits that may once have been part of a single thing, and an assessment of the evidential value of any fit.

e. Comparison of component parts to determine common source if conclusive fit cannot be established.

f. Consideration of how (including using reconstruction simulations) and when damage was caused.

g. Examination and analysis of damage caused by corrosive substances is covered under this FSA.

63.4 Note

63.4.1 Examination and analysis of thermal damage (e.g. from flash burning to clothing) is covered under this FSA, but not large-scale fire damage to structures or vehicles (for detail see FSA – INC 102 – Examination of fire scenes).

63.4.2 Examination and testing of discrete components removed from a vehicle or recovered from a collision scene is covered under this FSA but not examinations at a collision scene or site, including examination of vehicles involved in a collision, to identify, preserve and record areas of damage that could be relevant to the collision (FSA – INC 101 – Collision Investigation).

64. FSA – MTP 500 – Examination and analysis of particulate trace materials

64.1 Definition

64.1.1 The examination and analysis of particulate trace materials that could be transferred as a result of contact or close proximity to a source.

64.2 Required compliance

64.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 64.3.1 that the organisation undertakes on the schedule of accreditation.

64.3 Sub-activities

64.3.1 The following sub-activities are considered to constitute 'Examination and analysis of particulate trace materials':

a. Examination of an item/exhibit to locate relevant material (including with microscopy).

b. Preservation, recovery and/or recording of relevant material from an item/exhibit using such methods as are deemed appropriate for the material under consideration.

c. Examination and/or analysis of recovered relevant material and its comparison with a control sample, using such visual/microscopic, physical and analytical methods as are deemed appropriate.

d. Identification of questioned material, including the use of reference databases (section 27).

e. Examination and/or analysis of relevant material in relation to any of the following:

   i. potential source of relevant material;

   ii. originating source of the relevant material and/or information regarding manufacture/manufacturer.

Sub-activities not required to be included in accreditation scope

64.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Consideration of any of the following:

i. distribution methods or extent or distribution of the relevant material or the source from which it originated;

ii. where and/or when material was acquired; and/or

iii. an activity that may have led to the transfer of the relevant material(s).

64.4 Note

64.4.1 In this section ‘relevant material’ includes:

a. glass;

b. surface coatings, polymers and adhesives;

c. synthetic and natural fibres;

d. building material not contained within clauses a to c; and

e. other particulate material not contained within clauses a to d.

64.4.2 Sub-activities for particulates that may be conducted infrequently can be considered under the provision for infrequently used methods (section 24.2.8-24.2.16).

64.4.3 The following do not fall within the definition of ‘Examination and analysis of particulate trace materials’ but are the subject of a different FSA definition:

a. FSA – INC 200 – Forensic examination of witnesses/complainants/suspects.

b. FSA – INC 201 – Forensic examination of deceased.

65. FSA – MTP 600 – Examination and analysis of gunshot residue (GSR)

65.1 Definition

65.1.1 The examination and analysis of items/exhibits to determine the presence, or not, of gunshot residue (GSR), particulate residues of primer and propellant (if applicable) produced from the discharge of primed ammunition in a firearm.

65.1.2 Analysis of GSR particles to:

a. determine the elemental composition of GSR particles;

b. provide information on the primer, projectile and potentially other ammunition and firearm components; and

c. compare the GSR on an item/exhibit from a control sample, such as the muzzle of a firearm or a spent cartridge casing, to GSR identified on samples from examined items/exhibits.

65.2 Required compliance

65.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 65.3.1 that the organisation undertakes on the schedule of accreditation.

65.3 Sub-activities

65.3.1 The following sub-activities are considered to constitute 'Examination and analysis of GSR':

a. Examination of an item/exhibit to recover particulate residues of GSR. The residue can contain additional contributions from the firearm, cartridge case and projectile.

b. Presumptive testing for the presence of metals, particularly lead and copper.

c. Analysis of any recovered samples, such as adhesive lifts (e.g. stubs) or swabs, to determine:

i. whether it has GSR on it;

ii. the amount and distribution of GSR recovered from an examined item/exhibit; and/or

iii. whether or not there are particles on the sample that indicate material from a non-firearm source (e.g. fireworks or vehicle airbags) is present, which might detract from the classification of other particles on that sample as having originated from a firearm source.

Sub-activities not required to be included in accreditation scope

65.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Interpretation and opinions with regards to:

i. where and/or when particles of GSR were acquired by a person or item; and/or

ii. the activity that may have led to the transfer of particles of GSR to a person or item.

65.4 Note

65.4.1 This FSA does not cover activity carried out an incident scene.

65.4.2 The following do not fall within the definition of 'Examination and analysis of gunshot residue (GSR)' but are the subject of a different FSA definition:

a. FSA – MTP 601 – Examination, analysis and classification of firearms, ammunition and associated materials.

b. FSA – MTP 602 – Firearms: ballistics .

66. FSA – MTP 601 – Examination, analysis and classification of firearms, ammunition and associated materials

66.1 Definition

66.1.1 Examination of an item/exhibit suspected of being a firearm, ammunition, or component part of a firearm or ammunition, to determine its classification under the provisions of the Firearms Act 1968 as amended [94], and other relevant

legislation, and the functionality of the firearm, ammunition, and/or associated materials.

66.2 Required compliance

66.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 66.3.1 that the organisation undertakes on the schedule of accreditation.

66.2.2 In exceptional circumstances, such as where an urgent firearms classification is required to support a remand in custody application, it may not be feasible to undertake the classification in the required timescales using an accredited process. To accommodate this, the Regulator will enter into a general agreement with an organisation to put in place a process where accreditation will not be required for the support of such applications provided that, in each instance it is carried out, the activity is subsequently carried out by a forensic unit that holds relevant accreditation. This process will be based on:

a. the SAI making an application to the Regulator to put the process in place;

b. all firearms that are dealt with according to this process shall, without exception, be examined by a forensic unit that holds accreditation for this FSA as soon as practicable and in any event within 72 hours of the remand decision being made;

c. there is an operating framework in place which has been agreed with the Regulator and covers the procedures, competency of personnel involved and internal audit;

d. the Regulator can conduct an audit of this process and the agreement with the forensic unit carrying it out at any time;

e. the organisation will make an annual return to the Regulator setting out the number and types of firearms examined and other information specified by the Regulator;

f. the organisation will make a declaration defined by the Regulator; and

g. the Regulator can terminate the arrangement at any time, defaulting to a requirement for accreditation to ISO/IEC 17025:2017 [3].

66.3 Sub-activities

66.3.1 The following sub-activities are considered to constitute ‘Examination, analysis and classification of firearms, ammunition and associated materials’:

a. Examination and/or analysis of any item/exhibit to determine whether it can be considered a firearm under Section 5 of the Firearms Act 1968 as amended [94],. This includes:

   i. any weapon of whatever description designed or adapted for the discharge of any noxious liquid, gas or other thing; and

   ii. an electric stun-gun.

b. Any classification for the purpose of a charging decision, including production of a statement or SFR:

   i. Consideration of compliance with definitions of ‘component parts’, ‘firearm’ and ‘readily convertible firearm’ under the Firearms Act 1968 as amended [94], and other relevant legislation.

   ii. Measurement of firearm dimensions and/or magazine capacity to determine their classification under the provisions of the Firearms Act 1968 as amended [94],, and other relevant legislation.

   iii. Dismantling and testing of ammunition to determine its classification under the provisions of the Firearms Act 1968 as amended [94], and other relevant legislation.

c. Examination of firearms, firearm components or firearm accessories to identify type and origin via markers such as manufacturer, model, serial number, and calibre.

d. Any testing, including test firing, to determine viability and functionality of a firearm or ammunition.

e. Measurement of the kinetic energy of a projectile fired from a suspected firearm.

Sub-activities not required to be included in accreditation scope

66.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Test firing of a firearm to determine distance from muzzle on discharge and accuracy.

b. Examination of the sighting equipment on a firearm to assess an allegation of unintentional discharge of a firearm.

66.4 Note

66.4.1 In this FSA the term ‘firearm’ means any object which is subject to controls under the Firearms Act 1968 as amended [94], and other relevant legislation, and includes imitation firearms and weapons such as electric stun guns.

66.4.2 In this FSA the term ‘associated materials’ includes items related to firearms, including sound moderators, magazines, ammunition re-loading tools and firearm conversion tools and components.

66.4.3 The ‘make safe’ process does not form part of this FSA but is an important part of the workflow and should be carried out by practitioners competent to preserve other potential evidence types on an item/exhibit.

66.4.4 This FSA does not cover activity carried out at an incident scene or other related location, such as the proffering of non-technical advice in an operational capacity to:

a. inform an investigation; and

b. prioritise submissions for classification.

66.4.5 The following do not fall within the definition of ‘Examination, analysis and classification of firearms, ammunition and associated materials’ but are the subject of a different FSA definition:

a. FSA – MTP 600 – Examination and analysis of gunshot residue (GSR).

b. FSA – MTP 602 – Firearms: ballistics.

c. FSA – DTN 200 – Examination and analysis of corrosives and/or noxious substances.

67. FSA – MTP 602 – Firearms: ballistics

67.1 Definition

67.1.1 The examination and/or analysis of any mark/characteristics on cycled ammunition, components or related fired ballistic material, and the interpretation of damage or other effects caused by the discharge of a firearm.

67.2 Required compliance

67.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 67.3.1 that the organisation undertakes on the schedule of accreditation.

67.3 Sub-activities

67.3.1 The following sub-activities are considered to constitute 'Firearms: ballistics':

a. Examination using macroscopic techniques to assess whether or not the characteristics on fired, cycled ammunition or related fired ballistic material can be associated with a firearm class.

b. Examination and/or analysis using microscopic techniques to assess whether or not the characteristics on fired, cycled ammunition or related fired ballistic material can be associated with a firearm.

c. Examination of fired projectiles for impact damage and recovery of impacted material such as glass and fibres.

d. Intelligence linking any cycled ammunition, components or related fired ballistic material to an incident scene and/or a firearm.

e. Comparison of any cycled ammunition, components or related fired ballistic material to an incident scene and/or a firearm for evidential purposes.

f. Use of any database systems that record and/or compare features of cycled ammunition and/or components of related fired ballistic material to establish links between incidents.

g. Test firing of firearms to generate ammunition mark samples for use in database systems.

h. Ballistics calculations, including trajectories and maximum ranges using either manual or automatic methods.

i. Examination, analysis and interpretation of damage caused, or believed to have been caused, by the discharge of a firearm (e.g. ricochet and/or projectile strike marks, damage to clothing).

j. Analysis to determine the trigger-pull pressure required to discharge a weapon.

k. Examination of the mechanical condition of a weapon to assess potential causes of the discharge and determine whether it was unintentional.

l. Recovery of erased serial numbers from firearms for evidential purposes.

m. Examination of an area for close-range firing effects, including presumptive testing for cuprous material, heavy metals, and nitrites.

Sub-activities not required to be included in accreditation scope

67.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Analysis to assess whether a firearm is capable of inflicting a lethal injury.

b. Analysis for reconstruction and to provide opinion at the activity level, such as position of shooter, number of shots fired.

67.4 Note

67.4.1 In this section the term ‘firearm’ means any object which is subject to the controls of the Firearms Act 1968 as amended [94], and other relevant legislation, and includes imitation firearms and weapons such as electric stun guns [94].

67.4.2 ‘Ballistics’ is accepted as a term with a broader definition than projectiles in flight, and ‘ballistic material’ is a broad term used to describe items that are related to firearms, such as ammunition, ammunition components and associated materials.

67.4.3 This FSA does not cover work carried out solely at an incident scene, but should be considered when related work is carried out in that environment as a sub-activity of FSA – INC 100 – Incident scene examination.

67.4.4 The following do not fall within the definition of 'Firearms: Ballistics' but are the subject of a different FSA definition:

a. FSA – MTP 600 – Examination and analysis of gunshot residue (GSR).

b. FSA – MTP 601 – Examination, analysis and classification of firearms, ammunition and associated materials.

c. FSA – DTN 200 – Examination and analysis of corrosives and/or noxious substances.

67.4.5 The process for the recovery of erased serial numbers from firearms for evidential purposes should be carried out according to the requirements set out in FSA – MTP 300 – Marks visualisation and enhancement.

68. FSA – MTP 700 – Document handwriting

68.1 Definition

68.1.1 Examination and analysis of handwritten text on a document to determine the authorship of handwriting and/or signature(s) and the evaluation of evidential strength.

68.2 Required compliance

68.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and this FSA and the sub-activities of this FSA listed in section 68.3.1 that the organisation undertakes on the schedule of accreditation.

68.3 Sub-activities

68.3.1 The following sub-activities are considered to constitute 'Document handwriting':

a. Examination and analysis of handwritten text, including a signature, to determine whether handwriting and/or a signature(s) has been produced by:

i. a specific individual (by comparison with their reference writing and/or reference signature(s));

ii. the same individual as has produced handwriting and/or signature(s) on any other part of the same document; or

iii. the same individual as has produced handwriting and/or signatures on any part of a separate document.

68.4 Note

68.4.1 The sub-activities above apply to examination of any of the following:

a. Handwriting and/or signatures produced by human movement, whether or not visible to the unaided human eye.

b. Original handwriting and/or signatures produced by human movement or images of original handwriting and/or signatures produced by human movement.

c. Any handwriting and/or signature resulting from the human movement by an electronic capture device, including a signature executed and captured via a digitiser and stylus.

68.4.2 This FSA considers handwritten text on a document and not the authenticity and origin of the underlying document. That is considered under FSA – MTP 701 – Document authenticity and origin.

68.4.3 ‘A document’ refers to a physical item such as a piece of paper, a page in a book, an image(s) (electronic or printed) of a physical document(s) or parts of a physical document(s).

68.5 Exclusions from this FSA and the Code

68.5.1 The following do not fall within the definition of ‘Document handwriting’ and are not covered by the Code:

a. Consideration of the authorship of handwriting or signatures based on personal knowledge rather than scientific evaluation.

b. Consideration of personality traits of an individual by reference to features of their handwriting.

c. Consideration of the authorship of handwriting or signatures based on an assessment of personality traits.

d. Consideration of the authorship of any electronically generated handwriting or signature which is not the result of human movement.

69. FSA – MTP 701 – Document authenticity and origin

69.1 Definition

69.1.1 Examination and/or analysis of the authenticity of a document, and evaluation of the evidential strength, to determine whether it is (in its entirety or in part):

a. what it purports to be;

b. an imitation; and/or

c. an authentic but altered example of what it purports to be.

69.1.2 Examination and/or analysis of the origin or method of manufacture of the entirety or constituent parts of a document.

69.1.3 Examination and/or analysis of links between constituent parts of the same or different documents based on materials and methods of manufacture.

69.2 Required compliance

69.2.1 Compliance with the Code is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 69.3.1 that the organisation undertakes on the schedule of accreditation.

69.3 Sub-activities

69.3.1 The following sub-activities are considered to constitute ‘Document authenticity and origin’:

a. Macroscopic or magnified examination and/or analysis to determine whether a document, or any part of a document, including the text or images within a document, have been produced by:

i. any specific equipment;

ii. the same equipment as produced any part of a separate document;

iii. the same materials as any part of the same document (including physical fits between torn or cut paper); and/or

iv. the same materials as any part of a separate document (including physical fits between torn or cut paper).

b. Macroscopic or magnified examination and/or analysis to determine the type of equipment (e.g. type of printer or specific model of printer) and/or materials which were used to create, change or alter the appearance of a document.

c. Relative dating of a document or documents, or of a specified part of a document.

i. 'Relative dating' can include the determination of, for example, whether a document can only have been produced before or after a certain date because of its specific method of production, materials used in its production or the content of the text it bears. It can also include sequencing of entries.

d. Macroscopic or microscopic examination and/or analysis to determine whether a document has been altered or the appearance changed after its creation or after a relevant significant event (e.g. its signature, the affixing of any stamp/seal etc).

e. Anything done (whether directly or indirectly) to make visible, or to recover, text or images which are present but not visible to the unaided eye. This includes indented or erased writing.

f. Examination and/or analysis of a document for the purpose of determining the presence of security features by, but not limited to, the use of light sources (including those wavelengths outside the visible spectrum) and magnification, perhaps combined with imaging processes.

69.4 Note

69.4.1 The sub-activities above apply to any of the following:

a. Any document containing text or images, even if the text or image is not visible to the unaided human eye.

b. Any text, including indented or erased writing, or images, which forms part of the document.

c. Any marks on the document.

d. Any equipment which may be used to create, copy or alter the appearance of a document (even if the copy is not a physical document).

e. Examination of any materials which may form a document, part of a document or be used to change a document or alter the appearance of a document.

f. Paper or other substrate, including the physical fit of torn or cut paper.

g. Inks or other marking materials.

69.4.2 The term ‘materials’ means inks, paper, bindings and such like.

69.4.3 This FSA considers the materials making up documents in particular and not handwriting on a document. That is considered under FSA – MTP 700 – Document handwriting.

69.4.4 ‘A document’ refers to:

a. a physical item, such as a piece of paper or a page in a book; or

b. an image(s) (electronic or printed) of a physical document(s) or parts of a physical document(s).

69.4.5 The following does not fall within the definition of ‘Document authenticity and origin’ but is the subject of a different FSA definition:

a. FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis.

69.5 Exclusions from this FSA and the Code

69.5.1 The following do not fall within the definition of ‘Document authenticity and origin’ and are not covered by the Code:

a. any consideration of whether any of the following is true based on personal knowledge rather than scientific evaluation:

i. whether a document is genuine; and/or

ii. whether a document has been modified after its creation or any relevant significant event.

70. FSA – DIG 100 – Data capture, processing and analysis from digital storage devices

70.1 Definition

70.1.1 Includes methods conducted at, but not limited to, scenes of incident, fixed facilities or mobile facilities however named (e.g. mobile laboratories in vehicles) for:

a. screening of a digital storage media for a decision on seizure or prioritisation (e.g. using a triage software tool);

b. capture and processing of data from submitted/seized devices or digital storage media accessed from such devices.

70.1.2 Digital storage media comprises both standalone storage devices, components, remotely stored electronic data (e.g. cloud storage) accessed via a submitted/seized device, as well as volatile and non-volatile memory embedded within any electronic computing devices including but not limited to phones, personal computers, tablets, drones, satellite navigation systems and vehicle systems.

70.2 Required compliance

70.2.1 Compliance with the Code and the FSA specific requirements in section 97 (Digital forensics) is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 70.3.1 that the organisation undertakes on the schedule of accreditation.

70.3 Sub-activities

70.3.1 The following sub-activities are considered to constitute ‘Data capture, processing and analysis from digital storage devices’:

a. Any of the following performed on any storage device under examination which includes but is not limited to mobile devices and computer drives:

i. Screening devices for seizure/prioritisation using an off-the-shelf tool.

ii. Recovery of data from a device under examination using an off-the-shelf tool for factual reporting; all deployments in scope, unless specific implementation criteria are fulfilled as detailed in the implementation section of the digital forensic FSA specific requirement in section 97.4.13 - 97.4.15.

iii. Examination of a device, media or component to locate or capture and preserve (create a copy of the digital data in whole or in part and store the copy in a manner that allows subsequent processing and analysis to take place) any information stored on or accessible via the device in digital/electronic format (i.e. cloud storage).

b. Processing – conversion of digital data forensically captured in this FSA from or via submitted/seized devices to produce meaningful information, either by a manual or automated process, to allow for subsequent analysis and/or reporting to take place, including:

i. reverse-engineering undocumented data structures;

ii. manual parsing of data from an embedded database file (e.g. SQLite, LevelDB) into a human readable format.

c. Analysis – targeting digital data forensically captured in this FSA from or via submitted/seized devices via the application of a predefined and prescriptive examination strategy; specifically the following:

i. analysis of information related to communications (e.g. calls, e-mails, texts) (unless addressed in section 85 or subject to an exclusion));

ii. analysis of file data e.g. review of exchangeable image file (.EXIF) data;

iii. identification of files by known hash comparison;

iv. analysis of application data to identify how an application has been configured, e.g. peer-to-peer file sharing;

v. analysis of data from an embedded data structure (including SQLite searches, Plist tool searches).

d. The interpretation of any data or output of sub-activity described above in clause ‘c.’ with the purpose of providing opinion to include, but not be limited to, the following:

i. analysis of log-files and other such files to determine activities that have been performed or recorded on that digital device;

ii. provenance or integrity of files/data. User activity (e.g. file creation, patterns of use);

iii. reliability/accuracy of data (e.g. recovered timestamps/GPS locations); and/or

iv. whether steps had been taken to conceal data (e.g. file manipulation).

Sub-activities not required to be included in accreditation scope

70.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Providing opinion on the effect of any virus or malware presence.

70.4 Note

70.4.1 Investigative review of data supplied by a forensic unit with a statement/report with the required declaration of compliance/non-compliance to the investigator to identify relevant content does not currently fall within the definition of FSA - DIG 100 - Data capture, processing and analysis from digital storage devices if:

a. personnel acting as investigators are competent to use the SAI approved review method provided (e.g. a Cellebrite reader, eDiscovery tool, DEMs);

b. it is restricted to the content (i.e. a text message, a photo of an individual etc.) and not for the purpose of interpretation of associated meta data nor its location in a file structure; and

c. it is for purposes other than detailed in 70.3.1b - 70.3.1d.

70.4.2 Use or inclusion of excerpts of data captured and/or processed under DIG 100 in evidential products or reports to support the judicial process, unless for the purpose of the interpretation of the data as defined in 70.3.1c does not fall within the FSA - DIG 100. Any included excerpts should then be clearly labelled

as information obtained under FSA DIG - 100, traceable to the practitioner, who completed the data capture/processing and traceable to the entire data set produced as a result of this FSA.

70.4.3 The following do not fall within the definition of FSA – DIG 100 – Data capture, processing and analysis from digital storage devices but are the subject of other FSAs:

a. FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73).

b. FSA – DIG 400 – Audio acquisition, conversion and processing (section 74).

c. FSA – DIG 401 – Speech and audio analysis (section 87).

d. FSA – DIG 200 – Cell site analysis for geolocation (section 71).

e. FSA – DIG 101 – Analysis of communications network data (section 85).

f. FSA – DIG 102 – Digital network capture and analysis (section 86).

70.5 Exclusions from this FSA and the Code

70.5.1 The following do not fall within the definition of 'Data capture, processing and analysis from digital storage devices' and are not covered by the Code:

a. Screening of media for the purpose of offender management, i.e. post-sentencing monitoring under a supervision order; provided continuity information is available (e.g. which methods/tools were used in case seizure is required).

b. Screening devices prior to seizure of a device to form part of a criminal investigation at ports and other locations under Schedule 7 of the Terrorism Act 2000 [95], Schedule 3 of the Counter Terrorism and Border Security Act 2019 [96] using an off-the-shelf tool, provided continuity information is available (e.g. which tools were used prior to seizure).

c. Manual categorising of indecent images of children.

d. Tachograph analysis.

e. Routine extraction, processing and analysis of data from an Incident Data Recorder deployed by a body involved in the detection and/or investigation of crime.

f. Recording and transfer of emergency calls (e.g. 112, 999) using a controlled system.

g. Routine extraction of audio-video material from systems controlled by a body involved in the detection and/or investigation of crime (including in joint operations), and the editing and redaction of this material. Examples of this material include, but are not limited to, drones, body worn video, emergency calls (e.g. 112, 999) and video recorded interviews.

h. Download of audio-visual media from a DEMS/DAMS as part of an investigation.

i. Acquisition of data utilising the Crime (Overseas Production Orders) Act 2019 [97], and the analysis and processing of that data.

j. Data recovery via Internet Intelligence & Investigations (III), Open Source Intelligence (OSINT), Signals Intelligence (SIGINT), Communications Intelligence (COMMINT) and Geospatial Intelligence (GEOINT).

k. Activity relating to the INTERPOL database(s).

l. Acquisition of data from cloud storage as a result of login/connection data taken from a device under examination, but not via the seized or surrendered device itself.

m. Acquisition of data from cloud storage using just the seized or surrendered SIM card, but not via the seized or surrendered device itself.

71. FSA – DIG 200 – Cell site analysis for geolocation

71.1 Definition

71.1.1 Radio frequency (RF) survey, mapping and/or cell site analysis for geolocation of a device related to criminal activity.

71.2 Required compliance

71.2.1 Compliance with the Code, including FSA specific requirements in section 100 (Cell site analysis for geolocation) is required.

71.2.2 Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 71.3.1 that the organisation undertakes, on the schedule of accreditation.

71.3 Sub-activities

71.3.1 The following sub-activities are considered to constitute FSA – DIG 200 – Cell site analysis for geolocation:

a. Cell site analysis concerning the inference of the possible geolocation of a device of interest. Cell site analysis for geolocation includes but is not limited to the following:

   i. RF propagation survey of an area or location guided by case scenario and/or call data/detail records (CDR) as part of determining geolocation of a digital device;

   ii. processing and normalisation of CDRs or other network provider data for the purposes of cell site analysis for geolocation and related findings;

   iii. creating/adopting maps of cell sites and/or cell site coverage for the purpose of reporting to court; and/or

   iv. assessment and evaluation of CDRs or other network provider data against survey data.

b. Evaluation of the significance of propagation survey and/or network information using CDRs.

c. Any of the above sub-activities (or products of activities, e.g. maps) when used to determine the geolocation of the suspect device.

71.4 Note

71.4.1 This FSA is about historical cell site analysis for geolocation typically involving CDRs, it does not include the analysis of data as a result of a requests to

telecom operator for real time or near real time device location in missing persons or threat to life cases.

71.5 Exclusions from this FSA and the Code

71.5.1 The following do not fall within the definition of 'Cell site analysis for geolocation' and are not covered by the Code:

a. Acquisition of data utilising the Crime (Overseas Production Orders) Act 2019 [97], and the analysis and processing of that data.

72. FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS)

72.1 Definition

72.1.1 The recovery and processing of still and moving images from digital closed-circuit television (CCTV), video surveillance systems (VSS) and related digital media/systems.

72.2 Required compliance

72.2.1 The following requirements apply for this FSA:

a. compliance with the Code, including section 98 Video processing and analysis, is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 72.3.1 that the organisation undertakes on the schedule of accreditation; or

b. for processing sub activities listed in 72.3.2a–e, acting in accordance with the NPCC's Framework for Video Based Evidence [98], provided:

i. the organaisation has processes approved by its SAI, and the methods and tools to be used in this FSA are based upon current practices, such as the Defence Science and Technology Laboratory's (Dstl's) Recovery and Acquisition of Video Evidence [99];

ii. the organisation records and maintains the competence of personnel it authorises to conduct the above work (personnel conducting any FSA or part of an FSA are called 'practitioners'); and

iii. practitioners comply with the practices outlined in the FSA specific requirement 'Video processing and analysis' (section 98), including but not limited to use of the declaration set out in section 98.10.3.

c. for processing sub-activities listed in 72.3.2e: if further specialist analysis is not intended, it is permissible to work in accordance with the NPCC's Framework for Video Based Evidence [98] and the FSA specific requirement Video processing and analysis (section 98), using methods and tools that have been approved by or on behalf of the SAI.

72.2.2 However, 72.2.1a applies if:

i. the primary purpose is to undertake further specialist analysis (e.g. activities detailed in FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73); or

ii. criteria such as the framework listed are not adhered to (e.g. SAI approved methods, NPCC Framework).

72.3 Sub-activities

72.3.1 The following sub-activities are considered to constitute 'Recovery and processing of footage from CCTV/VSS'.

72.3.2 The recovery and processing of any part of the content of a video file, including:

a. recovery of footage from digital CCTV/VSS in situ utilising the CCTV system /VSS manufacturer's intended method:

i. export video (exporting files using the CCTV/VSS system, copying via analogue or digital output); and/or

ii. extraction of removable media intended by the manufacturer to be portable;

b. disconnection and removal of the complete digital video recorder (DVR) as an item from a working digital CCTV system/VSS;

c. creation of a master;

d. use of the Digital Evidence Management System (DEMS)/ Digital Asset Management System (DAMS) for the following:

   i. uploading to DEM/DAMS to secure or create a master;

   ii. transfer of data;

   iii. clipping for length - permitting the clipped sections (remaining as separate files) to be accessed as a collection of clips in a playlist;

   iv. compilation within the DEMS/DAMS of media files (based on level of training);

   v. creation of a still image for evidential use (this may include basic brightness and contrast adjustment to entire image);

   vi. redaction;

   vii. removing audio from footage;

   viii. use of video analytics tools for review purposes;

   ix. conversion of a single source video file.

e. processing activities outside of a DEMS/DAMS after a master is created of the original material, including:

   i. conversion of single source video file for viewing or presentation purposes (not the production of video compilations (see and glossary), including basic levels, basic brightness and contrast adjustment to entire clip);

   ii. adding highlighting elements (e.g. circles, arrows) or masking to a digital still;

   iii. clipping for length;

   iv. creation of a still image for evidential use (this may include basic brightness and contrast adjustment to entire image);

   v. removing audio from footage; and

   vi. use of video analytics tools for review purposes.

72.4 Note

72.4.1 Where the compliance route articulated in 72.2.1.b is used, then accreditation to ISO/IEC 17025:2017 [3] and compliance with parts B and C of the Code is not required. Where recovery and presentation of the footage as a clip or still is the expected end of the process, and the forensic unit is using methods approved by the SAI and adheres to the NPCC's Framework for Video Based Evidence [98] then accreditation to ISO/IEC 17025:2017 [3] and compliance with parts B and C of this Code is not required, provided the requirements in 72.2.1b are met.

72.4.2 Where the source is multimedia and the audio is not considered the relevant material at point of commissioning, additional compliance with FSA-DIG-400 – Technical Audio Operations or FSA-DIG-401 – Speech and Audio Analysis is not required. It shall be made clear to the commissioning party which FSA(s) has been applied.

72.4.3 The following FSAs do not fall within the definition of 'Recovery and processing of footage from CCTV/ video surveillance systems (VSS)' but are the subject of a different FSA definition:

a. FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73).

b. FSA – DIG 400 – Audio acquisition, conversion and processing (section 74).

c. FSA – DIG 401 – Speech and audio analysis (section 87).

72.5 Exclusions from this FSA and the Code

72.5.1 The following do not fall within the definition of 'Recovery and processing of footage from CCTV/ video surveillance systems (VSS)' and are not covered by the Code:

a. Receiving CCTV/VSS files from a third party (e.g. owner of CCTV system).

b. Receiving a DVR from the owner as an item/exhibit.

c. Activity to assist the controlled or uncontrolled viewing of films, photographs and images by an individual who is not an eye-witness for the purposes of obtaining suspect recognition, identification, potential links

and other lines of enquiry, e.g. circulation of an unidentified subject image on a police system or in accordance with police processes (i.e. an activity governed by the Code of Practice for the identification of persons by Police Officers: Police and Criminal Evidence Act (1984) (PACE), Code D [100]).

d. Searching of a captured image against a database of reference images or defined candidate list including, but not limited to, the use of a live or retrospective facial recognition system.

e. Routine extraction of audio-video material from systems controlled by a body involved in the detection and/or investigation of crime (including in joint operations), and the editing and redaction of this material. Examples of this material include, but are not limited to, drones, body worn video, emergency calls (e.g. 112, 999) and video recorded interviews.

f. Audio/visual replay/review as part of an investigation or for routine transcription services (i.e. not as covered in 87.3.1b on questioned content analysis);

g. Acquisition of data utilising the Crime (Overseas Production Orders) Act 2019 [97], and the analysis and processing of that data.

73. FSA - DIG 301 - Specialist video multimedia, recovery, processing and analysis

73.1 Definition

73.1.1 Recovery, processing and analysis, including comparison of digital multimedia of individuals (including faces) and items such as clothing or vehicles.

73.2 Required compliance

73.2.1 Compliance with the Code, including the FSA specific requirements in section 98 (Video processing and analysis) where relevant, is required. Compliance is demonstrated by having accreditation to ISO/IEC 17025:2017 [3], with the Code and the sub-activities of this FSA listed in section 73.3.1 that the organisation undertakes on the schedule of accreditation.

73.3 Sub-activities

73.3.1 The following sub-activities are considered to constitute ‘Specialist video multimedia, recovery, processing and analysis’:

a. Recovering, processing or analysing any part of the content of an image or video file (including associated metadata or configuration data if required), including any of the following:

i. Recovery of CCTV/VSS footage from a DVR removed from the CCTV/VSS system, i.e. when no longer ‘in situ’.

ii. Removal of DVR components (e.g. hard drive) and/or recovery of CCTV/VSS footage from such components.

iii. Recovery of CCTV/VSS footage from a DVR using a third-party tool, i.e. using methods other than the manufacturer’s intended methods (section 98.7.3).

iv. Data recovery of CCTV/VSS footage from a DVR file system through reverse engineering.

v. Legacy format conversion enhancement or demultiplexing; including analogue and digital tape conversion (section 98.6.11).

vi. Enhancement/processing of digital images/video and the application of filters or techniques.

vii. Production of digital stills for further specialist analysis, including but not limited to comparison.

b. Activity to also be included as part of the end-to-end process; if conducted, include the following:

i. Production of video compilations (combining into a single file i.e. not simply editing for length) outside of a DEMS solution;

ii. Redaction or masking of subjects or objects in footage using third-party tools or methods outside of DEMS/DAMS software;

iii. Data recovery of CCTV/VSS footage from a standard file system (e.g. FAT/NTFS/XFS etc);

iv. Repair of damaged/corrupt media files or physical media.

c. The examination/analysis of any part of the content of an image or video file (including associated metadata or configuration data if acquired) to produce an evidential report including any of the following (which are opinion evidence):

i. Pictorial image comparison.

ii. Comparison of an image against one or more other images e.g. for the purpose of facial comparison.

iii. Comparison of an image against one or more physical objects, e.g. weapons, vehicles and clothing.

iv. Height/distance estimation.

v. Speed estimation from video.

vi. Analysis of precision and accuracy of timing information related to video footage (e.g. associated system metadata or configuration data if acquired).

vii. Other image content analysis, to provide an expert opinion rather than a lay narration of events. Examples include identifying a firearm, use of a firearm, technical resolution of a number plate in footage, technical resolution of a logo. Except where it is explicitly part of another FSA e.g. section 42.3.1d.

Sub-activities not required to be included in accreditation scope

73.3.2 The following sub-activities are part of this FSA, the Code applies but any requirement for ISO accreditation does not apply:

a. Analysis of media for the purpose of giving opinion on whether it may have been edited/tampered and/or synthetic (e.g. deep fake) and/or to provide an opinion on how it was created.

73.4 Note

73.4.1 Where the source is multimedia and the audio is not the principal element (i.e. only the video is critical), compliance with FSA-DIG-400 – Technical Audio Operations or FSA-DIG-401 – Speech and Audio Analysis is not required. It shall be made clear to the commissioning party which FSA(s) has been applied.

73.4.2 The following does not fall within the definition of ‘Specialist video multimedia, recovery, processing and analysis’, but is the subject of a different FSA definition:

a. FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72).

73.5 Exclusions from this FSA and the Code

73.5.1 The following do not fall within the definition of ‘Specialist video multimedia, recovery, processing and analysis’ and are not covered by the Code:

a. Operation of automatic number plate recognition systems for the purpose of capture of registration numbers.

b. Activity to assist the controlled or uncontrolled viewing of films, photographs and images by an individual who is not an eye-witness for the purposes of obtaining suspect recognition, identification, potential links and other lines of enquiry. For example, circulation of an unidentified subject image on a police system or in accordance with police processes (i.e. activity governed by the Code of Practice for the identification of persons by Police Officers, PACE Code D).

c. Creation of E-fit, or digital facial composite images, for use under PACE Code D.

d. Searching of a captured image against a database of reference images or defined candidate list including, but not limited to, the use of a live or retrospective facial recognition system.

e. Download of audio-visual media from a DEMS/DAMS as part of an investigation.

f. Routine extraction of audio-video material from systems controlled by a body involved in the detection and/or investigation of crime (including in joint operations), and the editing and redaction of this material. Examples of this material include, but are not limited to, drones, body worn video, emergency calls (e.g. 112, 999) and video recorded interviews.

g. Audio/visual replay/review as part of an investigation or for routine transcription services (i.e. not as covered in 87.3.1b on questioned content analysis).

h. Acquisition of data utilising the Crime (Overseas Production Orders) Act 2019 [97], and the analysis and processing of that data.

74. FSA – DIG 400 – Audio acquisition, conversion and processing

74.1 Definition

74.1.1 Acquisition, conversion and processing of audio.

74.2 Required compliance

74.2.1 From the date of the Code coming into force, compliance is demonstrated by:

a. having accreditation to ISO/IEC 17025:2017 [3], with the Code, and the sub-activities of this FSA listed in section 74.3.1 that the organisation undertakes on the schedule of accreditation; or

b. working in accordance with the NPCC's Framework for Video Based Evidence [119] (including the training requirements), for the sub-activities listed in 74.3; or

c. where the source is multimedia, and the audio is not considered the most relevant material at point of commissioning (i.e. only the video is considered directly relevant), the compliance requirements of either the following FSAs may be applied instead:

   i. FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72); or

   ii. FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73).

74.3 Sub-activities

74.3.1 The following sub-activities are considered to constitute 'Audio acquisition, conversion and processing':

a. Acquisition of analogue or digital audio from a source item.

b. Digital audio file format conversion.

c. Editing and redaction (section 73.3.2 and exclusion 73.4.2a).

Sub-activities not required to be included in accreditation scope

74.3.2 The following sub-activity is part of this FSA, the Code applies but any requirement for ISO accreditation does not:

a. Processing of digital audio: enhancement, application of filters, voice disguise, speed and/or level control.

74.4 Note

74.4.1 The following sub-activities are part of this FSA, however accreditation and compliance with parts B and C of the Code does not apply provided there is compliance with the NPCC CCTV Framework (a declaration based on section 98.10.3 should be used):

a. Use of the Digital Evidence Management System (DEMS)/ Digital Asset Management System (DAMS) for the following:

i. uploading to DEM/DAMS to secure or create a master;

ii. transfer of data;

iii. clipping for length - permitting the clipped sections (remaining as separate files) to be accessed as a collection of clips in a playlist;

iv. compilation within the DEMS/DAMS of media files (based on level of training);

v. redaction;

vi. removing video from audio;

vii. conversion of audio.

74.4.2 Sub-activities in FSA - DIG - 400 may performed under FSA - DIG - 401 (Speech and Audio Analysis - section 87)) without additional Code or accreditation requirements provided the forensic unit:

a. complies with Part A of the Code; and

b. notifies the Regulator of their intention to perform sub-activities in FSA - DIG - 400 for the purposes of DIG - 401.

74.5 Exclusions from this FSA and the Code

74.5.1 The following do not fall within the definition of 'Audio acquisition, conversion and processing' and are not covered by the Code:

a. Routine extraction of audio-video material from systems controlled by a body involved in the detection and/or investigation of crime (including in joint operations), and the editing and redaction of this material. Examples of this material include, but are not limited to, drones, body worn video, emergency calls (e.g. 112, 999) and video recorded interviews.

b. Download of audio-visual media from a DEMS/DAMS as part of an investigation.

c. Acquisition of data utilising the Crime (Overseas Production Orders) Act 2019 [97], and the analysis and processing of that data.

d. Audio/visual replay/review as part of an investigation or for routine transcription services (i.e. not as covered in 87.3.1b on questioned content analysis).

D2 – FSAs to which the Code does not apply

75. FSA – INC 101 – Collision investigation

75.1 Definition

75.1.1 The controlled management, interpretation and examination of a collision scene, the site of a collision, or a vehicle (see Note), including identifying, preserving and recording contact traces, biological and physical material, to establish the circumstances which have resulted in the collision.

75.1.2 This activity applies to a practitioner who is commissioned to carry out all or part of the sub-activities specified in this FSA.

75.2 Required compliance

75.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

75.3 Sub-activities

75.3.1 The following sub-activities are considered to constitute 'Collision investigation':

a. Collision scene management, including but not limited to:

i. scene assessment and control;

ii. setting of an examination strategy, including joint examination strategies where necessary;

iii. identifying, preserving and recording biological and physical material that could be relevant to the collision;

iv. identifying, preserving and recording areas of damage and other marks and traces that could be relevant to the collision;

v. coordination of activities at the collision scene;

vi. management of other practitioners and activities; and

vii. interpretation of the collision scene(s).

b. Examination of a vehicle as a whole (see Note), including:

i. assessing the pre-collision condition of the vehicle, controls and components;

ii. identifying, preserving and recording areas of damage and other marks and traces that could be relevant to the collision;

iii. identifying, preserving and recovering devices fitted to record electronic data that could be relevant to the collision;

iv. identifying and recovering physical material such that further testing or examination could be carried out; and

v. assessing and recording of damage and physical fit of damaged components.

75.4 Note

75.4.1 Examination of a vehicle under this FSA may be carried out at a location other than the collision scene provided it is commissioned and directed by a Collision Investigator or a body involved in the detection and/or investigation of crime and:

a. is considered to be a service provided to that Collision Investigator or a body involved in the detection and/or investigation of crime; and

b. does not include examination or testing of individual, discrete components. This does not include removal of components as part of the examination process (such as removal of wheels to inspect brake pads); however, discrete components which can be removed from a vehicle for examination and testing should be examined in a facility which meets the requirements of ISO/IEC 17025:2017 [3]. If carried out by exception, then such components may be examined according to the criteria for specialists from outside the forensic science profession as set out at section 9 of the Code.

75.4.2 ‘Collision scene’ means a location where a vehicle has been involved in a suspected collision, before the on-scene examination is concluded. This includes investigation of collisions where the collision may have been non-accidental. Collision scenes also include a location where a vehicle suspected

of having been involved in a collision is found where the examination is for the purpose of establishing the circumstances which have resulted in the collision.

75.4.3 'Collision site' means a location where a collision involving a vehicle is suspected to have occurred, but the vehicle(s) is no longer in-situ.

75.4.4 The following does not fall within the definition of 'Collision investigation', but is the subject of a different FSA definition:

a. FSA – INC 100 - Incident scene examination (section 39).

b. FSA – DIG 100 – Data capture, processing and analysis from digital storage devices (section 70).

c. FSA – DIG 301 – Specialist multimedia recovery, processing, and analysis (section 73)

75.5 Exclusions from this FSA and the Code

75.5.1 The following do not fall within the definition of 'Collision Investigation' and are also not covered by the Code:

a. activity undertaken to protect/preserve items/exhibits from imminent alteration or destruction by persons not specifically commissioned to carry out an FSA as specified in the Code, e.g. first responders; and

b. any investigation related to determining the cause of an air or rail crash, or the sinking of a vessel (capable of travelling on or under the water) at sea or on inland waters.

76. FSA – INC 102 – Examination of fire scenes

76.1 Definition

76.1.1 The examination and interpretation of the scene of a fire and/or a gas (vapour) phase explosion to establish the origin, cause and development/spread of a fire/explosion.

76.1.2 Where it is known that an explosion is the result of condensed phase explosives the examination will fall under FSA - INC 103 – Examination of explosion scenes.

76.1.3 This activity applies to a practitioner who is commissioned to carry out all or part of the sub-activities specified in this FSA.

76.2 Required compliance

76.2.1 This version of the Code does not apply to this FSA, therefore this FSA has no requirements set for compliance, including any for accreditation.

76.3 Sub-activities

76.3.1 The following sub-activities are considered to constitute 'Examination of fire scenes':

a. Fire/explosion scene examination, including but not limited to:

   i. scene assessment and control;

   ii. setting of an examination strategy, including joint examination strategies where necessary;

   iii. identifying, preserving and recording physical material that could be relevant to assessing the origin, cause and/or spread of the fire;

   iv. coordination of activities at the scene;

   v. management of other practitioners and activities; and

   vi. interpretation of the scene(s).

b. Identification of items to be recovered for further examination to assist with establishing the origin, cause and/or spread of a fire/explosion.

c. Analysis to assist with establishing the origin, cause and/or spread of a fire/explosion, such as presumptive testing for ignitable liquid residues, fuse and circuit testing, and fire dynamics calculations.

76.4 Note

76.4.1 The following do not fall within the definition of 'Examination of fire scenes', but are the subject of a different FSA definition:

a. FSA – INC 100 - Incident scene examination (section 39).

b. FSA – INC 103 - Examination of explosion scenes (section 77).

76.4.2 Where activities that are specified as other FSAs are performed at a fire scene, those FSAs apply.

76.5 Exclusions from this FSA and the Code

76.5.1 The following do not fall within the definition of ‘Examination of fire scenes’ and are also not covered by the Code:

a. activity undertaken to protect/preserve items/exhibits from imminent alteration or destruction by persons not specifically commissioned to carry out an FSA as specified in the Code, e.g. first responders;

b. any investigation related to determining the cause of an air or rail crash, or the sinking of a vessel (capable of travelling on or under the water) at sea or on inland waters.

77. FSA – INC 103 – Examination of explosion scenes

77.1 Definition

77.1.1 The examination and interpretation of the scene of an explosion to establish the origin and cause of an explosion.

77.1.2 This activity does not include examination of gas (vapour) phase explosion scenes that are typically examined by fire investigators, see FSA - INC 102.

77.1.3 This activity applies to a practitioner who is commissioned to carry out all or part of the sub-activities specified in this FSA.

77.2 Required compliance

77.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

77.3 Sub-activities

77.3.1 The following sub-activities are considered to constitute ‘Examination to establish the origin and cause of an explosion’:

a. Explosion scene examination, including but not limited to:

i. scene assessment and control;

ii. setting of an examination strategy, including joint examination strategies where necessary;

iii. identifying, preserving and recording physical material that could be relevant to assessing the origin and/or cause of the explosion;

iv. coordination of activities at the explosion scene;

v. management of other practitioners and activities; and

vi. interpretation of the explosion scene(s).

b. Identification of items to be recovered for further examination to assist with establishing the origin and/or cause of an explosion.

c. Analysis and testing to assist with establishing the origin and/or cause of an explosion.

77.4 Note

77.4.1 'Scene of an explosion' means any location where an explosion has occurred.

77.4.2 The following do not fall within the definition of 'Examination of explosion scenes', but are the subject of a different FSA definition:

a. FSA – INC 100 - Incident scene examination (section 39).

b. FSA – INC 102 - Examination of fire scenes (section 76).

77.4.3 Where activities that are specified as other FSAs are performed at the scene of an explosion, those FSAs apply.

77.5 Exclusions from this FSA and the Code

77.5.1 The following do not fall within the definition of 'Examination of explosion scenes' and are also not covered by the Code:

a. activity undertaken to protect/preserve items/exhibits from imminent alteration or destruction by persons not specifically commissioned to carry out an FSA as specified in the Code, e.g. first responders; and

b. any investigation related to determining the cause of an air or rail crash, or the sinking of a vessel (capable of travelling on or under the water) at sea or on inland waters.

78. FSA – INC 200 – Forensic examination of witnesses/complainants/suspects

78.1 Definition

78.1.1 Examination of witnesses/complainants/suspects for contact traces and physical material, such that further examination/analysis would be subject to another FSA specified by the Code.

78.2 Required compliance

78.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

78.3 Sub-activities

78.3.1 The following sub-activities are considered to constitute 'Forensic examination of witnesses/complainants/suspects':

a. Examination with the aim of locating and recovering relevant material such that further testing or examination that is specified as an FSA could be carried out.

b. Documentation of relevant injuries and distinctive marks, including evidential photography and specialist imaging.

78.4 Note

78.4.1 The following does not fall within the definition of 'Examination of witnesses/complainants/suspects', but is the subject of a different FSA definition:

a. FSA – BIO 100 – Forensic medical examination of complainants (section 40).

78.5 Exclusions from this FSA and the Code

78.5.1 The following does not fall within the definition of 'Forensic examination of witnesses/complainants/suspects' and is also not covered by the Code:

a. Taking of custody images.

79. FSA – INC 201 – Forensic examination of deceased individuals

79.1 Definition

79.1.1 Examination of a body or body part for contact traces and physical material, such that further examination/analysis would be subject to another FSA specified by the Code.

79.1.2 The sub-activities listed below may occur at different locations, including at incident scenes (section 39) and facilities where forensic post-mortems are carried out.

79.2 Required compliance

79.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

79.3 Sub-activities

79.3.1 The following sub-activities are considered to constitute 'Forensic examination of deceased individuals':

a. Examination of a body or part of a body with the aim of locating and recovering material such that further testing or examination that is specified as an FSA could be carried out.

b. Documentation of relevant injuries and distinctive marks, including evidential photography and specialist imaging.

c. Ballistics activities, such as recognising projectile entry/exit wounds, wound angles, recognising effects from close range firing of a firearm and advice on imaging of the body.

79.4 Exclusions from this FSA and the Code

79.4.1 The following does not fall within the definition of 'Forensic examination of deceased individuals' and is also not covered by the Code:

a. Activities of a pathologist to assist with determining the cause and/or time of death.

80. FSA – BIO 302 – Non-human biological examination and analysis: plants, fungi, diatoms, microbes, and invertebrates

80.1 Definition

80.1.1 Examination and analysis to determine species and/or the potential source of plant, fungal, diatomical, microbial, and/or invertebrate material.

80.2 Required Compliance

80.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set including any for accreditation.

80.3 Sub-Activities

80.3.1 The following sub-activities are considered to constitute 'Non-human biological examination: plants, fungi, diatoms, microbes, and invertebrates':

a. Recovery of samples for further testing.

b. Morphological examination of relevant material.

c. Macroscopic, microscopic, and immunological tests for species identification.

d. DNA analysis for species identification, and microbial profiling.

e. The comparison, interpretation, including use of reference collections, and databases (section 27) and any statistical analysis.

f. Entomology, including analysis of other invertebrates to assess minimum time of death.

g. Analysis to determine geographical provenance of plant, fungi, diatom, microbe, and/or invertebrate material.

80.4 Exclusions from this FSA

a. The activities of an individual other than the practitioner, who is taking steps to protect/preserve or collect material for analysis.

80.5 Note

80.5.1 In this FSA the term ‘relevant material’ refers to any part of a plant, (including seeds, pollen, spores), fungi, diatoms, microbes, and/or invertebrates.

81. FSA – DTN 104 – Toxicology: alcohol technical calculations

81.1 Definition

81.1.1 Alcohol technical calculations and consideration of alternative propositions based on breath, blood or urine concentrations, critical timings, height, weight and gender, and claimed drinking patterns.

81.2 Required compliance

81.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

81.3 Sub-activities

81.3.1 The following sub-activities are considered to constitute ‘Toxicology: alcohol technical calculations’:

a. Any of the following activities undertaken in relation to an offence under the Road Traffic Act 1988 [81], the Transport and Works Act 1992 [82] or the Railways and Transport Safety Act 2003 [83] and, where appropriate, other forensic casework toxicology:

   i. estimation of breath, blood or urine alcohol concentrations at any time other than the time of measurement, based on the measurement of the concentration of alcohol in blood, breath or urine, and declared drinking pattern;

   ii. estimation of breath, blood or urine alcohol levels at any time based on a stated pattern of drinking;

   iii. consideration of the possible impact of drinking alcohol at a specific time based on the concentration of alcohol in breath, blood or urine at a specific time;

iv. consideration of the possible impact of imbibing a ‘spiked’ drink on the concentration of alcohol in breath, blood or urine at any time;

v. consideration of the concentration of alcohol in blood/breath at a stated time of next driving; and

vi. interpretation of the overall findings from aspects of mathematics, physiology and relevant contextual information, to assess the credibility of the driver’s account.

b. Consideration of any of the following matters:

i. findings from any of the work above;

ii. significance of the findings from the activities discussed above in relation to the concentration of alcohol in breath, blood or urine at any time;

iii. significance of the findings from the activities above in relation to the impairment of a driver at any given time; and

iv. rate at which alcohol may be absorbed and eliminated by a person.

c. If conducted, the following are covered by this FSA:

i. consideration of the potential impact of the measurement/analysis method on the reliability of the concentration of alcohol in breath, blood or urine, or whether that concentration was above a legal limit; and

ii. consideration of the potential impact of any factors extraneous to the measurement/analysis on the reliability of the determination of the concentration of alcohol in breath, blood or urine, or whether that concentration was above a legal limit.

d. Evaluation of the likelihood of alcohol appearing in the body by means of some route other than consumption, such as by inhalation, auto-brewery syndrome, vapes, foods, medications and through the use of skin wipes.

e. Possible effect, if any, of regurgitation and vomiting on breath analysis.

81.4 Note

81.4.1 The following do not fall within the definition of 'Toxicology: alcohol technical calculations' but are the subject of a different FSA definition:

a. FSA – DTN 100 – Toxicology: analysis for drug(s), alcohol and/or noxious substances (section 47).

b. FSA – DTN 101 – Toxicology: analysis for drugs and/or alcohol under the Road Traffic Act 1988, Transport and Works Act 1992, and Railways and Transport Safety Act 2003 (section 48).

c. FSA – DTN 102 – Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988 (section 49).

82. FSA – DTN 105 – Examination and analysis relating to the preparation and production of controlled drugs and/or psychoactive substances

82.1 Definition

82.1.1 Examination and/or analysis of materials (including packaging and paraphernalia) used, or suspected of use, in the preparation and/or production of material believed to be controlled drugs or psychoactive substances.

82.1.2 Consideration of the production, method of synthesis or cultivation, and/or yield of controlled drugs or psychoactive substances.

82.2 Required compliance

82.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

82.3 Sub-activities

82.3.1 The following sub-activities are considered to constitute 'Examination and analysis relating to the preparation and production of drugs and/or psychoactive substances':

a. Examination and/or analysis of any item/exhibit, or material recovered from an item/exhibit, and the interpretation of findings to determine:

i. whether it could be employed in the preparation to supply, or production of a relevant substance: and/or

ii. whether it can be connected to a particular production or supply source of a relevant substance.

b. Analysis to determine the actual yield, or potential yield, of any means of production of a relevant substance.

c. Controlled drug/psychoactive substance identification, including use of reference databases (section 27).

d. Consideration of any of the following:

i. synthetic routes to produce drugs/psychoactive substances;

ii. what drugs/psychoactive substances may be synthesised from given compounds;

iii. legal classification of any relevant substance that could be produced;

iv. common associated materials as evidence of preparation to supply particular drugs/psychoactive substances; and/or

v. common equipment/paraphernalia as evidence of production of particular drugs/psychoactive substances.

82.4 Note

82.4.1 In this section the term ‘relevant substance’ means anything falling within the descriptions below:

a. Any substance which is listed (by name or by virtue of its chemical structure) in any Schedule to the Misuse of Drugs Act 1971 [85].

b. Any substance which is a psychoactive substance within the provisions of the Psychoactive Substances Act 2016 [80].

82.4.2 In this section the term ‘associated material(s)’ includes cutting agents, additives, and diluents.

82.4.3 The following do not fall within the definition of ‘Examination and analysis relating to the preparation and production of drugs and/or psychoactive substances’ but are the subject of a different FSA definition:

a. FSA – DTN 100 – Toxicology: analysis for drug(s), alcohol and/or noxious substances (section 47).

b. FSA – MTP 100 – Friction ridge detail: visualisation and enhancement (section 56).

c. FSA – DTN 103 – Examination and analysis to identify and quantify controlled drugs and/or associated materials (section 50).

82.5 Exclusions from this FSA and the Code

82.5.1 The following do not fall within the definition of 'Examination and analysis relating to the preparation and production of controlled drugs and/or psychoactive substances' and are also not covered by the Code:

a. Testing of any item/exhibit, or part thereof, to determine whether it is comprised of or contains a relevant substance in the circumstances set out below:

   i. with a Home Office approved kit under the processes permitted by a HOC; and/or

   ii. with a Home Office approved kit under the processes set out in the EDIT programme;

b. controlled drugs value estimation;

c. provision of any evidence in relation to whether a particular compound (or group or class of compounds) is psychoactive in relation to the provisions of the Psychoactive Substances Act 2016 [80];

d. screening of items for drugs at an airport or other transport hub.

83. FSA – DTN 502 – Examination and analysis of radioactive material

83.1 Definition

83.1.1 The examination and analysis of radioactive material to provide information to a criminal investigation and evidence in criminal proceedings.

83.2 Required compliance

83.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

83.3 Sub-activities

83.3.1 The following sub-activities are considered to constitute 'Examination and analysis of radioactive material':

a. Examination of any item/exhibit to determine whether relevant material is present.

b. Recovery of any relevant material or item/exhibit of the descriptions below:

   i. an item/exhibit comprised of or containing relevant material; and/or

   ii. an item/exhibit which has relevant material on it.

c. Examination and/or analysis of any item/exhibit or matter to determine any of the following:

   i. identification of an isotope;

   ii. potential immediate source (i.e. device) of relevant material;

   iii. degree of similarity of different samples of relevant material; and/or

   iv. degree of similarity of a sample of relevant material to any reference material or sample of known origin.

d. Determination of the potential geographical origin (i.e. nation, geographical location or production facility) of any relevant material.

83.4 Note

83.4.1 Subject to the points below, 'relevant material' means any of the following:

a. A radioactive substance held in circumstances where the possession amounts to a criminal offence, other than an offence under laws related to:

   i. health and safety at work; or

   ii. environmental protection.

b. A radioactive substance which is held with the intention that it may be used for, or to facilitate, the commission of a criminal offence.

c. Any radioactive substance which is being used for, or to facilitate, the commission of a criminal offence.

d. Any radioactive material which has contaminated any person or location as the result of a criminal offence or attempt to commit an offence.

83.4.2 The radioactive nature of the substance shall be a significant factor in the nature of the criminal offence referred to above.

83.4.3 The definition of the criminal offence need not refer to radioactive material.

83.4.4 In this section 'radioactive substance' means material which would be radioactive material under the provisions of the Radioactive Substances Act 1993 [101].

84. FSA – DTN 503 – Examination and analysis of suspected explosive devices and associated material

84.1 Definition

84.1.1 Examination and analysis of suspected explosive devices, component parts of devices or remnant parts of such a device.

84.2 Required compliance

84.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

84.3 Sub-activities

84.3.1 The following sub-activities are considered to constitute 'Examination and analysis of suspected explosive devices and associated material':

a. Examination of any item/exhibit to determine whether relevant material is present.

b. Recovery of any relevant material or item/exhibit.

c. Examination and/or analysis of any item/exhibit to determine any of the following:

i. explosive significance of the relevant material;

ii. cause and/or circumstances of an explosion;

iii. composition of the explosive device;

iv. potential viability of the explosive device;

v. potential of the explosive device to cause harm to people or damage to property; and/or

vi. result, or potential result, of the use of an explosive device.

84.4 Note

84.4.1 In this section ‘relevant material’ includes any of the following:

a. Components of explosive devices, including electrical components.

b. Literature or other medium providing instructions for the preparation of explosive devices.

c. Materials other than an explosive substance or chemical accelerant which could be used to modify the nature of an explosion, including shrapnel.

84.4.2 The term ‘explosive substance’ covers any material which would be subject to the provisions of the Explosives Act 1875 [91], the Explosive Substances Act 1883 [88] or the Explosives Regulations 2014 [92].

84.4.3 The ‘make safe’ process does not form part of this FSA but is an important part of the workflow and should be carried out by trained specialists where preservation of life is the initial priority. Forensic practitioners should consider how the make safe process impacts preservation of other potential evidence types.

84.4.4 The following do not fall within the definition of ‘Examination and analysis of explosive devices’ but are the subject of a different FSA definition:

a. FSA – DTN 501 – Examination and analysis of explosives, explosives precursors and explosive residues (section 55).

b. FSA – INC 102 – Examination of fire scenes (section 76).

84.5 Exclusions from this FSA and the Code

84.5.1 The following does not fall within the definition of ‘Examination and analysis of suspected explosive devices and associated material’ and is also not covered by the Code:

a. Screening of items/persons/locations for explosives residue, including the screening of people at a port.

85. FSA – DIG 101 – Analysis of communications network data

85.1 Definition

85.1.1 Analysis of communications data as detailed in the sub-activities for the purpose of informing the investigation not covered by:

a. FSA – DIG 100 – Data capture, processing and analysis from digital storage devices (section 70); or

b. FSA – DIG 200 – Cell site analysis for geolocation (section 71).

85.1.2 Performing the analysis as detailed in the sub-activities in this FSA for the purpose of informing the investigation where reports to the investigator (including products such as maps and charts) are clearly marked as 'This forensic information is not intended as evidence' and meeting the other criteria of this FSA is not covered by the Code.

85.2 Required compliance

85.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

85.3 Sub-activities

85.3.1 The following sub-activities conducted for the purpose of providing advice, or to guide the investigation, are considered to constitute 'Analysis of communications network data (FSA – DIG 101 – Analysis of communications network data):

a. Processing and normalisation of CDR or other network provider data for the purposes of informing the investigation as to the geolocation of a suspect device.

b. Presumptive automated tools for analysing CDRs, including 'co-location' analysis, and accepting the risks and limitations, including confirmation bias.

c. Production of mapping of cell sites and/or cell site coverage for informing the investigation as to the geolocation of a suspect device.

85.3.2 The products of this FSA to meet the definition and not be subject to any other relevant FSA, shall include the header 'This forensic information is not intended as evidence' and instructions to the investigator in the following terms, or in terms substantially the same:

> 'The forensic information contained in this report is based on the information provided and contains initial findings and/or assessment of a crime scene and item(s)/exhibit(s). It is provided to the police investigator to support a line of enquiry and/or establish if there is evidential value in proceeding with the forensic information. Should further forensic analysis or comparison be required in this case, the investigator must contact the relevant practitioners with their requirements.'

85.3.3 Any products or reports produced under this FSA are not intended for court use or court presentation unless evaluated by a practitioner and adopted. Any products or reports that are used for court presentation and are detailed in any other relevant FSA are subject to the compliance criteria of that FSA.

85.4 Note

85.4.1 The following activities when not related to geolocation are not included in this FSA and are therefore not subject to 85.3.2 processing and normalisation of CDRs to identify:

a. common called numbers;

b. cross connectivity of common numbers;

c. International Mobile Equipment Identity number; and/or

d. presenting a-c graphically, but not in map form.

85.5 Exclusions from this FSA and the Code

85.5.1 The following do not fall within the definition of 'Analysis of communications network data' and are also not covered by the Code:

a. Data recovery via Internet Intelligence & Investigations (III), Open Source Intelligence (OSINT), Signals Intelligence (SIGINT), Communications

Intelligence (COMMINT) and Geospatial intelligence (GEOINT) is excluded from the Code.

b. Acquisition of data utilising the Crime (Overseas Production Orders) Act 2019 [97], and the analysis and processing of that data.

c. Acquisition of data from cloud storage as a result of login/connection data taken from a device under examination, but not via the seized or surrendered device itself.

d. Acquisition of data from cloud storage using just the seized or surrendered SIM card, but not via the seized or surrendered device itself.

86. FSA – DIG 102 – Digital network capture and analysis

86.1 Definition

86.1.1 Capture and analysis of network traffic to understand the properties/setup of the network, including at scenes of incident.

86.2 Required compliance

86.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

86.3 Sub-activities

86.3.1 The following sub-activities are considered to constitute 'Digital network capture and analysis'.

a. Traffic collection and analysis.

b. Packet collectors (sniffers), protocol analysers and network forensic analysers.

c. Network topology diagram, including information gathering about network setup.

d. Data-link and physical layer analysis (Ethernet).

e. Transport and network layer analysis (TCP/IP).

f. Netflow analysis.

g. DNS review/analysis.

h. Dynamic host configuration protocol review.

i. Application layer analysis (e.g. HTTP, FTP, SMTP encryption).

87. FSA – DIG 401 – Speech and audio analysis

87.1 Definition

87.1.1 The analysis of recorded speech and audio, and the assessment of complainant, suspect and/or witness claims relating to speech or other sounds.

87.2 Required compliance

87.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

87.3 Sub-activities

87.3.1 The following sub-activities are considered to constitute 'Speech and audio analysis':

a. Speaker comparison – comparison of recorded voices to assist the court in deciding whether they are the same or different speakers.

b. Questioned content analysis – includes both analysis of questioned speech and specialist forensic transcription for the purposes of providing expert evidence (does not include transcription by non-specialists e.g. by police staff/officers).

c. Authenticity analysis – analysis of recordings to assess their provenance and/or for evidence of the recordings having been edited/tampered with.

d. Electrical network frequency analysis of mains frequency interference in recordings.

e. Speaker profiling – analysis of a recording of an unknown voice for information about the speaker.

f. Voice parade design (the auditory equivalent of visual identification parades).

g. Sound propagation analysis to determine audibility at specific locations.

h. Analysis of a sound in a recording to determine its source/cause.

87.3.2 Where sub-activities in DIG 400 are performed for the purposes of FSA - DIG 401, they may be performed entirely under FSA - DIG 401 (i.e. without accreditation and compliance with all Parts of the Code) provided the forensic unit:

a. complies with Part A of the Code; and

b. notifies the Regulator of their intention to perform sub-activities in FSA - DIG 400 are performed for the purposes of FSA DIG 401.

87.3.3 This version of the Code does not apply to this FSA, therefore no declaration that infers compliance with the Code should be used, although stating that the Code does not apply, may be appropriate [70].

87.4 Note

87.4.1 The following do not fall within the definition of 'Speech and audio analysis' but are the subject of a different FSA definition:

a. FSA – DIG 100 – Data capture, processing and analysis from digital storage devices (section 70).

b. FSA – DIG 200 – Cell site analysis for geolocation (section 71).

c. FSA – DIG 400 – Audio acquisition, conversion and processing (section 74).

87.4.2 Where the source is multimedia, and the audio is not the principal element (i.e. only the video is critical), compliance with either of the following FSAs instead of this FSA is permitted:

a. FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72).

b. FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73).

87.5 Exclusions from this FSA and the Code

87.5.1 The following do not fall within the definition of 'Speech and audio analysis' and are also not covered by the Code:

a. routine extraction of audio-video material from systems controlled by a body involved in the detection and/or investigation of crime (including in joint operations), and the editing and redaction of this material. Examples of this material include, but are not limited to, drones, body worn video, emergency calls (e.g. 112, 999) and video recorded interviews;

b. audio/visual replay/review as part of an investigation or for routine transcription services (i.e. not as covered in 87.3.1b on questioned content analysis);

c. upload and download of audio-visual media from digital asset management systems;

d. acquisition of data utilising the Crime (Overseas Production Orders) Act 2019 [97], and the analysis and processing of that data; and

e. general transcription of audio recordings by non-specialists (by police staff/officers).

88. FSA – CDM 100 – Case review

88.1 Definition

88.1.1 The assessment of unsolved cases, findings, and/or interpretations to identify additional forensic opportunities and/or to address alternative propositions.

88.1.2 The assessment of cases, results, and/or interpretations to address alternative propositions, such as for the purpose of defence review.

88.1.3 The assessment can be performed by both the original forensic unit involved in the case or an independent forensic unit.

88.1.4 Post-conviction appeal cases and Criminal Cases Review Commission cases, where forensic science work is assessed, are within scope of this FSA.

88.2 Required compliance

88.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

88.3 Sub-activities

88.3.1 The following sub-activities are considered to constitute ‘Case review’.

a. Review of relevant previous forensic findings in the context of the most up-to-date case circumstance information (which may be different to that which was previously available):

    i. relevant findings, including physical and digital evidence, should be reviewed;

    ii. all sample types across multiple scientific disciplines may be considered – this will be dependent on the content of the original case.

b. Consideration of:

    i. whether the nature and scope of scientific investigations are/were appropriate to the case circumstances;

    ii. whether the examined items/exhibits were the appropriate ones;

    iii. the methodology for arriving at the scientific findings, and the limitations of applied methods;

    iv. the continuity and integrity of items/exhibits;

    v. the results, quality assurance measures, and critical findings checks to ascertain what can be reliability concluded and what might have been missed; and/or

    vi. the reliability and validity of previous findings.

c. Consideration to identify new opportunities, in the light of current and potential future technologies or alternative examination strategies.

d. Consideration to identify items/exhibits and/or retained materials to be located and submitted for examination/analysis.

e. Preservation of material, with a consideration of scientific developments, to facilitate future reviews.

f. Interpretation of findings from new examination/analysis, which may include interrogation of databases, with consideration given to scientific papers and new research.

88.4 Note

88.4.1 Where activities defined in other FSAs are performed as part of the case review process, such activities shall be performed in compliance with the requirements described in the Code for those FSAs.

88.5 Exclusions from this FSA and the Code

88.5.1 The following do not fall within the definition of 'Case review' and are also not covered by the Code:

a. review of work related to provision of medical care; and

b. review of forensic post-mortem examinations.

89. FSA – CDM 200 – Control and management of a forensic database service

89.1 Definition

89.1.1 The provision of a service through the operation and administration of forensic database systems to:

a. identify links between data recovered from incidents to other incidents and/or persons of interest; and/or

b. make inferences and/or interpret case-specific findings.

89.2 Required compliance

89.2.1 This version of the Code does not apply to this FSA therefore this FSA has no requirements set for compliance, including any for accreditation.

89.3 Sub-activities

89.3.1 The following sub-activities are considered to constitute 'Control and management of a forensic database service':

a. Receipt and acceptance of submitted data.

b. Control, management, quality oversight and monitoring of data integrity and processing.

c. Storage of data.

d. Searching and retrieval of data.

e. Control, management, quality oversight and monitoring of the database system.

f. Validation of database software, including matching algorithms and provision of validation results.

g. Provision of:

   i. potential forensic links;

   ii. statistical information; and/or

   iii. sample data.

h. Retention/destruction of data.

89.4 Exclusions from this FSA and the Code

89.4.1 The following does not fall within the definition of ‘Control and management of a forensic database service’ and is also not covered by the Code:

a. Activity relating to the INTERPOL database(s).

D3 – FSA specific requirements

90. Incident scene examination

90.1 Scope

90.1.1 This section sets out the specific requirements for incident scene examination and relates to the forensic science activity - FSA – INC 100 – Incident scene examination (section 39).

90.1.2 This section applies to practitioners who undertake FSA – INC 100 activities, including scene management (section 90.4), and dedicated scene managers who do not perform examination activities.

90.1.3 Incident scene examination is defined as the controlled management, examination, and interpretation of the location of an incident scene, or other related location, for contact traces and physical material such that any further testing or examination would be subject to another FSA specified by the Code.

90.1.4 The requirements may also be applicable to collision investigation (FSA – INC 101), the examination of fire scenes (FSA – INC 102), and the examination of the scene of an explosion (FSA - INC 103), however these FSAs do not require compliance with the Code.

90.1.5 Separate activities are specified for examination of witnesses/ complainants/ suspects (FSA – INC 200) and forensic examination of deceased individuals (FSA - INC 201) however these FSAs do not require compliance with the Code. These activities are not considered to be part of FSA – INC 100.

90.1.6 The scope of accreditation for organisations that undertake incident examination shall be defined on the basis that the field of inspection relates to the sub-activities listed in FSA – INC 100 (section 39.3). The methods and procedures referenced shall cover forensic scene management and the examination and recovery activities the forensic unit performs under FSA – INC 100.

90.1.7 Where activities that are specified in other FSAs are performed at an incident scene, such as FSA - BIO 201 – Human biological material distribution, or FSA

- DIG 100 – Data capture, processing and analysis from digital storage devices, those FSAs and their FSA specific requirements apply.

90.2 Competency

90.2.1 Incident scenes present a wide variety of circumstances and require the effective application of professional judgement (section 31.4.9). Forensic units shall ensure that this is reflected in all relevant procedures, and shall ensure through competence assessment and casework review that practitioners are competently using professional judgement.

90.2.2 All decisions arising from the use of professional judgement shall be based on information and/or knowledge held by the practitioner at the time the decision was made.

90.2.3 Decision making and examination activities may differ between practitioners, therefore, competency assessments shall be designed so that practitioners can demonstrate the achievement of expected outcomes through the use of professional judgement.

90.2.4 The assessment of competence shall cover the range of methods or examinations that the practitioner requires for their role. The competence framework will define the requirements to demonstrate that competence has been achieved. These requirements should reflect the level of uniformity of approach required as well as the complexity of the methods/examinations.

90.2.5 Initial or baseline competency assessments shall be defined by the forensic unit and shall include assessment at an incident scene with known outcomes.

90.2.6 The forensic unit shall retain records to demonstrate the competence of practitioners. The forensic unit shall ensure that there is an appropriate programme for the management of ongoing competency that is risk and needs based, taking into account;

a. the complexity of incident scenes attended;

b. the frequency of attendance at relevant incident scenes;

c. the experience of the practitioner;

d. the types of reporting undertaken;

e. the inherent risks in the activities being performed; and

f. any identified training needs.

90.2.7 The forensic unit shall define the types of reports, including oral reports, that may be produced by practitioners and the competency requirements to produce each type. Competency requirements should also include the provision of investigative opinion taking account of guidance issued by the Regulator (section 31.4.1; opinions and interpretation). Where reporting includes opinion provided in court proceedings the practitioner shall be considered an expert witness and shall be authorised by, or on behalf of, the SAI to report opinions (section 22.2; competence required for reporting).

90.2.8 Assessment of ongoing practitioner competency shall include:

a. Demonstration of an understanding and awareness of the methods the practitioner is authorised to carry out;

b. Demonstrating an understanding of the scientific basis for the method;

c. Knowledge of any limitations to the method and considerations around sequence of use;

d. The ability to explain how the methods will be used or adapted in a variety of operating environments;

e. Demonstration of ability to identify and manage contamination risks;

f. Periodic witnessing of a sample of activities at a live operating environment to cover the end-to-end process, i.e. including tasking activities, scene examination and reporting; and

g. Review of casework records, outputs and performance data.

90.3 Initial request to attend an incident scene

90.3.1 The forensic unit shall have a policy, which shall form part of the formal agreement or contract between the forensic unit with the commissioning party (section 16) that includes the following:

a. Agreement with the commissioning party of the incident types (for example, offence types, types of event, or organisational priorities) that the forensic unit should be notified of.

b. Definition of the incidents or circumstances that the forensic unit will assign resources to and the level and type to be assigned and any sub-contracting agreements.

c. Definition of the incident types or circumstances that require the examination strategy to be discussed and with whom.

d. Definition of the incident types or circumstances where examinations may be carried out at a location other than the scene (section 90.9).

e. How the request to attend an incident scene will be recorded.

f. A defined process for deployment of further or alternative personnel and/or resources where assessment of the scene indicates that this is required.

g. How the outputs from the examination will be reported and in what timescale.

h. How disputes between practitioners or between practitioners and the commissioning party can be raised, who they are escalated to, and how they will be addressed.

90.4 Forensic Scene Management

90.4.1 Forensic Scene Management is the oversight, direction, supervision, and review of incident scene activities. This could be performed by a single practitioner operating alone, a lead practitioner, a dedicated scene manager, for example a Crime Scene Manager.

90.4.2 This activity may be performed remotely provided that this is recorded and it can be demonstrated that the scene manager has access to sufficient information to carry out the activity effectively.

90.4.3 The forensic scene manager is the practitioner who will retain overall responsibility for the scene during the scene investigation and develop the examination strategy for the incident scene. If multiple practitioners are undertaking examinations at the same incident scene, then one practitioner shall be identified as the forensic scene manager. If the practitioner undertaking this role changes during an investigation this shall be clearly documented.

90.4.4 The forensic scene manager shall ensure that:

a. the incident scene is assessed in the context of the available information;

b. the examination strategy has been completed and that this is kept under review;

c. relevant aspects of the incident scene are preserved as far as reasonably practicable, throughout the examination process;

d. the incident scene is recorded and examined;

e. communication is maintained with the commissioning party as agreed (section 90.3.1c); and

f. responsibility is handed over to another scene manager effectively if necessary.

90.5 Initial actions at any incident scene

90.5.1 An initial assessment of the scene shall be carried out, and should:

a. include identifying and preserving the scene as initially understood (scene boundaries and preservation requirements may change during the examination and will be documented if this is the case);

b. be documented in proportion to the examination activities to be undertaken;

c. be undertaken prior to any recovery or examination activities, unless this would risk the loss of forensic material; and

d. identify and document whether additional personnel or resources are required (section 90.3.1f).

90.5.2 Initial assessments shall be recorded:

a. contemporaneously or at the first practical opportunity; and

b. in a manner sufficient that aspects of the scene relevant to the rationale for the examination strategy can be understood by those undertaking examinations, taking over subsequent forensic scene management responsibility, and investigating the incident.

90.5.3 Any amendments to this initial assessment shall be recorded in the examination notes together with the rational for the amendment.

90.6 Developing an examination strategy

90.6.1 An examination strategy shall be documented whether in a stand-alone document or as part of the examination notes, for all scenes examined, whether a generic strategy for commonly encountered incident types, or a bespoke strategy for more complex incidents.

90.6.2 The examination strategy shall take a holistic view of the incident scene and identify the necessary actions to carry out an effective examination. The examination strategy shall take into account and, where necessary, challenge the initial investigation requirements and information received.

90.6.3 The examination strategy shall take into account the initial assessment of the scene and information provided to the practitioner both prior to attending and during attendance at the scene. In order to demonstrate how practitioners manage the influences on their approach to examination of the scene, any relevant information received shall be documented, including the source of the information.

90.6.4 The examination strategy shall be sufficiently clear and detailed to be understood by those: undertaking examinations, taking over subsequent forensic scene management responsibility, and investigating the incident. The strategy shall also be sufficient to enable subsequent peer-review, assist case reviews, allow compliance audits, and support competency assessments.

90.6.5 Examination strategies shall be documented:

a. contemporaneously or at the first practical opportunity; and

b. in a manner sufficient that the sequence of actions, and the effect of any changes to the environment or information received can be understood.

90.6.6 The examination strategy shall set out what is to be examined, recorded and recovered and for what purpose and, where the practitioner considers it to be pertinent to aims of the examination, what is not to be examined, recorded or recovered (for example, where a specific examination was requested but was not appropriate to carry out). Significant limitations affecting the examination strategy for the incident scene, such as restricted access, shall be recorded.

90.6.7 In drafting the examination strategy the need for any additional practitioners should be considered. Any decision on whether or not to request additional

practitioners shall be documented in the strategy, including the rationale for the decision.

90.6.8 The level of detail in the examination strategy should be proportionate to the complexity and significance of the incident and/or activity but should include at a minimum:

a. how the scene is to be preserved, if preservation is needed;

b. how the scene is to be recorded;

c. an assessment of the risks of contamination and the measures by which these risks are to be managed, these measures shall follow the forensic unit's policies and procedures (see section 23) and be directly related to the risks from contamination to the examinations and the complexity and significance of the incident and/or activity at the scene;

d. any external advice received, including who provided the advice and the decisions made as a result; and

e. the sequence of examinations to take place, including, where relevant:

i. consideration of the impact of one method/examination on the recovery of another forensic material or the aims of the examination and how this will be addressed;

ii. sampling strategy;

iii. whether other practitioners will be assisting with the examination and what aspects they will undertake;

iv. issues arising where there are competing requirements or incompatibility of examinations, and decisions taken to prioritise or accommodate these requirements, with supporting rationale;

v. any physical reconstruction of the scene.

90.6.9 The practitioner shall keep their examination strategy under review and update as needed, with the date and/or time of the update clearly recorded, in the following circumstances:

a. A significant change in the information on which the strategy was based.

b. A significant change in circumstances or environmental conditions.

c. A significant finding or development arising from the examination of the incident scene.

d. At the completion of the scene examination.

90.7 Co-ordination of others at an incident scene

90.7.1 This section relates to the management or co-ordination of other practitioners at an incident scene by the forensic scene manager, this may include, but is not limited to; coordination of practitioners from the same forensic unit, external forensic units or others, such as pathologists.

90.7.2 The forensic scene manager is responsible for the oversight of the work of other practitioners and for ensuring they are provided with sufficient information to effectively undertake the required examinations and, where appropriate, interpretations. Other practitioners may develop their own examination strategies for their specific examinations, however the overarching strategy for examination of the incident scene is developed and maintained by the forensic scene manager.

90.7.3 The examination activities to be undertaken by other practitioners shall be discussed and agreed with the forensic scene manager prior to being conducted, this may involve amendments to the forensic scene manger's strategy. Where amendments are recommended by the other practitioner but not implemented by the forensic scene manager, the recommendation and the reason they were not implemented should be recorded. If the other practitioner does not accept this, for example as a result of their responsibility to the CJS as an expert, the forensic scene manager shall follow their forensic unit's policy and procedure for the management of disputes.

90.7.4 The forensic scene manager shall be informed if the practitioners they are co-ordinating are unable to effectively carry out the required examinations, either because the required examination is not within their range of competence; or they require further information/wider access to meet the requirements of the investigation, or as a result of their responsibility to the CJS as an expert. The forensic scene manager shall determine whether the examination strategy requires amendment, for example that alternative resources are required. The

forensic scene manager and the attending practitioner shall record the considerations, discussion and decision.

90.7.5 Where the practitioner is undertaking a specific activity or FSA (for example bloodstain pattern analysis) the forensic scene manager shall document and ensure that for the relevant activity, the practitioner has the opportunity to;

a. advise on the forensic scene manager's examination strategy;

b. advise on evidence recovery; and

c. request the use of other practitioners to carry out contributory activities, such as photography and sampling.

90.7.6 When a practitioner is providing findings to the forensic scene manager or commissioning party, the key discussion points, date, time, and details of those involved with the discussion shall be documented. The practitioner shall also ensure that it is clear when these are preliminary results and, if relevant to the activity, are subject to a formal peer review process. Where preliminary results have been shared which subsequently change following peer review, the forensic scene manager shall be informed at the earliest opportunity. If the preliminary results had been provided to the commissioning party they shall be informed of the change by the forensic scene manager.

90.8 Technical records

90.8.1 The forensic unit shall have a policy on the information required to be recorded in examination notes and other records, this policy shall be based on an assessment of the value of recording information and the risk of not recording the information. The practitioner shall be aware of and follow this policy.

90.8.2 The practitioner shall include in their examination notes relevant information provided to them and its source.

90.8.3 Once an incident scene is under the control of the forensic unit, it shall be possible to identify the individuals that have accessed the scene who may have an impact on the activities to be undertaken. The practitioner may make this record, or it can be accessible to the practitioner, such as cordon logs.

90.8.4 Examination notes shall record information relevant to the incident and the activities to be undertaken, for example a description of the location and surrounding area, weather conditions, and access.

90.8.5 Examination notes shall be produced contemporaneously or at the first practical opportunity. In situations where items/exhibits need to be recovered rapidly, such as in adverse weather conditions, or dynamic incidents, notes shall record the location and sequence of recovery of the items/exhibits in sufficient detail to meet the requirements of any subsequent review of use, for example examination or interpretation.

90.8.6 Decisions, such as but not limited to, contamination controls and examination strategy, and their supporting rationale shall be clearly recorded within notes, including the information the decisions were based on. Notes shall be such that decisions can be understood and peer reviewed at a later date if necessary.

90.9 Environment and facilities

90.9.1 To support the delivery of incident scene examination; the forensic unit shall identify and ensure that all practitioners have access to appropriate:

a. Facilities for storing equipment and consumables;

b. Vehicles for transporting practitioners, equipment, consumables and items/exhibits to and from incident scenes.

c. Facilities for the storage of recovered items/exhibits with adequate security and storage conditions to prevent loss, deterioration, and contamination.

90.9.2 Examinations can be undertaken at locations other than an incident scene, such as ad-hoc examination areas, or vehicle recovery garages, if all of the following conditions are met:

a. The incident scene is not conducive to effective examination of the item/exhibit;

b. Contamination risks relevant to the examination being performed are adequately managed;

c. That examining the item/exhibit at an alternative location poses no greater to the overall outcomes than carrying out the examination at the incident scene or seizing the item/exhibit for subsequent examination;

d. There is no increased risk to health and safety.

e. It is agreed by the commissioning party, either as part of an SLA or on a case-by-case basis.

90.9.3 The rationale for carrying out activity at an alternative location shall be recorded, including confirmation that each of the conditions listed above are met.

90.9.4 Activities that form part of the end-to-end process of incident scene examination may be performed at a location other than the incident scene, for example tasking, strategy setting, incident scene co-ordination and report writing. Regardless of the location where these activities are performed, the practitioner shall ensure that; the environment is appropriate, i.e. allows for effective actions to be taken, they have access to the required materials, information and equipment, and that information security (section 26.3) is not compromised.

90.10 Assuring the quality of results

90.10.1 The forensic unit shall have a policy and procedures for peer review of incident scene examinations, including the scene notes, examination strategy and decisions made. The proportion of examinations reviewed shall be sufficient to provide assurance that the requirements of this Code are met.

90.10.2 Methods used, data and records retained (such as examination notes and photographs) shall allow for peer review by suitably trained and competent practitioners at the incident scene as well as after conclusion of the examination.

91. Forensic medical examination of sexual offence complainants - assessment, collection and recording of forensic science related evidence

91.1 Scope

91.1.1 This section covers the forensic medical examination, recovery of items and samples, and recording of scientific relevant information from complainants of alleged sexual assault routinely examined in a dedicated facility (forensic unit) for that purpose. It does not include clinical practices or governance activities. For the purposes of this section, complainants will be referred to as patients.

91.1.2 Further detailed guidance is provided in FSR-GUI-0020 - Forensic medical examination of sexual offence complainants [102].

91.2 Organisation and management responsibility

91.2.1 A senior manager with responsibility for the oversight of the facility shall be identified to support the quality standards.

91.2.2 Management within the facility shall conform to the requirements of ISO 15189:2022 [5], substituting ‘facility’ where the standard states ‘laboratory’. The management requirements shall include:

a. defining and documenting the organisational structure and management responsibility of the facility; and

b. determining a legal entity and SAI (section 6) so that it is clear who can be held legally responsible for the facility’s activities (ISO 15189:2022 section 5 [5]) and who the contact is for the Regulator.

91.3 Management system

91.3.1 A management system, such as a quality management system (QMS) (however called) shall be established, shall comply with section 5.4.2 and 8.1 of ISO 15189:2022 [5] and shall incorporate the requirements of this Code into policy and procedures as appropriate to the activities being undertaken.

91.4 Technical requirements

Personnel: training and competence

91.4.1 The employer, whether responsible for the facility directly or as a provider commissioned to work at that facility, shall have a documented policy defining the knowledge, skills, experience and competency, and a procedure for the training, and ongoing competency for each role undertaken within the facility. This shall include:

a. records to evidence competency and authorisation to carry out specific tasks;

b. training and competency requirements, including retraining for any lapse of competence for each role profile;

c. where relevant, expert witness and CJS related training [11], [17], including written evidence, court skills and avoiding cognitive bias [72];

d. assessment of training and competency;

e. authorisation and commencement for the activities which their personnel undertake;

f. continuing professional development; and

g. maintenance of ongoing competency, including input from end user feedback.

91.4.2 If personnel are not employed by the legal entity or the forensic unit but are providing a service (ISO 15189:2022 6.7, 6.8, 6.2 [5] and ILAC G19 4.1.3 [6]), then assessment and approval to work at the facility shall be evidenced and documented by the facility/forensic unit, prior to the commencement of any work.

Accommodation and environmental conditions

General

91.4.3 Accommodation at the facility shall be fit to meet the forensic examination needs of all its end users in a secure environment.

91.4.4 The forensic unit shall have policies and procedures for authorised access to the building, rooms, areas, equipment and consumables. Access shall be recorded for the forensic medical examination room.

Layout of the accommodation

91.4.5 The design and layout of the facility should be unidirectional. This shall include measures to prevent cross-transfer and environmental contamination.

91.4.6 There shall be a designated DNA-clean patient bathroom(s) and forensic medical examination areas [104]. The designated DNA-clean areas shall be secure at all times and access controlled.

Air quality and air flow

91.4.7 The forensic unit shall have in place an air handling system that controls the quality and flow of the air entering the designated DNA-clean areas/rooms. The system shall ensure that levels of contamination, including trace material and

cellular debris in the air, are managed such that the risk of transfer from the patient to the environment and from the environmental background to the patient and samples is minimised. The document – FSR-GUI-0017 Guidance: DNA contamination controls – Forensic medical examinations, provides further guidance [104].

Forensic medical examination room furnishings, equipment, reagents and consumables

91.4.8 The furnishings, equipment, reagents and consumables which are utilised within the facility shall be such that they manage the risk of DNA contamination.

Environment, furnishings and equipment

91.4.9 The walls, floors, work surfaces and chairs should be of smooth finish, sealed, readily cleanable and resistant to degradation from frequent cleaning. Workstation/work surfaces shall be kept clear, other than of equipment in daily use.

DNA decontamination

91.4.10 The forensic unit shall have a policy in place which sets out DNA anti-contamination good practice and the control and management of DNA-clean areas. This shall include:

a. routine cleaning regimes for rooms, areas, equipment (including mobile equipment), furniture and consumable storage areas;

b. frequency of deep cleaning for the forensic medical examination room;

c. access control to the DNA-clean areas;

d. records of the name of the cleaner, and where and when cleaning was carried out; and

e. checking of the ongoing effectiveness of the cleaning through environmental monitoring.

Cleaning reagents

91.4.11 The forensic unit shall use cleaning products and spillage kits that have been demonstrated to be effective in removing and denaturing DNA in conjunction with appropriate cleaning procedures.

91.4.12 The forensic unit shall demonstrate that the cleaning product continues to be effective at removing and denaturing DNA to acceptable levels for example, through environmental monitoring.

Consumables, including personal protective equipment/barrier clothing

91.4.13 The forensic unit shall have a policy and procedures for the procurement, receipt and storage of reagents and consumables (including PPE) that are fit for their intended use [13], [14]. These shall also include instructions for use, handling and disposal.

91.5 Examination methods and procedures

91.5.1 The forensic unit shall have documented procedures for the examination processes undertaken by personnel at the facility. These shall include:

a. relevant skills, knowledge and competency requirements to work with patients;

b. a procedure for the initial contact prior to the patient's arrival at the facility; and

c. documenting relevant information pertaining to the patient throughout the process.

91.5.2 The facility shall provide accessible accurate information and advice about the facility to other relevant on-site providers.

91.5.3 The forensic unit shall be able to provide basic information to patients about the:

a. options available to them for examination and advice;

b. documentation of the presence or apparent absence of injuries;

c. importance of body fluids and the recovery of relevant material for forensic examination;

d. impact that actions following the alleged incident might have on the collection of evidence;

e. requirement for an early evidence kit sample, as appropriate; and/or

f. retention of relevant clothing worn at the time of, and subsequent to, the alleged incident.

91.6 Decision to undertake an examination

91.6.1 The decision to undertake a forensic medical examination shall be made by a forensic healthcare practitioner.

91.6.2 The forensic healthcare practitioner shall provide advice on the recovery of material of potential forensic value.

91.6.3 Where there is concern about child sexual abuse, personnel from the paediatric Sexual Assault Referral Centre should be consulted as part of the strategy discussion, in order to determine whether the child should be examined and if so, at what time and by which forensic healthcare practitioner(s).

91.6.4 Where the patient needs to be taken to an emergency department (or undergo an examination in other premises, e.g. residential property) the forensic healthcare practitioner shall either attend and/or provide instructions for the examination to other forensic healthcare providers. Offsite and examinations conducted in custody are excluded from accreditation for FSA BIO-100.

91.6.5 Samples shall be collected using forensic DNA grade [14] forensic sample kit modules. Consideration of the usefulness of blood and urine samples taken at hospitals for forensic analysis shall be based on individual case circumstances.

Attendance of the forensic healthcare practitioner

91.6.6 The forensic healthcare practitioner attending the forensic medical examination in a Sexual Assault Referral Centre shall not provide any service to custodial facilities, e.g. police stations and detention centres, during that shift.

91.6.7 Where more than one patient is referred who may be involved in the same alleged incident, or different patients are thought to be part of a linked series of cases, they should be examined in separate rooms or facilities and by different forensic healthcare practitioners. Where this is not possible, this should be documented and an explanation provided; measures taken to minimise the potential for cross-contamination shall be documented.

91.6.8 If an instance arises where the same forensic healthcare practitioner was used, this shall be documented and disclosed in any subsequent report or statement provided for the CJS as a non-compliance with the requirement in this Code.

91.7 Roles and responsibilities of those conducting the examination

91.7.1 Where more than one forensic healthcare practitioner is conducting the examination, their respective roles and responsibilities shall be agreed in advance of the examination, and these should be documented.

91.8 Removal of clothing

91.8.1 The forensic unit shall have a documented procedure for the removal, packaging, and labelling of clothing to minimise contamination and loss of evidence. The integrity and continuity of the items or samples once packaged shall be maintained, prior to handing over to the police.

91.9 Examination process

91.9.1 The examination process shall be defined and documented. The process shall include:

a. collection and documentation of relevant information;

b. development of the examination strategy;

c. development of the order of the examination activities based on the circumstances and patient consent;

d. photography; and

e. documentation.

Record of attendees

91.9.2 A record of all persons in attendance during the forensic medical examination shall be made. In addition to retaining this record with the case notes, it shall be securely retained and accessible for contamination investigations.

91.10 Sample collection and handling

91.10.1 The forensic unit shall have a documented procedure for taking appropriate samples on a case-by-case basis. These shall include:

a. DNA anti-contamination good practices;

b. sample recovery good practice;

c. recording, labelling and packaging of samples; and

d. chain of evidence and sample transfer.

Storage of samples

91.10.2 The forensic unit shall have a policy and procedures in place for the taking, storage, retention and destruction of samples. These shall comply with the Human Tissue Act 2004 [57].

Sample documentation

91.10.3 The forensic unit shall have a procedure in place for the documentation of sample collection, labelling, and the transfer and storage of samples and evidence collected.

Images

91.10.4 The forensic unit shall have a policy and procedures in place for the electronic capture, storage and transfer of images. These shall include:

a. personnel authorised to take images;

b. requirements for obtaining the resolution and image quality to demonstrate the features of interest clearly;

c. recording on case notes;

d. security and integrity of data;

e. access to images for peer review/second opinions; and

f. disclosure of images for CJS proceedings and dealing with the information security implications.

91.11 Ensuring the quality of examination procedures

Contamination minimisation

91.11.1 The forensic unit shall have a policy and procedures in place that minimise the possibility of contamination from the moment a patient arrives at the facility for a forensic medical examination until the completion of that examination.

91.11.2 Although the main focus is to minimise DNA contamination, other forensic science related evidence types, such as dried flaking body fluids, hairs, fibres, and particulate debris which can cross-contaminate, are just as important and shall be considered within the examination and recovery procedures.

91.11.3 To avoid cross contamination between sites/areas sampled during the forensic medical examination of sexual assault patients, gloves shall be changed between each site/area sampled.

Use of personal protective equipment/barrier clothing

91.11.4 Personal protective equipment (PPE)/barrier clothing shall be worn and changed between the examination of each patient to minimise contamination. [105]

91.11.5 The policy and procedures for the use of PPE/barrier clothing shall, as a minimum, include setting out the:

a. PPE/barrier clothing which the forensic healthcare practitioner and visitors at the forensic medical examination shall wear;

b. order in which to put on PPE/barrier clothing;

c. frequency of changing PPE/barrier clothing; and

d. disposal of PPE/barrier clothing.

DNA elimination samples

91.11.6 A policy and procedures shall be in place to require a DNA elimination sample from all personnel who work at the facility prior to entering the forensic medical examination areas of the facility to detect inadvertent contamination of samples processed and for the addition of their DNA profile to a DNA elimination database(s) to facilitate automated routine contamination checks. These personnel will include (but are not limited to) forensic healthcare practitioners, crisis workers, consumable store and cleaning staff.

91.11.7 All other visitors entering the facility, including the patient (whether police-referral or self-referral cases), interpreters, friends and family, are not required to give a DNA elimination sample prior to entry but shall have their details recorded in case there is a need to request a sample at a later date for contamination elimination purposes.

91.11.8 The policy and procedures for the management of elimination sampling shall include the following:

a. Taking of the DNA elimination samples.

b. Agreement/consent for sample donation from:

i. forensic healthcare practitioners, paediatricians and support staff, e.g. crisis workers; and

ii. visitors (e.g. interpreters, relatives, service engineers) if a sample is required at a later date for contamination elimination purposes.

c. Security and access of information.

d. Secure storage and recorded transfer of samples.

e. Investigation of an identified contamination event.

f. Details of those with whom the profile will be shared.

g. Retention period(s) for the elimination profiles (section 92.11.16).

91.12 Contamination prevention

91.12.1 A policy and procedures shall be in place for dealing with the management of contamination including cross contamination in the event of multiple patients from the same incident attending the facility at the same time.

Cleaning

91.12.2 A policy and procedures shall be in place for cleaning rooms, areas and equipment. These shall include:

a. training and authorisation of personnel;

b. cleaning methods demonstrated to effectively remove/denature DNA;

c. frequency of cleaning and deep cleaning;

d. decontamination of re-usable equipment (ISO 15189:2022 section 6.4.4 [5]); and

e. records of cleaning to include the name of the cleaner, employer (if cleans at multi-sites and custody areas) and when.

Environmental monitoring and gross contamination

91.12.3 A policy and procedures shall be in place to monitor the effectiveness of the cleaning regimes in place by monitoring the level of background DNA. These shall include:

a. an environmental monitoring sampling (EMS) programme that reflects the operational risk profile and is proportionate to the risk of transferring DNA;

b. the frequency of EMS;

c. training requirement for personnel;

d. personnel and methodology used for collecting the samples and timely – preferably immediate – submission for DNA analysis;

e. areas and equipment to be sampled for each monitoring event;

f. submission of DNA samples for analysis to a provider that is accredited to ISO/IEC 17025:2017 [3] or ISO 15189:2022 [5] and required to provide timely processing and reporting of results to allow quick action should any EMS result be in an unacceptable range;

g. advice and feedback from the provider undertaking the EMS analysis; and

h. defined follow-up processes to investigate and address gross contamination.

91.13 Documentation – recording of notes and reports

Note taking and record keeping

91.13.1 A policy and procedures shall be in place for documenting and storing information pertaining to each patient. These shall include requirements for:

a. the clarity, accuracy, legibility and permanency of notes and records;

b. detailing all activity and decisions which are directly relevant to the patient;

c. recording the notes contemporaneously;

d. recording PPE/barrier clothing worn by the forensic healthcare practitioner(s) and visitors during the forensic medical examination;

e. identification of the forensic healthcare practitioner, and the date and time (if appropriate) of the activity;

f. amendments made to the record(s);

g. generation of preliminary findings or final reports [67], [106];

h. secure retention of notes, including permanent records such as colposcope images; and

i. access to notes and images for second opinion, peer review, investigation and criminal justice proceedings.

Reports

91.13.2 The forensic unit shall have a process for the production of statements and reports in a format that complies with the disclosure obligations and the requirements set out in the Criminal Procedure Rules and Criminal Practice Directions [11].

91.13.3 Forensic healthcare practitioners shall be appropriately trained and supported to produce a report which is acceptable for use within the CJS [67] [106].

91.13.4 The forensic unit shall define a process that can be evidenced for the end-to-end peer review stages of the case as it progresses. There should be a critical findings check of the report/statement by a second competent individual with a suitable level of knowledge, experience and authority to perform such a review.

92. Human DNA examination and analysis

92.1 Scope

92.1.1 This section covers the requirements for the DNA examination and analysis processes specifically pertaining to the detection, recovery, analysis, interpretation and use of DNA findings.

92.1.2 For DNA analysis and interpretation, the requirements are for all short tandem repeat (STR) based analyses (including Y-STR), including related sequence technology and other chromosomal or mitochondrial DNA analyses conducted, whether performed in a static or mobile facility.

92.2 DNA consumables

92.2.1 Consumables and reagents used for recovery and analysis of DNA shall be demonstrated to be forensic DNA grade through batch testing to demonstrate successful clean production standards, or using a validated post-production treatment, such as ethylene oxide treatment, or both. This requirement also applies to reagents used in processes upstream from DNA processing in joint, split or sequential cases involving other disciplines.

92.2.2 Assurance is provided through the use of DNA consumables compliant with ISO 18385:2016 [14] or PAS 377:2023 [13], which incorporates the requirements of ISO 18385:2016 [14].

92.2.3 Consumables compliant with PAS 377:2023 [13] or ISO 18385:2016 [14] and declared as ‘Forensic DNA Grade’ negate the requirement for end user batch testing [107]. If end user batch testing of consumables is required, then the pass or fail criteria set out in PAS 377:2023 [13] shall be used. Where compliance is self-declared by the manufacturer/supplier then suitability can be assessed by the forensic unit, for example, using product preparation information, in addition to QC or negative test result data available for the product batch.

92.2.4 Materials used shall not:

a. leach any chemicals (e.g. plasticizers) that may affect the processes used or the results obtained from the analysis; should the composition of the material change then this shall be re-evaluated; nor

b. have levels of DNA that can be detected by the DNA analytical methods used for processing casework material.

92.2.5 The consistency in recovery and release of DNA for sampling materials used (e.g. swabs) shall be demonstrated. Ongoing verification of performance across batches shall be evidenced by quality control (QC) testing.

92.2.6 Any changes in composition of the sampling material shall be risk assessed and either validated or verified to ensure that the performance is as good as the previously validated sampling materials.

92.2.7 Post-production treatment of DNA consumables shall include a QC for each treatment, such as DNA-spiked samples placed at various locations throughout the batch to be treated, which demonstrate the required reduction level of amplifiable DNA (at least 1,000-fold) [13], [14]. Post-treatment QC testing is not required unless the QC monitoring the efficiency of the post-production treatment fails or casts doubt on the reduction level required.

92.2.8 For consumables that cannot undergo post-production treatment, evidence that there is no gross or systemic contamination shall be demonstrated by QC testing. PAS 377:2023 [13] sets out the batch testing criteria to be considered acceptable.

92.2.9 Consumables that fail batch testing shall be embargoed and investigated further. Following repeat batch testing, consumables that continue to fail should

be rejected for use. For consumables that have undergone post-production treatment, such as ethylene oxide treatment, another treatment might resolve the issue.

92.2.10 The testing shall be traceable, and the exact nature of the test and the results shall be made available to the users of the consumables and, if required, the CJS and end users.

92.2.11 Areas used for the storage and handling of consumables shall be clean, secure and access restricted to authorised personnel only.

92.3 Packaging and general chemicals/materials

92.3.1 The packaging for samples or items shall preserve the integrity of the material for forensic examination and minimise the risk of loss, degradation or contamination.

92.3.2 Policies and procedures for handling packaging, consumables and reagents shall include:

a. areas used for the storage and handling of consumables are secure;

b. access is restricted to authorised personnel only;

c. measures are taken to protect or minimise contamination from the environment; and

d. precautions are taken to minimise the contamination of consumables prior to and during use.

92.3.3 Any detected or reported problems with packaging or materials already in the evidential chain will require an appropriate risk or case assessment to be undertaken and, where appropriate, for the material to be removed from use.

92.4 Contamination avoidance, monitoring and detection

92.4.1 The forensic unit shall have policies and procedures in place for contamination management. Steps shall be taken to prevent or minimise contamination [108] between:

a. personnel and the exhibit/DNA sample;

b. contaminated consumables (e.g. swabs, tubes, PPE/barrier clothing) and the exhibit/DNA sample;

c. exhibits and DNA samples; and

d. contaminated equipment and the exhibit/DNA sample.

92.4.2 Appropriate precautions shall be taken to minimise the contamination of consumables prior to use.

92.4.3 PPE/barrier clothing shall be worn when entering scenes and examination, recovery and processing areas.

92.4.4 Procedures in place shall minimise the transfer of DNA by defining when PPE/barrier clothing shall be cleaned and/or changed.

92.4.5 Segregation and separate handling of items in the same case shall be observed at all times, e.g. scene and suspect, complainant and suspect, different suspects, different locations within a scene and multiple scenes. Any deviations from this shall be recorded.

92.4.6 Reference samples (for example, hair, buccal, blood, muscle and surrogate body fluids from known sources) shall be processed separately from crime related material. Separation should be either in time or physically, this includes from examination of items through to DNA sample batching.

92.4.7 All items shall be stored in such a manner to minimise the risk that they can be cross contaminated, tampered with or stolen.

92.4.8 The forensic unit shall have policies and procedures to ensure that the cleaning chemicals and methods used are validated and shown to be effective at reducing and denaturing DNA to acceptable levels.

92.4.9 Based on risk, equipment shall be cleaned prior to and/or after use according to documented standard operating procedures.

92.4.10 The forensic unit shall have policies and procedures to monitor the ongoing effectiveness of cleaning.

92.4.11 Anti-contamination records shall be kept; these include:

a. room access logs;

b. cleaning logs; and

c. environmental monitoring records.

92.4.12 The forensic unit shall have policies and procedures to ensure that access to scenes and examination, recovery and processing areas is restricted to personnel who provide DNA elimination samples for routine contamination checks and are covered by a DNA elimination database(s). Further guidance is provided in 'DNA contamination detection – The management and use of DNA elimination databases' [109] published on the Regulator's website.

92.4.13 The forensic unit shall control the air flow and the quality of the air through an air handling system entering the designated DNA clean areas/rooms, to minimise the number of vectors, including cellular debris, in the air, the movement of these around the environment and the build-up of background DNA.

92.5 Selection of methods

92.5.1 Forensic units shall use a validated method(s) for recovering body fluids and trace (touch) DNA for downstream testing.

92.5.2 Forensic units shall use a validated method(s) for the identification of body fluid material. Results obtained for body fluid identification screening tests that are presumptive should be provided as an opinion.

92.5.3 Forensic units analysing DNA shall use validated methods for extracting DNA, amplification, fragment-size separation (electrophoresis), sequencing, allele designation and profile interpretation.

92.5.4 Forensic units analysing DNA shall use a validated, human-specific, quantification technique for casework samples, which is verified to demonstrate that its limit of detection, limit of quantitation, accuracy and reproducibility, are appropriate to the sensitivity of the DNA profiling service offered. Quantification of reference samples from subject samples is not needed, as there is sufficient material for re-work.

92.5.5 Where the quantification method used is incapable of demonstrating whether PCR inhibition is likely to occur given the nature of the tested sample, then the possibility of inhibition shall be explored if an unexpected partial or no profile is obtained.

92.5.6 In exceptional instances where, in the opinion of the practitioner, a separate quantification step usually required in a protocol is not advisable (e.g. the amount of available evidential material may be insufficient to obtain an interpretable profile) or not required, this shall be documented and clearly communicated to the commissioning party, and made available for disclosure purposes.

92.5.7 For rapid DNA devices, if quantification is not an integral part of the casework analytical method, then alternative means to assess and address the effects of both degradation and inhibition for each casework sample type are required as some samples are of variable composition, quality and quantity. Rapid DNA devices shall not be used on sample types of limited quality that will prevent any reanalysis of the sample.

92.6 Validation

92.6.1 Whether it is an adopted method that has been developed and validated elsewhere or developed by the forensic unit, this Code allows for tailoring the validation procedure through verification of the extent and scope of supporting external validation studies.

92.6.2 For DNA methods, the parameters/characteristics in the validation plan shall include, as appropriate:

a. equipment calibration/performance, reagents, reference materials, consumables;

b. characterisation of the genetic markers (mode of inheritance, chromosomal location, detection mechanism, polymorphism);

c. species specificity (human/non-human, targeted species);

d. sensitivity (e.g. limits of detection, quantitation and/or the range of DNA quantity that will produce reliable results with reference to stochastic effects);

e. contamination;

f. matrix and substrate effects;

g. interferences and cross-sensitivities;

h. stability (e.g. to environmental and chemical factors);

i. repeatability and reproducibility (concordance);

j. ruggedness/robustness;

k. performance variation between representative case-type materials;

l. population studies (databases, independence);

m. effect of mixtures on obtaining reliable results;

n. precision;

o. accuracy (measurement standards);

p. measurement uncertainty;

q. match criteria;

r. amplification/PCR conditions (thermocycling parameters, concentration of primers, magnesium chloride, DNA polymerase, etc.) and preferential amplification/co-amplification; and

s. post-amplification/PCR treatments, electrophoresis and detection parameters.

92.7 Profile requirement

92.7.1 The forensic unit shall demonstrate that the method can obtain the 'expected correct profile' (i.e. accurate profile for both reference and casework). As a minimum this includes:

a. no errors using the same profiling chemistry kit;

b. one base pair resolution;

c. profile is not a result of contamination;

d. profile is not a result of a sample or demographic switch; and

e. discordance and mutations are identified and accounted for.

92.7.2 The forensic unit shall demonstrate that the method can obtain profiles of the appropriate quality for casework samples. As a minimum this includes optimal representation of the DNA content for:

a. single-source DNA;

b. low-template DNA; and

c. major/minor and equal mixtures from:

   i. good quality DNA;

   ii. degraded DNA; and

   iii. mixed quality (good quality and degraded DNA).

92.8 Quality assurance and quality control

92.8.1 Quality controls (QCs) shall be used to provide assurance of the test and monitor the methods used from sampling to profile designation.

92.8.2 For DNA profiling, the QCs shall be used to monitor extraction, amplification processes, fragment sizing, sequence or profile designation and contamination.

92.8.3 A negative (blank) control shall be used from extraction to monitor contamination through the analytical process.

92.8.4 Within and between batch profile checks shall be conducted to identify possible sample to sample contamination.

92.8.5 The forensic unit proficiency testing schedule shall include the processing of at least one two-person and one three-person mixture DNA sample per year.

92.9 Interpretation – profile

92.9.1 The profile interpretation method shall include consideration of:

a. allele drop-in;

b. allele drop-out;

c. gross or systemic contamination;

d. stochastic characteristics and, if used, any associated thresholds or triggers, such as heterozygote balance relative to peak height, area or DNA quality/quantity;

e. stutter and artefactual peak characteristics;

f. a mixture of two or more individuals covering a range of ratios per contributor, including male and female contributors;

g. determining the number of contributors;

h. methodology for reporting a single result or replicate analyses as a likelihood ratio; and

i. forming propositions (related or unrelated individuals).

92.10 Expression of opinion and interpretation

92.10.1 For interpreting and reporting DNA profiles in the context of the biological material and the case circumstances, the forensic unit shall comply with the UKAS publication LAB 13 [71].

92.11 DNA elimination databases

92.11.1 DNA elimination databases shall include personnel who are involved in the recovery or sampling of items; in particular, all personnel associated with the DNA process chain. These include:

a. those involved in the collection/recovery of DNA material, its analysis and the processing environment;

b. any personnel that have a high-risk of transferring their DNA to items or packaging, e.g. those who have access to items/exhibits; and

c. any personnel involved in the preparation or assembly of consumable kits and their handling.

General

92.11.2 Policies and procedures for elimination databases shall include, but are not limited to:

a. data formats and data;

b. searching procedures and algorithms;

c. retention periods;

d. legacy profiles and archive;

e. sharing agreements (i.e., between forensic units/providers and with international manufacturers' elimination databases);

f. agreements/consents;

g. release forms;

h. investigation process;

i. reporting policies; and

j. additional retained information.

92.11.3 Forensic DNA profiling units shall maintain local DNA elimination databases and include DNA profiles detected from batch testing of reagents, negative (blank/no template) controls, and from environmental monitoring, as a way of detecting contamination events as part of an integrated elimination database.

92.11.4 Profiles derived from these databases that are not identified to personnel in the DNA examination process shall be shared with the national contamination elimination database and checked against relevant manufacturer DNA elimination databases and international contamination databases (section 92.11.13).

Consent

92.11.5 Personnel shall be asked for their consent to provide a sample for the generation of a DNA profile for inclusion on one or more elimination databases for the purpose of detecting DNA contamination.

Retention periods on elimination databases

92.11.6 When personnel leave a forensic unit, the unit shall determine retention periods based on the expected period of time that material handled by exiting personnel takes to progress through the CJS.

92.11.7 The minimum retention period shall be 12 months; longer periods shall be considered based on:

a. the shelf life of the production of consumables kits by personnel;

b. time frames of DNA contamination detected in the laboratory processes (an 18-month interval has been observed, therefore, for DNA sampling and processing roles, an 18-month retention period may be considered as appropriate);

c. permanent retention to accommodate cold case reviews that tend to be decades old.

92.11.8 Consideration of the retention period shall be determined for each elimination database or personnel role, be relevant, proportionate and form part of the

consent or agreement. Access and searching against any archived profiles shall be restricted.

Matches

92.11.9 All matches against DNA elimination databases shall be investigated to determine the root cause.

92.11.10 All investigations shall be undertaken by nominated individuals authorised by the forensic unit.

92.11.11 Forensic DNA profiling units shall collaborate with DNA consumables manufacturers to address the issue of contamination of consumables.

92.11.12 It is the responsibility of forensic units, including forensic DNA profiling providers, law enforcement and forensic healthcare professionals, to maintain up-to-date DNA profile data on appropriate elimination databases. Where multiple forensic DNA profiling providers are used then data sharing agreements shall be in place and reflected in the consent or agreement from the donor of the elimination sample.

92.11.13 Security of the elimination database records shall be maintained by enforcing restricted access to nominated and authorised individuals by the forensic unit/elimination database administrator.

92.11.14 Unsourced contaminant profiles shall be shared with international elimination databases, such as the International Commission of Missing Persons elimination database.

Searching against elimination DNA profile records

92.11.15 All casework profiles meeting the minimum number of alleles for national DNA database searching criteria, either single source or mixtures, shall be compared against relevant elimination databases (e.g. the local staff elimination database held by forensic DNA profiling units, the national contamination elimination database held by the Forensic Information Database Service and the International Commission of Missing Persons elimination database).

Match regime

92.11.16 The searching and matching regime shall optimise the identification of contaminating profiles but minimise the number of adventitious matches. The regime shall take into account the:

a. number of alleles that will be used to report a likelihood ratio to the court;

b. minimum load criteria for the local, national and international databases;

c. number of records held in the elimination database;

d. discrimination of the elimination DNA profiles held; and

e. appropriate match stringency (exact) and one allele difference (near match/N-1) routine used for the multiplex kit(s) used to generate the profiles being compared.

Match investigations

92.11.17 All instances where a match against an elimination database profile is observed shall be recorded as a non-conformance and be investigated.

92.12 DNA allele frequency and haplotype reference databases

92.12.1 DNA allele frequency and haplotype (e.g. mitochondria, Y-chromosome) databases constructed without identifiable individuals shall be utilised as required for interpretation purposes. They shall be relevant to the issues on which an interpretation of the significance of the evidence is based.

92.12.2 Databases used for calculations shall be peer reviewed and robust. Any limitations on their use shall be documented and revealed alongside any interpretation or opinion provided.

93. Bloodstain pattern analysis

93.1 Scope

93.1.1 This section relates to the classification, identification and/or interpretation and evaluation of bloodstain patterns, including at incident scenes and in controlled facilities, and relates to FSA – BIO 201 – Human biological material distribution analysis (section 42).

93.2 Terminology

93.2.1 Forensic units shall specify the terms and definitions to be used, based on the profession's agreed terminology; any deviations or alternative phraseology shall be defined and explained in validation reports and when reporting BPA.

93.3 Personnel

93.3.1 Minimum qualifications and experience for bloodstain pattern practitioners shall be defined and documented by the forensic unit.

93.3.2 The competency requirements for activities shall be defined and documented.

93.3.3 The forensic unit shall document the authorisation process for BPA practitioners, and this shall specify the competency level and location (laboratory or incident scene) at which they are authorised to work.

93.4 Training

93.4.1 The training and ongoing professional development requirements for bloodstain pattern practitioners shall be documented for all competency levels, as defined by the forensic unit.

93.4.2 The training required to develop competency shall include instruction in all facets of BPA relevant to the desired level of competency.

93.4.3 Each area of instruction shall have documented objectives and shall have a formal assessment of the trainee's knowledge and/or competency (e.g. written test, practical test, PT and/or oral test).

93.4.4 During the course of training, a BPA trainee and trainer/mentor shall document and participate in a mentorship programme.

93.4.5 A training record shall be kept for each trainee.

93.5 Competency assessment

93.5.1 The forensic unit shall determine and document the requirements for competency and ongoing competency for each role. For peer review this shall be by a practitioner with an equivalent or greater level of competency.

93.5.2 Records of the assessment and subsequent authorisation shall be maintained (section 22.3.2).

93.6 Accommodation and environmental conditions

93.6.1 The forensic unit shall:

a. specify conditions required for the safe handling of bloodstained items;

b. specify procedural guidelines for best practice to preserve and avoid contamination of bloodstained items; and

c. have access to facilities to perform fit-for-purpose, task-relevant examination and experimentation.

93.7 Selection of test methods

93.7.1 End user requirements for BPA shall be articulated and the appropriate methods and their limitations specified, documented and communicated.

93.8 Validation

93.8.1 The forensic unit shall demonstrate, through the generation of validation data, that the procedures used produce consistent and valid results. This shall reflect the various aspects of BPA undertaken at the facility and at incident scenes.

93.8.2 As part of validation the forensic unit should identify the methods to be used in BPA and confirm that they are within the scope of the published scientific literature.

93.8.3 Any novel method used by the forensic unit that is not referenced in the peer-reviewed scientific literature (e.g. a new software method) shall require validation.

93.8.4 Computer-assisted methods (and software used) shall be validated.

93.9 Uncertainty of measurement

93.9.1 Those methods that require an estimation of uncertainty of measurement shall be understood and a list maintained.

93.10 Equipment

93.10.1 The types of equipment used for BPA and their calibration requirements shall be specified.

93.10.2 Requirements for the use and validation of software programs for BPA shall be specified.

93.11 Measurement traceability

93.11.1 The process to create reference bloodstain patterns that are used as working standards for bloodstain identification shall be documented. This process shall ensure that the creation of the bloodstain patterns is witnessed and catalogued by practitioners.

93.11.2 The requirements for the use of bloodstain pattern exemplars for interpretation shall be specified.

93.11.3 Original images shall be retained according to the forensic unit's retention and control of data procedures and in accordance with relevant legislation.

93.12 Assuring the quality of test and calibration results

93.12.1 A procedure for an independent assessment of any bloodstain pattern interpretation, evaluation, and fulfilment of the BPA strategy by a practitioner shall be specified.

93.12.2 Methods used, data and records retained (such as photographs) shall allow for retrospective full independent analysis/review (retention of serious crime-related data can be required for 30 years).

93.12.3 A procedure for addressing any differences in opinion in the BPA interpretation between the practitioner and the independent reviewer shall be specified.

93.12.4 The forensic unit shall have a documented audit schedule specifying the range of bloodstain pattern activities and practitioner roles that will be audited per year, per site and per accreditation cycle.

93.12.5 The forensic unit shall undertake at least one BPA PT per site, per year, relevant to the scope of activity.

93.13 Reporting results

93.13.1 Any forensic unit-specific requirements for using standardised terminology for reporting BPA shall be defined; deviations and alternative phraseology from the terminology shall be explained in reports. Also see competence required for reporting in section 22.2.

94. Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988

94.1 Introduction

94.1.1 This section establishes the requirements for, and a common approach to, the analysis and reporting of the concentrations of certain drugs in relation to FSA – DTN 102: Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988, which sets the compliance requirements for the analysis of blood and/or urine samples for the detection of drugs in relation to offences under s5A of the Road Traffic Act 1988 ('drug driving') [81].

94.1.2 Although s5A of the Road Traffic Act 1988 (s5A) [81] refers to both blood and urine samples, these requirements only apply to the analysis of blood samples, as the specified limits relate to blood concentrations [84].

94.1.3 These requirements will be supported by guidance on the analyses of s5A blood samples when the Code comes into force.

94.1.4 Lab 51 'UKAS accreditation of laboratories performing analysis of toxicology samples' does not apply to this FSA.

94.2 Scope and schedule of accreditation

94.2.1 The analytical method is required to establish the presence or absence of a specified controlled drug above or below (which includes at) a specified limit in a sample as the arithmetic mean of the result of a number of analyses.

94.2.2 The schedule of accreditation for this analysis should be defined as 'Detection and quantification of drugs in relation to s5A of the Road Traffic Act 1988 (as amended) and The Drug Driving (Specified Limits) (England and Wales) Regulations 2014 (as amended)'.

94.3 Sample storage

94.3.1 The blood concentrations of the drugs covered by the s5A offence [81] may be subject to degradation over time. The forensic unit shall use storage methods which are known to minimise such degradation.

94.3.2 The forensic unit should consider the storage of samples prior to submission and may advise whether analysis is likely to be worthwhile; the forensic unit

may also provide commissioning parties with advice as to how to store samples to maintain their integrity for analysis.

94.4 Requirements for analysis

94.4.1 Any forensic unit undertaking FSA – DTN 102: Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988 analysis of blood where the results may be used for investigation of a potential offence under s5A of the Road Traffic Act 1988 [81] shall meet these requirements for analysis.

Environmental requirements

94.4.2 The following environmental requirements shall be addressed:

a. Analysis for the purpose of s5A shall be conducted separately from work involving bulk drugs. This means that bulk drug cases shall not be conducted in the toxicology laboratory.

b. Analysis of samples for the purpose of s5A casework shall be conducted separately, in terms of both space and analytical batch, from batches of other toxicological casework (other than s5A or s4 of the Road Traffic Act 1988 [81]) that may contain high concentrations of drugs (e.g. suspected overdose cases in post-mortem casework), unless screening of samples is undertaken to identify possible high drug concentrations and steps taken to manage the risk of carryover. Separation may be achieved by management of space employed to ensure the risk of contamination is managed and minimised, by separating work in time, and carrying out appropriate environmental checks.

c. Procedures shall be adopted to minimise the risk of sample contamination. At a minimum this will include appropriate separation of working areas, and environment control with testing such as by swabbing of work areas to confirm absence of significant contamination.

d. Environmental monitoring shall be conducted to determine the presence and approximate concentration of any drug being tested for in relation to s5A in the laboratory in which the sample preparation and analysis are undertaken, in particular for cocaine, amphetamine and methylamphetamine. This shall include the use of matrix blank samples. The appearance of a drug in any sample or matrix blank where that drug

should not have been present will also be investigated and monitored (including the presence of cocaine without its metabolite BZE). The presence of a drug in a solvent blank where that drug was present in the case sample analysed immediately before the solvent blank shall be investigated to attempt to determine the source and the potential effect on the result.

e. Any contamination event shall be treated as non-conforming work and there shall be an appropriate investigation and action.

Analytical requirements

94.4.3 The analytical method shall, for each drug the forensic unit analyses in relation to a potential s5A [81] offence, achieve the following requirements:

a. The analysis shall be specific for each drug, such that the results can be relied on as establishing the presence or absence of a specified controlled drug above or below (which includes at) a specified limit in a sample. Where the specified controlled drug is reported as 'detected', this is the confirmed presence below the specified limit and not a screening presumptive indication.

b. The analytical method shall ensure that the results can be attributed to the correct sample. This will include procedures to ensure traceability as well as address the potential for drug carry over.

c. To protect against the risk of drug carry over, a solvent blank shall, subject to the following point, be run before each set of case sample replicates and the results from this blank should not show the presence of any drug relevant to the case sample and the forensic unit shall assess whether there is any risk to the final reported case sample results in a batch if a drug is detected.

d. The forensic unit shall calibrate the method for each batch run. A batch is the set of all samples, including calibrators, controls, blanks and case samples, that are extracted and analysed together.

e. For any part of the analysis employing a chromatographic method the forensic unit shall follow these requirements:

    i. Certified reference materials (CRMs) from different manufacturers shall be used to prepare calibrants and QCs for each analyte, but if

this is not possible then CRMs with different lot numbers from the same manufacturer is a suitable alternative option.

ii. shall ensure that quality control samples (QCs) are extracted and analysed alongside and in the same way as casework samples.

iii. shall ensure the calibration curve comprises a minimum of five calibration points, not including zero, and a maximum of 20% of data points can be removed if they are identified as outliers or justified due to gross error as detailed in (iv) and not solely to ensure the QC passes. The calibration curve shall include and encompass concentrations either side of the defined critical or cut-off concentration. The concentration range shall be appropriate for each analyte and shall encompass the critical concentration of interest, ideally at approximately 50-75% of the concentration range. Removal of any data point must be recorded.

iv. justifiable reasons for excluding data points can include but are not limited to: a catastrophic failure resulting in: no, or insufficient, extract to inject into the analytical instrument; no internal standard with which to compare the analyte response; no analyte with which to compare the internal standard response. Examples include but are not restricted to tube breakage, failure to add internal standard, failure to add analyte.

v. shall ensure that data points generated from calibrators are reviewed by the initial data processor prior to reviewing any QCs in a batch.

vi. shall ensure that if the coefficient of determination (R^2) is used to assess the fit of the calibration curve, R^2 must be greater than 0.990 for a linear fit or greater than 0.995 for a quadratic fit. Other equivalent models for 'goodness of fit' may be used in line with the accompanying guidance.

vii. shall ensure manual integration of peaks is justified and applied consistently throughout a batch and recorded. Manual integration of a peak shall not be undertaken solely to ensure an ion ratio passes or to improve the calibration curve.

viii. shall ensure that where manual integration has been used on a case sample, when the peak had already been integrated by the software, and this has caused the result to be reported as over the specified limit, where this would not have happened without the use of manual integration, the sample extract is reinjected or the sample is re-extracted and repeated.

ix. shall ensure that:

i. the retention time of the drug's chromatographic peak in the sample shall not differ by more than 1% or ±0.1 minute, whichever is greater, from that of the same drug in a QC or other control sample analysed in the same analytical batch or

ii. the relative retention time between the drug and associated internal standard in the case sample shall not differ by more than ±0.5% from the relative retention time of the same drug and associated internal standard in a QC or other control sample analysed in the same analytical batch.

f. For any part of the analysis employing a mass spectrometry method the following apply:

i. Acceptable ion ratios shall be no worse than those detailed within the World Anti-Doping Agency (WADA) Technical Document [110] or OJEC, [111] ASB/ANSI [112], GTFCh [105], EWDTS [113] guidelines.

ii. If an ion ratio fails within the case sample the drug concentration shall not be reported.

iii. If an ion ratio fails within a QC the result shall not be used.

g. A blank blood sample shall be run containing an internal standard in each analytical batch. This sample shall be monitored for the presence of any drug being analysed and the forensic unit shall assess whether there is any risk to the final reported case sample results in a batch if a drug is detected. This is particularly important when a case sample result is close to the specified limit and repeat analysis should be considered.

h. The method shall involve monitoring for analytical results which suggest there may have been a contamination event (e.g. the presence of cocaine without benzoylecgonine (BZE) or drugs appearing where not expected).

i. The reported result of the method shall be the arithmetic mean of the analysis of at least two aliquots from the casework sample. There shall be at least two results generated (i.e. the extraction of at least two aliquots). The final output of the arithmetic mean of a number of analyses will be used to calculate the 'not less than' figure (NLTF).

j. For QC samples the arithmetic mean shall be calculated from the extraction of two replicate aliquots.

k. For the arithmetic mean of a number of analytical results to be acceptable, all of the individual analytical results (e.g. drug concentrations in any case sample, calibrator or QC) shall be in the range of a maximum ±20% of the mean.

l. For each drug, the analytical method shall achieve the following:

   i. It shall have a lower limit of quantification (LLOQ) at a concentration equal to or lower than half of the specified limit.

   ii. It shall, subject to point (iii) below, have an upper limit of quantification (ULOQ) at a concentration of at least 25% greater than the common reporting threshold (see 94.5.10).

   iii. For diazepam, flunitrazepam, lorazepam, oxazepam and temazepam (where the sample and QCs may require dilution to bring them within the calibration range), the forensic unit shall have an ULOQ appropriate to the method used.

   iv. For each internal standard used in a method (and per instrument as required), a minimum acceptable recovery of internal standard shall be set. That limit shall be set such that the method is capable of reliably detecting the analytes at the smallest required concentration (LLOQ).

   v. For each internal standard in each batch, an average internal standard response shall be set from the responses in the calibrators, or the calibrators and the QCs, or the whole batch. Once set, the

acceptance range shall then be applied to the internal standard responses in the batch.

vi. The method shall have a systematic error (bias) of no more than ±20%.

m. The forensic unit shall be able to achieve the uncertainty of measurement requirements set out in 94.5.6. These requirements shall be maintained in routine work.

94.4.4 The forensic unit shall, for each drug, establish the uncertainty of measurement in a manner consistent with accepted guidance [114] [29] and accounting for all variables which may affect the results (e.g. different operators, analysis in different batches, analysis on different dates).

Positive quality control

94.4.5 The forensic unit shall undertake ongoing quality control monitoring using blood spiked at a minimum of two different concentrations.

a. A QC at the specified limit for each drug shall be run.

b. A QC spiked at a concentration of at least 50% of the top calibrant shall also be run for the following drugs: cocaine, benzoylecgonine, delta-9-tetrahydrocannabinol, ketamine, methylamphetamine, methylenedioxymethamphetamine, 6-monacetylmorphine, morphine.

c. The second QC concentration for the drugs not specifically mentioned shall be appropriate to the chosen calibration range.

d. Further QCs within the calibration range beyond the minimum requirement may be included in a batch.

94.4.6 Each QC sample shall be a replicate analysis that matches the samples, i.e. two aliquots of the same concentration.

94.4.7 The results shall be monitored in an appropriate manner (such as a Shewhart Chart) and subjected to suitable statistical rules (e.g. the Westgard Rules [115]). Results greater than the s5A specified limit concentration for the drugs shall only be reported if obtained while the method is under control.

94.4.8 The quality control monitoring shall use sufficient QC samples in each batch to ensure that the reliability of results can be assured. At least 10% of the samples

in each batch (including all QC values), shall be positive QC samples with at least two positive QC samples when the batch contains less than 20 samples.

94.4.9 A QC sample result shall be the arithmetic mean of the results from the analysis of two separate aliquots of control material. The aliquots may be taken from either a single spiked blood sample or from two samples of blank blood each spiked to the appropriate concentration.

94.4.10 QC sub-sample replicates shall be run together as a pair, in the same way as the samples, and not split across the batch. The quality control sample pairs should where possible be spaced evenly through the batch, during both the extraction and the analysis, being run at the beginning, end, and where possible, the middle of the batch.

94.4.11 The mean and standard deviation of each measured QC concentration shall be calculated during method validation from the analysis of QCs in at least 11 batches, each batch containing at least two QC samples, each QC 'sample' comprising of least two sub-sample aliquots. The term standard deviation refers to the sample standard deviation of the results. The standard deviation of the means shall not be used.

94.4.12 The 'preliminary' Shewhart chart warning limits shall be set as the greater of ±2 times the method standard deviation or ±60% of the Forensic Science Regulator's Expanded Uncertainty (FSREU) (see table 2 on page 270), from the arithmetic mean of the data.

94.4.13 The 'preliminary' Shewhart chart action limits shall be set as the greater of ±3 times the method standard deviation or 90% of the FSREU, from the arithmetic mean of the data.

94.4.14 These preliminary limits shall be replaced by initial limits once the data from a minimum of 30 batches have been collected.

94.4.15 The 'initial' Shewhart chart warning limits shall be set at ±2 times the standard deviation, calculated from a minimum of 30 batches, from the arithmetic mean of the data.

94.4.16 The 'initial' Shewhart chart action limits shall be set at ±3 times the standard deviation, calculated from a minimum of 30 batches, from the mean of the data.

94.4.17 An investigation shall be carried out, and documented if there is a breach of the rules used to monitor statistical control within a batch. This investigation should be as per Westgard Rules [115], when:

a. One or more quality control sample results are outside of the action limits; a '1 x $_{3s}$' failure. Negative sample results may be accepted where permitted by the forensic unit's procedures, such as for example when the result is below the LLOQ.

b. One or more QC sample results from two consecutive batches are between the warning and action limits; a '2 x $_{2s}$' failure. In this event it is the results of the second batch which must be investigated and it may be necessary to review the results of the earlier batch. Negative sample results may be accepted where permitted by the forensic unit's procedures, such as for example when the result is below the LLOQ and other criteria have been fulfilled.

c. QC sample results from within a single batch lie outside of both the upper and lower warning limits; a 'R x $_{4s}$' failure. Negative sample results may be accepted where permitted by the forensic unit's procedures, such as for example when the result is below the LLOQ and other criteria have been fulfilled.

94.4.18 Negative sample results may be reported where permitted by the forensic unit's procedures, such as for example when the result is below the LLOQ and other criteria have been fulfilled. Positive sample results above the ULOQ may also be reported where permitted by the forensic unit's procedures.

94.4.19 The batch sample results shall be accepted, but an investigation shall be carried out, and documented, when one or more quality control sample results, within a single batch, are outside, on the same side, the warning limit; a '1 x $_{2s}$','2 x $_{2s}$' etc. warning.

94.4.20 The forensic unit may additionally use other rules for the monitoring of trends in QC data as they see fit. Such rules include, but are not limited to:

a. The batch sample results may be accepted, but an investigation shall be carried out, and documented, when four consecutive QC results fall between 1 and 2 standard deviations, on one side, from the mean; A 4 x $_{1s}$ warning.

b. The batch sample results may be accepted, but an investigation shall be carried out, and documented, when 10 consecutive results lie on one side of the mean; A '10_x' warning.

c. The batch sample results may be accepted, but an investigation shall be carried out, and documented, when seven consecutive QC results fall or rise; a '7_t' warning.

94.4.21 The data on the charts shall be reviewed at least every three months to compare the mean and standard deviation of the QC results, using t- and F-tests, with the values used to set the chart limits. The mean and action/warning limits may be adjusted if the comparison shows significant differences and there is some explanation for those changes.

94.4.22 Where the monitoring indicates the forensic unit is no longer complying with the requirements in relation to uncertainty 94.4.3, work shall stop. A non-conforming work investigation shall be carried out and corrective action shall be taken to return the method to control and a review and impact assessment on case samples affected is to be undertaken.

94.4.23 Where a new lot of a certified reference material is introduced, it shall be compared by experiment, against the existing certified reference material to determine whether there might be a change in the operation of the method.

94.5 Reporting of results

Units

94.5.1 Results shall be reported in units of micrograms per litre (µg/L) to facilitate comparison against the specified limits and avoid any confusion. Results for drugs with a legal limit of less than 10 µg/L shall be rounded down and reported to one decimal place. Results for a drug with a legal limit equal to, or greater than 10 µg/L shall be rounded down and reported to integer values only.

Calculation

94.5.2 Where analytical results used to determine a reportable value include a value above the ULOQ, the arithmetic mean shall be calculated using (a) [each] analytical result which is below the ULOQ and (b) the ULOQ for [each] result which is above the ULOQ.

94.5.3 Where all analytical results are above the ULOQ, a subtraction of the FSREU shall be made from the ULOQ. See 94.5.7.

94.5.4 Where analytical results include a value below the LLOQ and above the limit of detection (LOD), the value should be reported as too small to report a meaningful concentration. The forensic unit shall determine a form of words to use in such cases.

94.5.5 Where an accurate figure is reported, i.e. for any numerical result reported above the LLOQ a NLTF must be used.

94.5.6 The Forensic Science Regulator's Expanded Uncertainty (FSREU) (see table on page 14) shall be deducted from the arithmetic mean of the analytical results. The final figure generated shall be rounded down. For example, a sample with concentrations of amphetamine in replicate one of 315 µg/L and replicate two of 323 µg/L leading to an arithmetic mean of 319 µg/L. The FSREU is 20% so the deduction would be 63.8 producing 255.2 µg/L. This would be rounded down to a NLTF of 255 µg/L.

94.5.7 Where all analytical results used to determine the reportable result are above the ULOQ, the normal reporting calculation as detailed above shall be carried out, but the figure should be reported as 'greater than ###'. For example, if the ULOQ for BZE is 250 µg/L and both analytical results exceed this figure, 20% should be deducted from 250, and the result reported as 'greater than 200 µg/L'.

94.5.8 The results shall be interpreted on the basis that the figure as rounded is the relevant figure for comparison against the specified limit.

Limits

94.5.9 Where the drug is detected but the NLTF is equal to or less than the specified limit for the drug, the results may be reported as the drug present, but it shall not be reported as being over the limit.

Analysis at the instruction of police or prosecution

94.5.10 The use of the FSREU gives rise to the concept of a 'common reporting threshold' (CRT) – the lowest measured concentration at which the result can be reported as being above the specified limit. The rounded-up CRT for each drug is listed as a whole number as per Table 2 (next page) of the FSREU.

94.5.11 The forensic unit shall only provide a figure if the forensic unit's expanded uncertainty of measurement for that drug is equal to or less than the FSREU at the specified limit.

94.5.12 This Code covers the process by which the analytical result is produced and a conclusion reported as to whether the concentration of the drug in the sample was greater than the relevant specified limit. The use of an agreed uncertainty and resultant common minimum reporting threshold does raise some additional points:

a. Any report/ statement on an analysis shall make clear that:

   i. the determination of the NLTF used the centrally set expanded uncertainty; and

   ii. the forensic unit's calculated uncertainty for the analysis was no greater (worse) than the FSREU at the specified limit.

b. The requirements in section (a) above shall be achieved by declaring compliance to the Code, as long as the provisions of FSA-DTN-102 and these requirements are met.

Table 2: The specified limits [84]**: FSREU and the CRT for each drug in England and Wales**

Controlled drug	Legal limit (µg/L)	FSR expanded uncertainty (%)	CRT (µg/L)	Date limit first established
Amphetamine	250	20	314	14 April 2015
Benzoylecgonine	50	20	64	2 March 2015
Clonazepam	50	20	64	2 March 2015
Cocaine	10	35	17	2 March 2015
Delta-9-tetrahydrocannabinol	2	30	3	2 March 2015
Diazepam	550	20	689	2 March 2015
Flunitrazepam	300	25	402	2 March 2015
Ketamine	20	20	27	2 March 2015
Lorazepam	100	25	135	2 March 2015
Lysergic acid diethylamide	1	45	2	2 March 2015
Methadone	500	25	668	2 March 2015
Methylamphetamine	10	40	19	2 March 2015
Methylenedioxymeth-amphetamine	10	25	15	2 March 2015
6-Monoacetylmorphine	5	35	8	2 March 2015
Morphine	80	25	108	2 March 2015
Oxazepam	300	20	377	2 March 2015
Temazepam	1000	20	1252	2 March 2015

95. Friction ridge detail: visualisation and enhancement

95.1 Scope

95.1.1 FSA – MTP 100 – Friction ridge detail: visualisation and enhancement (section 56) can be carried out at a dedicated facility or as a specialist activity carried out at an incident scene. Accreditation to ISO/IEC 17025:2017 [3] for facility and facility-based activities extended to incident scenes is required.

95.1.2 Visualisation and imaging of friction ridge detail do not operate in isolation, and it shall be recognised that the activities are part of the fingerprint examination workflow. It also includes activities relating to decision making prior to visualisation and post-visualisation.

95.2 Terms and definitions

95.2.1 The term ‘friction ridge detail’ includes all areas of the friction ridge skin system on the fingers, palms, phalanges and feet (plantar).

95.2.2 For the purposes of this set of FSA specific requirements, the term ‘process’ refers to the entire method/actions of recovering areas of friction ridge detail (i.e. multiple linked stages) whilst ‘technique’ refers to individual visualisation methods.

95.3 Personnel

Practitioner competence

95.3.1 The forensic unit shall implement a training and competency programme, recognising the different areas of competence required for a range of tasks within the workflow, to ensure the continual development of its practitioners.

95.3.2 The forensic unit shall establish a competency framework for all practitioners using criteria that have been established by the level of practitioner competence required for each job role.

95.3.3 This framework shall include the ongoing process of training, assessment and review to ensure the maintenance of practitioner competence. It shall define when competence has lapsed and the process for managing a practitioner in such circumstances.

Initial and ongoing competence

95.3.4 The details of a structured training programme to attain initial competence and a programme of periodic assessment to demonstrate ongoing competence shall be documented.

95.3.5 Training and ongoing competence assessment shall be determined and documented by the forensic unit and shall include:

a. aspects of technique selection;

b. aspects of technique application;

c. recognition of technique performance issues;

d. appreciation and accommodation of requirements of colleagues further along the workflow; and

e. an understanding of image capture techniques, including:

   i. an appreciation of image quality;

   ii. basic principles of photography; and

   iii. post-capture image enhancement.

95.4 Technical records

95.4.1 The forensic unit shall have procedures for the production of, and the recording of, changes to technical records; records may include photographs, images, hard-copy or electronic records of any documentation.

95.4.2 Documented procedures shall define and reference the documentation (also referred to as case notes) associated with the friction ridge detail visualisation process and image capture.

95.4.3 Any deviation in the application of a process, such as to take into account environmental change at an incident scene, and the reasoning behind the decision made, shall be documented.

95.4.4 The level of detail in the documentation shall be sufficient to allow for an audit trail.

95.4.5 The forensic unit shall have procedures that document the actions a practitioner should take to:

a. record the results of a process; and

b. recover the friction ridge detail for subsequent downstream processing.

95.5 Accommodation and environmental conditions

95.5.1 The facilities shall be appropriate for the effective implementation of the friction ridge detail visualisation techniques used within that facility.

95.5.2 The forensic unit shall have at least the following:

a. Space for managing items/techniques submitted for friction ridge detail evidence recovery, including secure storage and handling areas.

b. Areas for carrying out the processes, including:

   i. dedicated areas for the optical techniques; and

ii. ‘wet’ and ‘dry’ areas for the preparation of chemical and physical techniques.

c. Installed fixed equipment, e.g. fume cupboards, wet benches.

d. A range of general equipment, e.g. measuring equipment.

e. Specific equipment, used to capture friction ridge detail for subsequent search and comparison, that have been demonstrated as fit for purpose.

f. Suitable storage for equipment and chemical products.

g. Controlled areas of access, e.g. where there are health and safety precautions required to operate a technique or where secure areas of restricted access are required.

95.6 Test methods and method validation

95.6.1 The forensic unit shall demonstrate knowledge and understanding of the requirements for validation, and the validation of their processes for friction ridge detail visualisation and the subsequent image capture and transmission process.

95.6.2 The forensic unit shall undertake validation, using known source data, to ensure the reliability of examination outcomes.

95.6.3 Practitioners shall understand their data, limitations of their data and relevance of their findings based on the validation of their methods and processes.

95.6.4 The information provided in this section is supplementary to the validation guidance provided in this Code (section 24):

a. Processes and techniques described within the Fingermark Visualisation Manual [116] have varying amounts of testing and data supporting their use. Forensic units shall review this data and ensure that it is sufficient to support the methods as used in their operational work. Dstl has made documents, including the Fingerprint Source Book [117], available in order to assist with determining whether the Fingermark Visualisation Manual validation data is sufficient for operational activities.

b. Validation shall be undertaken in all cases where the forensic unit deviates from techniques and processes tested by other forensic units or wishes to

use a different treatment method/route they believe to be more effective from that set out within the Fingermark Visualisation Manual. Validation studies should evaluate the performance of new or altered techniques, sequences and procedures against current methods in order to assess suitability for potential operational use, and they should be planned with reference to published guidelines.

c. The forensic unit shall ensure that where external validation studies have been used, e.g. scientific journal publications, Fingermark Visualisation Manual, Fingerprint Source Book, these have been reviewed by the forensic unit and the strengths, weaknesses and any limitations are fully understood and addressed in-house to confirm suitability by verification.

d. If a technique is to be used on a substrate not tested within the validation plan, a practitioner shall determine if additional validation data is required. For example, the evaluation could be based upon the similarity of the substrate (porosity, colour, texture) to those previously tested. The decision to conduct or not conduct further studies or to extend the scope of an existing study shall be documented, with the rationale set out.

95.6.5 The forensic unit shall hold documentation for each validation and/or verification exercise that it completes.

95.6.6 The forensic unit shall determine whether measures aimed at preventing contamination or cross-contamination are fit for purpose.

95.7 Image capture and transmission

95.7.1 Image capture shall be carried out by practitioners who are suitably qualified.

95.7.2 Imaging should be optimised prior to capture by using appropriate lighting, camera settings and optics rather than by post-capture image processing, which may cause some of the original friction ridge detail to be lost.

95.7.3 The image capture and transmission process shall be validated or verified, with performance tests carried out to ensure the various elements within this process do not adversely affect the quality of the result for examination of friction ridge detail.

95.8 Estimation of uncertainty of measurement

95.8.1 The forensic unit shall identify the components of uncertainty and minimise their effect, as far as possible, through:

a. specification of equipment, chemicals and consumables;

b. anti-contamination procedures;

c. training;

d. practical validation or verification of methods;

e. selection of appropriate recovery techniques for the case circumstances; and

f. image capture methods.

95.9 Control of data

95.9.1 Procedures shall be in place for the control of data to protect and secure both the paper and electronic data generated by the forensic unit.

95.9.2 Policies and procedures shall be in place for the digital capture, storage, retrieval, display, transmission, retention and destruction of images.

95.9.3 An audit trail shall be created upon receipt and maintained with the image(s). The original image shall be retained securely, and any image processing and enhancement shall be carried out on a working copy, with all transformations included in the audit trail.

95.9.4 The forensic unit shall specify how it will handle images provided through a third party or via an uncontrolled capture (e.g. from video).

95.10 Measurement traceability

95.10.1 The forensic unit shall have traceable records to demonstrate that the calibration of equipment has been completed and reviewed, and to confirm that it is fit for purpose.

95.10.2 The forensic unit shall produce evidence of continuing compliance of equipment through a schedule of re-calibration.

95.10.3 The forensic unit shall maintain records that ensure any calibration or reference standards are traceable, e.g. to the international system of units (SI).

95.11 Sampling

95.11.1 Sampling in this context relates to a case assessment leading to the selection of appropriate items/exhibits and targeting specific friction ridge detail recovery processes to facilitate the expedient reporting of results based on the needs of the investigation.

95.11.2 The sampling of items/exhibits required in the friction ridge detail retrieval process may be determined prior to the submission of items to the forensic unit. This may be documented within a standard operating procedure determined by the forensic unit, such as a submission policy or an SLA.

95.11.3 When the forensic unit needs to sample items/exhibits, especially in a way that deviates from the documented sampling policy or agreed SLA, the sampling strategy shall be agreed with the commissioning party and shall be clearly documented.

95.11.4 Where only a sample of the developed friction ridge detail is progressed to the comparison and/or search processes, it shall be documented:

a. as part of the procedures of the forensic unit;

b. in a policy document; or

c. on a case-by-case basis and made clearly evident for disclosure.

95.12 Handling of items/exhibits

95.12.1 The origin of individual items/exhibits shall be traceable at all times during the process, including during treatments, and an audit trail shall be available to track the continuity of all case-related items/exhibits.

95.12.2 Unique labelling shall be in place to distinguish between items/exhibits.

95.12.3 Handling of items/exhibits shall be kept to a minimum to avoid contamination and they shall be packaged in such a way to minimise damage caused by contact between them and packaging.

95.13 Assuring the quality of results

95.13.1 Where contamination of an exhibit may have taken place, the practitioner shall inform the relevant personnel (usually the fingerprint bureau) so that the

practitioner's elimination prints can be checked against any friction ridge detail obtained for that exhibit.

95.13.2 The forensic unit shall have in place documented procedures for quality assuring any friction ridge detail submitted for comparison or search, whether that be recorded digitally or manually.

95.13.3 Where a technique has been applied, the forensic unit shall provide documentary evidence to demonstrate whether it has worked satisfactorily. Test strips or control samples shall be appropriate to the technique and the required result to add value to the quality assurance process.

95.13.4 Where a forensic unit uses filtering or assessment criteria to progress along the workflow, there shall be procedures in place to monitor the practitioners' adherence to those criteria.

95.13.5 The forensic unit shall devise a proportionate and representative schedule of dip sampling of case files by a practitioner. This shall include cases where friction ridge detail has been recovered and cases where the techniques utilised have not produced any friction ridge detail, or where the friction ridge detail has not been recovered by a practitioner for comparison and/or search purposes.

95.13.6 The forensic unit shall participate in suitable PT programmes and/or inter-laboratory comparisons (ILC). A plan for the level and frequency of participation, and a process for the review of the resulting outcomes, shall be documented.

95.13.7 Process performance shall be regularly reviewed using data from dip sampling, quality control, and competency and proficiency tests.

95.14 Reporting the results

General

95.14.1 The outcomes of any visualisation techniques shall be recorded. All processes applied and examinations carried out shall be documented, irrespective of the result.

95.14.2 The forensic unit shall have practitioner(s) capable of providing supporting information (technical and observed) to end user(s) who are required to make informed decisions or formulate opinion(s) about the deposition of the developed mark. Images that show the relative position of the marks in situ on

the item/exhibit shall be provided as required (and include images in technical records).

95.14.3 The results shall be updated/recorded on any organisational management system in use or communicated direct to the commissioning party. This communication shall be retrievable if needed.

Communication and collaborative working

95.14.4 The forensic unit shall have documented strategies, demonstrable as effective for communication and collaborative working, both as part of the overall fingerprint workflow and where multiple evidence types are required.

96. Friction ridge detail: comparison

96.1 Scope

96.1.1 The fingers, palms of the hand, toes and the soles of the feet comprise an intricate system of friction ridges and furrows, which are known as friction ridge skin. The arrangement and sequencing of characteristics within friction ridge skin are extremely variable between individuals, persist throughout life and are accepted as a reliable means of human identification.

96.1.2 Friction ridge detail is an area comprising the combination of friction ridge flow, friction ridge characteristics, and friction ridge structure to include other features such as creases. It is the examination of these characteristics and features that form the basis of the forensic science activity of friction ridge detail comparison defined in this Code. The undertaking of friction ridge detail comparison shall include all areas of friction ridge detail on the human body.

96.1.3 The method is the end to end process for each of the four (4) services defined in the FSA – MTP 101 - Friction ridge detail: comparison. ACE is the technical framework that facilitates each of those services.

96.1.4 These FSA specific requirements establish the specific requirements for friction ridge detail examination within the context of accreditation to ISO/IEC 17025:2017 and the Code and ILAC G19:06/2022. They set out the basis on which accreditation is achieved for undertaking this FSA. The Regulator will produce guidance to support effective regulation of this FSA including terminology used in friction ridge detail comparison.

96.1.5 The forensic unit shall recognise that friction ridge detail analysis and comparison activities are part of the friction ridge detail end-to-end workflow (recovery to final report) and are reliant on the quality of the product from upstream processes.

96.2 Defining the scope of accreditation

96.2.1 The scope of accreditation for organisations which undertake friction ridge detail comparison should be defined on the basis that material tested is friction ridge detail. The type of service which ACE is used to deliver should be described as;

a. Searching

b. identity check

c. scene linking

d. direct comparison

96.2.2 The services delivered shall be documented and validated in line with the requirements of the Code, and carried out by practitioners who have been deemed competent to do so.

96.3 Personnel ISO/IEC 17025:2017 Clause 6.2, ILAC-G19:06/2022 Clauses 3.3 and 4.8.3

Practitioner competence

96.3.1 The forensic unit shall have practitioners, recognising the different areas of competence required for a range of tasks within the workflow, and shall establish a competency assessment framework for new (including those with previous experience) and existing practitioners. This framework shall include:

a. the ongoing process of training, assessment and review to ensure the maintenance of practitioner competence; and

b. the process for managing and supporting practitioners whose competence has lapsed.

96.3.2 The details of a structured training programme to attain initial competence and a programme of assessment to demonstrate ongoing competence shall be documented.

96.3.3 Competency assessment shall include all comparison activities and the use of any automated fingerprint identification system (AFIS). Assessment of initial and ongoing competence shall be objective and therefore include items of known outcomes from all sources of friction ridge detail, utilising ground truth data.

96.4 Technical records ISO/IEC 17025:2017 Clause 7.5, ILAC-G19:06/2022 Clause 3.5

96.4.1 The forensic unit shall have procedures for the production of technical records, including recording examination notes contemporaneously in a format and with a level of detail that is clear and auditable.

96.4.2 Procedures shall define and reference the documentation (also referred to as case notes) associated with the friction ridge detail workflow process.

96.4.3 All records shall include the date they were made and the identity of the individual responsible for each entry. Technical records shall, as a minimum, demonstrate the examination sequence and include:

a. a unique reference number;

b. records of materials used in the course of the analysis and examination;

c. records of the analysis and examination;

d. sequence of recording contemporaneous notes;

e. results/outputs;

f. reporting outcomes of the fingerprint examinations; and

g. records of communication.

96.5 Accommodation and environmental conditions ISO/IEC 17025:2017 Clause 6.3, ILAC-G19:06/2022 Clauses 3.11 and 3.12

96.5.1 The workspace and equipment used for fingerprint comparison shall be fit for the effective carrying out of the FSA This should include an appropriate environment with suitable lighting.

Equipment

96.5.2 The requirements for computers and automated equipment are set out in the Code at section 26.1.

96.5.3 The forensic unit shall have procedures for the control, maintenance and performance checking of critical equipment. Maintenance and performance checks shall be recorded.

96.6 Methods and method validation ISO/IEC 17025:2017 Clause 7.2.2, ILAC-G19:06/2022 Clause 3.10

General considerations

96.6.1 The forensic unit shall have documented procedures describing the FSA sub-activities/services of FSA-MTP101 it undertakes encompassing the workflow from receipt to reporting.

96.6.2 The examination process shall consist of the stages referred to as analysis, comparison and evaluation (ACE) and apply to all sources of friction ridge detail. All sources and inputs typically encountered shall be included in the validation exercises.

96.6.3 ACE can be followed by a verification stage (ACE-V). This process provides a structure for the verification of fingerprint examination results. Verification requires an independent examination of the original material; it is an independent application of ACE.

96.6.4 The process for verification shall also be documented in the forensic unit's procedures.

96.6.5 Verification can be blind or open, and the circumstances where these options are used shall be clearly defined in the forensic unit's procedures.

96.6.6 The forensic unit shall clearly define and document a procedure for the management of circumstances where a variance in practitioner opinion has arisen.

Use of an automated fingerprint identification system in friction ridge detail examination

96.6.7 Where an AFIS is used, the forensic unit shall have a good practice guidance in order to achieve optimal performance. This guidance shall, as a minimum:

a. understand the model/basis of the search method employed;

b. understand the performance of the system's friction ridge detail auto encode function against manual encoding by practitioners;

c. understand the efficiency (i.e. success rate) of the search method to return the appropriate respondent lists (i.e. true positive);

d. understand the type (quality/sufficiency) of friction ridge detail where the appropriate respondent is not returned from one-to-many searches (i.e. false negative);

e. determine the re-launch strategies (manual and/or automated) for negative outcomes to address the incidence of false negative outputs;

f. determine the optimum number of respondents for conducting manual comparisons to minimise the risk of not identifying the appropriate candidate if different from the AFIS default;

g. process relevant results from an AFIS search in accordance with the established verification procedures. On-screen verification is acceptable providing that a documented audit trail is available;

h. manage the risk presented by updates to software for AFIS; and

i. understand the limitations of the system.

96.7 Validation ISO/IEC 17025:2017 Clause 7.2.2, ILAC-G19:06/2022 Clause 3.10

96.7.1 The forensic unit shall ensure that it has staff that are competent to develop appropriate validation plans to include the specific activities undertaken and completion of an appropriate validation with further validation and/or periodic validation reviews completed as required.

96.7.2 Validation shall be reviewed at least once within an accreditation cycle to evidence that methods remain fit for purpose and shall be reviewed when elements of the process are subject to change.

96.7.3 Significant changes to procedures, or equipment, shall be considered in a validation review and subject to validation or verification.

96.7.4 Validation and/or verification shall be undertaken by the forensic unit to ensure the reliability of reported outcomes.

96.7.5 The validation exercise shall incorporate impressions of known source friction ridge detail including, but not limited to, lifts, photographs and digital images of friction ridge skin where appropriate. In addition to the process detailed in section 24 of the Code, it shall include:

a. samples representative of the quality and variability of friction ridge detail typically encountered within each service;

b. procedures to ensure that the method delivers expected results;

c. some form of measure of uncertainty;

d. determination of the performance and limitations of the practitioner, environment and equipment;

e. management of the risk posed by transfer methods to and within the bureau; and

f. any post-production methods used by the bureau.

96.7.6 Where an AFIS is used the forensic unit shall either validate or verify the performance by using ground truth data of varying quality and representative of the range of friction ridge detail typically encountered in casework.

96.8 Estimation of uncertainty of measurement ISO/IEC 17025:2017 Clause 7.6

96.8.1 Procedures shall be put in place to estimate the uncertainty in the method under consideration. This could include, but not be limited to consideration of:

a. human factors;

b. procedures;

c. application of digital tools used within the ACE process; and

d. equipment for digital and manual processes.

96.8.2 Error rates can be determined initially from the validation of the methods and processes to assess consistency and variances of opinion.

96.8.3 The uncertainty of measurement shall be reviewed using data from scheduled dip sampling, quality control, and competence and proficiency tests.

96.9 Control of data ISO/IEC 17025:2017 Clause 7.11

96.9.1 Procedures shall be in place to protect, secure, control, review and retain the data generated by the forensic unit; these may relate to:

a. case management systems;

b. AFIS;

c. digital image transfer and storage systems; and

d. digital comparison software.

96.9.2 The forensic unit shall have policies and procedures in place for the digital capture, storage, retrieval, display and transmission of images used as evidence. The method(s) used shall maintain the identity, security, integrity and continuity of the data.

96.9.3 An audit trail shall be created upon receipt and maintained with the image(s). The original image shall be retained securely, and any image processing and enhancement shall be carried out on a duplicate.

96.10 Sampling ISO/IEC 17025:2017 Clause 7.3, ILAC-G19:06/2022 Clause 4.3.3

96.10.1 Sampling in this context relates to case assessment leading to the appropriate selection and targeting of comparisons to facilitate rapid reporting of results based on risk and the needs of the investigation.

96.10.2 The criteria for the selection of the friction ridge detail shall be determined by the relevance of the item/exhibit and consideration given to the quality of the friction ridge detail. This shall be recorded within the contemporaneous notes.

96.10.3 If any friction ridge detail is not subject to analysis, the reason for this shall be documented.

96.11 Handling of items ISO/IEC 17025:2017 Clause 7.4 ILAC-G19:06/2022 Clauses 3.5 and 4.7.7.2

96.11.1 The forensic unit shall have a documented item acceptance and rejection policy as set out in the Code.

96.11.2 Procedures detailing the storage and preservation of the media on which the friction ridge detail is recorded shall be documented.

96.11.3 The forensic unit shall have a documented procedure setting out how the continuity of the item is established and recorded.

96.11.4 Any adjustments made to optimise the appearance of the friction ridge detail shall be made to a working copy of it. The friction ridge detail shall be retained in the format in which it was originally retrieved.

96.11.5 An audit trail shall be available to track the continuity of all case-related items/exhibits.

96.12 Assuring the quality of results ISO/IEC 17025:2017 Clause 8.1.1 Option A

96.12.1 Forensic units shall have documented procedures for verification.

96.12.2 Forensic units shall have a documented procedure for the application of critical findings checks relevant to each of the services set out at 101.2.1. and shall include an element of blind checking.

96.12.3 In recognising that practitioners may be influenced in their decisions by contextual information, forensic units shall have processes and procedures in place to safeguard against the risk of cognitive bias and influence. Such processes could include, but not necessarily be limited to:

a. use of blind examination/verification; and

b. training and awareness.

96.12.4 Forensic units shall participate in suitable ILC, collaborative exercises and/or PT programmes. A plan for the level and frequency of participation, and for assessing the resulting outcomes and opportunities for learning and development, shall be documented.

96.12.5 The forensic unit shall determine a quality control process for reviewing decisions of insufficient detail for search or comparison.

96.12.6 The forensic unit shall determine a quality control process for where nominated candidates have been entirely excluded as the source of any of the friction ridge detail.

96.12.7 Procedures shall cover the provision of guidance and feedback to the friction ridge detail recovery and visualisation practitioners based on the quality of the submissions received; this might include what and how to prepare the friction ridge detail (lift, photograph or digital image) for subsequent processing.

96.12.8 The forensic unit shall have a monitoring process to identify trends and issues amongst practitioners so that the trends can be reviewed and the issues addressed..

Variance of opinion

96.12.9 The forensic unit shall have a documented procedure to deal with differences of opinion amongst practitioners, including a feedback mechanism for individuals involved.

96.12.10 Where there is an external challenge, a potential error, or conflicting opinions, the procedure shall include, as a minimum:

a. a fully documented linear ACE report, which shall record all observations at the analysis stage and interpretation of the friction ridge detail by all practitioners involved in the examination;

b. findings and conclusions reached by all practitioners involved in the examination; and

c. process used to reach a consensus on an agreed outcome.

96.12.11 An error should not be confused with a difference of opinion. When an error has been established, either technical or administrative, a non-conformance shall be raised.

96.13 Reporting the results ISO/IEC 17025:2017 Clause 7.8, ILAC-G19:06/2022 Clause 4.9

Reporting outcomes

96.13.1 The comparison of friction ridge detail is a cognitive process that relies on the competence of the practitioners to perform examinations and analyses, and form conclusions based on the outcomes. The conclusions drawn shall be made based on their training, skill and experience; the basis for these conclusions shall be traceable and clearly evidenced.

96.13.2 Regardless of the certainty in the mind of a practitioner once a conclusion is reached, the evidence presented shall be considered as an opinion, not a statement of fact.

96.13.3 The existence of any documentation or communications regarding differences of opinion, shall be declared in any reports or statements of evidence. This issue was specifically highlighted in the Court of Appeal judgment in R v Smith [2011] England and Wales Court of Appeal (EWCA) Crim 1296 where the judgment states, “The presentation to the jury must be done in such a way that enables the jury to determine the disputed issues.”

96.13.4 Where a different outcome is reported by an internal or external examination, including a referral to the Regulator in historical cases, the process described above shall be followed and reported.

96.13.5 The test method (ACE-V) will deliver one of the following outcomes:

a. Identified: A practitioner term used to describe the mark as being attributed to a particular individual/person. There is sufficient quality and quantity of ridge flow, ridge characteristics and/or detail in agreement with no unexplainable differences that, in the opinion of the practitioner, two areas of friction ridge detail were made by the same individual.

b. Excluded: There are sufficient features in disagreement to conclude that two areas of friction ridge detail did not originate from the same individual.

c. Insufficient: The ridge flow and/or ridge characteristics revealed in the area of friction ridge detail (mark) are of such low quantity and/or poor quality that a reliable comparison cannot be made. The area of ridge detail contains insufficient clarity of ridges and characteristics or has been severely compromised by extraneous forces (e.g. superimposition, movement) to render the detail present as unreliable and not suitable to proffer any other decision.

d. Inconclusive: A determination that the level of agreement and/or disagreement is such that it is not possible either to conclude that the areas of friction ridge detail originated from the same person or to exclude the particular individual as a source for the friction ridge detail.

96.13.6 When reporting an inconclusive outcome, the rationale for this should be clearly recorded and reported.

96.13.7 The forensic unit shall meet the requirements of LAB 13 [71] in relation to the provision of opinions and interpretations related to friction ridge detail comparison and have this included in their ISO/IEC 17025:2017 [3] scope of accreditation.

96.13.8 The forensic unit shall have a policy that clearly defines the process for the provision, amendment and retention of both written reports and any verbal communication.

96.13.9 Reports shall be subject to a defined quality check, according to a documented procedure, which includes a critical findings review, of the examination/analysis prior to being communicated to the recipient. If there is a need to provide results prior to the production of this quality-checked final report, then the provisional status of the results shall be made clear to the recipient through the use of appropriate caveats.

97. Digital forensics

97.1 Technical records

97.1.1 The forensic unit shall have policies and procedures appropriate to the examination/analysis of a device and/or scope of the planned activity, which incorporates:

a. keeping a record of the state, mode and physical condition of any seized/submitted device and any potentially relevant information; and

b. labelling the components of the device and taking photographs (screen, computer front and back, and the area around the device to be seized) and/or sketching the device's connections and surrounding area where relevant.

97.2 Externally provided services

97.2.1 A forensic unit may also obtain services from outside the forensic unit for activities directly related to the delivery of an FSA, but are not explicitly part of the FSA and delivered in a manner where application of all Parts of the Code could not reasonably apply. A related service may be a courier service for recovered items, a mobile phone repair, device unlocking or passcode recovery service. Setting requirements for such services is covered in 18.2.3.

97.2.2 Mobile phone repair (for example a screen replacement) may be an externally provided service provided continuity is maintained. It is not part of FSA DIG 100, however the policy and procedure for using an externally provided service should manage the risks appropriately (e.g. supervising a repair to deal with continuity).

97.2.3 Device unlocking and/or passcode recovery is typically part of the workflow for data capture in FSA DIG 100, but it is not a separate sub-activity and application of all Parts of the Code is not required. The service provider shall comply with Part A of the Code to ensure any quality issues are reported to the Regulator. As part of setting requirements for such a service, the following shall apply:

a. The Regulator shall be notified by the commissioning forensic unit of the agreement to use of externally provided FSA services (section 18.2.3),

with details of the service provider. The Regulator does not need subsequent notifications of individual cases being commissioned but does expect the commissioning forensic unit to maintain records capable of identifying any issues in using this service.

b. The service provider is bound by Part A of the Code, and therefore is required to nominate a SAI.

c. The commissioning forensic unit should have a risk assessment dealing with failure modes of the approach the service provider is taking; the risk assessment may be agnostic of the method used by the service provider.

d. As the method is not a separate sub-activity in FSA DIG 100, nor a test in its own right, the service provider should give the following declaration in a continuity statement.

   i. [The service provider] reports quality issues to the Regulator and control non-conforming work but there are currently no other technical requirements set in the Code of Practice [issue] published by the statutory Forensic Science Regulator; device unlocking/ passcode recovery with no other data recovery is not a sub-activity set out as the forensic science activity detailed in the Code.

97.2.4 The forensic unit commissioning the work should not use this approach for commissioning units within its own organisation.

97.3 Methods

Selection of methods

97.3.1 A method is a logical sequence of operations or analysis which may include the use of software, hardware, tools and actions by the practitioner.

97.3.2 The forensic unit shall take account of the need for backup and redundancy when working on cases, within any legal constraints, to ensure that a single technical failure (e.g. a power loss or disk corruption) will not result in irrecoverable loss of data (section 26).

97.3.3 Software, hardware and tools, where operation of these have an impact in obtaining results, will require validation within the method they are deployed, or any existing validation to be verified, as laid out in 97.4.7-97.4.9.

97.3.4 The forensic unit shall ensure that, for the range of the digital forensics methods it uses, the validation requirements take account of the competence that personnel hold or will require, the nature and difficulty of the tasks to be carried out, and the level of acceptability of the method in the wider forensic science and criminal justice community.

97.4 Validation of methods

Risk assessment of a method

97.4.1 The risk assessment process detailed in this Code (section 24.6) is intended to be used to determine the impact of the overall method used. It is important to look at how a method or tool is to be used. For instance, when imaging storage media, the risks may include:

a. altering data stored on the evidential item/exhibit;

b. returning incomplete and/or inaccurate data; or

c. incorrectly determining the media to be unreadable.

97.4.2 In certain parts of the method, the competent use of a suite of software tools or the use of visual/manual checks could be demonstrated to mitigate the identified risks in the method. Consideration of the nature of risks at this stage should feed into the development of a method as well as into the validation strategy.

97.4.3 The development of the method for the given FSA and the subsequent validation shall set out how the identified risks are being addressed and how the effectiveness of the method will be tested along with the end user requirements and specification.

97.4.4 A formal risk assessment method should be used. There are various risk assessment methods that may be chosen, one which may be suitable is ‘failure modes and effects analysis’. Failure modes and effects analysis is a step-by-step approach for analysing each stage of a method, looking for potential weakness that might result in a failure of some sort, with consideration of, if the failure were to occur, would it be detected without causing harm, e.g. an erroneous result being picked up by a quality control.

97.4.5 Controls included to manage risks are to be assessed during validation. Therefore, whichever risk assessment method is used, it is good practice to include cross referencing between the stage in the analytical method and the mitigation/control in the risk assessment table. This both assists in designing the validation study and in demonstrating the control of risk to the accreditation body.

Validation of measurement-based methods

97.4.6 This Code describes validation for measurement and interpretive methods. For the purposes of digital forensics, the section referring to measurement-based methods is applicable for most methods employed. This includes methods where direct measurements are not made, such as extraction processes using automated tools or manual methods for the purpose of providing data.

Verification of the validation of adopted methods

97.4.7 In most cases, adopted methods or software tools and scripts should follow a tailored process for the validation of measurement-based methods. However, an adopted method would usually be expected to be already well supported through documentation, available validation studies, testing-house studies or published papers. Confirmation of the applicability of the validation against the required end user requirement and specification is required, as is a documented demonstration that a method works within acceptable performance parameters (section 24.9.11).

97.4.8 There is a requirement in this Code (section 24.14) for the production of an available library of documents relevant to the authorisation of a method and the production of a statement of validation completion.

97.4.9 The final requirement in this Code is to demonstrate that a method works in the hands of the intended personnel.

Verification of minor changes in methods

97.4.10 Methods are validated to a specific configuration; any changes in any of the constituent parts (hardware, firmware, script, operating system etc.) may affect its overall operation and any dependent systems, and could invalidate the validation.

97.4.11 Any proposed change shall be risk assessed at the method level as even a patch in a software tool may adversely affect the operation of a second tool or process using its output, e.g. giving a plausible but incorrect date stamp. Other examples include a tool inadvertently becoming write-enabled through a firmware update.

Implementation plan and any constraints

97.4.12 The implementation plan is required to include monitoring of controls and communication that, in the digital forensic sciences, shall include configuration management, dependencies, how identified software/firmware/hardware bugs are to be handled and how patches, etc. are to be controlled.

Configured off-the-shelf tools deployed as kiosks

97.4.13 This refers to the use of a locked down, centrally configured off-the-shelf tool for the capture and preservation of digital data by frontline personnel, which is traditionally referred to as a kiosk. Although, such personnel might not usually be considered as practitioners, anyone conducting an FSA, or part of an FSA, is referred to as a practitioner in this Code.

97.4.14 All deployments of this type of tool may be included in the forensic unit's schedule of accreditation; however, this Code permits further deployments to be made which are not covered by their schedule of accreditation provided the following criteria are fulfilled:

a. The SAI notifies the Regulator that they intend using this dispensation, are overseeing its implementation and operation, and records/audits are available for review.

b. The forensic unit holds accreditation for the method using a specified configured tool for the deployment type (i.e. mobile or static) and any subsequent deployments are duplicates.

c. There is adequate control of configuration (e.g. locked down data recovery methods and control) to centrally support managing the risks of error.

d. Practitioners have been deemed and maintain competence and authorised to use the method by the SAI, or personnel acting on their behalf.

e. There is a documented method or standard operating procedure made available to practitioners undertaking the work which is subject to document control.

f. The tool has been validated in line with the requirements of the Code and users are aware of limitations and false negatives.

g. Each deployment is included on the forensic unit's internal audit programme (section 20.5).

h. Each deployment is subject to the control of the non-conforming work procedure (section 8.1).

i. Standard procedures for recording and secure retention of technical records and data produced from the method are in place to ensure traceability and management of data.

j. Reports intended for use in evidence shall clearly declare the status of the work against the Code:

   i. deployments covered under the accreditation scope should use the standard statement of compliance (i.e. section 31.3);

   ii. further deployments conducted in line with the Code, but unaccredited, shall be reported with the following declaration:

> 'I confirm that, to the best of my knowledge and belief, I have acted in accordance with the requirements in the Code of Practice [insert version] published by the Forensic Science Regulator for using a configured tool which is not included on the accreditation schedule.'

97.4.15 The further deployments are not accredited, and this should be declared. However, these further deployments are compliant with the requirements set out in the Code if the above implementation requirements are achieved.

97.5 Handling of items/exhibits

Item/exhibit handling, protection and storage

97.5.1 The forensic unit shall consider whether the value of any other type of evidence (e.g. friction ridge detail) that may be present could be compromised during the

capture, preservation and investigation of the digital evidence when conducting the FSA (i.e. post submission to the forensic unit).

97.5.2 The forensic unit shall create a documented case acceptance policy with a risk-based rejection procedure which covers how irregularities in packaging, seals and transportation are handled (section 29.3).

97.5.3 There are three main issues to consider in the transporting of digital evidence.

a. The security of the device and digital evidence to ensure that access to it is correctly supervised when transferring it from the incident scene to the forensic unit's facility or other location.

b. The protection of the device and digital evidence to ensure that it is not affected by physical shock, electromagnetic interference, extremes of heat and humidity or other environmental hazards.

c. Remote electronic features which may allow remote wiping, locating of the device for retrieval by associates and/or identification of discrete or covert locations.

98. Video processing and analysis

98.1 Scope

98.1.1 This FSA specific requirements section covers all forensic units conducting the following FSAs:

a. FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72).

b. FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73).

98.1.2 As this section covers two FSAs, forensic units should refer to both FSA definitions for the scope and specific compliance requirements.

98.1.3 Any personnel conducting any FSA, even if this is not their primary role, are considered practitioners for the purposes of this Code. This includes but is not limited to technical personnel, police personnel or police officers. These requirements are not limited to activity in a video or imaging unit.

98.1.4 This Code recognises that practitioners working in a frontline capacity may be trained to recover footage from CCTV systems in situ using the manufacturer's intended method of recovery from CCTV systems rather than via specialist tools. Provisions for frontline practitioners for limited processing are detailed in FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72). This dispensation of processing is not aimed at practitioners in a video or imaging unit under routine circumstances (exigent circumstances may apply and appropriate declarations made); it is intended for investigating officers to be able to exhibit material viewed without requiring recourse back to video specialists unless further analysis is required.

98.2 Personnel

Competence

98.2.1 All personnel directly involved in undertaking an FSA are known as practitioners. All practitioners shall be competent in those activities they perform, and records of that competence shall be held. Where the forensic unit holds accreditation and/or is required to hold accreditation, (rather than adherence to requirements of the NPCC Framework for FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS)) the competence framework shall be suitable for that purpose and comply with this Code.

98.2.2 All the FSAs in this Code contain sub-activities which have different requirements in terms of knowledge, training and experience to be considered competent.

98.2.3 The SAI is responsible for the procedure for approving methods, though this may be delegated; the procedure should be developed with input from practitioners competent to perform FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73).

98.2.4 FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72) is primarily aimed at permitting specified activity by frontline personnel, therefore the competency levels detailed in the NPCC*'s* Framework for Video Based

Evidence [98] may be used for determining the competence requirements for this FSA.

98.2.5 Any personnel performing an FSA are practitioners, and they shall have a clear understanding of the overall video forensic workflow they are permitted to conduct and be mindful of the objectives of all operations they perform.

98.2.6 Procedures issued for use under FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72) should have been formulated to achieve a desired task without unnecessary transformations.

98.2.7 Practitioners conducting FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73) shall be competent in the formulation of a process workflow to correctly achieve a desired task without unnecessary transformations and be able to assess and explain the impact of video transformations at all stages of the process.

98.2.8 Storage media from DVRs will often present unknown, proprietary file systems. These are not recognised or interpreted by common digital forensic hard disk drive interrogation tools. Thus, to avoid misinterpreting a storage medium as containing no CCTV, a practitioner working to FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73) should be competent at recognising the byte-level indicators of the likely presence of video or audio on such storage media if data recovery is part of their role.

98.2.9 Recognition, rather than an identification through comparison, is not subject to this Code; this is covered by the application of the PACE Code D [100].

98.2.10 All practitioners shall understand the distinction between giving interpretation/opinion evidence and evidence of fact [11]. Activity where interpretation/opinion are intrinsic to reporting the findings of the sub activity include, but are not limited to (section 73.3.1b):

a. Pictorial image comparison.

b. Height/distance estimation (e.g. photogrammetry).

c. Estimation of speed from CCTV footage.

d. Analysis to establish authenticity of video (e.g. deep fakes).

98.2.11 Any practitioner proposing to give opinion evidence shall be an expert in all relevant aspects they intend to give an opinion on. Expertise in CCTV, video, imaging, enhancement etc. does not equate to expertise on the content of the image. Practitioners may highlight features of note such as logos or damage features; however, unless they are also an expert in the content of the images, practitioners should not attempt to give opinion evidence on the meaning of a comparison between the objects in question. [118] For example, identifying the make/model/type of weapon seen in an image would require specialist expertise in firearms, but highlighting the unique scratches/wear/stickers affixed would normally not require domain specific expertise.

98.2.12 Image analysis requires specific subject matter expertise of both the system and the subject to be analysed.

98.3 Review of requests, tenders and/or contracts

98.3.1 There shall be a procedure for case acceptance (see also section 16 and 29.3.2), that includes consideration of the following.

a. suitability of footage;

b. availability of validated methods;

c. practitioner competence;

d. available competent personal to review and undertake critical finding checks.

98.3.2 The procedure should include a process to follow where the forensic unit cannot perform the commissioned work and/or rejects the commission. This may include when to engage externally provided services or when to advise the commissioning party to do so in their own right. It may also be appropriate to provide advice to the commissioning party on alternative investigative approaches, particularly where the footage is not suitable for analysis.

98.4 Developing an examination strategy

Speed estimation

98.4.1 Where a forensic unit is requested to undertake estimation of speed from video, whether as part of a collision investigation or as an isolated activity, acceptance of the work shall:

a. identify the points to be tested in the case;

b. develop an appropriate examination strategy;

c. determine the sequence of examination and need for site visits;

d. identify resourcing requirements for critical finding check, primary and peer review (section 20); and

e. determine if the forensic unit has the required competence and/or validated methods to deliver the examination strategy or if the FSA should be delivered from outside the forensic unit (section 17).

98.4.2 Where a forensic unit undertakes speed estimation from video, they should have a procedure within the development of any examination strategy that enables method selection based on the circumstances and capability of the forensic unit (e.g. accreditation status, validated methods, practitioner competence).

98.4.3 The procedure should include the following.

a. An evaluation of the submitted material to establish:

   i. Suitability for analysis

   ii. Requirement for site visits

   iii. Quality of the footage (e.g. resolution)

   iv. If the derivation of date/time/frame rate can be achieved (e.g. is there metadata present, was the date or system verified at point of collection/ingestion)

b. Influence of:

   i. video frame timing

   ii. positioning of vehicle, person or object

iii. camera rolling shutter

iv. video compression

c. Correcting for distortion

d. Consideration of parallax error

e. Derivation of date/time/frame rate

f. Determine if the submitted material is suitable for analysis by a method available to the forensic unit or requires rejection (section 98.4.3).

98.5 Checking and review

General

98.5.1 The checking and review requirement detailed in section 20 of this Code applies to all forensic activities in FSA DIG-300 and FSA DIG-301 which are subject to accreditation (rather than adherence to the NPCC Framework), and all forensic activities detailed in FSA DIG 301. Note that Code section 20.1.2 requires effective checks of those calculations and/or critical data transfers. This includes applies to, but is not limited to, photo/videogrammetry and derivation of date/time/frame rate, as the activity of speed estimation from video footage typically draws from both activities.

98.5.2 Where the Code applies, section 20.2.4 requires records on critical findings checks to indicate:

a. that each critical finding has been checked;

b. whether the finding was agreed or not;

c. the name of the checker; and

d. when the checks were performed.

98.5.3 Those individuals conducting the critical finding checks shall be competent in the method being checked, but may be external to the forensic unit carrying out the work (section 20.2.3). The records on checks in case notes should be contemporaneous, a formal and recorded difference resolution process is required (section 20.4).

98.5.4 A critical finding is an output from a test, analysis of an item/exhibit, or examination of a scene that:

a. has a significant impact on the opinion provided; and.

b. cannot be repeated to confirm the finding; and/or

c. a different opinion could be provided by a suitably qualified practitioner in the FSA under consideration.

Speed estimation

Examination strategy check

98.5.5 Speed estimation from video footage as included in FSA - DIG 301 - Specialist video multimedia, recovery, processing, and analysis includes but is not limited to photogrammetry, determination of frame rates, and use of frame interval timers. It does not include the use of Home Office approved speed detection devices or other methods which do not make use of the video footage to determine time or distance measurements.

98.5.6 Where the method is selected solely on the basis of a structured procedure without the need for practitioner experience, the examination strategy check may proceed as an open check, i.e. it can be carried out with knowledge of the original selection.

98.5.7 The purpose of the check is to assess whether the requirements of the instructing party are met, including the following.

a. The investigative points to test.

b. Applicability of the method to address the points to test.

c. Limitations of the method considered, including the estimation of uncertainty, against the points to test and set out in reports.

Technical check

98.5.8 The technical check in primary review is carried out to assess whether the requirements set out have been met, and the forensic unit's policies and processes have been followed. Where it is an open review, it may be combined with other checks, provided all the required checks are completed and recorded clearly against the forensic unit's requirements.

98.5.9 The procedure shall include checking the stages defined in section 98.4.3, including but not limited to checking that:

a. the method defined in the procedure to check integrity of the data was completed;

b. the derivation of timing including the application of any frame interval timing analysis performed and applied correctly; and

c. all calculations and data transfers are correct.

Critical finding check

98.5.10 Checks shall be performed regarding the following:

a. the integrity of the evidence used as part of the analysis;

b. the authenticity of the video evidence;

c. the timing analysis;

d. the application of any established frame interval timing to the subject of the analysis;

e. the distance estimation;

f. the speed estimation;

g. all associated uncertainties.

98.5.11 Checks shall be performed blind, i.e. without knowledge of the original result, when:

a. the critical finding check is the only substantive quality control procedure for checking that finding; and/or

b. the finding or opinion to be checked is based on the experience of the practitioner rather than direct objective data.

98.5.12 Open checks should include:

a. the timing analysis; including:

i. if a sufficient duration of frame interval timer footage was analysed; and

ii. there was a comparison of metadata to frame interval timing analysis.

98.5.13 Blind checks should include:

a. the application of any frame interval timing analysis to the to the subject of the analysis, including:

   i. if there was a correct metadata comparison between analysed footage and that of the subject; and

   ii. confirmatory object movement analysis;

b. the distance estimation within the footage; including

   i. if the method minimises uncertainty; and

   ii. the practitioner is competent in chosen method;

c. the speed estimation.

98.5.14 Findings which have a blind check involve a second expert providing an independent technical opinion in isolation of the original opinion to be checked; this may be for those aspects of opinion identified by the expert generating the original report during the technical check or by another rules-based aspect of the procedure.

98.6 Selection of methods

General

98.6.1 Forensic units conducting FSAs shall have methods or procedures which are fit for purpose issued by, or on behalf of, the SAI. Where further analysis is expected or accreditation is required (i.e. part of FSA – DIG 301), the method shall be validated in line with this Code.

98.6.2 Procedures for FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72) should be developed and/or overseen by practitioners competent to perform FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73) and aligned to the following:

a. NPCC – Framework for Video Based Evidence [98];

b. Dstl – Recovery and Acquisition of Video Evidence [99];

c. Dstl – Digital Imaging and Multimedia Procedure [119]; and/or

d. this section (i.e. 98) on FSA specific requirements.

98.6.3 The following methods in the remainder of section 98.6 are for conducting FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73) unless otherwise indicated.

Video transformations

98.6.4 Where a forensic unit undertakes the transformation of video material, the transformations shall be appropriate for the intended use of the transformed material and shall be documented. Video is subject to a series of transformations from its initial creation through to rendering on a display surface for human interpretation; these transformations should be as non-destructive as is practicable.

98.6.5 Forensic units should aim to work from original media or a bit-for-bit copy of the original data (i.e. from the master copy) when conducting FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73).

98.6.6 Workflows using DEMS/DAMS are prone to automatically process and transform video material in ways invisible at point of use. There should be procedures to ensure that DEMS/DAMS are only used in a manner that has been approved by, or on behalf of, the SAI. Where a forensic unit is instructed to conduct FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73), even if receiving media through a DEMS/DAMS, they should aim to use the bit-for-bit copy of the original data. For some examination types (e.g. authenticity analysis), the forensic unit may need to request submission of the pre-DEMS/DAMS original (if available) from which to work.

98.6.7 Often video material received by a forensic unit from a third-party will already have undergone transformations such as spatial and temporal sampling, digitisation, transcoding and compression. The effect of those transformations shall be taken into account in all subsequent processing, interpretation and reporting.

Legacy video

98.6.8 Where analogue video is to be digitised, the conversion should take place as soon as possible in the process once it has been identified that the footage may be of interest.

98.6.9 As with all transformations, where digitisation is performed it needs to be done so as to minimise any loss of information that may be relevant to the investigation. Equally, any decision not to digitise shall take into account the risks of degradation to the medium and the rationale shall be documented.

98.6.10 Appropriate hardware is required to extract the maximum amount of information in terms of image quality, audio tracks and associated metadata. Any departures from this shall be justified and documented.

98.6.11 Legacy video conversion as part of data maintenance, such as for cases retained under CPIA long after the footage has been used in cases is a necessary task. This could be analogue video, but increasingly includes other legacy formats. The bulk conversion of media from legacy formats as part of maintenance of data storage to current approved secure storage formats is likely to be an infrequently used method not on the scope of accreditation. Bulk processing has different risks than processing a single case, even if it uses various well used methods. Therefore, the activity shall be a planned activity and include the following:

a. A documented procedure approved by the SAI and a subject matter specialist.

b. A risk assessment that considers the risks associated with both carrying out and not carrying out the bulk conversion.

c. Use equipment and tools that have been tested to be fit for purpose by subject matter specialists on behalf of the SAI.

d. Production of contemporaneous records.

e. Include quality checks on the converted product as appropriate and identified in the risk assessment (e.g. dip sampling).

98.6.12 Staff who undertake both these conversions and quality checks shall be trained and competent in these activities.

Enhancement

98.6.13 The basic brightness and contrast adjustment to the entire image are permitted under FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72) under

specified constraints; enhancement is part of a workflow for FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73).

98.6.14 Forensic units shall be clear on the purpose of any image enhancement that is to be carried out and anticipate any data losses that may occur as a side effect. Practitioners performing any enhancement shall be competent to apply and explain the enhancements selected.

98.6.15 Where the material is of too poor quality to be enhanced with the methods available, practitioners may need to explain to the commissioning party the reasons to reject the task (section 29.3). If practitioners are required undertake an enhancement task when an image is of too poor quality, it should be clearly marked as being potentially unreliable as evidence.

98.6.16 Images enhanced for one purpose shall not be used for another purpose without fully reconsidering the appropriateness and the risks.

98.6.17 In forensic applications, enhancements should not generally be applied to selective portions of an image unless these regions and the enhancements within them are clearly identified. However, it is permissible to enhance the whole of a cropped image, again with the enhancement/transformations detailed in the documentation.

98.6.18 It is important that recipients of enhanced images (e.g. investigators, experts or jury members) are not misled. To this end, care shall be taken to ensure that enhanced images are identified as such and that sufficient information on the performed enhancement is available in the case notes. Where compilations are intended to be illustrative, the target audience may be informed of basic brightness and contrast adjustments in title frames.

Tracking in footage

98.6.19 The following methodologies shall be documented with risks identified and mitigated, whether using specialist standalone tools or, if the SAI has approved, when using a DEMS/DAMS system for this purpose:

a. Tracking (e.g. arrowing or circling) objects or people (either manually or automatically) through recorded footage.

b. Redaction (e.g. masking, blurring or pixelating) objects or people (either manually or automatically) through recorded footage.

98.6.20 Note that redaction also refers to the elimination of approved unneeded audio; when audio is redacted, practitioners should consider if lipreading may remain an issue.

Image comparison

98.6.21 Forensic units that undertake image comparison shall do the following:

a. Use valid methods. Validations should include an objective literature review so that the design of the validation study considers shortcomings previously identified. Methods that have been challenged in the scientific literature should not be used unless the validation is shown to overcome previous shortcomings, and the court must be made aware of the previous criticism even if they have been overcome. Previous acceptance in this jurisdiction does not provide evidence of validation. The methodology used for comparison activities should include the sequence used to review and comment on any the questioned imagery before the practitioner views or accesses the reference material.

b. Recognise that image comparison is a form of opinion evidence [120] and is admissible where the judge and jury require the assistance of evidence which depends on the application of a specialist skill or knowledge in the field that is under comparison (i.e. from experts).

c. Demonstrate the appropriate competence in relation to the image-based processes that have been undertaken.

d. Demonstrate competence in comparing the type of material being compared in an image.

e. To reduce the risk of confirmation bias, incident footage containing unknown persons or objects of interest shall be analysed to identify distinguishing features before known footage of the suspect objects of interest is viewed or information revealed to the analyst expected to form an opinion as to the activity or identity, or to perform any comparison. Such bias is a subconscious act and prior knowledge by the practitioner of certain information (e.g. the target number plate, injury, congenital disorders, damage features) may be seen as a source of such bias.

i. The forensic unit commissioned to do the work may be able to insulate the practitioner conducting the examination from non-task-relevant information by having a different practitioner being involved in the contract review and/or case conference. This should ensure that the practitioner receives only the information appropriate for each stage of the examination, while still ensuring that proper case assessment can be made and that the most appropriate methods are used.

ii. Experts in sole practice should consider how to advise prospective commissioning parties as to whether phased disclosure of the details of the case to them is appropriate, and how this will be managed.

f. Ensure that all task-relevant information in relation to image processing undertaken by a third party is communicated to the practitioner undertaking the comparison. Information on image processing is required to understand the processing of artefacts. Procedures should ensure the practitioner receives information appropriate for each stage of the examination/analysis, including identifying when information on image processing is required.

g. Demonstrate the decision process and basis for critical findings.

Reliability of proprietary CCTV players

98.6.22 Many CCTV players will distort the original recorded material by light, colour, shape and size. They may also not display all frames or playback recorded audio. They may also detail a timecode and frame rate that is calculated during playback and may not be frame accurate. When using a player, either in review or to achieve a task, reliability of the player should be considered and tested. They also commonly re-sample and transcode images when exporting still images. The nature of the transformations introduced by tools used for exporting video and stills from CCTV shall be assessed so that their impact on the subsequent use of the transformed material can be determined.

98.6.23 Digital CCTV systems often have an export function so that video footage can be backed up to removable media (e.g. a USB hard disk). Proprietary replay software that has been developed and distributed by the system's manufacturer may generally be initially treated as reliable, as forensic units do not have

access to the coding in order to verify its implementation. However, if conducting further examination/analysis other than viewing, the risk assessment the validation requires may indicate that the method requires a step to provide assurance that the software is working as expected on this workstation. Such a step may require the method to include using other replay software if there are any signs of replay issues (e.g. dropping frames, rescaling issues, wrong proportions) that may affect such examination/analysis. It should be noted that there may not be obvious signs when replay software is performing incorrectly, so where the footage is to be used for further analysis, rather than simply viewing the footage it is good practice to follow the dual approach, and to document any reason why this has not been possible or relevant in the case. It is also worth noting that the video files exported from the digital systems may contain additional information, e.g. audio and GPS data, which is not presented by the replay software. If this type of information is of relevance to the case, the practitioner should investigate further. It is expected that the practitioner will have been trained to identify issues with replay software in the competence section.

98.6.24 In many instances practitioners will have no option but to utilise proprietary replay software but will not have the practical means of comprehensively validating it. Consideration shall be given to the associated risks and how these may be mitigated in a proportionate manner. For example, the risk mitigation approach may take into account:

a. the context, including what the tool is required to do and how the data will be used;

b. the competence of the practitioner; and

c. how well-established the body of knowledge for the replay tool is, e.g. within the forensic literature.

98.6.25 The version of software used shall always be included as part of the record. In the absence of this information being available, preservation of one or more screenshot images may provide a basis for identification of the version used.

98.7 Validation of methods

Data recovery

98.7.1 The procedure for recovery of CCTV footage from a digital CCTV system in situ using the system manufacturer's intended method, as detailed in FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72) may be considered fit for purpose without a validation study.

98.7.2 The NPCC's Framework for Video Based Evidence [98], and associated procedures, detail the steps and training to ensure methods used are appropriate for use in FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72) without a validation study. All personnel performing an FSA are practitioners. Procedures produced for practitioners performing FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72) should contain steps to direct the practitioner as to when the procedure is applicable and also when to cease/not-start a recovery and seek specialist assistance.

98.7.3 When video data are not readily accessible by standard/manufacturers' methods (e.g. due to technical difficulties), recovery in a process akin to reverse engineering or by using third-party tools may be required. When undertaking this casework, the method shall be subject to validation in line with the Code, noting in the risk assessment especially the following:

a. Not all video material will necessarily be recovered.

b. Data might be incorrectly interpreted (e.g. time and date stamps).

Image comparison

98.7.4 The forensic unit shall demonstrate that the methods used for comparison are appropriate, through validation, for the image characteristics of the case material. For example, methods developed for high-quality recordings may not be valid for low-quality CCTV images.

98.7.5 Where the comparison uses proportional relationships and/or metrics, the validation shall include an appropriate, robust and repeatable method for quantifying the associated uncertainties (section 98.8.4 Photo/videogrammetry).

98.7.6 Forensic units shall review the scientific literature to identify the following:

a. scientific basis for the method;

b. studies critical of the method;

c. examples of testing methodologies;

d. end user requirements to be included in the validation, including avoiding any biasing effect of the observer (including juror);

e. reproducibility of the finding(s);

f. reproducibility of any verbal confidence scale;

g. false inclusion/exclusion rates.

98.7.7 Image comparison methods which are cited in the scientific literature as unreliable or biased should not be used unless comparable research and validation indicates the issues identified are now controlled. Irrespective of the findings of any such study, the fact that the method was criticised remains disclosable and should be addressed in the statement/report, with the remedial actions that address the issues.

Speed estimation

98.7.8 The forensic unit shall demonstrate that the methods used for the estimation of speed from video footage are appropriate. The way this is performed is through method validation (section 24).

98.7.9 Calculations performed in software and/or critical data transfers should be included in the validation, unless they are subject to specific manual checks.

98.7.10 The validation shall include the method for quantifying the associated uncertainties to ensure it is appropriate, robust and repeatable (sections 24 and 98.8.11).

98.7.11 Where the forensic unit is verifying validation data produced for an adopted method, this shall be reviewed to ensure fitness for purpose and a verification can be undertaken to demonstrate suitability when deployed within forensic units' own system therefore verification requires testing, which may include:

a. Tests specifically against the fulfilment of the specification requirements; and/or.

b. A ‘black box’ approach (i.e. a whole method tested against ground truth) mapped across to demonstrate the fulfilment of specification requirements, for example the impact of the quality of footage (e.g. resolution, distortion, image sharpness) on photogrammetry.

98.8 Estimation of uncertainty

98.8.1 The Code requires that a forensic unit performing testing evaluates measurement uncertainty, even where the test method precludes rigorous evaluation of measurement, such as a test that is qualitative in nature.

98.8.2 The impact uncertainty may have on the finding shall be included in reports, where it is relevant to the CJS, whether giving fact or opinion.

98.8.3 Though only three example methods are included here, all analytical methods subject to compliance with the Code are in scope for this requirement.

Photo/videogrammetry

98.8.4 When estimating dimensional information from imagery, it is essential that there is an appropriate, robust and repeatable method for quantifying the uncertainties associated with any quoted value.

98.8.5 Issues that contribute to uncertainties include, but are not limited to:

a. Resolution accuracy;

b. Image alignment, where required;

c. Accuracy of distance measuring device or data;

d. Camera or subject positioning.

98.8.6 Empirical research indicates photo anthropometry/proportional alignment should not be used in facial comparison involving images from an uncooperative/uncontrolled setting (i.e. CCTV) until methods advance and further research indicates the issues identified are controlled.

Derivation of date/time/frame rate

98.8.7 In cases where the precisions and/or accuracy of timing information from a video recording is crucial (e.g. speed estimations of vehicles from CCTV), a suitable method for quantifying the uncertainty in such a measurement, as well as other factors such as measuring the frame rate, shall be employed. This

method will take account of the whole recording process (image capture, image encoding, metadata assignment, data storage).

98.8.8 The date/time information provided by the multitude of CCTV systems in use is of highly variable quality. The following shall be taken into account where the date/time information may be important:

a. The displayed timestamp may not represent the actual capture time.

b. Both the precision and the accuracy of any displayed time, as apparent precision may not be an indicator of accuracy.

c. There may be more than one displayed clock.

d. The image capture rate may not be fixed so a calculated average frame rate cannot always be applied to a single specific frame interval.

e. The frame rate setting information contained within the system menu will not always be a true reflection of the actual recorded rate.

f. All computer-based systems are prone to hesitation under load, which can introduce unpredictable interruptions in record sequences.

g. What is displayed might not correspond to what is stored. For example, a CCTV system may display an on-screen clock to the second, whereas the data stored on the system may actually be stamped to the millisecond.

h. Timestamps might be a network timestamp relating to the point when information is received by centralised network storage, and not at the earlier point of digitization in the camera.

98.8.9 Methods such as extended section analysis, analysis of camera sequence order, interrogation of the system menu and independent timing of the system performance may be considered to provide a holistic view of the accuracy of the derived times/rates. Test recordings cannot confirm the precision or accuracy of the recording at the time of an incident, but they can be used to provide an estimate of uncertainties provided the assumption is stated that the recording device was operating in the same manner as at the time of recording.

98.8.10 If the method includes analysis of footage containing variable rates, the validation and estimate of measurement uncertainty shall include this use.

Speed estimation

98.8.11 Speed estimation includes multiple sources of measurement uncertainty to be considered, including but not limited to the following:

a. Limitations of the optical system.

b. Positioning of vehicle, person and object.

c. Camera positioning.

d. Quality of footage (e.g. Resolution, distortion, image sharpness).

e. Video frame timing.

f. Video encoding stress factors.

g. File structure/metadata.

h. Placement of any measuring device (including pixel selection).

i. Accuracy of any measuring device.

j. Camera rolling shutter.

k. Video compression.

l. Other instability including camera movement.

98.8.12 See also section 98.8.4 Photo/videogrammetry and 98.8.7 Derivation of date/time/frame rate.

98.8.13 The uncertainty shall be given when reporting results, and it shall be in a manner which makes it clear that although presented with the calculated speed estimation figure as a calculated figure with a tolerance, it is still an estimate based upon the practitioner's assessment of the identified sources of uncertainty and not a factual finding.

98.8.14 The report should also detail how the uncertainty was estimated, and/or factors considered.

98.9 Control of data

Recovery of data

98.9.1 The overarching requirement of the control of data is to be able to show that the recovered footage is true to the original video recording and remains so from

the point of recovery; in practice, this means a bit-for-bit copy of the original with a method to show it has not been tampered with (see [121]). Video footage should be extracted in its native format in order to maintain image quality and be stored as a master copy to be available for any future forensic examination/analysis, e.g. defence experts (see Dstl's Recovery and acquisition of video evidence [99]).

98.9.2 Some systems may provide an option to write the sequence to standard playable format, such as .VOB or .AVI, which may seem to be an advantage in that the video will be playable using standard software; however, the generation of the playable formats often requires the video to be recompressed, resulting in a loss of quality, and so this method should be avoided at the initial recovery stage.

Inadvertent overwriting by digital/network video recorders

98.9.3 When processing a DVR/NVR device, due to their proprietary nature and often limited functionality, it is necessary to consider and prevent mechanisms that could either:

a. result in the loss of data, e.g. due to recording behaviour when powering up (overwriting earliest recordings); or

b. render data inaccessible by the DVR/NVR, e.g.:

   i. due to settings such as 'timed expiry' (refer to section 103 Glossary) which renders data inaccessible after a set period of time has elapsed since the time of recording;

   ii. through disturbing the connection between the hard drive and the main board, e.g. via disconnection of the hard disk drive or the insertion of clones or in-line write blocking devices – all of which could render footage on the original or clone disk inaccessible for both replay or download (permanently for some DVRs if disk disassociation occurs).

98.9.4 Due to the risks above, data recovery from the DVR once it is no longer in situ (no longer in the original working system) is a specialist activity and is covered by FSA – DIG 301 – Specialist video multimedia, recovery, processing and analysis (section 73).

Creation of a master and working copies

98.9.5 A master exhibit/item of the source/original data shall be preserved; the forensic unit should define in the method what constitutes a master.

98.9.6 Write-once read many media, with information on continuity and with sufficient protections against tampering, are typically used as master discs. However, if the intention is to use a USB stick or CD/DVD only as a transport medium and to store the master evidence on a secure server then the methodology would require validated steps to demonstrate that the master data remains as recovered. This may include matched hash values at the point of transfer from the transport medium to the server deemed suitable for storage of master evidence (see [119] for further guidance on storage of master evidence).

98.9.7 Working copies of the video footage may be produced and these will typically be:

a. a bit-for-bit copy of the master in its native format, suitable for further examination/analysis by specialists instructed by either the prosecution or the defence; or

b. a bit-for-bit copy of the master in its native format, supplied with a player suitable for investigating officers to view the footage; or

c. a 'playable' format suitable for investigating officers to view the footage and potentially for supplying to the CPS, marking this as 'Converted format' and therefore no longer a true copy of the original.

98.9.8 Any media produced whereby original data has been converted to a different format should be clearly marked as 'Converted format', or identifiable as such in some other way defined in the procedure. The forensic unit producing working copies of the video footage should keep a record and implement controls for that footage if appropriate and technically practicable.

Conversion from proprietary to generic video format

98.9.9 Video material from CCTV sources often does not conform to the constraints of broadcast video. Transforming video from CCTV sources often requires spatial and temporal re-sampling, which leads to a loss of information that may be important in subsequent processing and interpretation. Therefore, any media produced whereby original data has been converted to a different format should

be conspicuously marked or uniquely identifiable as such in some other way defined in the method (section 98.9.8).

Export of video and stills from CCTV players

98.9.10 Many CCTV players perform a conversion to a broadcast video format either implicitly during playback or explicitly during video export; export should be in native format where it is an available option and this native format is what should be used to create the master copy.

Analytics and tools

98.9.11 The declared performance, in terms of probability detection (PD) and false alarm rates (FAR), of video content analysis tools is dependent on the quality of the video to be analysed. When using video analytic tools for post-event analysis, the forensic unit shall be aware of the impact of video quality on performance. Video analysis tools shall be validated as part of the method they are deployed in; the risk analysis of the actual PD and FAR on the required task shall be undertaken as part of that validation and communicated to the commissioning party.

98.9.12 Video content analytics tools can include any or all of the following:

a. Motion detection.

b. Object or person detection.

c. Tracking/reidentification.

d. Auto redaction.

e. Crowd dynamics.

f. Behaviour analytics.

Integrity and authenticity

Video material is often received from uncontrolled sources; therefore this can raise questions regarding its integrity and authenticity.

98.9.13 Integrity verification is the process of confirming that the data (image, CCTV clip, etc.) presented is complete and unaltered since time of acquisition, whereas authentication is the process of substantiating that the data portrays an accurate representation of events [119].

98.9.14 Both integrity and basic authenticity may routinely be part of many forensic science workflows. Integrity checks may be hash value based, basic authenticity checks may involve verifying the timing offset.

98.9.15 Forensic units may be commissioned to carry out authenticity analysis to examine the provenance of the video material, where this is doing more than time and location against the EXIF information, it is likely to be a specialist activity.

98.9.16 This authenticity analysis can be carried out either with the use of specialist software tools and a practitioner or as a purely human examination process. However, the use of authenticity and integrity tools incorporated into DEMS/DAMS and their output should only be used as an aid to an investigation for intelligence purposes. Statements on integrity or authenticity would be expected to be expert opinion.

98.9.17 For integrity and authenticity examinations a forensic unit may be commissioned to look for evidence of:

a. image content manipulation;

b. deep fakes;

c. recordings purporting to be from a different date and time;

d. association to a particular recording device (authenticity only);

e. editing to remove pertinent content; and

f. editing to add pertinent content.

98.9.18 Software may be deployed by the forensic unit to automatically scan multimedia content at the point of submission or ingestion into a forensic unit's system. These tools shall only be used to give an indication that an asset may require further specialist integrity and/or authenticity analysis.

98.10 Statements, reports and the presentation of evidence

General

98.10.1 Guidance setting out the legal requirements for non-expert technical statements [106] and expert reports [67] has been issued by the Regulator. Compliance or

non-compliance with the requirements set out in the FSA definitions shall be declared in statements/reports from all practitioners.

98.10.2 Where the FSA requires accreditation, Part B of the Code applies, therefore the practitioners should use the standard declarations detailed in section 31.3.2 or 31.3.4.

98.10.3 However, where the forensic unit is reporting on findings from performing FSA – DIG 300 – Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS) (section 72) and compliance is with the NPCC's Framework for Video Based Evidence rather than accreditation, the practitioner should make the following declaration:

a. I confirm that, to the best of my knowledge and belief, I have acted in accordance with the NPCC Framework for Video Based Evidence [insert version] as required by the statutory Forensic Science Regulator.' or

b. 'I have not complied with the NPCC Framework for Video Based Evidence [insert version]. The details of this non-compliance are included to the best of my knowledge and belief in Annex [x], with details of the steps taken to mitigate the risks associated with non-compliance.

Statements and reports

98.10.4 Practitioners shall understand the distinction between expert evidence and evidence of fact, and be aware of the relevant legal requirements in preparing reports.

Displaying images

98.10.5 In cases where the detail of an image or the colour of an item is important, (e.g. in court), the optimised set up of viewing screens, prints and other presentation media should be recommended to the commissioning party to be considered in conjunction with the use of high-quality originals (see also section on Wi-Fi enabled courts below).

98.10.6 Care shall be taken to ensure that recipients of enhanced images (e.g. investigators, experts or jury members) are given sufficient information as to the enhanced nature of the image so as not to be misled.

Wi-Fi enabled courts

98.10.7 Court Wi-Fi systems intended for displaying material such as static images and documents may be considered adequate for the majority of cases. However, caution should be exercised when using wireless presentation systems for displaying video material, particularly in cases where there is lots of movement or high-resolution footage. In such cases, there is a risk of lost frames, jitter or loss of resolution. If replay through wireless systems is identified as inadequate, provision of appropriate playback equipment in court should be sought; if these arrangements are not already in place the forensic unit should inform the commissioning party. Where the commissioning party is the officer in the case, the CPS Complex Casework Unit may need to be engaged and/or CPS caseworkers may outline requirements via EPPE.Enquiries@cps.gov.uk – a minimum of two weeks' notice is advisable.

98.10.8 The forensic unit should ensure that any material produced that would not be suitable for display via a wireless presentation system is conspicuously marked as such.

Interpretation

98.10.9 All imagery viewing requires a degree of interpretation. If considered as expert opinion, then all reasoning and justification behind the interpretation shall be explicitly noted in reports. When identification is performed through controlled or uncontrolled viewing under PACE Code D [100] for factual reporting, the safeguards and records detailed in PACE Code D are required rather than this Code (section 73.5.1b).

Multiple evidential approaches

98.10.10 Where the expert is reporting on several forms of analysis (e.g. height analysis and the comparison of physical features), the report shall make clear the opinions and conclusions reached by the expert in relation to each of these individually and be clear which aspects which are subject to the Code, were performed in compliance with the Code. The expert may then provide an overall opinion and conclusion.

99. Cell site analysis for geolocation

99.1 Scope

99.1.1 Cell site analysis relies on:

a. communications data (i.e. CDR);

b. processing of those data, sometimes in association with data captured during an RF propagation survey; and

c. presentation of those data in the form of maps and tables with an expert report.

99.1.2 This FSA specific requirement covers the forensic unit's work as applicable to the scope of performing the following (FSA – DIG 200 – Cell site analysis (section 71)):

a. Identifying data required to progress the analysis.

b. Normalising CDRs in order to present call data in the form of maps/tables and produce a report required for court or as an expert summary.

c. Conducting an RF propagation survey to capture all the cell sites that serve, Wi-Fi, if applicable.

d. Cell site analysis using CDRs and an RF propagation survey information and the presentation of an expert report.

99.2 Independence, impartiality and integrity

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

99.2.2 This Code includes various impartiality requirements to be included in policies and procedures, not only to prevent internal and external influence on the results of their examination/analysis, but also to 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. Where accreditation is required, standards of conduct in part B also apply.

99.2.3 All examinations/analysis shall be conducted in an unbiased manner. For example, consideration of both the prosecution and defence proposition, if available, or attempting to determine the defence proposition.

99.2.4 All forensic units are required to demonstrate that they meet these requirements, which shall include the following:

a. The forensic unit's policies and procedures are compliant with this Code and practitioners adhere to them.

b. Consideration of one or more alternative proposition(s). In the absence of a stated or obvious defence position (e.g. home address), a null proposition (e.g. whether there is data in conflict with the prosecution proposition) may be adopted.

c. Terminology used in reports shall be clearly defined and imply no bias.

   i. Phrases in reports such as 'in the vicinity of' may only be used if qualified (i.e. given a specific and consistent indicative value).

   ii. Phrases such a 'consistent with' should not be used in reports unless all other scenarios the findings would be consistent with are given.

d. Cell site analysis may be used to propose investigative avenues (i.e. to help form a proposition). If a proposition has been produced through a different process, cell site evidence should only be used to test whether the call data is expected given the proposition; it should never be used to test whether the proposition supports the allegations or scenarios being put forward in the case independently of the evidence. Care should be taken not to transpose the conditional aspects of any assertion.

e. Use of an independent review of casework including, where appropriate, that this is done independently without prior knowledge of the original outcome.

f. Documentation and review of individual specific case assessments and strategies.

99.3 Review of requests, tenders and/or contracts

99.3.1 As part of this review the forensic unit shall ensure that the commissioning party is made aware of any limitations, false negative rates or caveats that are already known to apply to the method offered by the forensic unit.

99.3.2 For example, analysis of CDRs may demonstrate that the phone was within the area covered/served by a specific cell at the time of the beginning and/or end of the call. The commissioning party shall be made aware that, although locations of interest may be surveyed, pinpointing the phone to a specific location is almost always impossible (there may be rare exceptions with an indoor cell or femtocell, see 99.11.5). Additionally, a location of interest and an alternative location may be so geographically close that the radio survey data obtained at them is the same or substantially similar. In that case the commissioning party shall be informed that there is no reasonable way of inferring at which location the call event was more likely to have occurred.

99.4 Setting an examination strategy for cell site analysis

99.4.1 This strategy should focus on ensuring a request is appropriate, material supports the request and there are clear propositions to be addressed, and that an outline plan/strategy exists of how the practitioner plans to evaluate the proposition. It could include an independent review of the proposed survey strategy or justification for not surveying.

99.4.2 There shall be a procedure defining the setting of examination strategy. The procedure shall include the following:

a. Dealing with task-relevant case circumstances (i.e. information that is required for the task and not likely to result in confirmation bias).

b. Data available (CDR, cell information, etc.).

c. Limitations of the data. For example, where conclusions are solely or largely based on interpretation of General Packet Radio Service (GPRS) billing data, or in situations in which the prosecution and defence scenarios are so similar that cell site techniques will be of little use in attempting to discriminate between them.

d. Suspect’s personal situation (for example, place of work, home address).

e. Known or suspected attribution of phones.

f. Survey requirements for:

i. location survey (including potential requirements for elevation, e.g. high floors in tower blocks);

ii. area survey, to distinguish whether the service between two or more locations can be differentiated; and

iii. cell mapping, to make measurements in the service area of a given cell where relevant to the case.

99.4.3 If the circumstances of the case change or results/information indicate the strategy needs to be amended, the strategy will need updating and independently reviewed/checked.

99.4.4 Plotting of locations of interest (scene, mast locations and other specified addresses) may be conducted to provide an overview of the mobile telecommunications aspects of the case. These maps may be used to inform a more detailed surveying strategy or serve as the output in their own right (i.e. a theory-based 'desk exercise'), including identifying the following:

a. potential survey locations;

b. relevant network(s) to the survey; and

c. any variations from the scope as detailed in the quote/briefing sheet that may be required following an evaluation of the case scenario and case data.

99.4.5 Although the plotting of mast locations and estimated direction of service (e.g. sectors) may be used in the planning process, any estimations or unverified information shall be marked up as such.

99.4.6 There are many ways in which analyses may be undertaken; case circumstances vary and so the methods used may also vary. The strategy shall therefore detail the rationale for the approach taken with reference to the survey type (e.g. location, area surveyed, cell mapping) and mode selected (e.g. idle, connected, software defined radio).

99.5 Checking and review

General

99.5.1 The forensic unit shall have a procedure for checking (including for critical findings).

99.5.2 This section describes the following types of check and their expected application:

a. Examination strategy check.

b. Technical check.

c. Critical finding check, including the manner of triggering the check with the correct level of independence, i.e.:

i. with full sight of the original practitioner's findings (i.e. open);

ii. with no sight of the original practitioner's findings; or

iii. with no sight of the certain aspects of the original practitioner's experience-based findings (section 99.7.4).

99.5.3 The procedure shall ensure that check stages are clear and it is clear when the independent check is to be performed blind. The expectation is that decisions to blind any finding are made in the preceding stage(s); the practitioner may have a rule-based escalation route within their procedures to flag and/or separate out checks to be performed blind (section 99.7.6 for the criteria for triggering blind review). The identification of blind checks is enabled by either:

a. the expert generating the original report identifying those aspects of opinion that will require blind check;

b. the technical checker identifying those aspects that were critical findings but that they could not check via referenceable data or deductive inference.

99.5.4 The procedure does not have to specify the checks listed in 99.5.2 to be conducted in that order. Forensic unit's may find that if the expert generating the original report can identify aspects of opinion that will require blind check (i.e. 99.5.3a) and can present these separately for checking as in 99.5.2c.iii then this check may be performed first. Checking the aspects identified here

before the technical check may allow for the same practitioner to then perform the other checks. The procedure may include other alternative workflows; the intention is however for the practitioner performing the blind check to not be sighted on the original practitioner's experience-based findings.

99.6 Examination strategy check

99.6.1 The procedure for carrying out checks shall establish if work carried out conformed to the following:

a. Has the question presented been addressed?

b. Is the process adopted to answer the question legitimate and have the limitations been declared?

c. Is the method used applicable to the purpose? For example, a limited survey may demonstrate service of a cell at a given location at the time of that survey. If the cell does serve an area including the scene, in the absence of a testable alternative proposition, finding and/or conclusion shall reemphasise that the device could have been at anywhere in the coverage of that cell and that coverage has not been established. It may be appropriate to give an opinion as to the level of discrimination (e.g. a rural area may cover more than 10km).

d. An indication as to whether that cell is a particularly large cell (and therefore a less discriminating finding than otherwise might be the case) may be appropriate this opinion may or may not be informed by survey data.

e. If a conclusion has been reached, is the question presented within the expertise of the practitioner? Is the evidence expected given the conclusion drawn (i.e. is the supporting summary of findings correct and relevant)? For example, it is normally not possible to address legitimately whether it is likely that a person used a phone (rather than whether the data for a phone would be expected, given that a specific person used it).

99.7 Technical check

99.7.1 A technical check of the evidential product is made with reference to the report, supporting exhibits and data on which the examination/analysis has relied. It is

therefore an ‘open’ check, with awareness of the conclusions reached and with full access to the material relied on. The technical check is to ensure the following:

a. Factual information (e.g. times, dates, locations, cell IDs) are correctly presented both in the report and supporting items/exhibits.

b. Opinions on technical matters, such as whether a given cell serves an area including a specific location are overt, based on verifiable information (e.g. survey data) and are supportable.

c. Appropriate methods have been used and followed.

d. Data relied upon has been converted/presented/referenced correctly.

e. Survey data (if used) is appropriate and presented correctly.

f. Caveats concerning the findings are presented.

g. There is sufficient data to draw the conclusion offered.

h. The method used to draw the conclusion offered is appropriate.

i. The work is fully documented in the case notes.

j. There are appropriate checks on critical findings, calculations and data transfers.

k. Work is produced in compliance with the forensic unit’s documented policies and procedures.

l. Conclusions are consistent with the broader contents of the report or statement.

99.7.2 The forensic unit shall ensure that methods that require calculations (including those embedded in spreadsheets) and/or critical data transfers that do not form part of a validated process include checks carried out by a second practitioner. A policy/procedure shall define the nature of the transfers and the checking procedure that shall consider the accuracy and/or applicability of the following:

a. CDR:

   i. The CDR are the foundation of cell site analysis. They are supplied in varying formats (according to network) and in a format that usually

requires reformatting and/or normalisation, which should be validated (section 99.10.3).

ii. Specific call data that have been determined to be unreliable have been correctly excluded (e.g. other party cell site information).

iii. Format of data (e.g. call event nomenclature, time, date etc.).

iv. Normalisation of data (e.g. conversion of latitude and longitude to British national grid, postcode to a coordinate system).

b. Mapping:

i. Presented data (e.g. cell site locations, locations of interest) are correctly positioned and labelled. An indication should be given to how the cell mast locations were derived, e.g. verification through actually visiting the location or as presented by the service provider. Presented data (either digital or paper) shall use a common mapping projection so as to correct any potential distortions, such as in location, area or distance.

ii. If a period of call data is illustrated, the map should illustrate all of that data. If presenting only a selection of data, this should be clearly stated.

c. Survey:

i. Do the data correspond to the location of interest?

ii. If serving cell data (all cells that serve a location or area) are presented, are these data an accurate reflection of the survey data (e.g. correct network and protocol, correct cell ID)?

iii. Are there sufficient data to adequately answer the question presented?

99.7.3 Reasoning for clarity of and supporting objective (referenceable) data (e.g. survey data indicates that the cell serves an area including the location of interest) for opinion on specific technical matters arising shall also be checked; this includes when:

a. cell usage at specific dates and times contradict other events in a similar period, and cannot be easily explained;

b. a cell was expected to provide service at a location of interest, was on air during the survey, but was not detected there and opinion has been given on whether it would be expected to have served or not;

c. service of a given cell was detected but not as expected (e.g. the survey results suggest irregularities with the reported azimuths from the CDR as might occur with 'crossed-feeders' i.e. two or more sector feeds connected incorrectly); or

d. cells which are detected serving at more than one of the key locations are highlighted (i.e. that other possible explanations of the data relevant to the propositions are raised, rather than 'cherry picking' data expected given only one of the propositions).

99.7.4 Where all findings reviewed are fully supported by objective (referenceable) data then the critical finding check may proceed as an open check; however, if the finding(s) is based on the experience of the practitioner rather than direct objective (referenceable) data, this shall be considered for a blind check.

99.7.5 The procedure shall detail how casework is identified for checking blind, how individual aspects will be presented for checking, and/or how the full report is to be verified blind. If the forensic unit has correctly implemented phased disclosure with discrete aspects pared off for checking, it may be possible for the same individual to perform both the technical and a blinded critical findings check.

99.7.6 Examples of situations which may trigger a blind check include the following:

a. Where a cell is used during the incident, the cell has not been measured, and comment is made on its potential service area, including the locations specified in the prosecution and/ or defence propositions.

b. Where a cell is used during the incident, the cell has not been measured, and comment is made on its potential service area, excluding the locations specified in the prosecution and/or defence propositions.

99.8 Critical finding check

99.8.1 A critical finding is information (a fact or opinion) which directly and substantively affects the overall conclusions (i.e. whether the data as a whole might be expected given the declared propositions):

a. For example, if a cell was listed during the period of the offence, opinion on whether the time can be relied upon (e.g. for GPRS events) and whether the cell served an area including the scene and/or alibi locations would be a critical finding (potentially amongst many other, similar findings).

b. Conversely, other parts of the analysis (e.g. a commentary of general cell usage in periods where nothing specific is alleged by either prosecution or defence) would not be a critical finding.

99.8.2 Where a critical finding check is the only substantive quality control procedure for checking that finding, then this check shall be performed without knowledge of the original result (i.e. blind) and this independence shall be identifiable from the records. Findings which have a blind check involves a second expert providing an independent technical opinion in isolation of the original opinion to be checked; this may be those aspects of opinion identified by the expert generating the original report during the technical check or by another rules-based aspect of the procedure.

99.8.3 The critical finding check involves the review of the technical findings (with some elements being blind as required and as outlined above) against the proposition, and an independent conclusion is then drawn which, on completion, is compared to the original conclusion by the first practitioner.

99.8.4 This stage can be combined with the technical check (i.e. section 99.7) if considered appropriate, as long as the independent blind checks are completed first if they are to undertaken by the same practitioner.

99.8.5 This check will also review the complete report in context after the check on the conclusion is completed (with some elements being blind as required and as outlined above). Any disagreement is logged, after which a conclusion acceptable to both practitioners is reached, with reasons declared.

99.8.6 The forensic unit shall have a process in place to resolve differing opinions for the circumstance in which no such agreement can be reached, including how the issue is raised in the expert's report, as part of the critical finding check.

99.9 Competence

99.9.1 Each role in the examination/analysis shall be defined in the method, including the requirements for knowledge, training, experience and any specific qualifications for the tasks assigned to each role.

99.9.2 For practitioners involved in handling CDRs and producing maps or tables from them, the training records shall define which aspects they are trained in. The competences to be addressed shall include the following:

a. knowledge of relevant communications data;

b. normalising data;

c. quality assurance stages; and

d. accepted practices for differentiating between estimated coverage plotted for planning purposes and factual plotted data.

99.9.3 Practitioners conducting an RF propagation survey shall be assessed to demonstrate the following:

a. Ability to contribute to the development of a survey strategy or implement given or standardised strategies.

b. Competence of the individual to:

i. select the survey method:

ii. idle mode;

iii. connected mode (e.g. dedicated);

iv. software defined radio (if validated for use in the forensic unit);

v. location survey;

vi. select the route and/method of survey:

vii. area survey;

viii. cell mapping;

ix. apply the survey method; and

x. correctly interpret the output of the survey.

c. Use of survey equipment in idle and connected modes.

d. Understand the limitations of survey types and use of data. This shall be specific to the survey equipment in use as well as the generic types derived from the information collated or produced in the validation study.

e. Where part of the practitioner's role, have knowledge of Wi-Fi or other RF communications standards.

f. Understand the responsibilities of practitioners conducting the sub activities in the related FSA (i.e. practitioners conducting the RF survey, expert witnesses).

g. Preparation of reports.

99.9.4 The forensic unit shall demonstrate ongoing competence of all practitioners. This may involve the following:

a. reviewing technical records;

b. completing a competence test involving a known outcome exercise or a repeatability study; or

c. a witnessing procedure to ensure that those conducting RF propagation surveys retain competence (ILAC-G19 3.8 [6]).

99.9.5 Training programmes shall include legal awareness training to include how the forensic unit's procedures comply with the following:

a. Criminal Procedure Rules, specifically Parts 1, 3, 16 and 19 [11]; and

b. Criminal Practice Directions 2023, specifically direction 7 [11].

99.9.6 Training programmes shall also include legal awareness training to include an overview of the following legislation:

a. Investigatory Powers Act 2016 [79] (if relevant to role); and

b. Criminal Procedure and Investigations Act 1996 [9].

99.9.7 Evaluative evidence in cell site analysis includes assessments, for example whether:

a. the data might be expected given that the user of the phone was at the scene during the offence (as alleged by the prosecution) or at their home address (as claimed by the defence); and/or

b. the call data might be expected if the suspect was the user of the device, or whether there is any data in conflict with that proposition.

99.9.8 As well as the skill and competence required for technical activities (e.g. surveys, mapping, CDR normalisation), training programmes for practitioners involved in this activity shall include the following:

a. Development of an examination strategy.

b. Assessment and interpretation skills including:

i. formulating and testing propositions;

ii. awareness of the risk of transposing conditionals (prosecutor's fallacy); and

iii. use of appropriate terminology (section 99.2.4c).

c. Suitable theory training on what inference might be drawn from consideration of:

i. survey data (limitations from validation studies);

ii. network-appropriate knowledge of RF technology (i.e. network design and operation); and/or

iii. different types of CDR artefacts (e.g. GPRS or end cells).

d. Awareness of cognitive bias [72].

e. Preparation of expert reports and statements.

99.9.9 Where practitioners are expected to give evidence in court, training programmes shall also include training in the roles and responsibilities of the expert, as most findings in the FSA may involve providing opinion or being asked opinion on matters related to the findings. In addition to an understanding of the Criminal Practice Directions 2023 (direction 7) [11], training material may include reference to other guidance on legal obligations (e.g. [10]).

99.9.10 The location of the device is not in the CDRs, but the area in which it was operating may be inferred from the detail within the records. Inference is

synonymous with opinion, and therefore should be given by a practitioner who is competent to provide evidence of opinion (i.e. an expert). If the purpose of the analysis is to assess where the phone was, this will require the practitioner reporting the finding to be giving an expert opinion.

99.9.11 Expressing opinions is the role of the expert witness; this includes providing evaluative evidence. Practitioners interpreting results shall have been assessed and deemed competent in interpretation and opinions.

99.10 Validation

Selection of methods

99.10.1 All methods of examination/analysis shall be fit for purpose; in demonstrating this, the forensic unit will need to have supporting validation/verification material compliant with the requirements of this Code (section 24).

99.10.2 The overall method selected shall be validated; tools are tested within the validation. Cell site analysis can comprise sub-methods, selected as required; each of these (e.g. survey) can be validated as separate entities. The most appropriate method should be selected based on the strengths and limitations of those available to answer the needs of the commissioning party and the CJS.

Validation of methods

99.10.3 The whole process (i.e. from request/receipt of call data through to provision of final opinion) shall be validated for the method to be acceptable. Any non-compliance shall be declared.

99.10.4 Validation is about providing objective evidence that the method is fit for purpose; this is described in the end user technical requirements and acceptance criteria. Objective evidence to demonstrate aspects of the end user requirements may be drawn in part from the following:

a. A literature review.

b. The practitioner community.

c. Academic studies.

d. Collaborative trials.

e. Data collated by the forensic unit or training establishments (which require verifying by the forensic unit) using defined scenarios.

99.10.5 Where relevant, the validation procedure shall include, but is not limited to, the following:

a. Determining the end user requirements and specification;

b. Risk assessment of the method;

c. A review of the end user requirements and specification;

d. The acceptance criteria;

e. The plan to demonstrate the validity of the method;

f. The outcomes of the validation exercise;

g. Assessment of acceptance criteria compliance;

h. Report on method validity;

i. Statement that the method is valid; and

j. Implementation plan.

99.10.6 This Code describes in detail the requirements of all the above in section 24. However, some introductory words on the end user requirement and further information on risk assessment requirements is given in the following sub-sections.

Determining the end user requirements and specification

99.10.7 The end user requirements include interim-user requirements but should be framed by the end user being the wider CJS.

99.10.8 This is about the method not the requirements of the specific equipment used. It is not a reiteration of the user manual of survey equipment or phone emulator. The requirements and specification are used to gauge the scale of validation study based upon the acceptance criteria defined.

Risk assessment of a method

99.10.9 A risk assessment is required and is used to determine the hazards of a method. The validation shall test the mitigation strategy to control the identified risks. The test employed may vary according to the method.

99.10.10 Within the CJS, some risks may be defined as:

a. false positives (e.g. stating that a phone was, or may have been, in an area where it could not); or

b. false negatives (e.g. stating that a phone could not have been in an area where it could).

99.10.11 The risk assessment is used to develop the validation plan; risks identified should be tested against the overall method. The method is more than the test of survey equipment; e.g. the method may require additional activity to give assurance that the risk of identified types of false negatives are managed in a way that the testing of instrumentation alone would not give (e.g. in section 99.11.6).

99.10.12 The risk analysis shall assess all of the technical stages that may contribute to these risks being realised. Examples include the following:

a. CDR normalisation:

i. transcription errors;

ii. inclusion of incorrect information (e.g. ‘other party’ cell site) without recognising it as such;

iii. exclusion of legitimate information (e.g. transcription errors); and

iv. use of GPRS without recognising limitations.

b. Mapping:

i. misrepresentation of a cell site in the wrong location, e.g. labelled with an incorrect time of usage and/or cell identification; and

ii. inappropriate sector representation.

c. Survey:

i. failing to detect a legitimately serving cell relevant to the case (methods that rely solely on a static survey are prone to this); and

ii. failing to recognise that there may have been a network change (e.g. not checking that a cell of interest is off air at the time of the survey).

d. Interpretation:

i. cognitive bias;

ii. incorrectly identifying reasonable propositions;

iii. not assessing and expressing uncertainty in findings in a meaningful way; and/or

iv. inadequate quality management of any of the risks above.

Statement of validation completion

99.10.13 This Code requires that a statement of validation completion is prepared. The forensic unit may conduct an RF propagation survey as a separate service (such as for virtual 'scene preservation' in response to an incident to capture serving cell activity) to cell site analysis. In this instance, although aspects of the validation study may be shared, separate statements of validation completion may be appropriate.

99.11 Uncertainty of measurement

99.11.1 There is inherent uncertainty of measurement within cell site analysis no matter which methods have been applied. This Code and ISO/IEC 17025:2017 [3] require the forensic unit to identify the contributions to measurement uncertainty, noting that ISO/IEC 17025:2017 [3] accepts that where "the test method precludes rigorous evaluation of measurement uncertainty, an estimation shall be made based on an understanding of the theoretical principles or practical experience of the performance of the method".

99.11.2 Networks can change over time and there may be differences in network operation between the time that the event of interest took place and the time the investigation begins or the FSA is performed. Some aspects may be physical changes (e.g. changes to the built environment, cells being added, removed or reoriented, decommissioning of assets in the 3G network, stacked cells) or organisational (e.g. routing or location area boundaries that may affect cell boundaries). There may also be temporary equipment faults.

99.11.3 Full cell site surveys assist in estimating the area where a mobile device was. However, further uncertainty within surveys can result from the following:

a. Any changes to the network in the area considered during the time that has elapsed since the event of interest and that of the survey.

b. Survey equipment may not directly reflect the operation of the questioned device.

c. Interpretation of the data (false positives/negatives).

d. The height at which the survey was undertaken compared with the actual location and the height that the original connection was made to the cell site in question.

99.11.4 Given these uncertainties, cell site analysis will not be able to pinpoint the location of the subject device. The terminology used in reports shall reflect this when referring to specific locations that were assessed. For example, phrases such as “the cell used by the subject phone was detected providing service over a cell service area that includes [the location of interest]” may be appropriate.

99.11.5 For example, a practitioner with the appropriate competence may be able to comment on the general anticipated coverage area of cells of interest and thereby provide some context to their findings. For example, assessing the expected coverage area of a cell from the network information, if it is any of the following:

a. An indoor cell (in which case usage implies that the user was within the building – a very precise assessment; however, additional work may be necessary to prove that a ‘femtocell’ was actually located at the stated address at the time as such devices can be moved and connected to the network from other locations);

b. A 3m street works dwarfed by the surrounding buildings (in which case the service area may only be that and possibly a few adjoining streets; again, a relatively precise assessment); or

c. A large rural macro cell based on the top of a 60m tower (which may provide a service over a large area, perhaps 10 or 20km from the mast and thus provides much lower precision and is potentially of lesser evidential impact).

99.11.6 There shall be a policy or procedure that includes additional activities that are undertaken if it has been concluded that a cell does not serve at a specific location when it is expected to and that is relevant to the case. This shall include one or more of the following:

a. Assessing antenna point direction (azimuth).

b. Examining the path profile between mast and location to check for obvious terrain obstructions, etc.

c. Reviewing survey data to identify if the cell seen in other locations contributes to verifying that it is on air without visiting the cell.

d. Reviewing neighbour data to see if the frequency that the cell is on is visible or used by a different cell.

e. Checking the mast location by visiting or even via Google Maps Street View to see if the cell is:

    i. physically present; and

    ii. links appear intact and/or if visiting is on air.

Part E – General information

100. Scope of Forensic Science Activities (FSAs)

100.1 Legal basis

100.1.1 The Act (see s11 of the Act) establishes the concept of 'FSA'. The Act (see s2) requires that the Regulator specify the FSAs which are subject to the Code. This places responsibility on the Regulator for defining, with sufficient clarity, what activities are subject to the Code.

100.2 Definition

100.2.1 Section 11 of the Act defines FSA as follows:

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

(2) Those purposes are-

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

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

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

100.3 Territorial extent

100.3.1 The Act creates a territorial limit to the scope of an FSA by reference to 'England and Wales'.

100.3.2 The terms 'England' and 'Wales' are defined in The Interpretation Act 1978 [122].

100.3.3 In relation to s11(2)(a) of the Act, the limit is taken to mean that the work must relate to crime in England and Wales.

100.3.4 In relation to s11(2)(b) of the Act, the limit is taken to mean the criminal proceedings must occur in England and Wales. The Code imposes no restriction on where the crime, or suspected crime, occurred.

100.3.5 The provisions of s2 of the Act mean that this Code only applies to FSAs which are undertaken in England and Wales.

100.3.6 Where an FSA is undertaken in part in England and Wales, and in part outside England and Wales, the Code will only apply to the part of the FSA undertaken in England and Wales.

100.4 Limits on FSA – link to crime

100.4.1 The definition of FSA in section 100.2.1 makes clear that an FSA must be undertaken for one of the purposes set out in s11(2) of the Act.

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

100.4.3 The Act uses the text ‘relating to’ which indicates the work does not have to be directly for the purposes stated.

100.5 Approach to FSA definition

100.5.1 The Act (see s2(2)(a) of the Act), requires that the Code specifies those FSAs to which the Code applies. It follows that, in relation to any version of the Code:

a. a declaration that an activity is an FSA to which the Code applies is conclusive; and

b. a declaration that an activity is an FSA to which the Code does not apply is conclusive.

100.5.2 The FSAs to which the Code applies and does not apply may be different in future versions of the Code.

100.5.3 To ensure it is clear what is covered and which provisions apply for each FSA, the FSAs may include exclusions. In some cases these exclusions will make clear the activities that are not of themselves considered FSAs are excluded from a particular FSA.

100.6 Commissioning – detection and/or investigation of crime

100.6.1 For the purposes of the Code, to fall within the purpose in s11(2)(a) of the Act, the requirements in this section apply. This includes externally provided services obtained by a forensic unit.

100.6.2 The activity must have been originally commissioned by, or undertaken by (or on behalf of), one of the following for a purpose related to the detection and/or investigation of crime:

a. A body involved in the detection and/or investigation of crime.

b. A prosecuting authority.

c. A suspect, accused or convicted individual (in relation to the offence for which they are suspected, accused or convicted) where the relevant criminal investigation and/or prosecution was by a body listed in the sub-clauses above.

d. A legal representative for a person within the description in section c above.

e. A body (not a court of law) with legal authority to investigate potential miscarriages of justice.

f. The Regulator.

100.6.3 For the purposes of the Code, detection and/or investigation of crime means the following:

a. Establishing whether a crime has occurred, has been attempted or is planned.

b. Establishing whether information related to the investigation of crime is accurate and eliminating the innocent from criminal investigations.

c. Establishing by whom, for what purpose, by what means, and generally in what circumstances any crime was, or may have been, committed.

d. Obtaining and recording such information as may be needed in the criminal investigation and prosecution of any offence, including as part of an appeal process.

e. The apprehension of an individual by whom any crime was committed.

100.6.4 A body involved in the detection and/or investigation of crime means any of the following bodies, in relation to their work in England and Wales:

a. The 43 territorial police forces in England and Wales, including any unit (e.g. a counter terrorism unit or regional organised crime unit) which includes, or is comprised of, constables from one of the territorial forces and is not a separate legal entity from the force(s) from which the constable(s) come.

b. The following limited territorial forces:

   i. Kew Constabulary;

   ii. Mersey Tunnels Police;

   iii. Port of Bristol Police;

   iv. Port of Dover Police;

   v. Port of Felixstowe Police;

   vi. Port of Liverpool Police;

   vii. Port of Tilbury Police; and

   viii. Tees and Hartlepool Harbour Police.

c. The following non-territorial police forces:

   i. British Transport Police;

   ii. Civil Nuclear Constabulary; and

   iii. Ministry of Defence Police.

d. The following military law enforcement bodies:

   i. Royal Navy Police;

   ii. Royal Military Police;

   iii. Royal Air Force Police; and

   iv. Royal Marines Police.

e. Fire and rescue services.

f. National Crime Agency.

g. Serious Fraud Office.

h. HM Revenue & Customs.

i. Home Office.

j. Independent Office for Police Conduct.

k. The following security and intelligence agencies:

   i. Government Communications Headquarters;

   ii. Secret Intelligence Service; and

   iii. Security Service.

l. Any person responsible for, or operating, the following databases:

   i. National DNA Database;

   ii. National Footwear Database;

   iii. National Footwear Reference Collection;

   iv. National Ballistics Intelligence Service; and

   v. National Fingerprint Database.

100.6.5 A prosecuting authority means:

a. HM Attorney General;

b. Director of Public Prosecutions;

c. Crown Prosecution Service; or

d. Serious Fraud Office.

100.6.6 Investigations by armed services/military police organisations (section 100.6.4d) that are dealt with under the Service Justice System are outside of the remit of the Regulator. Criminal investigations and subsequent proceedings for the Criminal Justice System of England and Wales that involve military personnel, where forensic science activities that are subject to the Code are undertaken, fall within the remit of the statutory regulation of forensic science.

100.7 Commissioning - preparation, analysis or presentation of evidence

100.7.1 For the purposes of the Code, to fall within the purpose in s11(2)(b) of the Act, the activity must have been commissioned by one of the following

persons/bodies with the intention that the output is used for a purpose related to criminal proceedings:

a. A body involved in the detection and/or investigation of crime.

b. A prosecuting authority.

c. A suspect, accused, or convicted person (in relation to the offence for which they are suspected, accused, or convicted) where the relevant criminal investigation and/or prosecution was by a body listed in the sub-clauses above.

d. A legal representative for a person within the description in section c above.

e. A body with legal authority to investigate potential miscarriages of justice.

f. The Regulator.

100.7.2 The term “criminal proceedings” means, subject to sections 100.7.3 and 100.7.4, any proceeding covered by the following provisions:

a. Section 51 of the Criminal Justice Act 2003 [123].

b. Section 14 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012 [124].

100.7.3 The following proceedings shall not be considered ‘criminal proceedings’ for the purpose of this Code:

a. Proceedings for dealing with an individual under the Extradition Act 2003 [125].

b. Proceedings for binding an individual over to keep the peace or to be of good behaviour under section 115 of the Magistrates’ Courts Act 1980 [126] and for dealing with an individual who fails to comply with an order under that section.

c. Proceedings for contempt committed, or alleged to have been committed, by an individual in the face of a court.

d. Proceedings before the Judicial Committee of the Privy Council.

100.7.4 The term ‘criminal proceedings’ shall not cover any activities related to the imposition or management of a sentence imposed on a convicted person.

100.7.5 Where any activity that is carried out for purposes other than those described in s11 of the Act (i.e. where the output of the activity is not intended to be used for a purpose related to criminal proceedings) generates material which is subsequently of relevance to the CJS, the initial work is not considered an FSA. Any work (e.g. any additional work, the production of reports or the presentation of evidence) commissioned for CJS use will be an FSA if it falls within the definitions in this Code.

101. References

[1] "Forensic Science Regulator Act 2021," [Online]. Available: www.legislation.gov.uk/ukpga/2021/14/contents/enacted. [Accessed 08 09 2022].

[2] Forensic Science Regulator, "Forensic science activities: statutory code of practice," [Online]. Available: www.gov.uk/government/publications/statutory-code-of-practice-for-forensic-science-activities. [Accessed 13 11 2023].

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

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

[5] International Organization for Standardization, "BS EN ISO 15189:2022, Medical laboratories. Requirements for quality and competence".

[6] International Laboratory Accreditation Cooperation, "ILAC-G19:06/2022 Modules in a Forensic Science Process," [Online]. Available: https://ilac.org/latest_ilac_news/ilac-g19082014-published/. [Accessed 13 11 2023].

[7] "The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018," [Online]. Available: www.legislation.gov.uk/uksi/2018/952/contents/made. [Accessed 24 01 2023].

[8] Forensic Science Regulator, "Policy on Enforcement Action taken by the Forensic Science Regulator," [Online]. Available: www.gov.uk/government/publications/enforcement-action-taken-by-the-forensic-science-regulator. [Accessed 29 10 2024].

[9] "Criminal Procedure and Investigations Act 1996," [Online]. Available: www.legislation.gov.uk/ukpga/1996/25/contents. [Accessed 19 07 2023].

[10] Forensic Science Regulator, "FSR-I-400, Legal Obligations," [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance. [Accessed 13 11 2023].

[11] "Criminal Procedure Rules 2020 and Criminal Practice Directions 2023," [Online]. Available: www.gov.uk/guidance/rules-and-practice-directions-2020. [Accessed 30 03 2023].

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

[13] British Standards Institution, "Publicly Available Specification (PAS) 377:2023 Specification for consumables used in the collection, preservation and processing of material for forensic analysis - Requirements for product, manufacturing and forensic kit assembly," 2023.

[14] *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.*

[15] 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 17 11 2020].

[16] Cabinet Office, "Government Security Classifications," [Online]. Available: www.gov.uk/government/publications/government-security-classifications. [Accessed 16 12 2024].

[17] 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 13 11 2023].

[18] Warwickshire Police, "Police National Vetting Service," [Online]. Available: www.warwickshire.police.uk/police-forces/warwickshire-police/areas/warwickshire-police/about-us/about-us/police-national-vetting-service/. [Accessed 16 12 2024].

[19] "United Kingdom Security Vetting," [Online]. Available: www.gov.uk/government/collections/national-security-vetting. [Accessed 16 12 2024].

[20] I. W. Evett, "The Logical Foundation of Forensic Science: Towards Reliable Knowledge," *Phil. Trans. R. Soc. B,* p. 370, 2015.

[21] D. Rogers and B. Found, "The initial profiling trial of a program to characterize forensic handwriting examiners' skill," *Journal of American Society of Questioned Document Examiners,* no. 6, pp. 72-81, 2003.

[22] Forensic Science Regulator, "Crime Scene DNA: Anti-contamination guidance," [Online]. Available: www.gov.uk/government/publications/crime-scene-dna-anti-contamination-guidance. [Accessed 29 11 2023].

[23] "The Accreditation of Forensic Service Providers Regulations 2018," [Online]. Available: www.legislation.gov.uk/uksi/2018/1276/contents. [Accessed 16 12 2024].

[24] United Kingdom Accreditation Service, “TPS 68: UKAS Policy on Accreditation of Infrequently Performed Conformity Assessment Activities,” 2020. [Online]. Available: https://www.ukas.com/wp-content/uploads/schedule_uploads/759164/TPS-68-UKAS-Policy-on-Accreditation-of-Infrequently-Performed-Conformity-Assessment-Activities.pdf. [Accessed 21 07 2022].

[25] *R v. Bonython [1984] 38 SASR 45.*

[26] 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 13 11 2023].

[27] United Kingdom Accreditation Service, “M3003, The Expression of Uncertainty and Confidence in Measurement,” [Online]. Available: www.ukas.com/wp-content/uploads/2023/05/M3003-The-expression-of-uncertainty-and-confidence-in-measurement.pdf. [Accessed 06 12 2024].

[28] International Laboratory Accreditation Cooperation, “ILAC G17: 01/2021 Guidelines for Measurement Uncertainty in Testing,” [Online]. Available: https://ilac.org/publications-and-resources/ilac-guidance-series/. [Accessed 13 11 2023].

[29] EuraChem, “Quantifying Uncertainty in Analytical Measurement, 3rd Edition (2012),” [Online]. Available: www.eurachem.org/index.php/publications/guides/quam. [Accessed 16 12 2024].

[30] The National Cyber Security Centre, “Secure Sanitisation of Storage Media,” 2016. [Online]. Available: www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media. [Accessed 21 07 2022].

[31] National Protective Security Authority, “Secure Destruction,” [Online]. Available: www.npsa.gov.uk/secure-destruction-0. [Accessed 13 11 2023].

[32] The National Cyber Security Centre, “Acquiring, managing, and disposing of network devices,” [Online]. Available: www.ncsc.gov.uk/guidance/acquiring-managing-and-disposing-network-devices. [Accessed 13 11 2023].

[33] International Organization for Standardization, “BS ISO/IEC 27001:2022 Information technology – Security techniques – Information security management systems – Requirements”.

[34] International Organization for Standardization, “BS ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection”.

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

[36] The National Cyber Security Centre, “Setting up two-factor authentication (2FA),” [Online]. Available: www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa. [Accessed 13 11 2023].

[37] The National Cyber Security Centre,, “10 Steps to cyber security,” [Online]. Available: www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps. [Accessed 21 07 2022].

[38] The National Cyber Security Centre, “Password administration for system owners,” [Online]. Available: www.ncsc.gov.uk/collection/passwords/updating-your-approach. [Accessed 13 11 2023].

[39] The National Cyber Security Centre, “Three random words or #thinkrandom,” [Online]. Available: www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0. [Accessed 13 11 2023].

[40] The National Cyber Security Centre, “Password manager buyers guide,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/passwords/password-manager-buyers-guide. [Accessed 13 11 2023].

[41] The National Cyber Security Centre, “Passwords, passwords everywhere,” 2019. [Online]. Available: www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere. [Accessed 21 07 2022].

[42] The National Cyber Security Centre, “Using IPSec protect data,” [Online]. Available: www.ncsc.gov.uk/guidance/using-ipsec-protect-data. [Accessed 13 11 2023].

[43] 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 13 11 2023].

[44] The National Cyber Security Centre, “Device security principles for manufacturers,” [Online]. Available: www.ncsc.gov.uk/collection/device-security-guidance/security-principles. [Accessed 13 11 2023].

[45] The National Cyber Security Centre, “Preventing lateral movement,” [Online]. Available: www.ncsc.gov.uk/guidance/preventing-lateral-movement. [Accessed 13 11 2023].

[46] The Australian Cyber Security Centre, “Implementing Network Segmentation and Segregation,” [Online]. Available: www.cyber.gov.au/acsc/view-all-content/publications/implementing-network-segmentation-and-segregation. [Accessed 12 11 2023].

[47] The National Cyber Security Centre, “Mitigating malware and ransomware attacks,” [Online]. Available: www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks. [Accessed 13 11 2023].

[48] The National Cyber Security Centre, “Phishing attacks: defending your organisation,” [Online]. Available: www.ncsc.gov.uk/guidance/phishing. [Accessed 13 11 2023].

[49] The National Cyber Security Centre, “All products & services,” [Online]. Available: www.ncsc.gov.uk/section/products-services/all-products-services-categories?&start=0&rows=20. [Accessed 21 07 2022].

[50] The National Cyber Security Centre, “Small Business Guide: Response and Recovery,” [Online]. Available: www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery. [Accessed 13 11 2023].

[51] The National Cyber Security Centre, “Incident Management,” [Online]. Available: www.ncsc.gov.uk/collection/incident-management. [Accessed 13 11 2023].

[52] The National Cyber Security Centre, “Offline backups in an online world,” [Online]. Available: www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world. [Accessed 13 11 2023].

[53] The National Cyber Security Centre, “Using TLS to protect data,” 2017. [Online]. Available: www.ncsc.gov.uk/guidance/tls-external-facing-services. [Accessed 13 11 2023].

[54] The National Cyber Security Centre, “Cloud Security Guidance,” [Online]. Available: www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles. [Accessed 21 07 2022].

[55] The National Cyber Security Centre, “Introduction to logging for security purposes,” [Online]. Available: www.ncsc.gov.uk/guidance/introduction-logging-security-purposes. [Accessed 13 11 2023].

[56] The National Cyber Security Centre, “Logging made easy (LME),” 2019. [Online]. Available: www.ncsc.gov.uk/blog-post/logging-made-easy. [Accessed 13 11 2023].

[57] “Human Tissue Act 2004,” [Online]. Available: www.legislation.gov.uk/ukpga/2004/30/contents. [Accessed 19 07 2023].

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

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

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

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

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

[63] European Network of Forensic Science Institutes, “Guidance on the conduct of proficiency tests and collaborative exercises within ENFSI,” 2014. [Online]. Available: https://enfsi.eu/wp-content/uploads/2017/07/QCC-PT-001-_-Guidance-on-PT-CE.pdf. [Accessed 11 11 2023].

[64] International Organization for Standardization, “ISO/IEC 17043:2023, Conformity assessment — General requirements for proficiency testing”.

[65] European Proficiency Testing Information System, “About EPTIS,” [Online]. Available: www.eptis.bam.de/en/index.htm. [Accessed 13 11 2023].

[66] European Network of Forensic Science Institutes, “Welcome to ENFSI!,” [Online]. Available: https://enfsi.eu/. [Accessed 10 11 2023].

[67] Forensic Science Regulator, “FSR-G-200, Expert Report Guidance,” [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance. [Accessed 21 07 2022].

[68] Forensic Capability Network, “Streamlined Forensic Reporting (SFR),” [Online]. Available: www.fcn.police.uk/library. [Accessed 16 12 2024].

[69] “Road Traffic Offenders Act 1988,” [Online]. Available: www.legislation.gov.uk/ukpga/1988/53/contents. [Accessed 16 12 2024].

[70] Forensic Science Regulator, “Declaring compliance with the code of practice,” [Online]. Available: www.gov.uk/government/publications/declaring-compliance-with-the-code-of-practice. [Accessed 29 11 2023].

[71] 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/wp-content/uploads/schedule_uploads/759162/LAB-13-Guidance-on-the-Application-of-ISO-IEC-17025-Opinions-and-Interpretations.pdf. [Accessed 13 11 2023].

[72] Forensic Science Regulator, Cognitive Bias Effects Relevant to Forensic Science Examinations FSR-G-217, Forensic Science Regulator.

[73] “Data Protection Act 2018,” [Online]. Available: www.legislation.gov.uk/ukpga/2018/12/contents. [Accessed 19 07 2023].

[74] “Police and Criminal Evidence Act 1984,” [Online]. Available: www.legislation.gov.uk/ukpga/1984/60/contents. [Accessed 19 07 2023].

[75] “Protection of Freedoms Act 2012,” [Online]. Available: www.legislation.gov.uk/ukpga/2012/9/contents. [Accessed 07 09 2022].

[76] “The Security Service Act 1989,” [Online]. Available: www.legislation.gov.uk/ukpga/1989/5/contents/enacted. [Accessed 12 12 2024].

[77] “Intelligence Services Act 1994,” [Online]. Available: www.legislation.gov.uk/ukpga/1994/13/contents/enacted. [Accessed 12 12 2024].

[78] “Regulation of Investigatory Powers Act 2000,” [Online]. Available: www.legislation.gov.uk/ukpga/2000/23/contents. [Accessed 12 12 2024].

[79] “Investigatory Powers Act 2016,” [Online]. Available: www.legislation.gov.uk/ukpga/2016/25/contents. [Accessed 16 12 2024].

[80] “Psychoactive Substances Act 2016,” [Online]. Available: www.legislation.gov.uk/ukpga/2016/2/contents. [Accessed 16 12 2024].

[81] “Road Traffic Act 1988,” [Online]. Available: www.legislation.gov.uk/ukpga/1988/52/contents. [Accessed 16 12 2024].

[82] “Transport and Works Act 1992,” [Online]. Available: www.legislation.gov.uk/ukpga/1992/42/contents. [Accessed 16 12 2024].

[83] “Railways and Transport Safety Act 2003,” [Online]. Available: www.legislation.gov.uk/ukpga/2003/20/contents. [Accessed 16 12 2024].

[84] “The Drug Driving (Specified Limits) (England and Wales) Regulations 2014,” [Online]. Available: www.legislation.gov.uk/uksi/2014/2868/contents/made. [Accessed 16 12 2024].

[85] “Misuse of Drugs Act 1971,” [Online]. Available: www.legislation.gov.uk/ukpga/1971/38/contents. [Accessed 16 12 2024].

[86] FCN, “Evidential Drug Identification Testing (EDIT) – Good Practice Guide 2023,” [Online]. Available: www.fcn.police.uk/news/2023-01/evidential-drug-identification-testing-edit-good-practice-guide-2023.

[87] “Offensive Weapons Act 2019,” [Online]. Available: www.legislation.gov.uk/ukpga/2019/17/contents/enacted. [Accessed 16 12 2024].

[88] “Explosive Substances Act 1883,” [Online]. Available: www.legislation.gov.uk/ukpga/Vict/46-47/3/contents. [Accessed 16 12 2024].

[89] “Chemical Weapons Act 1996,” [Online]. Available: www.legislation.gov.uk/ukpga/1996/6/contents. [Accessed 16 12 2024].

[90] “Biological Weapons Act 1974,” [Online]. Available: www.legislation.gov.uk/ukpga/1974/6/contents. [Accessed 16 12 2024].

[91] “Explosives Act 1875,” [Online]. Available: www.legislation.gov.uk/ukpga/Vict/38-39/17/contents. [Accessed 16 12 2024].

[92] “Explosive Regulations 2014,” [Online]. Available: www.legislation.gov.uk/en/uksi/2014/1638/contents/made. [Accessed 16 12 2024].

[93] “NPCC Framework for Footwear Coding v1,” [Online]. Available: https://fcn.police.uk/publications/npcc-framework-footwear-coding-v1. [Accessed 16 01 2025].

[94] “Firearms Act 1968,” [Online]. Available: www.legislation.gov.uk/ukpga/1968/27/contents. [Accessed 16 12 2024].

[95] “Terrorism Act 2000,” [Online]. Available: www.legislation.gov.uk/ukpga/2000/11/contents.

[96] “Counter-Terrorism and Border Security Act 2019,” [Online]. Available: www.legislation.gov.uk/ukpga/2019/3/2021-06-29.

[97] “Crime (Overseas Production Orders) Act 2019,” [Online]. Available: www.legislation.gov.uk/ukpga/2019/5/contents/enacted.

[98] National Police Chiefs' Council, “NPCC Framework for Video Based Evidence,” 2023. [Online]. Available:

https://library.college.police.uk/docs/NPCC/Framework-Video-Evidence-v3.1-2022.pdf . [Accessed 27 10 2023].

[99] Dstl, “Recovery and Acquisition of Video Evidence v3.0,” 15 6 2022. [Online]. Available: https://www.gov.uk/government/publications/recovery-and-acquisition-of-video-evidence/recovery-and-aquisition-of-video-evidence-v30. [Accessed 16 11 2022].

[100] Home Office, “Police and Criminal Evidence Act 1984 (PACE) codes of practice,” 23 02 2017. [Online]. Available: https://www.gov.uk/government/publications/pace-code-d-2017. [Accessed 22 07 2020].

[101] “Radioactive Substances Act 1993,” [Online]. Available: www.legislation.gov.uk/ukpga/1993/12/contents. [Accessed 16 12 2024].

[102] Forensic Science Regulator, “Forensic medical examination of sexual offence complainants (FSR-GUI-0020),” [Online]. Available: www.gov.uk/government/publications/forensic-medical-examination-of-sexual-offence-complainants. [Accessed 24 02 2025].

[103] Forensic Science Regulator, “FSR-GUI-0017 DNA contamination controls – Forensic medical examinations,” [Online]. Available: www.gov.uk/government/publications/dna-contamination-controls-forensic-medical-examinations. [Accessed 16 12 2024].

[104] GTFCh, “Guideline for quality control in forensic-toxicological analyses”.

[105] Forensic Science Regulator, “Non-Expert Technical Statement Guidance,” [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance. [Accessed 13 11 2023].

[106] M. Gaskell, J. Guiness and K. Sullivan, “Validation of consumables used in the recovery of DNA evidence within Sexual Assault Referral Centres (SARCs),” *Forensic Science International: Synergy,* vol. 9, no. https://doi.org/10.1016/j.fsisyn.2024.100559, 2024.

[107] Forensic Science Regulator, “Laboratory DNA: anti-contamination guidance,” [Online]. Available: www.gov.uk/government/publications/dna-contamination-controls-laboratory. [Accessed 29 11 2023].

[108] Forensic Science Regultor, “DNA contamination detection - The management and use of staff elimination DNA databases Guidance,” [Online]. Available: www.gov.uk/government/publications/dna-contamination-detection. [Accessed To be reissued].

[109] World Anti-Doping Agency, “Minimum Criteria for Chromatographic-Mass Spectrometric Confirmation of the Identity of Analytes for Doping Control Purposes - Technical Document – TD2023IDCR”.

[110] OJEC, “Commission Decision of 12 August 2002 implementing Council Directive 96/23/EC concerning the performance of analytical methods and the interpretation of results. (2002/657/EC).,” The Official Journal of the European Communities, 2002, L221/8..

[111] ANSI/ASB, “ANSI/ASB STANDARD 098,” [Online]. Available: www.aafs.org/asb-standard/standard-mass-spectral-analysis-forensic-toxicology.

[112] EWDTS, “European Guidelines for Workplace Drug Testing in Urine,” [Online]. Available: www.ewdts.org/data/uploads/documents/2022-10-ewdts-guidelines-urine-final.pdf. [Accessed 16 12 2024].

[113] International Laboratory Accreditation Cooperation, “ILAC G17: 01/2021 Guidelines for Measurement Uncertainty in Testing,” [Online]. Available: https://ilac.org/publications-and-resources/ilac-guidance-series/.

[114] Westgard, “Westgard Rules,” [Online]. Available: https://westgard.com/westgard-rules.html#howmrl. [Accessed 16 12 2024].

[115] Dstl, “Fingermark Visualisation Manual: notice of publication,” [Online]. Available: www.gov.uk/government/publications/fingermark-visualisation-manual-notice-of-publication. [Accessed 16 12 2024].

[116] Dstl, “Fingermark visualisation newsletters,” [Online]. Available: www.gov.uk/government/publications/dstl-forensic-publications. [Accessed 16 12 2024].

[117] *R v. Barnes [2005] EWCA Crim 1158.*

[118] Dstl, “Digital Imaging and Multimedia Procedure v3.0,” 16 11 2021. [Online]. Available: www.gov.uk/government/publications/digital-investigations-digital-imaging-and-multimedia-procedure/digital-imaging-and-multimedia-procedure-v30. [Accessed 16 11 2022].

[119] *R. v. Cooper [1998] EWCA Crim. 2258.*

[120] Crown Prosecution Service, “Legal guidance, exhibits: Video recordings,” [Online]. Available: www.cps.gov.uk/legal-guidance/exhibits.

[121] “The Interpretation Act 1978,” [Online]. Available: www.legislation.gov.uk/ukpga/1978/30/contents. [Accessed 16 12 2024].

[122] “Criminal Justice Act 2003,” [Online]. Available: www.legislation.gov.uk/ukpga/2003/44/contents. [Accessed 16 12 2024].

[123] “Legal Aid, Sentencing and Punishment of Offenders Act 2012,” [Online]. Available: www.legislation.gov.uk/ukpga/2012/10/contents.

[124] “Extradition Act 2003,” [Online]. Available: www.legislation.gov.uk/ukpga/2003/41/contents. [Accessed 16 12 2024].

[125] “Magistrates' Courts Act 1980,” [Online]. Available: www.legislation.gov.uk/ukpga/1980/43/contents. [Accessed 16 12 2024].

[126] United Nations, “Guidance for the Validation of Analytical Methodology and Calibration of Equipment used for Testing of Illicit Drugs in Seized Materials and Biological Specimens,” 2009. [Online]. Available: www.unodc.org/unodc/en/scientists/guidance-for-the-validation-of-analytical-methodology-and-calibration-of-equipment.html. [Accessed 01 09 2022].

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

[128] “Coroners and Justice Act 2009,” [Online]. Available: www.legislation.gov.uk/ukpga/2009/25/contents. [Accessed 16 12 2024].

[129] “Local Government Act 1972,” [Online]. Available: www.legislation.gov.uk/ukpga/1972/70/contents. [Accessed 16 12 2024].

[130] Casetext, “United States v. McConney,” [Online]. Available: https://casetext.com/case/united-states-v-mcconney/. [Accessed 16 12 2024].

[131] “Fire and Rescue Services Act 2004,” [Online]. Available: www.legislation.gov.uk/ukpga/2004/21/contents. [Accessed 16 12 2024].

[132] C. Tapper, “Cross & Tapper on Evidence,” Oxford University Press, 2010, 12th Edition.

[133] “Rehabilitation of Offenders Act 1974,” [Online]. Available: www.legislation.gov.uk/ukpga/1974/53/contents. [Accessed 16 12 2024].

[134] “Medical Act 1983,” [Online]. Available: www.legislation.gov.uk/ukpga/1983/54/contents. [Accessed 16 12 2024].

[135] “Sexual Offences Act 2003,” [Online]. Available: www.legislation.gov.uk/ukpga/2003/42/contents. [Accessed 16 12 2024].

102. Acronyms and abbreviations

Acronym/ abbreviation	Meaning
3D	Three dimensional
3G	Third generation
ACE	Analysis, comparison, and evaluation
ACE-V	Analysis, comparison, evaluation, and verification
Admin	Administrative Court
AFIS	Automated Fingerprint Identification System
AVI	Audio Video Interleave
BPA	Bloodstain pattern analysis
BS	British Standard
BSI	British Standards Institution
BZE	Benzoylecgonine
CCTV	Closed-circuit television

Acronym/ abbreviation	Meaning
CD	Compact Disc
CDI-SPoC	Communications Data Investigations Single Point of Contact
CDR	Call detail record or call data record
CJS	Criminal Justice System
CPS	Crown Prosecution Service
CrimPR	Criminal Procedure Rules
CRM	Certified reference material
CRT	Common Reporting Threshold
DAMS	Digital Asset Management System
DEMS	Digital Evidence Management System
DNA	Deoxyribonucleic acid
DNS	Domain name server
Dstl	Defence Science and Technology Laboratory
DV	A family of codecs and tape formats used for storing digital video
DVC	Digital video cassette
DVD	Digital Versatile Disc
DVR	Digital video recorder
EDIT	Evidential Drug Identification Testing
eFIT	Electronic Facial Identification Technique
EM	Electro-magnetic
EMS	Environmental monitoring sampling
ENF	Electrical network frequency
ENFSI	European Network of Forensic Science Institutes
EU	European Union
EWCA	England and Wales Court of Appeal
EWHC	High Court of England and Wales
EXIF	Exchangeable image file
F.2d	Federal Reporter
FAR	False alarm rates
FSA	Forensic science activity
FSM	Forensic Scene Manager
FSR	Forensic Science Regulator

Acronym/ abbreviation	Meaning
FSREU	Forensic Science Regulator Expanded Uncertainty
FTP	File transfer protocol
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSR	Gunshot residue
HDTV	High-definition television
HM	Her Majesty's, His Majesty's
HOC	Home Office Circular
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
ID (Cell ID)	Identification
IEC	International Electrotechnical Commission
ILAC	International Laboratory Accreditation Cooperation
ILC	Inter-laboratory comparison
INTERPOL	The International Criminal Police Organization
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Organization for Standardisation
IT	Information technology
LevelDB	An open source on-disk key-value store, not an acronym
LLOQ	Lower limit of quantification
LOD	Limit of detection
NABIS	National Ballistics Intelligence Service
NLTF	Not less than figure
NPCC	National Police Chiefs' Council
NPPV	Non-Police Personnel Vetting
NTSC	National Television System Committee, a television standard
PACE	Police and Criminal Evidence Act 1984
PAL	Phase Alternating Line
PAS	Publicly Available Specification
PCR	Polymerase chain reaction
PD	Probability detection

Acronym/ abbreviation	Meaning
PDF	Portable document format
Plist	Property List
PPE	Personal protective equipment
PT	Proficiency test
QC	Quality control
QMS	Quality management system
R	Regina or Rex
RF	Radio frequency
SAI	Senior Accountable Individual
SC	Security Check
SDM	Standard deviation of the mean
SECAM	Séquentiel de couleur à mémoire, an analogue colour television system
SFR	Streamlined Forensic Report
SI	International system of units, Statutory Instrument
SLA	Service level agreement
SMTP	Simple Mail Transfer Protocol
SQLite	A relational database management system, which uses Structured Query Language
STR	Short Tandem Repeat
TCP	Transmission Control Protocol
TLS	Transport Layer Security
.UFDR	File extension created by UFED Physical Analyzer
UFED	Universal Forensics Extraction Device, a product series by Cellebrite
UK	United Kingdom of Great Britain and Northern Ireland
UKAS	United Kingdom Accreditation Service
ULOQ	Upper limit of quantification
USB	Universal Serial Bus
VHS	Video Home System
VOB	Video Object
VSS	Video surveillance system

Acronym/ abbreviation	Meaning
WADA	World Anti-Doping Agency
Wi-Fi	A wireless network protocol, not an actual acronym.
WLR	Weekly Law Reports
WPA	Wi-Fi Protected Access
Y-STR	Y-chromosome short tandem repeat

103. Glossary

The Act	The Forensic Science Regulator Act 2021 [1].
Accredit(ation)	Procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks.
Accuracy	Ability to get the true result (see True value). For quantitative tests, the accuracy expresses the closeness of agreement between the true value and the value obtained by applying the test procedure a number of times [127].
Administrative check	A review to establish that the records/reports comply with the forensic unit's policies with regard to content and structure of such documentation.
Allele	A genetic variant at a particular location within a person's genome.
Analogue video	Video that is in non-digital form and the maximum detail is determined by the frequency response of the analogue system. It is generally stored on magnetic tape and as such shall be regarded as being fragile since repeated use may result in damage and/or degradation.
Analysis	The term 'analysis' refers to any form of test, comparison or analytical method performed on an item/exhibit or relevant material recovered from an item/exhibit.

Analyte	Substance to be identified or measured; in digital forensic science it may be taken to include data as the focus of the analysis.
Artefact	Something observed in an examination or analysis that was not originally present but occurs as a result of the procedures employed for examination or analysis.
Assessment	The application of expert judgement to devise an examination strategy (see Examination strategy) based upon a framework of circumstances in the form of written submission details, photographs, ‘preview’ examinations of items, discussions with submitting officers etc., that addresses in an effective way the identified key issues in the case.
Attribution (digital)	Attribution is the process of attempting to assign a device to an individual and may be progressed through a number of different methods, each method having different risks. Cell site analysis may be one method by which patterns of usage may be assessed against what would be expected if a given device was used by a specific person, as opposed to if it was not used by that person.
Attribution (biological material)	Determination based on; the physical appearance of the material; characteristics of DNA profiling results including extraction method; and presumptive and/or confirmatory test results, of whether a DNA profile or part of a DNA profile can be said to have originated from a specific type of biological material.
Audit	A systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which specified criteria are fulfilled. In forensic

	science an audit usually involves determining whether the forensic unit's quality procedures have been complied with.
Audit (external)	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 commissioning parties, 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 [128].
Audit (internal)	Sometimes called a first-party audit, conducted by, or on behalf of, the organisation itself for internal purposes.
Best serving cell	An engineering term referring to the cell selected by a device at a given time for service, disregarding other cells that may also serve. The use of this phrase is misleading in the forensic arena, as it implies only a single cell would usually be available to provide service at any given location. Caution should be given if this phrase is encountered; it should not be used in reports unless a full description of the limitations of usage is provided.
Blank	A sample containing no detectable amount of the analyte of interest, used in analysis for detecting the background level of the analyte in the matrix or contamination (see Negative control).
Broadcast video	Video material from one of the four broadcast and video standards and recording formats commonly in use around the world: NTSC, PAL, SECAM and HDTV. Tools for broadcast video typically assume a fixed frame rate and a limited set of image sizes and pixel aspect ratios.

Biological material	Material that originated from the body of a human. For the purposes of FSA – BIO 200 and FSA – BIO 201 this includes; hair, bone, muscle, teeth, blood, saliva, semen, faeces, urine, vaginal material, cellular material, and vomit.
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.
Case assessment	See Assessment.
Casework sample	Material of unknown origin believed to have originated from a person of interest (suspect or victim), a location, a specific item/source or illegal substance, sometimes referred to as the questioned sample.
Cell ID	A number used in cell site analysis that uniquely identifies the cell for a given network operator.
Certificate	A specific format for evidence allowed by certain statutes. For example, a certificate issued under the provisions of section 16 of the Road Traffic Offenders Act 1988 [69] can be used to establish the concentration of alcohol in samples.
Code	The code of practice issued under the provisions of s2 of the Act [1].
Cognitive bias	A pattern of deviation in judgement whereby inferences about other people and situations may be drawn in an illogical fashion. These include expectation, confirmation, contextual and motivational biases, anchoring effects or focalism (related to expectation and confirmation biases), role effects (e.g. adversarial roles) and reconstructive effects (rely on memory rather than contemporaneous notes).

Collaborative Exercises	Comparisons between forensic units usually designed to address specific issues such as troubleshooting, method validation or characterization of reference materials. They may also be used for monitoring of laboratory performance and/or interpretation, although that is more typically through proficiency testing. [63]
Competence	The skills, knowledge and understanding required to carry out a role, evidenced consistently over time through performance in the workplace. The ability to apply knowledge and skills to achieve intended results.
Complainant	A person who makes a complaint or allegation that a criminal offence has, or may have, occurred.
Complaint	In relation to the work of a forensic unit means any expression of negative feedback.
Compliance action	Action taken by the Regulator under the provisions of ss6–8 of the Act [1].
Consumable	Materials (other than items/exhibits), including equipment and chemicals, which are either consumed or used once and disposed of.
Contaminant	Any substance not relevant to examination and/or analysis of a particular evidence type, but that is present on the item/exhibit and may interfere with the examination/analysis.
Contamination	The undesirable introduction of material to an item/exhibit or sample which is to be examined/analysed.
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.
Controlled drug	Any substance which is listed (by name or by virtue of its chemical structure) in any Schedule to the Misuse of Drugs Act 1971 [85].
Coroner	Any person falling within the classes below: a. The Chief Coroner. b. A person holding the position of Senior Coroner, Area Coroner or Assistant Coroner under the provisions of the Coroners and Justice Act 2009 [129]. c. Any person exercising the functions of a coroner in a particular case.
Criminal investigation	Anything falling within the definition of ‘detecting and/or investigation of crime’ in section 100.6.3 of this Code.
Criminal Justice System	This comprises the structures in place in England and Wales to detect/investigate crime, prosecute criminal offences, investigate potential miscarriages of justice and consider any appeals against conviction and/or sentence. It does not cover the systems and/or processes which deal with the punishment and/or rehabilitation of convicted persons.
Criminal proceedings	A proceeding falling within the definition in section 100.7.2 of this Code.

Critical data	Data that are identified during the risk assessment process as crucial to the method and/or finding, particularly in terms of the accuracy or traceability, therefore protection steps should be in place to reduce the risk of irretrievable loss or data corruption.
Critical findings	Findings or results that: a. Have a significant impact on the opinion provided; and b. Cannot be repeated or checked in the absence of the item/exhibit or sample, or after completion or conclusion of the examination of an incident, fire, collision or explosion scene; and/or. c. Could be interpreted differently by a suitably qualified practitioner in the FSA in question.
Critical findings check	A check on any critical finding to ensure they are acceptable.
Data	Information which in the context of clauses in this document referring to protection or loss is not restricted to inputs or readings, and may include all information, particularly when stored electronically (e.g. a QMS document when on a server is data, but it would rarely be referred to as data if printed or even while being viewed).
Database	A collection of information (often but not exclusively electronic) in a structured format allowing searching which may be used for purposes of interpretation.
Dedicated facilities	A site (whether permanent or temporary), or part of a site, owned or controlled by the forensic unit, which is routinely used for undertaking one or more FSAs.
Detection and/or investigation of crime	Anything falling within the definition in section 100.6.3 of this Code.

Detainee	Any individual detained (whether arrested or not) by a body involved in the detection and/or investigation of crime as part of the investigation/prosecution of crime.
Developmental validation	The validation typically performed on a new or novel methodology (typically by the developer of the method but) sometimes involving collaboration on aspects of the validation study by the community depending on the scale required, e.g. introduction of a new DNA analysis chemistry.
Digital Asset Management system (DAMs)	A searchable repository usually of 'media', such as audio, video and photo files. These systems often include input and output decoders deployed automatically when items are added to or exported from the system. This may or may not be hosted locally.
Digital Evidence Management system (DEMs)	Similar to a Digital Asset Management system but optimised for storing evidence and related files.
Digital metadata	The file system information of the file, any other external information about the data, e.g. an image file and any data contained in the image file beside the pixel data.
Digital object	A discrete digital structure that contains meaningful data.
Disposable equipment	A sub-class of consumable. Equipment which is used once and then disposed of.
DNA artefact	Artefacts are 'nuisance' peaks in a profile; often associated with the amplification and detection processes, such as spikes, dye blobs, spectral pull-up. They do not represent genuine alleles.
DNA clean area	Area in which appropriate DNA contamination prevention measures shall be maintained at all times.

DNA profile	A format for the representation of an individual's genetic information that can be compared to other profiles, e.g. stored on a database.
Drop-in	Additional random alleles present in a profile originating from random fragmented sources and regarded as independent events.
Drug	Any substance which has a physiological effect when introduced to the human body.
Elimination database	Collection of DNA profiles or friction ridge detail held in a searchable format from personnel and visitors (e.g. service engineers) whose access/role/activities are deemed to be a potential contamination risk. The data are used to identify instances of inadvertent contamination.
End user	Anyone who works within a forensic unit or the CJS who will receive the output from a forensic unit.
England	Subject to any alteration of boundaries under Part IV of the Local Government Act 1972 [130], the area consisting of the counties established by section 1 of that Act, Greater London and the Isles of Scilly. See the Interpretation Act 1978 [122].
Enhancement	The application of process(es) to reveal additional detail or make that which is already visible more readily distinguishable from the background.
Environmental monitoring	Routine (at scheduled intervals) or ad hoc targeted, based on risk sampling to monitor for introduced or background contamination resulting from the environment. This monitoring serves to assess and facilitate control of contamination levels under normal operating (and storage) conditions through identifying any trends and potential

	issues that may indicate improvement is required to the anti-contamination measures in place.
Error	Anything which affects the accuracy and/or precision of an observation.
Evaluative opinion	An opinion on the value of the findings, based upon a pair of case-specific propositions and clear task relevant information (framework of circumstances) that is provided for use as evidence in court (other than as agreed facts). In this Code the term refers only to opinions based on propositions at the activity, source and sub-source level as defined.
Evidence	Anything which is (or may be) admissible in criminal proceedings to assist the court in making any decision. This includes physical items/exhibits and information. The convention has been adopted that the 'evidence' will be used to describe the reporting of the facts and opinions related to findings to the CJS.
Evidence of fact	Evidence which contains statements of fact only.
Evidence of opinion	Evidence which contains opinion.
Examination	The convention has been adopted that the term 'examination' refers to the investigation of an item/exhibit, person or location with the intention of locating, identifying and recovering material or information of interest.
Examination strategy	A documented plan of work designed to meet the needs identified through a case assessment. The term 'examination strategy' has been used for some time to cover all work planned in the case and is used in that sense in this document.

Exhibit	A sub-class of item which is presented or identified as evidence in a court of law.
Exigent circumstances	Exigent circumstances are circumstances which: a. could not have been prevented by reasonable preparation; and b. would cause a reasonable practitioner to believe that prompt action was necessary to prevent physical harm to persons, prevent crime, prevent destruction of relevant evidence, and/or frustrating the interests of justice. Exigent circumstances persist only until it becomes practicable to return to the use of normal methods. This definition is based on *United States v. McConney* 728 F.2d 1195 (9th Cir. 1984) [131].
Expert	A practitioner who is competent to provide evidence of opinion in the CJS in relation to an FSA.
Explanation	A proposition (theory) that can account for scientific findings. It is formulated after the scientific findings have been obtained and may be useful in generating investigative opinions.
Externally provided services	Any service provided to a forensic unit from outside the forensic unit.
Fact	A truth known by actual experience or observation; something known to be true.
Fact in issue	Those purported facts that the prosecution is required to prove or disprove in order to establish the guilt of the accused and those facts the defence asserts or seeks to put in play.

Femtocell	A low-power cellular base station serving a small area such as a home, office or small business.
Finding(s)	The results of the examination and analyses carried out according to the documented examination strategy.
Fire and rescue service	Any service maintained by a Fire and Rescue Authority under the provisions of the Fire and Rescue Services Act 2004 [132].
Forensic DNA grade	DNA consumables that are compliant with the requirements set out in BSI PAS 377:2023 [13] and/or ISO 18385:2016 [14].
Forensic healthcare practitioner	The term used to describe forensic physicians (including paediatricians), forensic nurse examiners, forensic midwife examiners and forensic paramedics.
Forensic medical examination	Activity or process of observing, assessing, prioritising, recording and collecting samples from a patient for scientific analysis, documenting injuries and interpreting with reference to sexual offences.
Forensic post-mortem	A forensic pathology examination in cases where there is, or is likely to be, an investigation leading to serious criminal charges and information from the post-mortem examination may be used in the investigation or in court proceedings. A forensic post-mortem can assist a coroner and/or police force with determination of: a. the identification of the deceased; b. the cause and circumstances of the death; and c. whether a criminal offence has occurred.

Forensic science activity	Is defined in the Act as any activity relating to the application of scientific methods for the detection or investigation of crime in England and Wales and/or the preparation, analysis and presentation of evidence in criminal proceedings in England and Wales and or any other purpose specified by the Secretary of State in regulations.
Forensic science activity subject to the code	Any FSA for which the specified FSA states that compliance with the Code is required.
Forensic Science Regulator	The Regulator appointed under the provisions of the Forensic Science Regulator Act 2021.
Forensic unit	A legal entity or a defined part of a legal entity that performs any part of an FSA (see ILAC-G19 [6]). Historically the term 'forensic science provider' has been used. This is not considered appropriate as a forensic unit is often a sole practitioner or a small group which may, for accreditation purposes, be viewed as a legal entity.
Geolocation	Determining the approximate physical location of object(s) or device(s); this may be relatively precise depending on the technology, or even an area or region.
Ground truth data	A data set made from known source material. Examples of data where the truth is known (not inferred) include datasets created from known donors of samples (such as DNA extracted and analysed from stains produced using body fluids from known donors) or call data records created by staged calls at specific coordinates.
Haplotype	A group of alleles that are inherited together from one parent. The Y-chromosome represents a single haplotype inherited from father to son.

Ignitable liquid	Any liquid that is capable of burning and has a measurable flash point. A flash point is the lowest temperature at which a liquid will give off sufficient vapour to momentarily support a flame.
Image enhancement	A transformation of a pictorial image that seeks to increase the value of the information of interest that potentially diminishes other information. Enhancement may actually reduce the information content of the imagery but can aid its interpretation.
Imagery	A general term that denotes still and/or video images.
Infrequently used method	Methods used once in every three-month period across a forensic unit in separate cases are considered to be infrequently used.
Inter-laboratory comparison	A widely recognised generic term for an exercise carried out between a group of organisations conducting comparable testing activities. In the Code, laboratory means the forensic unit.
International standard	A standard published by the International Organization for Standardization.
Interpretation	The consideration of the findings from the work implementing the examination strategy. Interpretation may be investigative, evaluative or, in certain circumstances, categorical.
Investigation	When referring to action by the Regulator means an investigation employing powers under s5 of the Act.
Investigative opinion	An opinion that arises in casework and in which explanations are generated to account for findings. The provision of an

	explanation for an observation is termed an investigative opinion.
Item	Anything that is submitted, recovered, collected, sampled or derived as part of the forensic process.
Lachrymator	A substance that may be used in an attack with the intent of causing irritation to the eyes. The following are examples of lachrymators: a. (6E)-N-[(4-Hydroxy-3-methoxyphenyl)methyl]-8-methylnon-6-enamide. b. N-[(4-Hydroxy-3-methoxyphenyl)methyl]nonanamide. c. (2-Chlorophenyl)methylidene]propanedinitrile. d. Dibenzo[b,f][1,4]oxazepane. e. 2-Chloro-1-phenylethan-1-one. f. (phenacyl chloride). g. 1-Bromopropan-2-one. h. Xylyl bromide.
Latent print/mark	Transferred impression of friction ridge detail not readily visible.
Law enforcement agency	A body defined as a law enforcement agency in section 100.6.4 of this Code.
Medical practitioner	See Registered medical practitioner.
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).
Miscarriage of justice	A term that covers the following: a. An unsafe conviction. b. A wrongful acquittal. c. Inability to bring an offender to justice. d. Delaying bringing an offender to justice. e. Inability to clear the innocent. f. Delaying the clearing of the innocent.
Network perimeter	The secured boundary between the private and locally managed side of a network, often a company's intranet, and the public-facing side of a network, often the Internet.
Non-conformity	The non-fulfilment of a requirement.
Non-dedicated facilities	A facility (whether permanent or temporary) where an FSA is undertaken which falls within a description below: a. is not owned or controlled by the forensic unit; or b. is not routinely used for undertaking an FSA.
Non-Statutory Forensic Science Regulator	The role which operated before the creation of the Forensic Science Regulator under the provisions of the Act [1].
Observation check	A check that findings being recorded by a practitioner are acceptable (e.g. that the interpretation of the output from a method are sound).
Off-site	Away from the dedicated facility (or if authorised, the non-dedicated work area (see 29.1).

Opinion	An inference drawn from perceived facts (based on views from a legal standpoint [133]).
Pathologist	A registered medical practitioner who holds, or is working towards obtaining, specialist registration with the General Medical Council as a histopathologist or pathologist.
Patient	In the context of 'Sexual assault examination: requirements for the assessment, collection and recording of forensic science related evidence' (section 91 91), a patient is an individual subjected to or suspected of being subjected to a sexual offence(s).
Peer review	A complete check of the work done involving reviewing all of the analytical work. It does not include re-analysing the items/exhibits.
Person	Any person, including a body of persons corporate or unincorporate. See Interpretation Act 1978 [122].
Personnel	Any individual working within or on behalf of a forensic unit (whether employed by the forensic unit or not). The term covers practitioners and others such as administrative staff and site support staff.
Personal protective equipment	Barrier clothing and gloves that are used to prevent skin and mucous membrane exposure when in contact with blood and body fluid(s) on or from any person. PPE is also worn to protect the practitioner from contact with harmful chemicals, e.g. during decontamination and to minimise the chance that the wearer causes inadvertent contamination.
Photogrammetry	Attempts to compare the proportional relationships of one photo usually using metrics. Related terms include videogrammentry, photoanthropometry and to a lesser extent proportional alignment.

Practitioner	An individual (whether an employee of the forensic unit or not) who is directly involved in undertaking an FSA.
Precision	Closeness of agreement between independent test results obtained under prescribed conditions [127].
Presumptive test	A rapid and often simple preliminary test to establish the possibility that a specific analyte is present often for screening purposes. Many presumptive tests are simple colour change tests, however certain devices used as screening tools and may also be considered presumptive tests if validated for that purpose e.g. portable raman spectrometers.
Primary review	A review which occurs as part of the originally commissioned work by a forensic unit.
Proceedings	Proceedings before a judicial authority including any of the ordinary courts of law, any tribunal, body or person having power to determine any question affecting the rights, privileges, obligations or liabilities of any person, or to receive evidence affecting the determination of any such question. This power may be exerted: a. by virtue of any enactment, law, custom or practice; b. under the rules governing any association, institution, profession, occupation or employment; or c. under any provision of an agreement providing for arbitration with respect to questions arising thereunder. See s5(11) of the Act [1] and s4(6) of the Rehabilitation of Offenders Act 1974 [134].
Professional judgement	The application of professional knowledge and experience to reach a conclusion or recommendation about a situation.

	Professional judgement involves considering the information available, the professional standards, the legal and the ethical principles that are relevant to the situation. Professional judgement also requires an element of decision-making and problem-solving
Proficiency test	The determination of the testing performance of a forensic unit, i.e. tests to evaluate the competence of practitioners and the quality performance of the forensic unit. These tests can vary: a. external proficiency test: a test conducted by an agency independent of the practitioner or forensic unit being tested; b. blind or undeclared proficiency test: a test in which the practitioners are not aware that they are being tested; and c. open or declared proficiency test: a test in which the practitioners are aware that they are being tested.
Prosecutor's fallacy	Also known as the 'fallacy of the transposed conditional' or 'confusion of the inverse', this is a fallacy of reasoning. It is where the conditional part of the assertion and its probable result are moved around so it no longer remains true.
Proof read	A check to ensure a document is properly written and that the English and grammar are acceptable.
Proposition	A statement that is either true or false and is generated, in part, from the background information but may also depend upon the findings that have been made at the alleged crime scene (or other information obtained before consideration by the expert).

	In the context of a criminal trial there will most often be a pair of propositions – one representing the prosecution's position, the other representing the defence's position in relation to a particular issue. Propositions shall be mutually exclusive (i.e. if one is true then the other can only be false) and will often, but not always, be exhaustive (i.e. they cover all possibilities within the framework of circumstances of the case).
Prosecuting authority	A body defined as a prosecting authority in section 100.6.5 of this Code.
Psychoactive substance	Any substance which is a psychoactive substance within the provisions of the Psychoactive Substances Act 2016 [80].
Qualitative	A description of an examination/analysis that results in findings that cannot be expressed numerically.
Quality management system	Documentation of a forensic unit's policies, systems, procedures and instructions to the extent needed to assure the quality of its results, to meet relevant jurisdictional, regulatory and safety requirements and to satisfy the needs of the clients. It covers the overall activities of the unit, including sampling, analysis and reporting, whether these are within the main unit facility itself, in mobile/temporary facilities or at external locations such as a clandestine laboratory, the roadside or the locus of a large drug seizure.
Quantitative	A description of an examination/analysis that results in findings that can be expressed numerically.
Radio Frequency Propagation Survey	A survey that captures details of cell coverage and/or the cells that can be detected at specific locations using equipment ranging from phones with specific applications and phone emulators to scanners. The closeness to the time

	of the event of interest and the survey strategy may dictate the overall usefulness of the survey to the investigation.
Reagents	A substance used in a chemical reaction.
Reference collection	A collection of material or information (whether physical or electronic) which is maintained by a forensic unit to support the undertaking of any FSA.
Reference sample	A sample obtained from a known person, location or item that is used for the purpose of comparison against an unknown questioned or casework sample.
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.
Registered medical practitioner	A fully registered practitioner with the General Medical Council within the meaning of the Medical Act 1983 [135] who holds a licence to practise under that Act. See Interpretation Act 1978 [122].
Regulator	The Forensic Science Regulator appointed under the provisions of the Act [1]. See also Non-Statutory Forensic Science Regulator.
Relevant party	Any person who is a party in the case (e.g. the prosecution and the defence), any person directly involved in the use of the output (e.g. law enforcement bodies, the Criminal Cases Review Commission) or the CJS.

Replay software	Proprietary replay software that has been developed and distributed by the system's manufacturer to be compatible with the codec used to encode/decode their video format.
Report	Any written document (including certificates, SFR and statements) setting out the practitioner's findings, conclusions and/or evidence. A statement admissible under s9 of the Criminal Justice Act 1967 [11] is one form of report.
Reverse engineering	The process of deconstructing and interpreting an electronic device or data format without prior access to the creator's specification or design.
Review	A re-assessment or re-evaluation of any of the following: a. Findings from an examination/analysis. b. Evaluation/interpretation of findings from an examination. c. Contract requirements (includes MoU, SLA etc.). d. Process.
Re-working	A complete repetition of the work undertaken in an FSA or part of an FSA.
Routinely	Not 'infrequently used'.
Sample	A part of an item/exhibit or reference material which is selected for examination/analysis.
Schedule of accreditation	A document issued by the national accreditation body specifying the examinations or tests the forensic unit has been accredited for, and for which it could issue certificates or reports bearing the testing mark.

Senior Accountable Individual	A role to be filled in each forensic unit as a result of section 6 of this Code.
Sexual offence	An offence contrary to the provisions of the Sexual Offences Act 2003 [136] and any offence which is related to an offence under the Act (e.g. conspiracy, attempt, assisting or encouraging).
Streamlined Forensic Report	A case management procedure for producing scientific evidence at court whilst seeking to reduce unnecessary costs, bureaucracy and delays in the CJS.
SFR1	An SFR which is intended to provide a summary of the practitioner's evidence. An SFR1 is not admissible as evidence other than as agreed fact.
SFR2	An SFR, usually issued after questions have been raised about information provided in an SFR1.
Short tandem repeat	A short repetitive DNA sequence where the repeats are adjacent to each other.
Specialists from outside the forensic science profession	An individual from outside the forensic science profession occasionally called to give evidence on an aspect of an FSA covered by the Code.
Sporadic contamination	Unpredictable, erratic contamination event of unknown cause during examination and/or analysis. This may arise due to contamination of consumables which is not detected by quality control batch testing of those consumables prior to use in an FSA or the introduction of an analyte of interest into a blood sample or analytical method in an unknown and unpredictable way.
Standard method	Published by certain prescribed organisations and has the following characteristics:

	a. it contains concise information on how to perform tests; b. it does not need to be supplemented or rewritten as internal procedures; and c. it can be used as published by the operating personnel in a laboratory. Even if a method were to be recognised as standard, the requirement is for the forensic unit to demonstrate with objective evidence that it is appropriate/valid and verify it can properly perform the method to achieve the required performance.
Standard operating procedure	A written procedure that describes how certain examination or test activities are carried out in a given forensic unit.
Standards of conduct	The standards of conduct contained in section 34 of this Code.
Standards of practice	The standards of practice set out in part C of this Code.
Statement (CJS)	One form of report which complies with the provisions of s9 of the Criminal Justice Act 1967 [11].
Taggant	Coding material used to mark objects or persons.
Technical (factual) reporting	The reporting of findings based solely on the technical competence of the individual. No inferences/explanations (opinion) are drawn from the findings. An example would be where a digital forensics practitioner has used a specified software tool to extract data from a mobile phone. A factual report explains what the practitioner has done and the findings, such as a list of the files of a certain type that were retrieved. It offers no opinion on how the files came to be on the device or whether any of their content is relevant to a fact in issue in the case.

Test-impression	A mark made with a suspect item for comparison with a mark recovered from an incident scene to establish, or otherwise, whether the item could have made the mark.
Testing	The determination of one or more characteristics according to a procedure and, although typically quantitative, it can be qualitative (e.g. a presumptive test with a colour change).
Timed expiry	A feature of DVRs that allows the equipment to adhere to data retention policies that may be mandated in certain parts of the world and that result in video data becoming inaccessible after a certain date. This may happen even when the DVR is switched off.
Tracking	In the context of video, moving objects or people are often tracked through a scene by applying arrows or highlights on a digital editing suite in order to draw attention to the object or person of interest.
Transcription check	A check to ensure that any data transferred between any records and/or systems has been transferred correctly.
Transcoding	The process of converting a file from one form of coded format to another.
True value	Value that characterizes a quantity perfectly defined in the conditions which exist when that quantity is considered. The true value of a quantity is an ideal concept and, in general, cannot be known exactly [127].
Uncertainty of measurement	The estimation of the uncertainty of measurement is a Codes and accreditation requirement and is 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 is fit (or remains fit) for the specific purpose intended. The forensic unit shall demonstrate the reliability of the procedure in-house against any documented performance characteristics of that procedure.
Video Surveillance Systems	A term to refer to all relevant components of a system intended to capture video in a private or public setting including the cameras and video storage, including but not limited to public space camera and cameras mounted on a vehicle dashboard. It is analogous to a closed-circuit television (CCTV) system, recognising some systems are no longer ‘closed circuit’.
Video transformation	Any process that alters the format or information content of video (e.g. transcoding, enhancement, printing, rendering to computer display). Many transformations add or remove information from the video material.
Wales	The combined area of the counties which were created by section 20 of the Local Government Act 1972 [130], as originally enacted, but subject to any alteration made under section 73 of that Act (consequential alteration of boundary following alteration of watercourse). See Interpretation Act 1978 [122].
Wi-Fi	A local area network that uses high frequency radio signals.

104. Highlighted changes

104.1.1 To comply with the Regulations on accessibility to not convey information only with colour, a list of changes highlighted in text are set out below:

1.1.1, 1.1.2, 1.1.3, 1.3.3, 1.3.5, 1.4.1, 1.4.3, 1.4.5, 1.4.6, 1.4.7, 1.5.1, 1.7.1, 1.7.2, 1.7.3, 1.7.4, 1.7.5, 2.1.2, 2.1.3, 3., 3.1, 3.1.1, 3.1.2, 3.1.3, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6, 3.3, 3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.4, 3.4.1, 1.5, 1.1, 5.1.2, 6.2.1, 6.3.2, 7.1.3, 7.1.4, 7.3.2, 6.3, 7.3.3, 7.1, 7.4.2, 7.4.3, 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.2, 8.2.1, 8.2.2, 8.2.3, 8.3, 9., 9.1.1, 9.1.2, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.2.1, 9.2.2, 10., 10.1.1, 11.1.1, 11.1.2, 11.1.3, 12.1.5, 13.1.1, 13.1.2, 13.1.3, 13.1.4, 13.1.5, 15.1.1, 16.1.1, 16.1.2, 16.1.3, 18.1.2, 18.2.1, 18.2.2, 18.2.3, 18.2.4, 18.2.5, 18.2.6, 18.2.7, 18.2.9, 18.2.10, 18.2.11, 19.1.2, 19.2.1, 19.2.2, 19.2.4, 19.2.7, 19.2.8, 19.2.9, 20.1.1, 20.1.3, 20.1.4, 20.2.1, 20.2.2, 19., 20.2.8, 20.2.9, 20.3.1, 20.3.2, 20.3.3, 20.3.4, 20.3.5, 20.4.1, 20.4.2, 20.4.3, 20.4.6, 20.4.8, 20.4.9, 20.4.10, 20.4.11, 20.5.1, 20.5.2, 20.5.3, 20.5.4, 21.1.2, 21.1.4, 21.2.1, 21.2.2, 22.1.1, 22.1.2, 22.1.3, 22.1.4, 22.2.1, 22.2.3, 22.2.4, 22.2.5, 22.2.6, 22.3.1, 22.3.2, 22.3.3, 23.1.1, 23.1.3, 23.1.4, 23.2.1, 23.2.2, 23.3, 23.1, 23.3.1, 22.2, 23.3.4, 23.3.5, 23.3.6, 23.3.7, 23.3.8, 23.3.9, 23.3.10, 23.3.11, 23.3.12, 24.1.1, 24.1.2, 24.1.4, 24.1.5, 24.1.6, 24.2.1, 24.2.2, 24.2.4, 24.2.5, 24.2.6, 24.2.7, 24.2.9, 24.2.10, 24.2.11, 24.2.12, 24.2.13, 24.2.14, 24.2.15, 24.2.16, 24.3, 24.3.1, 24.3.2, 24.3.4, 24.3.8, 24.3.9, 24.4.1, 24.4.3, 24.4.5, 24.4.6, 24.5.1, 24.6.2, 24.6.4, 24.6.5, 24.7.1, 24.8.1, 24.9, 24.9.1, 24.9.2, 24.9.3, 24.9.6, 24.9.8, 24.9.9, 24.9.10, 24.9.12, 24.9.15, 24.9.16, 24.4, 24.9.18, 24.10.1, 24.11.2, 24.11.3, 24.12, 24.12.2, 24.12.3, 24.12.4, 24.13, 24.13.1, 24.13.2, 24.13.3, 24.14, 24.14.1, 24.15.1, 25., 25.1.1, 25.1.2, 25.1.3, 25.1.7, 26.1.2, 26.1.3, 26.2.1, 26.2.6, 26.4.5, 26.9.8, 26.10.4, 29.2.8, 29.2.10, 29.2.11, 29.3.4, 29.3.7, 30.1, 30.1.1, 30.1.2, 30.1.3, 30.1.4, 30.1.5, 30.1.6, 30.1.7, 30.1.8, 31.1.2, 31.1.3, 31.1.4, 31.1.7, 31.1.8, 31.2.1, 31.2.2, 31.2.3, 31.2.4, 31.2.5, 31.3.1, 31.3.2, 31.3.3, 31.3.4, 31.3.6, 31.4.1, 31.4.2, 31.4.3, 31.4.5, 31.1, 31.4.6, 31.4.7, 31.4.8, 31.4.9, 32.1.1, 32.1.2, 32.1.3, 33.1.4, 33.1.6, 33.1.7, 33.1.8, 33.1.10, 34.1.1, 35.1.1, 35.2.1, 35.2.2, 36.1.1, 36.1.2, 36.2.1, 36.2.2, 37.2, 37.2.1, 37.3, 37.3.1, 39.1.1, 39.2.1, 39.2.2, 39.2.3, 39.3.1, 39.4.3, 40., 40.2.1, 40.2.2, 40.3.2, 41., 41.1.1, 41.2.1, 41.3.1, 41.3.2, 41.4.1, 41.4.4, 41.4.5, 42., 42.1.1, 42.2.1, 42.3.1, 42.4.2, 42.4.3, 42.4.4, 43., 43.2.1, 44., 44.2.1, 45., 45.2.1, 45.3.2, 45.4.1, 45.5.1, 46.2.1, 46.3.1, 47.2.1, 47.2.2, 47.3.2, 48.2.1, 48.2.2, 48.3.2, 49.2.1, 49.2.2, 50.2.1, 50.3.1, 50.4.1, 50.5.1, 51.2.1, 52.2.1, 52.4.2, 53.2.1, 53.3.2, 54.2.1, 54.4.1, 54.4.2, 55.2.1, 55.3.2, 55.4.1, 55.4.2, 55.4.5, 56.2.1, 56.3.2, 57.1.1, 57.2.1, 57.2.2, 57.3.1, 57.3.2, 57.4, 57.4.1, 58.2.1, 58.2.2, 58.1, 58.4.2, 59.2.1, 60.2.1, 60.3.2, 61.2.1, 62.2.1, 63.2.1, 63.4.2, 64.2.1, 64.3.2, 65.2.1, 65.3, 65.3.2, 66.2.1, 66.3.1, 66.3.2, 66.4.4, 67.2.1, 67.3.2, 68.1.1, 68.2.1, 69.1.1, 69.2.1, 70.1.2, 70.2.1, 70.3.1, 70.3, 70.3.2, 70.4.1, 70.4.2, 70.4.3, 70.5.1, 71.2.1, 71.2.2, 71.4, 71.4.1, 72.1.1, 72.2.1, 72.2.2, 72.3.2, 72.4.1, 72.4.2, 72.4.3, 72.5.1, 73., 73.2.1, 73.3.1, 73.3.2, 73.4.1, 73.5.1, 74., 74.1.1, 74.2.1, 74.3.1, 74.2, 74.3.2, 74.4.1, 74.4.2, 74.5.1, 75.1.1, 75.3.1, 75.4.1, 75.4.2, 75.4.4, 76.1.1, 76.1.2, 76.3.1, 76.4.1, 77, 77.1.2, 77.4.2, 77.5.1, 78., 78.1.1, 78.3.1, 78.4, 78.4.1, 78.5.1, 80., 80.1.1, 80.3.1, 80.4, 80.5.1, 83.4.2, 84.4.3, 85.3.1, 85.2, 85.3.3, 85.4, 85.4.1, 87.3.1, 87.3.2, 87.3.3, 87.4.1, 87.5.1, 88.1.2, 88.4.1, 90., 90.1, 90.1.1, 90.1.2, 90.1.3, 90.1.4, 90.1.5, 90.1.6, 90.1.7, 90.2.1, 90.2.2, 90.2.3, 90.2.4, 90.2.5, 90.2.6, 90.2.7, 90.2.8, 90.3, 90.3.1, 90.4.1, 90.4.2, 90.4.3, 90.4.4, 90.5, 90.5.1, 90.5.2, 90.5.3, 90.6, 90.6.1, 90.6.2, 90.6.3, 90.6.4, 90.6.5, 90.6.6, 90.6.7, 90.6.8, 90.6.9, 90.7, 90.7.1, 90.7.2, 90.7.3, 90.7.4, 90.7.5, 90.7.6, 90.8, 90.8.1, 90.8.2, 90.8.3, 90.8.4, 90.8.5, 90.8.6, 90.9, 90.9.1, 90.9.2, 90.9.3, 90.9.4, 90.10, 90.10.1, 90.10.2, 91.1.2, 91.2.1, 91.2.2, 91.3.1, 91.4.2, 91.4.7, 91.4.8, 91.4.10, 91.4.12, 91.4.13, 91.6.4, 91.6.6, 91.6.8, 91.11.6, 91.12, 91.12.1, 91.12.2, 92.1.2, 92.2.2, 92.2.3, 92.2.8, 92.4.6, 92.5.2, 92.8.1, 92.8.4, 93.1.1, 93.3.3, 94., 94.1, 94.1.1, 94.1.2, 94.1.3, 94.1.4, 94.2, 94.2.1,

94.2.2, 94.3.1, 94.4.1, 94.4.2, 94.4.3, 94.4.5, 94.4.6, 94.4.7, 94.4.8, 94.4.9, 94.4.10, 94.4.11, 94.4.12, 94.4.13, 94.4.14, 94.4.15, 94.4.16, 94.4.17, 94.4.18, 94.4.19, 94.4.20, 94.4.21, 94.4.22, 94.5.1, 94.5.2, 94.5.3, 94.5.6, 94.5.7, 94.5.8, 94.5.9, 94.5.10, 94.5.11, 94.5.12, 95.1.1, 96.1.1, 96.1.2, 96.1.3, 96.1.4, 96.2, 96.2.1, 96.2.2, 96.3, 96.3.3, 96.4, 96.5, 96.5.1, 96.6, 96.6.1, 96.6.2, 96.6.3, 96.6.7, 96.7, 96.7.1, 96.7.2, 96.7.3, 96.7.4, 96.7.5, 96.8, 96.8.1, 96.9, 96.9.2, 96.10, 96.10.1, 96.11, 96.11.1, 96.11.2, 96.11.3, 96.11.4, 96.12, 96.12.2, 96.12.3, 96.12.5, 96.12.6, 96.12.7, 96.12.8, 96.12.9, 96.12.10, 96.13, 96.13.3, 96.13.5, 96.13.6, 96.13.7, 96.13.9, 97.2, 97.2.1, 97.2.2, 97.2.3, 97.2.4, 97.5.1, 97.5.3, 98.1.4, 98.2.1, 98.2.7, 98.2.8, 98.2.10, 98.2.11, 98.3, 98.3.1, 98.3.2, 98.4, 98.4.1, 98.4.2, 98.4.3, 98.5,98.5.1, 98.5.2, 98.5.3, 98.5.4, 98.5.5, 98.5.6, 98.5.7, 98.5.8, 98.5.9, 98.2, 98.5.10, 98.5.11, 98.5.12, 98.5.13, 98.5.14, 98.6.1, 98.6.3, 98.6.5, 98.6.6, 98.6.11, 98.6.12, 98.6.18, 98.6.21, 98.6.22, 98.7.2, 98.7.8, 98.7.9, 98.7.10, 98.7.11, 98.8.3, 98.8.5, 98.8.10, 98.8.11, 98.8.12, 98.8.13, 98.8.14, 98.9.4, 98.9.6, 98.9.13, 98.9.14, 98.9.15, 98.9.17, 98.9.18, 98.10.1, 98.10.2, 98.10.3, 98.10.5, 98.10.6, 98.10.10, 99.2.2, 99.3.2, 99.5.4, 99.6.1, 99.7.3, 99.9.4, 99.9.5, 99.9.8, 99.9.9, 99.10.1, 99.11.1, 100., 100.1.1, 100.3, 100.3.2, 100.5.1, 100.6.1, 100.6.3, 100.6.4, 100.6, 101.6.6, 101, 103., 102, 104, 104.1.1

E03313596

978-1-5286-5516-3