Forensic Science Regulator
Overseeing Quality

Codes of Practice and Conduct

for forensic science providers and practitioners in the Criminal Justice System

Pre-'Dry Run' Draft

This draft is intended to be used by UKAS to conduct dry runs of the accreditation process in existing ISO 17025 forensic science providers

January 2011

Date	Title/Version	Notes
03/08/2010	2010 08 03 Codes of Practice and Conduct - Published.doc	Published version
26/11/2010	QSSG 2010.12.16 -4 The Codes – Post-Consultation Draft v0-45.doc	QSSG meeting version
17/12/2010	2010 12 17 The Codes – Pre-Dry Run draft v0-5.doc	Draft incorporating comments from the QSSG meeting – supplied to UKAS
17/01/2011	2011 01 17 The Codes – Pre-Dry Run draft v0-55.doc	Foreword added and formatting changes only – typographical errors to be picked up at post Dry Run editorial

Foreword

I received feedback from some forty individuals and/or organisations with over four hundred specific comments on the draft text from my consultation on the last version of the Codes of Practice and Conduct. Thank you to all those who responded. The attached revised document is based upon the hard work of a small editorial group of my Quality Standards Specialist Group in addressing the many helpful comments received.

These interim Codes are to be used by the United Kingdom Accreditation Service in dry runs to ensure they do not add disproportionate, unnecessary or unintended additional regulatory requirements on organisations. They will dry run these interim Codes with several ISO 17025 accredited organisations in February 2011, and I will act on lessons learnt prior to the formal publication of the Codes in summer 2011.

The Code of Conduct in the last draft, and its predecessor, were adopted into the text directly from the former Council for the Registration of Forensic Practitioners (CRFP) code of conduct. The CRFP used their text as the standard to judge any information that called into question an individuals fitness to stay on their register. It was therefore relevant to have a wider remit than is required now. Many aspects of the Code of Conduct are now covered in greater depth in the remainder of the Codes of Practice. Prompted by feedback received, my Quality Standards Specialist Group concluded that a trimmed down Code of Conduct is now appropriate.

Running up to the formal publication of the Codes in the summer, I intend to continue consulting providers, meeting large and small stakeholders, listening to comments and acting on lessons learned from the dry runs. I also intend developing a clearer statement of accreditation requirements to be included in the Codes setting out the timescales for the disciplines that are in scope. My new foreword for the next version will also outline the next steps in the development of my quality framework.

Andrew Rennison

Contents

Code of Conduct for forensic science practitioners

The Forensic Science Regulator sets out for all practitioners, whether called for the Prosecution or Defence, the values and ideals the profession stands for.[1] This Code of Conduct provides a clear indication to customers and the public of what they have a right to expect.

As a practitioner:

1. Your overriding duty is to the court and to the administration of justice.
2. Act with honesty, integrity, objectivity, impartiality and declare any personal interest that could be perceived as a conflict of interest.
3. Provide expert advice and evidence only within the limits of your professional competence.
4. Take all reasonable steps to maintain and develop your professional competence, taking account of material research and developments within the relevant field.
5. Establish the integrity and continuity of items as they come into your possession and ensure it is maintained whilst in your possession.
6. Seek access to exhibits / information which may have a significant impact on your findings.
7. Conduct casework using methods of demonstrable validity.
8. Be prepared to review any casework if any new information or developments are identified that would significantly impact on your findings.
9. Inform a suitable person within your organisation if you have good grounds for believing there is a situation which may result in a miscarriage of justice.
10. Preserve confidentiality unless the law obliges, a court/tribunal orders, or a customer explicitly authorises disclosure.

[1] Developed from work by the former Council for the Registration of Forensic Practitioners.

Code of Practice for providers of forensic science services

Preamble

1. The Code of Practice aligns with BS EN ISO/IEC 17025:2005 (for testing and calibration laboratories[2] as interpreted by ILAC-G19:2002) and specifies the requirements for a management system for providers of laboratory-based forensic science services to demonstrate their ability to consistently deliver products and services that meet the requirements of their customers.
2. The United Kingdom Accreditation Service (UKAS®) will assess laboratory-based providers of forensic science services against BS EN ISO/IEC 17025:2005 utilising any of the relevant UKAS laboratory publications[3] and the supplementary requirements of this Code of Practice, and include compliance with this Code of Practice in the Schedule of Accreditation.[4] UKAS® can assess providers of forensic science services at scenes of incident against BS EN ISO/IEC 17020:2004 and any subsequent published appendices when enacted.
3. The main headings in this Code of Practice follow the BS EN ISO/IEC 17025:2005 and ILAC-G19:2002 headings (e.g. **5.8 Handling of test items**), but since not all clauses require interpretation, the numbering may not be continuous. Italicised sub-headings are to further contextualise the requirements for forensic science provision (e.g. ***Contamination avoidance, monitoring and detection***).
4. This Code of Practice is not a substitute for the complete version of the international standards BS EN ISO/IEC 17025:2005 and BS EN ISO/IEC 17020:2004 or the interpretative documents ILAC-G19:2002 and IAF/ILAC-A4:2004.
5. Appendices complementary to the Code will be produced and when enacted are to be read as part of the Code, expanding and interpreting it, where necessary, for specific activities, processes or evidence types.
6. The Code of Practice also incorporates, where applicable, any specific requirements determined by the Criminal Justice System (CJS) in England and Wales.[5]
7. Compliance with this Code of Practice is intended to provide the courts and the public with confidence in the reliability of forensic science evidence and to enhance customer satisfaction through the effective application of the management system.
8. The Code and any subsequent appendices will be updated to reflect any relevant changes in the requirements of BS EN ISO/IEC 17025:2005, BS EN ISO/IEC 17020:2004, ILAC-G19:2002, IAF/ILAC-A4:2004 and the CJS. The updated version will be made available to all interested parties.

---

[2] This Code of Practice does not specifically address the requirements of calibration laboratories. Laboratories providing calibration services should comply with the requirements of BS EN ISO/IEC 17025 for this aspect of their work.

[3] A list of UKAS *Publications for Laboratory Accreditation to ISO/IEC 17025* is available from: http://www.ukas.com/technical-information/publications-and-tech-articles/publications.asp

[4] The Regulator has a Memorandum of Understanding with the national accreditation body UKAS®, agreements with other national accreditation bodies may be entered into if required.

[5] The Codes can be extended or adopted by other jurisdictions and consultation with the appropriate Ministers, governing bodies and prosecuting authorities will be entered into.

9. Other standards currently used for certification or accreditation of organisations that provide forensic science services (e.g. GLP, GMP, ISO 15189:2003[6] and CPA Standards) are not alternatives to BS EN ISO/IEC 17025:2005 or BS EN ISO/IEC 17020:2004, although they do overlap to some extent and provide compatible guidance on good practice.
10. All practitioners should comply with the principles contained in the Code of Conduct at the beginning of this document. Taken together with the Code of Practice these are referred to collectively from this point forward as the Codes.

1 Scope

1. The Codes are for providers of forensic science services to the CJS. Forensic science is taken to include the sciences traditionally performed by the police service and the public and private sector forensic science laboratories and to a lesser extent academia. They are intended to cover sciences with scene and/or laboratory based elements and therefore are not intended for disciplines' such as forensic accountancy or psychiatry. Although the Codes could be extended to forensic medicine, they have not been drafted with that in mind. They cover the forensic science provider's:
    a. initial forensic science activity at the scene;
    b. the scene examination strategy;
    c. the recovery, preservation, transport and storage of exhibits;
    d. screening tests for use in the field;
    e. the examination, sampling, testing and/or analysis of exhibits;
    f. testing activities using laboratory-based methods;
    g. the recording of actions taken;
    h. assessment of examination and test results; and
    i. the reporting and presentation of results with associated interpretations and opinions.
2. The Codes specify the general requirements for competence to carry out scene examinations, sampling, laboratory examinations and tests and the provision of expert testimony. Where relevant, appropriate legal, regulatory and information security is included.
3. All practitioners and providers offering forensic science services to the CJS are to be bound by these Codes; however it is accepted that experts from other professions will be called to give evidence from time-to-time and the customer should make such providers aware of, and require that they are bound by, the Code of Conduct as a minimum.

2 Normative references

BS EN ISO 9001:2008, *Quality Management Systems – Requirements*

[6] Although this is based on BS EN ISO/IEC 17025, it is designed and assessed for a separate purpose; preliminary work is underway to look at the feasibility whether a bolt-on enhancement and inspection could be devised to make it applicable to these Codes.

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

ILAC-G19:2002, *Guidelines for Forensic Science Laboratories*

BS EN ISO/IEC 17020:2004, *General criteria for the operation of various types of bodies performing inspection*

IAF/ILAC-A4:2004, *Guidance on the Application of ISO/IEC 17020*

HMG Security Policy Framework, 2009, *Security Policy No.2: Protective Marking and Asset Control*

3 Terms and definitions

1. For the purposes of these Codes, the definitions of terms are given in the Glossary.
2. The meanings of abbreviations are also given.

4 Management requirements

1. The provider shall have a Schedule of Accreditation covering compliance with BS EN ISO/IEC 17025:2005 and/or BS EN ISO/IEC 17020:2004 and the supplementary requirements of this Code of Practice for the methods, products and services it is routinely providing.
2. BS EN ISO/IEC 17025:2005 requires that the roles and responsibilities of the technical management are defined. Top management should also be defined which would usually be at Chief Officer or Board level.
3. For novel techniques or non-routine activities the provider should have validated the method, product or service in accordance with the requirements of these Codes and should ensure that the status of the product, method or service is clearly understood by the customer prior to commissioning any such work. If these activities are to become part of the routine activities of the provider, accreditation should always be sought.

Business continuity[7]

4. The provider shall develop procedures to be implemented following interruption to, or failure of, business critical processes to maintain or restore operations and ensure continuous availability, confidentiality and integrity of information.
5. Where applicable, continuity plans shall include the arrangements that have been made to preserve the contents of retained material, including those where the provider or a provider's contracted storage facility goes out of business and has no legal successor.
6. Business continuity plans shall be tested on a regular basis and the results documented. Any identified need for action to modify the plans shall be implemented and the plans re-tested.

[7] Further guidance can be obtained from BS 25999-1:2006: Business continuity management - Part 1: Code of practice.

Independence, impartiality and integrity

7. The provider shall ensure all of its practitioners adhere to the Code of Conduct in respect of their independence, impartiality and integrity, and that the organisational structure and policies and procedures to support this rather than hinder this.
8. The conflicts of interest, perceived or otherwise, and threats to impartiality may include a practitioner:
    a. having the perception of, or being coerced, openly or secretively;
    b. being the sole reviewer of their own work;
    c. being involved with activities which could be perceived as witness coaching or being coached rather than training or familiarisation;
    d. being over-familiar with or trusting another person instead of relying on objective evidence;
    e. having organisational and management structures which reward, encourage or support bias;
    f. having a close/significant personal or financial relationship with a party likely to be affected by the outcome;
    g. having a close/significant personal or financial relationship with any person acting as an expert witness in the case; and
    h. acting in self-interest.
9. It is expected that the expert, in assessing the results obtained, would not only consider the relevant hypothesises which could explain their findings prior to presenting relevant hypothesises as propositions to the case.
10. The remuneration (salaries and all other benefits) of practitioners shall not depend on whether the results they obtain support or detract from any perceived expectations of those commissioning the work.
11. The required policies and procedures shall not only prevent internal and external influence on the results of their examinations and tests, but also cover the corrective action (such as formal disclosure) to be taken if there is a possibility of a practitioner's judgement having, or perceived to have been compromised,

Confidentiality

12. All providers shall comply with the requirements of Her Majesty's Government's (HMG) Security Policy Framework, 2009, Security Policy No.2: Protective Marking and Asset Control[8] for the purposes of classification of information held electronically or in paper documents and application of the necessary controls and technical measures.
13. If information is required under the disclosure rules, it must be provided to those instructing the provider, irrespective of its classification.[9]

[8] Available from:

http://www.cabinetoffice.gov.uk/intelligence-security-resilience/intelligence-and-protective-security.aspx

[9] See ACPO/CPS Guidance Booklet for Experts, Disclosure: Experts' Evidence, Case Management and Unused Material, May 2010.

14. The provider shall ensure that the documented policies and procedures for confidentiality requirements, including any disclosure requirements, are applied to any subcontractors.

4.3 Document Control

1. The provider must ensure that document control procedures are applied to the following where they are integral to the forensic process, including:
    a. both hard copy and electronic systems;
    b. procedures – technical and quality;
    c. software;
    d. technical methods;
    e. forms;
    f. external documents; and
    g. statutory documents.
2. The retention period for obsolete/superseded documents should be defined and should take in to account customer, regulatory and legal requirements.[10]

4.4 Review of requests, tenders and contracts

1. The processes surrounding the review of requests, tenders and contracts may occur at several different levels and at several key stages through the processing of forensic work. These may include but not be limited to:
    a. the processes leading to the documentation of an overarching Service Level Agreement (SLA)/contract between the customer and the provider;
    b. the management of the adherence to the agreed SLA/contract;
    c. the documentation and review of more detailed case specific requirements through the use of submission forms etc;
    d. outcomes from case conferences; and
    e. significant discussions with the Officer In Charge (OIC), solicitors etc.
2. The aspects discussed and agreed as part of the review of requests, tenders and contracts may include but not be limited to:
    a. turn around times;
    b. report format;
    c. items to be examined;
    d. case assessment and strategy;
    e. sequence of examination;
    f. precautions to be taken to preserve additional evidence ;
    g. methods to be used;
    h. products to be delivered;

[10] See ACPO (2003) The Forensic Science Service: retention of case material a memorandum of understanding between ACPO and FSS.

i. costs;

j. collection/transfer of items; and

k. retention, destruction or return of items (see ***Exhibit return and disposal***).

3. The documented procedure and associated records must describe all instances when work requirements are discussed and reviewed such that a demonstrable audit trail including appropriate justifications and authorisations is available for each piece of work undertaken.

4.5 Subcontracting

1. A provider may need to subcontract work and in all cases the customer shall be informed in writing and approval is required.
2. If other necessary approvals are required by rules or convention such as with certain DNA services, the subcontracted provider must also be approved.

4.6 Purchasing services and supplies

Packaging and general chemicals and materials

1. The provider shall specify the preferred quality of packaging and general chemicals and materials to be used by the customer.
2. Providers shall ensure that any sample collection kits they use are fit for purpose.

4.8 Complaints

1. The provider shall have policies and procedures for dealing with complaints. These procedures shall define what constitutes a complaint in relation to the work undertaken by the provider, and shall ensure that appropriately thorough investigations are instigated on receipt of any complaints.
2. The Regulator shall be informed about any complaint if it has significantly disaffected the customer such that it could attract adverse public interest or lead to a miscarriage of justice. The policies and procedures relating to complaints shall also indicate the individual responsible for notifying the Regulator.
3. Complaint investigations shall include examination of the potential impact on any work that has already been undertaken by the provider. In the event that it is shown that there could have been an impact on any work this should be dealt with through the non-conforming work process.
4. Records shall be retained of all complaints and of the subsequent investigations and outcomes.
5. Complaints may be received from many sources including customers, victims of crime, police forces, other departments within the same provider (e.g. laboratory, scene of crime unit, investigation unit) and the judicial system including adverse court decisions pertinent to the work.

4.9 Control of non-conforming testing

1. The Regulator shall be informed about any non-conforming test if it has potential to significantly disaffect the customer such that it could attract adverse public interest or lead to a miscarriage of justice. Examples of non-conforming testing which after investigation could require escalation to the Regulator could include, but are not limited to:

a. unexpected performance in proficiency testing/inter-laboratory comparison;
b. unauthorised access to restricted areas;
c. missing items/casefiles;
d. equipment failing to receive timely calibration or maintenance;
e. failure of staff to follow procedures;
f. contamination incidents;
g. a technical method is found to be producing erroneous results; and
h. any standards/reference materials, equipment or reagents found to have defects or deficiencies.

2. The provider shall maintain a record of the nature of non-conformities capable of being used to identify trends, any concessions obtained to use non-conforming work, and any corrective and/or preventive actions taken.

4.13 Control of records

4.13.1 General

1. The provider shall establish retention times that satisfy the requirements of legislation, its accrediting body and its customers, as appropriate.
2. Records should be stored and subsequently disposed of in a manner appropriate to their sensitivity and/or protective marking (e.g. incinerated or shredded).

4.13.2 Technical records

1. As a minimum, the technical records shall contain all relevant information relating to:
   a. the collection and movement of material (physical exhibits and information), including the date on which the material was taken or received; the date of subsequent movement of the material to another party; from whom or where and to whom or where the material was moved; and the means by which the material was received or passed from/to another party (see **5.8 Handling of Test Items**);
   b. sufficient detail to be able to trace any analytical output to:
      i. a specific instrument;
      ii. a specific version of software/firmware;
      iii. the operator; and
      iv. the date of the run.
   c. the examination of exhibits, and materials recovered from exhibits, whether made by the practitioner or an assistant;
   d. verbal and other communications, including reports and statements;
   e. meetings attended and telephone conversations, including points of agreement, or disagreement, and agreed actions; and
   f. e-mails and other electronic transmissions (e.g. images), sent or received.
2. The records, in whatever form, shall be clear and comprehensive, and expressed in such a manner and in sufficient detail, that another practitioner, in the same field, and

in the absence of the original practitioner, can follow the nature of the work undertaken, any interpretations/opinions made and the inferences drawn from the work. This is particularly important in situations where an insufficient quantity of the exhibit remains for independent re-examination or testing, or the form of the exhibit is altered.

3. Whenever practicable, technical records shall be produced contemporaneously. The practitioner shall normally begin making records from the time instructions are received and shall continue making records throughout their involvement in the case, although, in some circumstances, it may be appropriate to start making records prior to any formal instructions from the customer.
4. When an examination, test result or observation is rejected, the reasons shall be recorded.
5. For the period of record retention, traceability should be maintained for all names, initials and/or identifiers and for these to be legible.
6. It shall be possible to associate all changes to data with the person having made those changes, for example by the use of timed and dated (electronic) signatures. Reasons for changes shall be given.
7. The practitioner's examination records shall be paginated using a page numbering system which indicates the total number of pages.[11] Each page of every document in the case record shall be traceable to the analyst or examiner responsible for the sampling and/or performance of each examination or test, to a uniquely identified case and exhibit. It shall be clear from the case record who has performed all stages of the analysis or examination and when each stage of the analysis or examination was performed. Alterations or comments in the records shall be clear and be signed or otherwise attributable to the individual who made them and dated.
8. The provider shall have a documented procedure to ensure that it maintains a co-ordinated record relating to each case under investigation.
9. The provider shall have a documented procedure for finding all relevant information linked to a particular scene or offence, and any connected scenes or offences.

Checking and review

10. The provider shall have a procedure for carrying out checks on critical findings[12] and designated staff authorised to carry out such checks. Where independent checks on critical findings are carried out by authorised staff, the records shall indicate that each critical finding has been checked and agreed, and by whom and when the checks were performed. The procedure should include a process for resolving any non-conforming results or findings.
11. The provider shall ensure that checks of all calculations (including those embedded in spreadsheets) and data transfers which do not form part of a validated electronic

[11] Alternative arrangements for demonstrating that all pages are present and the sequence of these pages are possible but must be agreed with UKAS.

[12] Critical findings are observations or results that have a significant impact on the conclusion reached, the interpretation, an opinion provided, cannot be repeated or checked in the absence of the exhibit or sample, and/or could be interpreted differently.

process are carried out preferably by a second person, and the case record shall indicate that such checks have been carried out and by whom and when. Where other programming approaches are used to effect data manipulation and transfer, a method to ensure that these are checked shall also be established.

12. The provider shall have documented policies and procedures and authorised staff for the review of case records, including reports and statements. The review shall establish from the case notes and discussion with the practitioner that the work carried out is:
    a. appropriate to the requirements of the case;
    b. fully documented in the case notes, with appropriate checks on critical findings, calculations and data transfers;
    c. in compliance with the provider's documented policies and procedures; and
    d. consistent with the contents of the report or statement.
13. The case record shall indicate that the review has been carried out, by whom and when.
14. The checks and reviews shall be recorded as entries against each finding or on a summary of findings or on a report, as appropriate. If the checker/reviewer disagrees on any point and the matter cannot be resolved, the reason(s) for the disagreement and any action taken as a result shall be recorded.

4.14 Internal audits

1. The annual audit programme shall cover all aspects of the management system, including but not be limited to:
    a. implementation of the management system;
    b. records of individual files; and
    c. information security.[13]
2. All technical methods and procedures shall be audited and technical processes witnessed on a rolling plan over at least a 3-4 year cycle.[14]
3. A representative sample of all practitioners shall be included.
4. Where the provider undertakes to make statements of opinions and interpretations, the audits shall include an appraisal of the basis on which these are made and of the competence requirements of the individuals authorised to make such statements.
5. 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.

[13] This may not be required where the Management of Police Information (MoPI) applies and this is within the scope of the required MoPI audit.

[14] The frequency of audits should take account of the size of the organisation, the complexity of the work being audited, the frequency of use of specific technical methods or procedures and the potential consequences of noncompliance with the requirements of the Standard. The value of occasional unannounced audits should also be considered.

6. When the results of the audit cast doubt on the effectiveness of examinations, or the correctness or validity of the provider's test results to the extent that misleading information may have been reported, the provider shall treat this as a non-conforming test.

5 Technical requirements

5.2 Personnel

1. The provider shall carry out background verification checks on all candidates for employment and contractors in accordance with relevant laws, regulations and ethics. These checks shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
2. The contracts for all staff, permanent and temporary, shall contain confidentiality agreements,[15] their own and the provider's responsibility for information security, and details of their expected conduct.

Code of Conduct

3. The provider shall have a Code of Conduct compatible with the Regulator's; staff should be made aware of it and how it relates to the objectives of the management system.

Training

4. The provider and/or individual members of staff, including contracted staff, shall maintain and keep readily available appropriate records of education, training, skills and experience in sufficient detail to provide evidence of proper training and formal assessment. These records shall include:
    a. academic and/or professional qualifications;
    b. internal/external courses attended;
    c. relevant training/retraining received whilst employed by the provider;
    d. any substantive complaints, errors or adverse judicial comments and any subsequent remedial action;
    e. the tasks for which the individual has been assessed as competent and authorised to carry out; and
    f. the date(s) on which competence and authorisation were confirmed.
5. The training system shall be fully documented and the provider shall have a policy for retention in line with that of case files for training manuals and training records. Retention times should take into account the requirements of legislation and legal proceedings.

Competence

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

[15] The confidentiality agreements should cover the intellectual property of the provider and all information relating to casework and shall not conflict with any disclosure requirements.

7. Consideration of any adverse judicial comments and complaints which may undermine an individuals credibility or prevent them being used in certain roles should be included in the required policies and procedures.
8. For individuals required to present expert oral evidence in court, policies and procedures should include a programme to ensure competence (e.g. through witnessing actual or mock court appearances).[16]
9. The provider shall have policies and procedures for taking remedial action when competence is found to have lapsed.
10. The provider should utilise available National Occupational Standards produced by Skills for Justice® for determining the appropriate competence framework for technical roles.

5.3 Accommodation and environmental conditions

1. The laboratory facilities shall include, as appropriate:
    a. suitable laboratory accommodation and appliances (e.g. laboratory benches, safety cabinets, refrigerators, freezers) and space (per employee) and to carry out the work to the required standard, safely and without cross-contamination;
    b. provision of appropriate environmental conditions (e.g. lighting, temperature, humidity, ventilation/air flow) required to facilitate correct performance of examinations or tests, and not adversely affect the required quality of any measurement or invalidate results;
    c. proportionate physical protection against likely risks such as arson, theft or interference with exhibits;
    d. archive/storage facilities with adequate storage conditions to prevent loss, deterioration and contamination, and maintain the integrity and identity of documents/records/exhibits both before, during and after examinations or tests have been performed; and
    e. facilities for the secure disposal of confidential waste and the safe disposal of hazardous materials.
2. The access and use of exhibit storage areas and server rooms should be controlled in addition to laboratory areas where work is carried out. The provider shall hold on record a list of all staff who are authorised to enter these areas. This shall be reviewed and updated regularly.
3. Delivery and loading areas, and other points where unauthorised persons may enter the building, shall be isolated from casework and information processing areas and access shall also be controlled. Unauthorised persons needing to enter controlled areas shall be escorted at all times by authorised staff and a record of these entries shall be maintained.

[16] Ideally this ought to be in line with the normal accreditation cycle (normally 4 years) with a representative sample of experts should be witnessed, or tranches of mock courtroom experience be scheduled, in each year.

Contamination avoidance, monitoring and detection

4. The provider shall have risk based policies and procedures for the prevention, monitoring and detection of contamination. The steps[17] in establishing the processes and procedures should include, but are not restricted to:
    a. conducting a hazard or risk-based analysis of the entire process (e.g. process mapping);
    b. identifying points in the process where contamination events could occur (e.g. consumable selection, transfers etc.);
    c. establishing acceptable control limits at each point or stage of the process;
    d. establishing monitoring requirements (e.g. frequency);
    e. establishing preventative and corrective actions (e.g. when acceptable or control limits are found to be exceeded);
    f. establishing requirements for record keeping; and
    g. establishing procedures for verifying the system remains fit for purpose.
5. The processes and procedures shall also include consideration of, but not be restricted to:
    a. limiting and recording access by internal and external visitors taking into account any recent activities relevant to casework, including but not limited to:
        i. crime scene attendance;
        ii. prisoner handling; and
        iii. firearm and drug handling.
    b. effective separation of incompatible activities to prevent cross-contamination. This includes, but is not limited to:
        i. un-amplified and amplified DNA;
        ii. high and low level drugs work;
        iii. examination of firearms and firearm discharge residues;
        iv. examination of accelerant and fire scene debris; and
        v. examination of exhibits from suspects and victims.
    c. use of disposable gloves, face masks, mop caps and equipment;
    d. testing before use of standards, record keeping of batches of consumables and reagents in all areas of the examination/analytical processes and where appropriate for contaminants that could interfere with the success or interpretation of the examination or test;
    e. good working practices (e.g. protecting exhibits/samples in wrapping/containers when not being worked on or used; not introducing contaminated spatulas/pipettes into stock bottles of solvent, standard or reagent; not pouring unused portions of solvent, standard or reagent back into bulk supplies; frequent changing of solvent used for rinsing equipment);

[17] Based upon the seven principles of the Hazard Analysis Critical Control Point System.

f. good housekeeping practices;

g. analysis of blank controls; and

h. relevant environmental sampling/monitoring with particular reference to acceptable levels of relevant potential contaminants should be carried out to include equipment, work areas, consumables and clothing to ensure that any contamination of accommodation and equipment that does occur is recognised and controlled.

6. The policies and procedures shall ensure access to laboratory areas is restricted to authorised individuals and they are covered by relevant elimination databases and any unexpected profiles found in casework screened against them. These databases may be locally or remotely maintained (see ***Databases***).

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

   a. reporting policies;

   b. data formats;

   c. searching procedures and algorithms;

   d. retention periods;

   e. sharing agreements (i.e. between laboratories/providers);

   f. agreements/consents; and

   g. release forms.

5.4 Test methods and method validation

5.4.2 Selection of methods

1. All test/sampling/analysis methods are required to meet the needs of the different layers of the CJS which collectively is the end-user; this is demonstrated through validation.

2. Even where a method is considered standard and is in widespread use, the provider shall verify the existing validation study against an end-user specification, compile the validation library and statement and demonstrate the method works in their hands.

5.4.5 Validation of methods

1. Validation should be conducted prior to implementation of the method; this may be performed by the provider, manufacturer or another provider.

2. Where the validation has not been conducted in-house by the laboratory that will be using the method, the provider must still verify the scope of the validation and that the method performs reliably at the given location by the provider's own competent staff by following the validation process outlined here.

3. The procedure for verification will normally mirror that of validation, with the required activity at the steps scaled according to the adequacy and relevance of the available existing validation study. Therefore the term validation is used in this section to cover both validation and verification unless specified.

4. The validation policy or procedure shall set out roles and responsibilities of staff involved in conducting validation, reviewing outcomes and authorisation of key stages.
5. To ensure validation studies are conducted on the final method, there should a clear boundary between development and validation. This should include consideration of how to prevent inadvertent re-entering of the development process once validation has started.
6. The validation procedure shall include where relevant, but is not limited to:
    a. determining the end-user's requirements and specification;
    b. risk assessment of the method;
    c. a review of the end-user's requirements and specification;
    d. the acceptance criteria;
    e. the validation plan;
    f. the outcomes of the validation exercise;
    g. assessment of acceptance criteria compliance;
    h. validation report;
    i. statement of validation completion; and
    j. implementation plan.
7. In certain circumstances implemented methods will require revalidation, for example when:
    a. quality control indicates that an established method, is changing with time;
    b. equipment which was not validated to be mobile or portable is moved to a new location;
    c. deficiencies have become apparent after the method has been implemented; or
    d. the end-user identifies a change in requirement.

Determining the end-user's requirements and specification

7. The process of innovation ending in the implementation of a validated method is more likely to be instigated by the provider than the end-user. However to meet the needs of the CJS, which is the end-user, the range of end-user's requirements need to be determined.
8. The amount of direct input from the CJS end-user should be determined by the provider based on the type of innovation; certain requirements may be generic and form a set of core requirements to the casework type.
9. The end-user's requirement shall take account of, as appropriate:
    a. who will operate or use the new method, product or service post-delivery and in what environment;
    b. what the new method or product is intended to deliver for the end-user;
    c. what statutory and regulatory requirements related to development and use of the method or product apply;

d. whether there are any compatibility issues to be considered;

e. what level of quality performance is expected; and

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

10. End-user requirements should conform to the following rules:

a. each requirement is a single statement;

b. each requirement is testable;

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

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

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

11. Where the method is part of a service to be provided to a specified customer, the provider shall also ensure their formal agreement.

12. The end-user's requirements shall then be written as a detailed specification for the method product or service, and shall include the technical quality standards.

Risk assessment of the method

13. 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, the following:

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

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

14. 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.

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

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.

16. Where exhibits provided by end-users, or data derived from these, are required for the development work or validation, the provider shall obtain prior permission for their use[18] and include their use in the risk assessment.

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

Review of the end-user's requirements and specification

18. The provider shall review the end-user's requirement/specification to ensure that it has been translated correctly, is consistent and the specification is fit for purpose. Where appropriate the intended end-user may be involved in this review process.

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

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

21. The provider shall ensure that all staff involved in the development and validation/verification of the method are informed of any agreed changes to the end-user's requirements or specification.

The acceptance criteria

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

23. The acceptance criteria shall be used to demonstrate the effectiveness of the method and control strategy with-in measurable and set tolerances.

The validation plan

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

25. Where appropriate, the validation plan shall also include a requirement to check the relevant parameters and characteristics of the procedures for sampling, handling and transportation. The same level of confidence in the results obtained shall be required whether the method is to be used routinely or infrequently.

26. The provider shall record any modifications to the validation plan, and review, verify, validate, approve and authorise the changes before proceeding with development of the method. The review of the validation plan shall include evaluation of the effect of the changes on related methods already delivered.

27. The validation shall be carried out using simulated casework material in the first instance and subsequently, where possible, permitted and appropriate, with actual casework material to confirm its robustness.[19]

[18] The legal decision on ownership of exhibits and data and the protocol for use of dead and live casework samples and data still has to be agreed.

28. The validation plan will need to be tailored depending on whether it is intended for:
    a. validation of measurement based methods;
    b. validation of interpretive methods;
    c. verification of adopted methods; and/or
    d. verification of minor changes in methods.

Validation of measurement based methods

29. The validation plan should ensure the required parameters and characteristics are studied:
    a. using an analyst or examiner competent in the field of work under study who has sufficient knowledge of the work to be able to make appropriate decisions from the observations made as the study progresses; and
    b. using equipment that is within specification, working correctly and, where appropriate, calibrated.
30. The functional and performance requirements and relevant parameters and characteristics for measurement based methods which shall be considered include:
    a. the competence requirements of the analyst/user;
    b. environmental constraints;
    c. exhibit/sample size;
    d. exhibit/sample handling;
    e. exhibit/sample homogeneity;
    f. the ability of the sampling process to provide a representative sample of the exhibit;
    g. the efficiency of recovery of the analyte(s) of interest during sample preparation for analysis;
    h. the presence or absence of the analyte(s) of interest in the sample analysed;
    i. the minimum amount of each analyte that can be reliably detected;
    j. the minimum amount of each analyte that can be accurately measured;
    k. that the identification/measurement relates to the analyte(s) alone, and is not compromised by the presence of some matrix or substrate effect or interfering substance;
    l. that the method is robust and produces consistent, reliable, accurate results, with a known acceptable level of uncertainty, compatible with those obtained by other analysts using different equipment and different methods; and
    m. limitations of applicability.

[19] See footnote 18; legal advice should also be sought for the use of casework material which is covered by the Human Tissue Act 2004.

Validation of interpretive methods[20]

31. The functional and performance requirements for interpretive methods are less prescriptive than for measurement based methods and shall concentrate on the competence requirements for the staff involved and how the staff shall demonstrate that they can provide consistent, reproducible, valid and reliable results that are compatible with the results of other competent staff. This may be achieved by a combination of:
    a. independent confirmation of results/opinions by another competent examiner (i.e. without prior knowledge of the first result/opinion provided);
    b. participation in interlaboratory comparisons (collaborative exercises or proficiency tests);
    c. external recognition with a recognised and relevant professional body; and
    d. design frequent in-house assessment into the process using positive and negative competence tests.
32. An interpretive method shall require only the relevant sub-set of the parameters and characteristics for measurement based methods to be determined.

Verification of adopted methods

33. When a provider introduces a method developed and validated in a different laboratory, it shall demonstrate that it performs reliably at the given location by the provider's own competent staff.
34. The amount of work required to be carried out in verification exercises when introducing methods developed and validated elsewhere shall take account of the adequacy of the available existing validation data and the familiarity and experience of the provider's staff with the techniques, equipment and facilities involved.
35. The provider shall check its performance against the required end-user specification for the method rather than against existing published data.
36. The 'validation' report shall have as a minimum a summary of the experimental work/review, results, staff training/competence requirement and assessment plans. The required validation library and statement of validation completion shall be produced.

Verification of minor changes in methods

37. Minor changes to established methods used by the provider may not require a full re-validation exercise. The impact of the change shall be risk assessed, verified and authorised in line with other validation studies. A revalidation exercise should be carried out should changes be assessed to have the potential to influence the results obtained.

Validation outcomes

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

[20] Examples of interpretive methods may include the comparison of marks, handwriting or microscopic comparisons.

method. A fuller record of the validation exercise shall be maintained for the functional life of the method and shall include:

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

b. all experimental results from the validation exercise;

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

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

e. any corrective actions identified; and

f. independent approval of the validation.[21]

Assessment of acceptance criteria compliance

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

40. The person(s) shall have demonstrated they have sufficient knowledge of the issues involved to be able to identify and assess the significance of any deficiencies.[22]

41. The *independent authorisation* shall typically establish whether:

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

    b. the method is fit for its intended use.

42. For novel methods and higher risk methods that are likely to attract challenge once implemented, the validation details and data shall be further offered for review by the end-user and/or others in the CJS with a declared interest. If there is any doubt about the need for wider review and/or publication prior to implementation, the Regulator shall be consulted.

Validation report

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

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

    a. a title and unique identifier;

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

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

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

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

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

e. the validation plan;

f. risk assessment;

g. any authorised changes to the validation plan and justifications for the changes;

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

i. details of any review reports produced;

j. conformity with the specified user requirement and acceptance criteria (expected vs. actual and pass/fail);

k. any limitations/constraints applicable;

l. any related published papers and similar methods in use by the provider;

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

n. the date of the report.

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

46. All records relating to the development and validation of the method, product or service shall be archived, together with the means of accessing the records which will normally be for 30 years following the its last use in casework.[23]

A statement of validation completion

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

48. The approval by the provider must be clear on the scope of the validation.

49. The provider should provide any further information which would be useful to the CJS. Examples would include, but probably not be limited to, the following:

a. caveats about the use of the method;

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

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

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

[23] The blanket retention period is an alternative to tracking a method's use in casework and applying the correct retention period in accordance with the CPIA 1996, as amended.

Validation library

50. The provider shall have available a *library* of documents relevant to the authorisation of the method through validation or verification. Where the following are not already distinct sections in the validation report the content of this library shall include, but need not be limited to, the following:
    a. the specification for the method approved;
    b. the risk assessment for the method approved;
    c. the validation plan for the method approved;
    d. the validation report;
    e. the record of approval; and
    f. the statement of validation completion.
51. Where the method implements a scientific theory and/or model or an interpretation or evaluation model the library should include a record of information supporting the use of the model/theory.
52. Where the method relies on reference collections or databases, the nature, access and their availability should be described.
53. The information in the library shall be disclosable[24] and should be prepared with that requirement in mind.

Implementation plan and any constraints

54. The provider shall have a plan for implementation of the method, product or service. This plan shall address, where relevant:
    a. if revisiting old cases should be explored where the revised or new method offers new analytical opportunities and if relevant communicated to the customer the benefit or risks;
    b. the standard operating procedure (including the process for assessment/interpretation/reporting of results) or instructions for use;
    c. requirements for staff training, competence assessment and on-going monitoring of staff competence;
    d. integration of the method with what is already in place;
    e. if the method is intended to be included in the scope of accreditation and what steps are required;
    f. the monitoring mechanisms to be used to demonstrate that the method remains under satisfactory control during its use;
    g. the protocols for calibration, monitoring and maintenance of any equipment;
    h. the supply and traceability of any standards/reference materials;
    i. the supply and quality control of key materials, consumables and reagents;
    j. the exhibit handling and any anti-contamination protocols;

[24] Commercial-in-confidence does not override the disclosure requirements of the CPIA and may prevent methods, products or services being used.

k. the accommodation plan;

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

m. the communication plan; and

n. the schedule for post-implementation review.

5.4.6 Estimation of uncertainty of measurement

1. Guidance on the estimation of uncertainty of measurement is contained in appendix N of the UKAS publication 'The Expression of Uncertainty and Confidence in Measurement (M 3003)'.
2. When a procedure is modified, in addition to any validation or verification, providers should also review the uncertainty of measurement.

5.4.7 Control of data

1. The provider shall have procedures within its management system to ensure that all information is recorded accurately, maintained so that its authenticity and integrity is not compromised, and it is retained and destroyed in accordance with the provider's retention and destruction policy.

Electronic information capture, storage, transfer, retrieval and disposal[25]

2. The provider shall establish procedures for the capture and retrieval of electronic information to ensure that all the necessary information is captured without change and any information lost as a result of the capture process is acceptable.
3. Where scanning technology is used, the provider shall establish procedures and quality control for the scanning of documents in paper form, microforms and other forms of information, as appropriate, to ensure that any potential information loss as a result of the scanning is within acceptable limits.[26]
4. Where information is extracted from image files the original images shall be retained and linked with the captured information including metadata.
5. Where information in the form of a compound document is stored, the linkage of all elements of the compound document shall be stored in line with the provider's retention policy along with their content.
6. Information should be in an accessible file format throughout its period of retention.
7. When information is migrated to new storage media, the provider shall establish procedures to ensure that all digital objects[27] have been successfully migrated to the new storage technology and the digital object and file format of the migrated digital objects have not changed, or the changes are known, have been audited and meet requirements.

[25] Further information and guidance can be found in BS 10008:2008, Evidential weight and legal admissibility of electronic information – Specification.

[26] Further information and guidance can be found in BS ISO 12653-1 BS ISO 12653-2.

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

8. If replacement software (e.g. an operating system or application software) is implemented, the provider shall ensure that procedures are established to retain access to the relevant information.
9. Where information is compressed during the storage and transfer processes (e.g. in order to reduce stored file size), the compression method used shall not affect the authenticity and integrity.
10. Information shall be retained in audit trails, or using other appropriate processes, which record the disposal of information as specified by the retention and disposal policy.

Electronic information security[28]

11. The provider shall establish and document a policy and procedure for management of electronic information based on business and security requirements and include this in the schedule of regular audit and review.
12. The policy and procedure should include a formal method of granting and removing access rights, privileges and password control.
13. The policy and procedure should include:
    a. the selection and use of passwords;
    b. that unattended equipment has appropriate protection;
    c. a clear desk and screen policy;
    d. management of removable storage media; and
    e. segregation of developmental and operational IT environments.
14. The provider shall have procedures to protect or back-up electronic records, to prevent loss, corruption (actual or suspected) and unauthorised access to and/or amendment of the records, and for maintaining an audit trail. The back-up data shall be stored for as long as necessary at a separate and secure location. The back-up and restore/recovery procedures shall be tested at regular intervals to ensure that information can be retrieved in the event of an information loss. Details of all recovery operations shall be retained for as long as the information to which they relate.

Databases

15. Providers shall have a process for determining the requirements of the CJS for internally developed databases used to make inferences and interpretations.
16. Information included in such databases shall be capable of authentication through documentation to its original source, meet a minimum quality standard specified by the owner of the database, be validated for accuracy of transcription on entry to the database and be auditable for corruption.
17. Any programs employed within electronic databases for data manipulation shall be fully validated as fit for purpose.

[28] More detailed good practice guidance can be obtained from BS ISO/IEC 27001:2005 (Information technology – Security techniques – Information security management systems – Requirements) and BS ISO/IEC 27002:2005, (Information technology – Security techniques – Code of practice for information security management).

18. All databases shall be covered by formal documentation specifying, as a minimum:
    a. their purpose;
    b. their location and identification;
    c. their scope and content;
    d. the origin of the data;
    e. any known significant limitations or restrictions;
    f. the person responsible for management of the database;
    g. the authorisation and competence requirements of organisations/practitioners contributing to the database;
    h. the arrangements and format for data collection and submission;
    i. the process for authentication or validation of the data;
    j. the arrangements and format for data storage;
    k. the process for making updates and amendments, and maintaining audit trails;
    l. the protocols for access to the database and its interrogation and use;
    m. the quality assurance requirements, including those for data integrity, transfer, inconsistency and error checking;
    n. the confidentiality and security requirements;
    o. the format and content of results and reports from interrogation of the database, including the provision of any caveats relating to any limitations with the results provided;
    p. the projected shelf life of the data;
    q. the arrangements for review for relevance, use and effectiveness; and
    r. all relevant legal, commercial and ethical requirements covering their registration, data content, retention, accessibility or use.

5.5 Equipment

Computers and automated equipment

1. The provider shall ensure that any software used on computers or automated equipment is documented in sufficient detail and is suitably validated or verified as being adequate for use. This includes any software, developed, configured or modified by the provider or by other outside agencies working on the provider's equipment.
2. User acceptance testing shall be performed prior to software and/or related equipment being placed in service. For example when returning from calibration/maintenance or following a move.
3. Commercial off-the-shelf software and software tools whose operation has an impact in obtaining results will require validation, or any existing validation to be verified, as laid out in **5.4.5 Validation of methods**.
4. Other commercial off-the-shelf software (e.g. Microsoft® Word and Excel) which does not directly contribute to results obtained shall be considered suitably validated for general use. However, calculations embedded in spreadsheets which do not form

part of a validated electronic process should be included in the required systematic checks.

5. The provider shall maintain records of software products installed on specific computer systems, and shall ensure that only specified versions of software and firmware are in use.[29] The provider shall have documented procedures for configuration management to ensure that all changes to software/hardware are controlled and that all individual software installations are known and are periodically checked that the correct version is installed and no unauthorised modifications have occurred.
6. All items of equipment containing sensitive data shall be checked to ensure the data has been removed or securely overwritten prior to disposal.

5.6 Measurement traceability

5.6.3.3 Intermediate checks

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

5.8 Handling of test items

Receipt of cases and exhibits at the laboratory

1. There should be a documented risk based case acceptance procedure for the handling of recoverable irregularities or rejection of an exhibit for examination arising from, but not limited to:
    a. a missing exhibit label;
    b. an unacceptably low level of agreement between the details on an exhibit label and those on the accompanying submission documentation;
    c. inconsistency between the details on an exhibit label and/or accompanying submission documentation and what the exhibit actually is;
    d. illegibility in the name, identification number or any other information on an exhibit label;
    e. there being more than one label on an exhibit;
    f. appropriate control samples not submitted;
    g. repeat of the same identification details on different exhibit labels;
    h. inadequate or untimely packaging or sealing of an exhibit that could prejudice its integrity;
    i. previous handling, storage or evidence of tampering with an exhibit that could prejudice its integrity; and
    j. insufficient material being available for meaningful examination or analysis.
2. If the provider is unable to accept the submission the reasons for rejection shall be recorded.

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

3. Any evidence of tampering with an exhibit shall be investigated. If the outcome of the investigation indicates a deliberate attempt has been made to influence the results of the laboratory examination, the Regulator shall be informed.

4. The case acceptance procedure shall also specifically address the handling and receipt or rejection of potentially hazardous exhibits that might pose a risk to the health or safety of staff,[30] or potentially compromise other work carried out at the laboratory,[31] or which may not be lawfully retained or handled if accepted by the laboratory.[32]

Case assessment and prioritisation

5. Prior to commencing work the provider shall, in consultation with the customer, identify the issue(s) in the case, develop an appropriate examination strategy and agree the timescale for the delivery of the results. This may be in an overarching SLA/Contract for more routine casework.

6. In developing the examination strategy, as appropriate and as far is practicable the practitioner shall:[33]

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

    b. ensure that either all the necessary information and exhibits required for an effective examination strategy are provided or that any resultant limitations to the scope of the examination are discussed with the customer;

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

    d. select and prioritise the examinations according to the needs of the investigation, or the instructing solicitor, and with consideration to the exhibits available.

Exhibit handling, protection and storage

7. The provider shall ensure that exhibit handling policies and procedures address continuity requirements including but not limited to:

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

    b. that the exhibit can be conclusively shown to be the exhibit submitted to the provider;

[30] For example when handling hypodermic syringe needles or blood samples.

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

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

[33] For further guidance, see Skills for Justice CN702 Determine the forensic examinations to be undertaken.

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

d. any results can be conclusively linked back to the exhibit or sub-sample from which it came; and

e. the provider can show whether the exhibit was retained, returned to the organisation that submitted it or destroyed.

f. the measures to secure exhibits which have to be left unattended.

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

Exhibit return and disposal[34]

9. The provider shall have an agreement with its customers for the return or disposal of exhibits, and evidential material recovered from exhibits, once the laboratory examination has been completed.

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

    a. human tissue;[35]

    b. drugs;

    c. section 5 firearms; and

    d. indecent images of children.

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

12. Biohazardous exhibits shall be destroyed by the provider in accordance with Health and Safety legislation and Regulations and Home Office Guidelines.[36]

---

[34] Also see ACPO (2003) *The Forensic Science Service: retention of case material a memorandum of understanding between ACPO and FSS*.

[35] See Human Tissue Act 2004

[36] See HOC 40/73: Handling and disposal of blood samples in criminal cases (other than those brought under the Road Traffic Act 1972): recommends to Chief Police Officers that on completion of examination the sample should be retained at the laboratory and the Defence notified that it will be destroyed after 21 days unless they request otherwise. However, if the sample is exhibited, it should not be destroyed without the permission of the committing court. HOC 41/73 provides similar recommendations to HOC 40/1973, but to the courts. HOC 125/76 extends the arrangements of HOC 40/1973 and 41/1973 to the handling and disposal of saliva samples. HOC74/82: Disposal of blood samples, saliva samples and swabs stained with

5.9 Assuring the quality of test results

Interlaboratory comparisons (proficiency tests and collaborative exercises)

1. The provider shall investigate the availability and appropriateness of schemes for interlaboratory comparisons which are relevant to their scope of accreditation.[37,38,39]
2. The provider shall participate in appropriate schemes, in order to monitor the validity of its examinations or tests, and its performance, both against its own requirements and against the performance of peer providers.[40]
3. When participating in interlaboratory comparison schemes, the provider's own documented methods and procedures shall be used.
4. Unexpected performance in inter-laboratory comparisons shall be handled as non-conforming testing (**4.9 Control of non-conforming testing**).

5.10 Reporting the results

5.10.1 General

1. The provider shall have a detailed communications strategy and procedures, and assign roles and responsibilities, to ensure the appropriate exchange of information, reports and evaluative statements with the police and prosecuting authorities, both nationally and locally, or with the instructing solicitor, as appropriate, within agreed timescales in accordance with the requirements and needs of each specific case and the known key dates in the criminal justice system process.[41]
2. The provider shall provide early warning of any operational or scientific issues which could unavoidably affect the timeliness of service delivery.
3. The reporting scientist shall be appropriately competent and have had sufficient involvement in the work carried out to meet any requirements of the CJS and relevant National Occupational Standards.
4. Full records shall be kept of work done and the results obtained even if the customer does not require a detailed report or statement.[42]

---

body fluid: handling of exhibits: extends the arrangements of HOCs 40/1973, 41/1973 and 125/1976 to the disposal of swabs stained with body fluid. HOC25/87 extends the provisions of HOC 74/1982 to cover the disposal of urine and any other body samples not previously covered.

[37] Laboratories may refer to the EPTIS database or the ENFSI website (http://www.enfsi.eu/page.php?uid=93) for the availability of PT Schemes.

[38] ISO/IEC 17025 requires laboratories to evaluate suppliers, this includes PT providers. ISO/IEC 17043:2010, Part 1 and ILAC G13:08/2007 contain recommendations and guidance on the requirements for the operation of PT schemes. These documents should be used as a basis for such an evaluation.

[39] UKAS accredits PT Providers to ISO/IEC 17043:2010; a list of accredited schemes/providers is available on www.ukas.com. UKAS recommends the use of an accredited scheme where one exists.

[40] See TPS 47 UKAS Policy on Participation in Proficiency Testing.

[41] See Protocol for the Supply of Forensic Science Services to the Police and the Crown Prosecution Service, 2006.

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

5.10.2/5.10.3 Test reports,[43] statements and the presentation of evidence

Reports and statements to the CJS

1. Providers shall ensure that all staff who provide expert evidence have a sufficient level of experience, knowledge, standing in the peer group and, where appropriate, qualifications, relevant to the type of evidence being adduced, to give credibility to the reliability of the work undertaken and the conclusions drawn. They shall also ensure that they are able to explain their methodology and reasoning, both in writing and orally, concisely and in a way that is comprehensible to a lay person and not misleading.
2. Providers shall ensure that all staff who provide expert evidence based on scientific methodology are additionally able to demonstrate, if required:
    a. whether there is a body of specialised literature relating to the field;
    b. that they have complied with part 33 of the Criminal Procedure Rules 2010[44] and that the principles, techniques and assumptions they have relied on are valid;
    c. that any database they have relied on is sufficient in size and quality to justify the nature and breadth of inferences drawn from it, that the inferences are logically sound and that alternative hypothesises in the investigative mode and alternative propositions in the evaluative mode have been properly considered;
    d. their methodology, assumptions and reasoning have been considered by other scientists and are regarded as sound, or where challenged, the concerns have been satisfactorily addressed; and
    e. the impact the uncertainty of measurement associated with the application of a given method could have on any conclusion.
3. Providers shall ensure that all staff who provide expert evidence based on their practical experience and/or their professional (non-scientific) knowledge are additionally able to provide:
    a. an explanation of their methodology and reasoning;
    b. reference to a body of specialised literature relating to the field of expertise and the extent to which this supports or undermines their methodology and reasoning;
    c. an assessment of the extent to which their methodology and reasoning are now accepted by their peers together with details of any outstanding concerns; and
    d. specific instances which support or undermine their claim to expertise or accepted professional practice and methodology resulting in demonstrably valid or misleading opinion, and an explanation of how these have a bearing on the matter(s) in issue.

[43] The provider should indicate the accreditation status for the work undertaken on the report.

[44] Part 33 of Criminal Procedure Rules 2010 applies to experts giving evidence in the criminal courts in England and Wales; available at: http://www.justice.gov.uk/criminal/procrules_fin/part_33.htm

Self certification

4. Unless otherwise mandated, all experts instructed by the police/prosecuting authorities shall complete, upon receipt of their instructions, a signed and dated self certificate as laid out in the Guidance Booklet for Experts[45] and send it to the disclosure officer or investigating officer.

Mandatory requirements, declarations and content for reports and statements from experts[46]

5. Where an expert's evidence/opinion is to be presented in court, the provider shall ensure that the expert practitioner's report or statement is signed and dated by the person who made it and contains:
    a. a declaration of the age of the author, if under 18 years, or a declaration that the author is 'over 18';
    b. a declaration that the author makes the statement believing its contents to be the truth (to the best of their knowledge and belief) and understanding that if it is tendered in evidence they would be liable to prosecution if they wilfully stated in it anything they knew to be false or did not believe to be true;[47]
    c. a declaration that the expert has complied with their duty to the court to provide independent assistance by way of objective unbiased opinion in relation to matters within their expertise and an acknowledgement that the expert will inform all parties, and where appropriate the court, in the event that their opinion changes on any material issues;
    d. a declaration which confirms that the expert understands their duty to the court in respect of disclosure,[48] as laid out in the Guidance Booklet for Experts.[49]
6. The expert practitioner shall also provide in their report or statement, in addition to complying with these requirements:
    a. the findings on which they have relied in making the report or statement;
    b. details of which of the findings stated in the report or statement are within their own knowledge, which were obtained as a result of an examinations, measurements, tests, etc. carried out by another person and whether or not those examinations, measurements, tests, etc. were carried out under the expert's supervision;
    c. the identity, qualifications, relevant experience and any certification of the person who carried out the examination, measurement, test, etc.;

[45] Appendix C of ACPO/CPS Guidance Booklet for Experts, Disclosure: Experts' Evidence, Case Management and Unused Material, May 2010.

[46] See Criminal Procedure Rules 2010.

[47] Declarations of truth in witness statements are required by section 9 of the Criminal Justice Act 1967 and by section 5B of the Magistrates' Courts Act 1980.

[48] In compliance with the overriding objective of Rule 1 of the Criminal Procedure Rules 2010.

[49] As detailed in Appendix B of ACPO/CPS Guidance Booklet for Experts, Disclosure: Experts' Evidence, Case Management and Unused Material, May 2010.

d. details of any statements of fact, literature or other information upon which they have relied, either to identify the examination or test requirements, or which are material to the opinions expressed in the report or statement or upon which those opinions are based;

e. a summary of the conclusions and opinions reached and a rationale for these;

f. a statement that if any of the information on which their conclusions or opinions are based changes then the conclusions or opinions will have to be reviewed;

g. where there is a range of opinion on the validity or robustness of a scientific technique on the matters dealt with in the report or statement, a summary of the range of opinion, and reasons for the expert's own opinion;

h. any information that may cast doubt on their interpretation or opinion; and

i. if the expert is not able to give an opinion without qualification, what the qualification is.

Report types

7. Providers can be required to supply both expert advice to support the investigative process and expert evidence to support the judicial process.

8. This can involve the provision of:

a. Interim progress reports to support investigations: an initial forensic investigation report used for an initial assessment of the forensic exhibits that may help an enquiry, interview or strategy. This report is non-evidential but can be used for disclosure.

b. Streamlined Forensic Report, Stage 1 (non-section 9[50]): this is a three page document for where experts are not intended to give evidence at Court:

i. Page 1 - Initial Forensic Result / Key evidence suitable for Charge and First Hearings

ii. Page 2 - Prosecution to record identified issues where they exist through the Case Management process or where SFR Stage 1 evidence is agreed, CJA 1967 Section 10 admittance to be signed by Prosecution and Defence.

iii. Page 3 - Disclosure - Unused material

c. Streamlined Forensic Report, Stage 1 (section 9): this is a one page report produced in section 9 format added three page SFR after case management for the committal stage.

d. Streamlined Forensic Report, Stage 2, Case Issues: this is required if the Defence either do not accept the information in the SFR 1 or contest any forensic issues in the case then the customer will request further work to be done and reported using the SFR 2 or request a full evaluative statement.

e. Full evaluative statements for use in court proceedings.

[50] Section 9 of the Criminal Justice Act 1967

Retention, recording, revelation and prosecution disclosure

9. If a practitioner has carried out a test at the request of the police or prosecution, or if such a test has been carried out at their laboratory and is known to him, which casts doubt on their opinion, they shall also reveal this to the police and prosecuting authorities.

10. Experts instructed by prosecuting authorities must assist their customers to discharge their statutory responsibilities regarding disclosure.

11. The aim of disclosure is to ensure that there is a fair system for informing the defence of relevant unused material which may assist it in timely preparation of its case. The term 'material' comprises the primary records contained on the case file, any pertinent materials recovered or generated during the testing or examination and any secondary records such as batch records, standardisation and calibration records, audio and video tapes, computer records and survey information. 'Unused material' is that which is not identified within the expert's report(s) or statements(s).

12. Suppliers must conform to the requirements of the Memorandum of Understanding between ACPO and forensic service providers,[51] which outlines how providers are to support the disclosure process and provide access to the defence, and the further guidance which is set out in the ACPO/CPS Guidance Booklet for Experts on Disclosure: Experts' Evidence and Unused Material.

13. All documents, exhibits and evidential material recovered from exhibits that are retained by providers shall be archived in secure storage, in conditions to prevent damage or deterioration, and indexed so as to facilitate orderly storage and retrieval.[52]

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

Defence examinations

15. The provider must have defined policies and procedures to facilitate access by defence examiners to carry out a review of the work already completed by the provider in the relevant case.

16. The policies and procedures shall be based appropriate guidance such as the ACPO/CPS Guidance Booklet for Experts, Disclosure: Experts' Evidence, Case Management and Unused Material, May 2010.

17. The policies and procedures must ensure the security and integrity of the exhibits and records requested for review but must also ensure the confidentiality of other work in progress or previously undertaken by the provider to which access has not been granted.

18. A Defence practitioner seeking pre-trial access to any case material shall first obtain written approval for access to these from the prosecutor (or Coroner if the prosecuting authority is not involved at that stage).

---

[51] ACPO (2003) The Forensic Science Service: retention of case material a memorandum of understanding between ACPO and FSS.

[52] The cost of archiving documents relating to the provider's testing and examinations is a business cost to be borne by the provider. Reimbursement of the costs for archiving exhibits and evidential material recovered from exhibits is a business matter to be agreed between the provider and police.

19. The provider shall make available to the Defence practitioner only what has been deemed by the prosecutor to be relevant.
20. The provider shall ensure that all examinations and tests carried out on the provider's premises by the Defence are adequately supervised to ensure that they are carried out in accordance with the instructions given by the prosecutor and that nothing is altered, damaged or destroyed without the prior permission of the prosecutor.
21. The provider shall provide copies of any relevant case file records, documents and supporting information, etc. reasonably requested by the Defence, in hardcopy or secure electronic form, to take into their possession for examination away from the provider's premises.[53] The provider shall require that all such material is returned or destroyed, as appropriate, once it has served the specific purpose for which it was provided.
22. The provider shall only release exhibits to the Defence, or any part of them, or evidential material recovered from them, for examination or testing away from the provider's premises, on receipt of written instructions from the prosecutor. Where the examinations or testing might affect their condition, the provider shall ensure that the prosecutor is aware of this before they are released.
23. The provider shall ensure that all exhibits, or parts of exhibits, or evidential material recovered from them, that are to be released to the Defence are securely packaged and labelled. The provider shall also retain a signed record of the transfers for continuity purposes.
24. The Defence practitioner shall ensure that any tests or examinations they conduct, or are conducted on their behalf by someone other than the original provider, are carried out in accordance with the requirements set out in these Codes and that they also comply with any conditions attached by the prosecutor to the release of the exhibits, or parts of exhibits, or evidential material recovered from them.
25. The provider shall check the integrity and continuity records of the returned exhibits, or parts of exhibits, or evidential material for compliance with any conditions of release. Any deficiency in these respects shall be communicated immediately to the prosecutor and police.

5.10.5 Opinions and interpretations

1. Providers working in the forensic field are often asked to offer an opinion or an interpretation in order to assist in the understanding of the results they have produced as part of the analysis or examination of forensic exhibits.
2. Where a provider wishes to have this aspect included within their accredited scope they will need to ensure that they are in compliance with the UKAS publication LAB 13.[54]

[53] It would be reasonable to charge the Defence for any use of facilities or equipment, or for the provision of copies of documents in hardcopy or electronic form under the disclosure regime.

[54] See UKAS LAB 13: Guidance on the Application of ISO/IEC 17025 - Dealing with Expressions of Opinion.

Bibliography

Home Office Circulars

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

HOC 41/73: *Handling and disposal of blood samples.*

HOC 125/76: *Handling and disposal of saliva samples.*

HOC 55/1980: *Risk of infection from stained exhibits.*

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

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

Standards and related documents

BS 10008:2008, *Evidential weight and legal admissibility of electronic information – Specification.*

BS 25999-1:2006, *Business continuity management – Part 1: Code of practice.*

BS 25999-2:2007, *Business continuity management – Part 2: Specification.*

BS EN ISO 9001:2008, *Quality Management Systems – Requirements.*

BS EN ISO/IEC 15189:2007*, Medical laboratories - Particular requirements for quality and competence*.

BS EN ISO/IEC 17020:2004, *General criteria for the operation of various types of bodies performing inspection*.

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

BS ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements.*

BS ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management* .

Clinical Pathology Accreditation (UK) Ltd., *Standards for the Medical Laboratory.*

EA-5/03: ENFSI/EA, *Guidance for the Implementation of ISO/IEC 17020 in the field of crime scene investigation.*

Good Manufacturing Practice, *The Rules and Guidance for Pharmaceutical Manufacturers and Distributors (The Orange Guide).*

ISO/IEC 17043:2010, *Conformity assessment -- General requirements for proficiency testing*.

IAF/ILAC-A4:2004, *Guidance on the Application of ISO/IEC 17020.*

ILAC-G13:08/2007: *Guidelines for the Requirements for the Competence of Providers of Proficiency Testing Schemes*.

ILAC-G19:2002, *Guidelines for Forensic Science Laboratories.*

ISO/IEC Guide 99:2007: International vocabulary of metrology -- Basic and general concepts and associated terms (VIM).

National Occupational Standards. Available from: http://www.skillsforjustice.com/template01.asp?pageid=509. [Accessed 19 July 2010].

Statutory Instrument 1999 No. 3106, *The Good Laboratory Practice Regulations 1999.*

UKAS® LAB 13: 2001: *Guidance on the Application of ISO/IEC 17025 Dealing with Expressions of Opinions and Interpretations.*

UKAS® LAB 39: 2004: *UKAS Guidance on the Implementation and Management of Flexible Scopes of Accreditation within Laboratories.*

UKAS® M 3003: 2007: *The Expression of Uncertainty and Confidence in Measurement.* Edition 2.

Other documents

ACPO (2003) *The Forensic Science Service: retention of case material a memorandum of understanding between ACPO and FSS*. Available from:

http://www.acpo.police.uk/asp/policies/Data/baker_mou_retention_case_material_main.doc

[Accessed 04/11/10].

ACPO (2010) *Guidance on the management of police information*, Second Edition. Available from: http://www.acpo.police.uk/asp/policies/data/MoPI%202nd%20Ed%20Published%20Version.pdf [Accessed 19/07/10].

ACPO/CPS (2010) *Guidance Booklet for Experts, Disclosure: Experts' Evidence, Case Management and Unused Material*. Available from:http://www.cps.gov.uk/publications/docs/experts_guidance_booklet.pdf. [Accessed 19/07/10].

Cabinet Office (2008) *HMG Security Policy Framework*, V 1.0. Available from: http://www.cabinetoffice.gov.uk/media/111428/spf.pdf. [Accessed 19/07/10].

CPS (2006) *Protocol for the Supply of Forensic Science Services to the Crown Prosecution Service*. Available from: http://www.cps.gov.uk/publications/docs/forensic.pdf. [Accessed 19/07/10].

CPS (2009) *Convention Between Prosecuting Authorities: to provide arrangements for ensuring effective co-ordination of decision making and handling in related cases which are the responsibility of different authorities*. Available from: http://www.cps.gov.uk/legal/a_to_c/convention_between_prosecuting_authorities/#a02. [Accessed 19/07/10].

Criminal Procedure Rules (2010). Available from: http://www.justice.gov.uk/criminal/procrules_fin/part_33.htmENFSI (2007)

ENFSI (2007) Guidance for best practice sampling in forensic science, Available from: www.enfsi.eu/get_doc.php?uid=181. [Accessed 19/07/10].

Frieberg, A. (2010). *Re-stocking the regulatory tool kit*. Biennial Conference of the European Consortium on Political Research Standing Group on Regulatory Governance, June 17-19, 2010, Dublin. Available from: http://regulation.upf.edu/dublin-10-papers/1I1.pdf. [Accessed 19/07/10].

SWGDAM (2004) Revised Validation Guidelines, Scientific Working Group on DNA Analysis Methods (SWGDAM), Forensic Science Communications July 2004 – Volume 6 – Number 3. Available from: http://www.fbi.gov/hq/lab/fsc/backissu/july2004/standards/2004_03_standards02.htm. [Accessed 19/07/10].

Abbreviations

ACPO	Association of Chief Police Officers of England, Wales and Northern Ireland
BS	British Standard
CJS	Criminal Justice System
CPIA	Criminal Procedure and Investigations Act 1996
CPS	Crown Prosecution Service
DNA	Deoxyribonucleic Acid
EN	European Norm
ENFSI	European Network of Forensic Science Institutes
FSP	Forensic Science Provider
FSS	Forensic Science Service
GLP	Good Laboratory Practice Regulations 1999
GMP	Medicine and Healthcare Products Regulatory Agency, Inspection and Standards Division, Rules and Guidance for Pharmaceutical Manufacturers and Distributors, 2007, Section II: Guidance on Good Manufacturing Practice
HACCP	Hazard Analysis and Critical Control Point
HOC	Home Office Circular
IAF	International Accreditation Forum
IEC	International Electrotechnical Commission: an organisation that prepares and publishes International Standards for all electrical, electronic and related technologies.
ILAC	International Laboratory Accreditation Cooperation
ISO	International Organisation for Standardisation: a network of the national standards institutes of 157 countries.
MG	Prosecution Team Manual of Guidance - 2004
MoPI	Management of Police Information
PT	Proficiency Testing
SFR	Streamlined Forensic Report
SLA	Service Level Agreement
UKAS®	United Kingdom Accreditation Service: the sole national accreditation body recognised by government to assess UK organisations that provide certification, testing, inspection and calibration services.

Glossary

Accreditation

Third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks.

Accuracy

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

Analyte

Substance to be identified or measured.

Audit

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

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

External audit: includes what are generally termed a "second-" or "third-party audit". Second-party audits are conducted by parties having an interest in the organisation, such as customers, or by other persons on their behalf. Third-party audits are conducted by external independent organisations. Such organisations provide certification or registration of conformity with requirements such as those of BS EN ISO 9001:2008.

Blank

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

Calibration

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

Collaborative exercise

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

Contamination

The undesirable introduction of substances or trace materials.

Control sample

A matrix-matched standard used to determine the linearity and stability of a quantitative test or determination over time, prepared from a reference material

(weighed or measured separately from the calibrators), purchased or obtained from a pool of previously analysed samples.

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

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

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

Critical findings

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

- have a significant impact on the conclusion reached and the interpretation and opinion provided;
- cannot be repeated or checked in the absence of the exhibit or sample;
- could be interpreted differently.

Customer

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

Databases

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

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

b) providing statistical information.

Expert (witness)

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

Firmware

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

Hazard Analysis and Critical Control Point (HACCP)

HACCP is a process control methodology used in the food and pharmaceutical industry to prevent the introduction of undesirable substances at specific points and stages of a process.

Investigating body

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

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/shoemark/toolmark examination; microscopic identifications).

Nonconformity

The non-fulfilment of a requirement either within the organization's policies, procedures or the specification of the customer.

Organisation

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

Practitioner

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

Product

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

Proficiency tests

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

Open or declared proficiency test: a test in which the analysts are aware that they are being tested.

Blind or undeclared proficiency test: a test in which the analysts are not aware that they are being tested.

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

Precision

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

Provider

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

Quality

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

Quality manual

A document specifying the management system of an organisation.

Recovered sample

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

Reference material

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

Reference standard

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

Requirement

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

Risk

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

Robustness

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

Ruggedness

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

Sample

A representative portion of the whole material to be tested.

Scene

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

Schedule of accreditation

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

Scope of accreditation

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

Selectivity (or Specificity)

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

Standard operating procedure

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

Subcontractor

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

Supplier

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

Uncertainty of measurement

The estimation of the uncertainty of measurement is ISO/IEC 17025:2005 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 specific purpose intended.

Verification

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