Understanding the Forensic Science Regulator (FSR) Statutory Code of Practice

A deep dive into the Code, what it means for you, and paving the next steps for your organisation

Chorus

Discover · Link · Solve

1.0 Executive Summary

The 2nd of October 2023 marked a milestone for the policing and criminal justice industry with the enforcement of the Forensic Science Regulator's Statutory Code of Practice ('The Code'). The Code sets out quality standards for Forensic Science Activities (FSAs) related to criminal investigations in England and Wales and aims to ensure that forensic evidence used in criminal proceedings is of the highest quality.

The Forensic Science Regulator, Gary Pugh, hailed the Code as a "significant achievement", confirming that it was "the first time that a statutory Code of Practice relating to the provision of forensic science has been produced anywhere in the world." We couldn't agree more and welcome the regulations as a positive leap forward for the industry and an empowering opportunity for practitioners to deliver a standard of excellence.

Steps must be taken to prepare for and ensure compliance to the Code, and we have received many enquiries from our user community seeking clarity on what must be done to achieve this. Rest assured; Chorus will provide full support throughout this process.

Chorus recently met with representatives from the FSR to get some key questions answered and to ensure we are fully up to date. This report sets out confirmations from that meeting, including everything you need to know about the regulations, how it will affect you, how it will affect Chorus, what you must do to ensure compliance and when it needs to be achieved.

Whilst the Code consists of over 300 pages and applies to more than 30 FSAs, this report focuses solely on the Digital (DIG) FSAs that directly impact Chorus users. This includes:

DIG 100 - Data capture, processing, and analysis from digital storage devices; and

DIG 200 – Cell site analysis for geolocation.

2.0 Understanding the Code

2.1 Why is the Code being introduced?

As laid out in the Code, forensic science plays a critical role in criminal investigations, not only for identifying offenders and providing key evidence to courts, but it also safeguards against false allegation and wrongful conviction.

However, forensic science examinations by their nature also carry significant risks. If individual and/or system errors occur, incorrect evidence could be put forward, resulting in quality failures that could lead to miscarriages of justice or failed prosecutions.

The Code has been put in place to ensure that quality failures do not occur, and that accurate and reliable scientific evidence is continually put forward.

2.2 How does the Code define 'Quality Management'?

The Code defines the key elements of quality management as follows:

1. Validation of methods.
2. Defining, demonstrating, and testing the initial and ongoing competence of personnel.
3. Having documented and controlled procedures, and an internal audit process to ensure they are effective and being followed.
4. Commitment from senior leadership, including making available sufficient resources

5. Enabling continual improvement.

It is of the utmost importance that these quality management standards are complied with. The Code is a direct response to the Forensic Science Regulator Act 2021 and as such, provides the Regulator with legal powers to intervene if quality standards are not being demonstrated.

3.0 Achieving Compliance

3.1 When do you need to be compliant?

The Code has already come into force (2nd October 2023). However, for practitioners undertaking FSAs in relation to cell site analysis for geolocation (FSA - DIG 200), there is a **24-month period** from this date to achieve compliance (2nd October 2025).

3.2 How to achieve compliance and when to declare it

Compliance is demonstrated by having accreditation to ISO/IEC 17025. Rest assured; many law enforcement organisations already hold a level of accreditation to this. Policies, procedures, and processes will already be in place across various departments to ensure sufficient quality management and standards of practice.

The Code acts as an extension to this to ensure excellence in FSAs.

During this time, you should undertake careful gap analyses and make any necessary adjustments before making a concluding declaration of compliance or non-compliance.

Chorus is here to support you in achieving compliance we have detailed how we can help throughout this document, particularly in regard to competence and training support as well as validation processes.

4.0 Eligibility

4.1 Who does the Code apply to?

A key takeaway from our conversations with representatives from the FSR is that the Code does not relate to a specific job role or department. It relates to key activities that are undertaken by practitioners. The Code is therefore job role agnostic.

This is important to note as from conversations we have had with users, some perceive the Code to only apply to Analysts and RF technicians. This is not the case.

To clarify, **The Code must be adhered to by practitioners who work with/provide communications data as evidence and/or appear in court as a witness of fact. These individuals must gain ISO/IEC 17025 accreditation.**

The Code and associated ISO/IEC 17025 accreditation must also be adhered to by practitioners who engage in Radio Frequency (RF) surveying, cell site analysis and who may offer expert opinion on the data.

The roles that would fall under regulation from the Code would typically include Analysts, Investigators, RF technicians and/or similar. But if any role outside of these areas engage in such activities, they must also adhere to and be aware of the regulations.

4.2 Who is exempt from the Code?

Practitioners who work with communications data (e.g., Call Data Records (CDRs), cell site analysis, geolocation data) but their work is not intended as evidence i.e., it is purely for *investigative purposes*, **are exempt from the Code**.

For more information on exemption, refer to section 6.0 'Key FSAs to which the Code does not apply' in this document.

4.3 What does the Code mean for Chorus?

Chorus provides its users with the tools to cleanse, format, filter and query CDR data and plot cell site locations on maps. It does not offer opinions on those data points or perform the actual analysis. For this reason, Chorus, as a software tool, does not fall under the requirement to become ISO/IEC 17025 accredited. This has been confirmed by the FSR.

Although the Code doesn't directly impact Chorus as a software tool, it does impact most of our customer base across UK law enforcement. For this reason, Chorus is dedicated to fully supporting its users on their journey to accreditation and in ensuring that evidential products generated through its software are fully compliant. Whilst Chorus has always adhered to clear and transparent processing of data, we are currently discussing with ISO accreditors what more we can do to demonstrate that our tools and processes follow best practice.

5.0 Key FSAs to which the Code applies

5.1 FSA – DIG 100 – Data capture, processing, and analysis from digital storage devices

FSA – DIG 100 is the section of the Code which covers FSAs related to the capture, processing, analysis, and interpretation of data using both manual and automated processes.

5.1.1 Activities covered under FSA - DIG 100

Practitioners should refer to **section 82** of the Code to familiarise themselves with all activities covered. These include:

1) **Screening of a digital storage media/device for a decision on seizure/prioritisation (e.g., using a triage software tool or off-the-shelf tool).** Media includes but is not limited to:

- Standalone storage devices
- Components
- Remotely stored electronic data (e.g., cloud storage)
- Phones
- Personal computers
- Tablets
- Drones

- Vehicle systems

2) **Capture and processing of data from submitted/seized devices or digital storage media accessed from such devices**. Activities include, but are not limited to:

- **Examination of a device**, media, or component to locate or capture and preserve.
- **Processing of digital data** to produce meaningful information, either by a manual or automated process, to allow for subsequent analysis and/or reporting to take place.
- **Analysis of information** related to communications (e.g., calls, emails, texts), records related to the location of a device e.g., GPS, file data, malware etc.

5.1.2 What is excluded from FSA - DIG 100?

The following key activities are not covered by the Code.

- Screening of media for the purpose of offender management.
- Screening devices prior to seizure of a device at ports and other locations under Schedule 7 Terrorism Act 2000, Schedule 3 Counter Terrorism and Border Security Act 2019 (provided continuity information is available).
- Tachograph analysis.
- Recording and transfer of emergency calls using a controlled system.
- Extraction and editing of force-generated audio-video material from force-controlled systems.
- Upload and download of audio-visual media from digital asset management systems.
- Acquisition of data utilising the Crime (Overseas Production Order) Act 2019, and the analysis and processing of that data.
- Data recovery via Internet Intelligence & Investigations (III), Open-Source Intelligence (OSINT), Signals Intelligence (SIGINT), Communications Intelligence (COMMINT) and Geospatial Intelligence (GEOINT).
- Activity relating to the INTERPOL database(s).

5.1.3 How to achieve compliance with FSA – DIG 100

The activities outlined in FSA - DIG 200 must be complied with in accordance with the Code and by having the appropriate accreditation (ISO/IEC 17025).

Practitioners should also adhere to the specific requirements for this FSA (**see section 108: Digital Forensics**). This section outlines clear standards of practice relating to method development and validation. Refer to section ‘9.0 - Methods and validation’ in this document for a summary of the criteria required for the validation process.

5.1.4 When is compliance required?

The Code has already come into force for FSA – DIG 100 (2nd October 2023).

5.2 FSA – DIG 200 – Cell site analysis for geolocation

FSA - DIG 200 is the section of the Code which outlines regulatory standards for FSAs related to Radio Frequency (RF) surveys, mapping and/or cell site analysis for geolocation of a device.

5.2.1 Activities covered under FSA - DIG 200

Cell site analysis effectively relies on the processing of communications and survey data and presentation of that data in the form of maps, tables, charts or other reports and is covered by DIG 200. Key activities covered include:

- The production and evaluation of RF propagation surveys of an area or location guided by CDRs.
- Processing of CDRs for the purposes of cell site analysis.
- Creating/adopting maps of cell sites and/or cell site coverage for the purpose of reporting to court.
- Assessment and evaluation of CDRs against survey data.
- Any of the above to determine the geolocation of a suspect device.

5.2.2 What is excluded from FSA - DIG 200?

The following key activities are not covered by the Code:

- Acquisition of communications data performed in accordance with the Investigatory Powers Act 2016 and related codes of practice.
- Acquisition and analysis of data utilising the Crime (Overseas Production Order) Act 2019.
- Acquisition of data from cloud storage as a result of login/connection data taken from a device under examination.
- Acquisition of data from cloud storage using just the seized or surrendered SIM card.

5.2.3 How to achieve compliance with FSA - DIG 200

The activities outlined in FSA - DIG 200 must be complied with in accordance with the Code and by having the appropriate accreditation (ISO/IEC 17025).

Practitioners should also adhere to the specific requirements for this FSA (see section 110: Cell site analysis for geolocation). This section outlines clear standards of practice for setting an examination strategy, what to do in the checking and review process, key competencies, and method validation. Key requirements include, but are not limited to:

Setting an examination strategy

The examination strategy of any given Police Constabulary should focus on ensuring that all requests for data are appropriate, material supports the request, there are clear propositions to be addressed, and that an outline plan/strategy exists on how the practitioner plans to evaluate the proposition. It could include an independent review of the proposed survey strategy or justification for not surveying.

Checking and review

Practitioners undertaking cell site analysis for geolocation analysis should carry out the following checks:

- **Examination strategy check** – You should ask the following questions during an examination check:
    - Has the question presented been addressed?
    - Is the method used applicable to the purpose?
    - Is the question presented within the expertise of the practitioner etc.

- **Technical check –** This is a process to ensure information is correctly presented, opinions are supported and that methods have been followed.

- **Critical finding check –** This should involve the review of technical findings against the proposition and an independent conclusion is drawn.

Competence

FSA – DIG 200 sets out specific competency and training requirements for individuals engaged in cell site analysis for geolocation purposes. These competencies relate to technical activities including surveys, mapping, and CDR normalisation. The responsibility is on the forensic unit to develop a competency framework and to ensure individuals engaged in these activities have received the necessary training and level of expertise required.

Method development and validation

Much like FSA – DIG 100, method development and validation is also a key requirement when conducting cell site analysis for geolocation purposes. The whole process i.e., from request/receipt of call data through to provision of final opinion must be validated for the method to be acceptable. Refer to section '9.0 - Methods and validation' in this document for a summary of the criteria required for the validation process.

5.2.4 When is compliance required?

Compliance to FSA – DIG 200 must be achieved within 24 months from when the Code comes into force. To clarify, this would be **2nd October 2025**.

6.0 Key FSAs to which the Code does not apply

6.1 FSA – DIG 101 – Analysis of communications network data

Practitioners that analyse network communications data purely to provide advice, guide or inform an investigation (i.e.: their analysis will not be used as evidence) are exempt from the Code and any requirements for accreditation.

It is important that any reports generated by an unaccredited practitioner, such as products, maps, charts etc. are clearly marked as ***'This forensic information is not intended as evidence'.***

Chorus can help with this. We are currently making changes to our software to add a watermark which can be turned on and off for labelling purposes. This watermark will be able to be applied to signify whether a product has been produced for evidence ('This forensic

information is intended as evidence') or for information only ('This forensic evidence information is not intended as evidence').

Key activities covered by FSA – DIG 101 and are therefore exempt from the Code include:

- Processing and normalisation of CDRs or other network provider data for the purposes of informing the investigation.
- Relational or temporal analysis of CDR information.
- Presumptive automated tools for analysing CDRs, including 'co-location' analysis, and accepting the risks and limitations, including confirmation bias.
- Production of mapping of cell sites and/or cell site coverage for informing the investigation.

7.0 Standards of practice required

Section D of the Code sets out the expected standards of practice for FSAs. Key takeaways from this section include:

7.1 Appoint a Senior Accountable Individual (SAI)

Forensic units must appoint a Senior Accountable Individual (SAI) to be accountable for their compliance with the Code. For units comprising of two or more practitioners, the SAI should be at the level of director, partner, board, chief officer or equivalent. For units with only one practitioner, this individual should be the SAI.

Key requirements of the SAI include:

- Monitor and mitigate the risk of quality failures which could adversely affect an investigation, impede, or prejudice the course of justice in any proceedings.
- Be accountable, on behalf of the forensic unit, in relation to any investigation or compliance action by the Regulator.
- Have the authority to make decisions and deploy resources to address quality matters in the forensic unit.

7.1.1 Ensure business continuity

Forensic units must have business continuity procedures in place to maintain and restore the availability and confidentiality of information, should interruption or failure of processes occur. The business continuity procedures should then be tested, for each area of work and/or site, at least once in an accreditation cycle and the results documented.

7.1.2 Maintain document control

Forensic units must have a policy for document/version control procedures. The retention period for obsolete/superseded documents should also be defined.

7.1.3 Review requests, tenders and/or contracts

Any review taking place at whatever level should be documented. Forensic units should also ensure that a demonstrable audit trail, including justifications and authorisations, is available for each piece of work undertaken.

7.1.4 Create an examination strategy

Forensic units should, prior to commencing work, develop an appropriate examination strategy. This should be included in an overarching SLA contract for more routine case work/examination or developed in consultation with the commissioning party. (Refer to section 20.2 of the Code for full details of what must be included).

Setting an examination strategy for cell site analysis is a key focus of FSA – DIG 200 Cell site analysis for geolocation purposes. Specific requirements for this FSA are set out in section 110 of the Code.

7.1.5 Carry out open and blind critical findings checks

Forensic units should have a procedure for carrying out critical findings checks. A critical finding is information (a fact or opinion) which directly affects the overall conclusions. The forensic unit should designate individuals, whose competence to do so can be demonstrable, to carry out these checks.

If your findings are fully supported by objective data, then the critical finding check may proceed as an *open check*. However, checks should be performed *blind* if the critical finding check is the only substantive quality control procedure for checking that finding and/or the finding to be checked is based on the experience of the practitioner rather than direct objective data. In this instance, blind checks require a second expert, who was not involved in the work being reviewed, to provide an independent opinion.

The checking and review process is a key focus of FSA – DIG 200 Cell site analysis for geolocation. Specific requirements for this FSA are set out in section 110 of the Code.

7.1.6 Perform primary and peer reviews

Primary reviews should be carried out and documented to assess whether the requirements set out have been met, and the forensic unit's policies and processes have been followed.

Peer reviews should also be undertaken. Forensic units should have documented policies, procedures and authorised practitioners for the peer review of case records, including reports. In all reviews, the case record should indicate that the review has been carried out, by whom and when.

If the review process leads to a difference of opinion between the initial and reviewing practitioner, forensic units must have a documented procedure in place for resolution.

8.0 Competence

The Code clearly states that the onus is on the forensic unit to determine a competency framework for its practitioners, dependant on their role.

An emphasis is put on practitioners who report factual evidence based on a validated scientific methodology. They should have a sufficient level of skill, experience, knowledge and, where appropriate, qualifications relevant to the type of evidence being presented. They should also be able to explain their methodology and reasoning, both in writing and orally.

Section 28 of the Code outlines the full criteria for competency compliance. Forensic units should refer to this to understand what is required of its practitioners before undertaking an assessment of their current competence.

8.1 Competence and training support from Chorus

Chorus is here to support you in achieving competency compliance and we are fully engaged with the national working groups to understand exactly what is required and how best to approach this.

We speak regularly with the '*National Analysis Business Group (NABG) FSR Code Sub-group'* to discuss the major requirements concerning competency compliance, in addition to the validation process, training, timescales etc. This group comprises of key practitioners which then provides feedback into the *National Analysis Capability Board (NACB) FSR Code Strategic Group.*

We understand that many of the forces we are working with are also engaged with the national working groups and completing the groundwork to create their own standard operating procedures.

The competency standards are being finalised and once agreed, Chorus is here to fully support you in the competency assessment and training of staff. We can work with you to review current vs required competencies and determine a training path to ensure all practitioners are sufficiently upskilled, where needed.

We are also working closely with our training partner, CloudBreak Analysis, to ensure we can provide the highest standard of training possible.

9.0 Methods and validation

To define, a method is a logical sequence of operations or analysis which may include the use of software, hardware, tools and actions by the practitioner. Validation is required if any of these have been used as part of a method, and if they have an impact in obtaining results.

The Regulator defines validation as: "The process of providing objective evidence that a method, process or device is fit for the specific purpose intended." As defined in Section 30 of the Code, the validation procedure should include where relevant, but is not limited to:

- **Determining the end-user requirements** - Who will use the new method, what it is intended to deliver to them, what statutory and regulatory requirements apply, are there any compatibility issues to be considered etc.?

- **Determining the specification -** A detailed specification should be written for the method, explaining what it can and cannot be used for, and should include technical quality standards.

- **Risk assessment of the method** – Many risk assessment templates are available but one which may be suitable is 'failure modes and effects analysis'. This provides is a step-by-step approach for analysing each stage of a method, looking for potential weakness that might result in a failure and what controls should be put in place to catch, detect or prevent this.

- **Review of the end-user requirements and specification -** The forensic unit must review the requirements collated to ensure that those deemed essential/mandatory have been translated correctly into the specification.

- **Setting the acceptance criteria –** This should be established in advance of the validation study and be based upon the specification, the risk analysis and any control strategies put in place to control identified risks.

- **Validation plan –** This should be carried out once the specification (based on the end-user requirements) has been formally accepted. It should identify 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 have been met.

- **Outcomes of the validation exercise -** A summary of the outcome of the validation exercise should be included in the validation report and a full record of the validation process retained by the forensic unit.

- **Assessment of acceptance criteria compliance -** To establish if the validation work is adequate and has fully demonstrated compliance of the method with the acceptance criteria for the agreed specification and end-user requirements, the evaluation must be carried out by a competent practitioner not involved in the process.

- **Validation report -** The forensic unit should produce a validation report in sufficient detail to allow independent assessment of the adequacy of the work carried out in demonstrating that the method conforms to the specification and is fit for the purpose as stated in the end-user requirements.

- **Statement of validation completion -** The forensic unit should prepare a 'statement of validation completion' on the successful completion of a validation exercise.

- **Implementation plan -** Forensic units should have a plan in place for implementing new methods. Key criteria for this plan can be found in section 30.20 of the Code.

9.1 Validation support from Chorus

Chorus recently met with the National Analysis Capability Board (NACB), to understand how we can support users in the validation process and make it as seamless as possible.

A logical approach discussed, would be for a nominated lead force to own the validation process of Chorus software on behalf of all other forces/organisations that are Chorus users. If this approach is agreed, when a software update is released, any changes to how data is processed will be tested and validated by the lead force only. All other forces/organisations will then be notified and provided all necessary information to reference this process in their Standard Operating Procedure (SOP) documentation.

Once we have further clarity on this suggested process, we will disseminate all details amongst our user community.

Rest assured, we will continue communicating with these groups to ensure the most logical, efficient, and unified processes are agreed.

10.0 Consultation guidance

At this current time (February 2024) the Forensic Science Regulator is undertaking a consultation process to review the draft for the development of version two of the Code. This version will include some amendments to the Code issued under the Forensic Science Regulator Act 2021.

The FSR welcomes representations from persons who are, or are likely to be, carrying on activities to which the proposed code or the Code as proposed to be altered will apply.

The consultation will be open for 4 weeks from the 12th of February 2024 to 00:00 on the 11th of March 2024.

10.1 After the consultation

Following the consultation period, responses will be analysed, and the draft Code will be revised as the Regulator determines. The Regulator will send the Code to the Secretary of State for the Home Department for approval. Following this, the Code will then be laid before Parliament for approval. A response to this consultation exercise will be published on Gov.uk.

Rest assured, Chorus is following this consultation process closely and we will ensure that all updates are communicated to users, as they become available, along with an explanation of what this means for you.