Communication Data Investigation & Intelligence Service Definition

Document title	Communication Data Investigation & Intelligence Service Definition		
Reference No.	IF-SER-008	**Version**	1.0
Author	Simon Young, Digital Investigations Manager		
Reviewed by	Lisa Washer, Head of Cyber		
Issue date	27/01/2026		

UNCONTROLLED WHEN PRINTED

Communication Data Investigation & Intelligence Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Simon Young	Review and amendments	27/01/2026
1.0	Lisa Washer	Final review and publish	27/01/2026

Correlation Chart

Clause	FSR Code of Practice v2	ISO/IEC 17025:2017	ILAC-G19 :06/2022	ISO 9001:2015	ISO/IEC 27001:2022
Review of Requests, Tenders and Contracts	16	7.1	4.1, 4.7	8	4.2

Communication Data Investigation & Intelligence Service Definition

Contents

Communication Data Investigation & Intelligence Service Definition

1. Communication Data Investigation & Intelligence Service

1.1 Service Overview

1.1.1 The Communication Data Investigation & Intelligence Service provides specialist analysis and interpretation of communication data to support investigations, litigation, regulatory enquiries, public inquiries, and internal reviews. The service focuses on identifying, analysing, and contextualising communication records and metadata to establish patterns of contact, timelines of interaction, and relationships between individuals, devices, and accounts.

1.1.2 The service supports lawful and proportionate examination of communication data derived from sources such as telephony records, messaging platforms, email systems, and collaboration tools, enabling evidence-based understanding of communication activity and intent.

1.2 Service Objectives

1.2.1 The objectives of the Communication Data Investigation & Intelligence Service are to:

a) Identify and analyse communication activity relevant to an investigation

b) Reconstruct communication timelines and interaction patterns

c) Establish links between individuals, devices, and accounts

d) Provide intelligence-led insight to support investigative decision-making

e) Deliver defensible findings suitable for legal and regulatory scrutiny

2. Service Features

2.1.1 Key features of the service include:

a) **Call Data Records** – Focus on communications data records provided by Telecoms Operators

b) **Multi-Platform Coverage** – Telephony, messaging, email, and collaboration tools

c) **Timeline and Link Analysis** – Reconstruction of interactions and relationships

d) **Intelligence Visualisation** – Charts, graphs, and relationship mapping

e) **Defensible Methodology** – Transparent, auditable analytical processes

3. Service Benefits

3.1.1 The service delivers the following benefits:

a) Clear understanding of who communicated with whom, when, and how

b) Identification of hidden relationships or patterns of behaviour

c) Improved investigative focus and prioritisation

d) Defensible intelligence suitable for legal or regulatory review

e) Enhanced evidential context for decision-making

f) Evidentially robust, Court-ready outputs

4. Scope of Service

4.1.1 The service is delivered in alignment with applicable laws governing access to and use of communication data, including data protection and investigatory frameworks. Analysis is conducted on lawfully obtained data only. Outputs are prepared to support legal proceedings, regulatory enquiries, and audit requirements. Engagements may be coordinated through legal counsel where legally privileged handling is required.

4.2 In-scope activities

4.2.1 The Communication Data Investigation & Intelligence Service includes:

a) Scoping and definition of communication data requirements

b) Identification of relevant communication platforms and data sources

c) Analysis of call data records (CDRs) and messaging metadata

d) IP address analysis

e) Examination of email headers and communication artefacts

f) Timeline reconstruction of communication activity

g) Link analysis between individuals, accounts, devices, and locations

h) Pattern and frequency analysis to identify anomalies or behaviours

i) Correlation of communication data with other investigative evidence

j) Intelligence reporting and visualisation

k) Advisory support to investigators and legal teams

4.3 Out-of-scope activities

4.3.1 Unless agreed separately, the following are excluded:

a) Interception or real-time monitoring of communications

b) Content monitoring without lawful authority

c) Provision of legal advice or regulatory interpretation

d) Continuous intelligence monitoring services

4.4 Assumptions, Dependencies and Constraints

4.4.1 Delivery of the Communication Data Investigation & Intelligence Service is based on the following assumptions:

a) The client has lawful authority and a valid legal basis to access, process, and analyse all in-scope communication data, including metadata and any associated records.

b) All communication data provided to the service provider has been lawfully obtained and is supplied in accordance with applicable legislation, regulatory requirements, and organisational policies.

c) The scope of the investigation, including relevant individuals, devices, accounts, platforms, and time periods, is clearly defined and approved prior to analysis.

d) Communication datasets provided are complete, accurate, and representative of the agreed scope, subject to known retention or availability limitations.

e) The client will provide timely contextual information, including investigative objectives, incident timelines, and relevant background, to support accurate interpretation of findings.

f) Any legal privilege, confidentiality, sensitivity, or disclosure considerations are identified and communicated at the outset or as they arise during the engagement.

4.4.2 Service delivery is dependent on the following factors:

a) Availability and timely provision of communication data in accessible and supported formats, including call data records, messaging metadata, email headers, or platform exports.

b) Cooperation from internal stakeholders, system owners, telecommunications providers, platform vendors, or third-party service providers where data is externally hosted or managed.

c) Timely input and decisions from client legal, compliance, investigation, or governance teams, particularly where regulatory, inquiry, or court-imposed deadlines apply.

d) Stability of investigative scope and objectives; material changes may require additional analysis, re-processing, or revised timelines.

e) Quality and completeness of metadata, logs, and associated records required to support reliable timeline, link, and pattern analysis.

f) Availability of specialist analytical resources and secure processing environments appropriate to the sensitivity of the data and investigation.

4.4.3 The following constraints may impact the scope, timelines, certainty, or outcomes of analysis:

a) Communication data is often metadata-based; absence of content or incomplete records may limit the ability to infer intent or context.

b) Data retention policies, provider limitations, or prior deletion may result in gaps or incomplete datasets.

c) Encryption, anonymisation, or platform-specific technical restrictions may limit visibility into certain communication attributes.

d) Time zone inconsistencies, clock drift, or platform-specific timestamp handling may affect temporal accuracy unless corroborated with additional evidence.

e) Jurisdictional, regulatory, or contractual restrictions may constrain how communication data can be accessed, processed, or reported.

f) Intelligence analysis identifies patterns and relationships but does not, in isolation, establish intent, causation, or wrongdoing.

g) Findings represent a point-in-time assessment based on the data available at the time of analysis.

h) Best practice prioritises accuracy, transparency, and defensibility over speed, which may affect delivery timelines.

i) Service delivery is subject to specialist availability, technical feasibility, and agreed commercial terms.

5. Service Delivery Model

5.1.1 The Communication Data Investigation & Intelligence Service is provided on an ad-hoc or project basis. Scope, timelines, service levels, and fees are agreed per engagement.

5.1.2 All communication data is handled using secure systems, controlled access, and confidentiality safeguards. Data is processed solely for the agreed purpose and retained only for the agreed duration.

5.2 Engagement approach

5.2.1 The Communication Data Investigation & Intelligence Service is delivered through a structured, phased approach:

a) **Engagement Initiation and Scoping** – Confirmation of objectives, lawful authority, and data scope

b) **Data Identification and Collection** – Identification and ingestion of relevant communication datasets

c) **Data Processing and Normalisation** – Preparation of datasets for analysis

d) **Analysis and Intelligence Development** – Timeline, link, and pattern analysis

e) **Interpretation and Validation** – Contextual review and validation of findings

f) **Reporting and Briefing** – Delivery of intelligence outputs and advisory support

5.2.2 Delivery may be remote, on-site, or hybrid depending on data location, sensitivity, and engagement requirements.

5.3 Reporting and Deliverables

5.3.1 Deliverables may include:

a) Communication timelines and activity summaries

b) Link and relationship analysis outputs

c) Intelligence reports and briefings

d) Visualisations and analytical exhibits

e) Methodology and limitation statements

6. Exit and Offboarding

6.1.1 Upon completion, data is securely returned, retained, or destroyed in accordance with agreed instructions and applicable legal obligations. Access is revoked and engagement closure confirmed.

7. Roles and Responsibilities

7.1 Service Provider Responsibilities

7.1.1 The service provider is responsible for delivering the Communication Data Investigation & Intelligence Service in accordance with the agreed scope, applicable legal and regulatory requirements, and recognised investigative and analytical best practice. This includes advising on investigative strategy, proportionality, and analytical approaches appropriate to the nature of the matter and the available communication data.

7.1.2 The service provider will conduct structured analysis of communication data, including call data records, messaging metadata, email headers, IP data and communication artefacts, to reconstruct timelines, identify interaction patterns, and develop intelligence-led insights. Responsibilities include normalising and correlating datasets, applying link and pattern analysis techniques, and producing clear, defensible intelligence outputs supported by transparent methodology and documented assumptions.

7.1.3 The service provider is responsible for maintaining secure handling of all in-scope data, applying appropriate access controls, and maintaining auditability throughout the engagement. Quality assurance and validation activities will be undertaken to ensure accuracy, consistency, and reproducibility of findings. Any risks, data limitations, or uncertainties impacting analytical confidence will be documented and escalated promptly.

7.2 Client Responsibilities

7.2.1 The client is responsible for confirming lawful authority and legal basis to access, process, and analyse communication data. This includes ensuring that data has been lawfully obtained, defining investigative objectives, identifying relevant individuals, devices, accounts, and time periods, and providing accurate contextual information to support analysis.

7.2.2 The client retains responsibility for investigative decisions, legal interpretation, and any actions taken as a result of the intelligence findings. The client is also responsible for communications with courts, regulators, inquiry bodies, service providers, or affected individuals and for ensuring compliance with applicable legal, regulatory, and organisational requirements.

7.3 Legal, Compliance, and Governance Responsibilities (Where Applicable)

7.3.1 Where legal counsel, compliance teams, or governance stakeholders are involved, these parties are responsible for advising on legal and regulatory frameworks governing the use of communication data, including privacy, data protection, and investigatory powers. They may review intelligence outputs for compliance, advise on disclosure obligations, and oversee privileged handling where required.

7.4 Joint Responsibilities

7.4.1 The service provider and client share responsibility for effective communication, timely decision-making, and escalation of issues that may impact scope, timelines, analytical confidence, or legal compliance. All parties are responsible for maintaining confidentiality, supporting transparency and auditability, and ensuring that communication data analysis is conducted lawfully, proportionately, and defensibly.

*****END OF DOCUMENT*****