Corporate Investigation – E-Discovery Support Service Definition

Document title	Corporate Investigation E-Discovery Support Service Definition		
Reference No.	IF-SER-009	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Chris De Wit, Senior eDiscovery Analyst		
Issue date	27/01/2026		

Corporate Investigation – E-Discovery Support Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Chris De Wit	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

Corporate Investigation – E-Discovery Support Service Definition

Contents

1. Corporate Investigation Support Service

1.1 Service Overview

1.1.1 The Corporate Investigation and e-Discovery Service provides structured, defensible support for organisations undertaking internal investigations, litigation, regulatory enquiries, and dispute resolution. The service enables the identification, preservation, collection, review, and production of electronically stored information (ESI) in a legally defensible manner.

1.1.2 The service supports matters including employee misconduct, fraud, regulatory investigations, litigation, arbitration, and compliance reviews, ensuring that relevant data is handled proportionately, securely, and in accordance with applicable legal and regulatory requirements.

1.2 Service Objectives

1.2.1 The objectives of the Corporate Investigation and e-Discovery Service are to:

a) Enable defensible identification and preservation of relevant data

b) Support efficient and proportionate investigations and disclosure

c) Reduce legal, regulatory, and reputational risk

d) Provide clear audit trails and evidential transparency

e) Support legal teams with accurate, review-ready datasets

2. Service Features

2.1.1 Key features of the service include:

a) **Defensible Data Handling** – Aligned to recognised e-discovery and forensic best practice

b) **Cross-Platform Coverage** – Email, endpoints, cloud platforms, collaboration tools

c) **Proportionate Collection** – Targeted acquisition to minimise disruption and cost

d) **Privacy and Privilege Controls** – Controlled handling of sensitive and privileged data

e) **Audit-Ready Outputs** – Clear documentation of decisions and processes

3. Service Benefits

3.1.1 The service delivers the following benefits:

a) Reduced litigation and regulatory risk

b) Faster access to relevant information

c) Defensible investigation outcomes

d) Improved cost control through targeted scope

e) Increased confidence in disclosure decisions

4. Scope of Service

4.1 In-scope activities

4.1.1 The service includes the following activities:

a) Matter scoping and investigation planning

b) Legal hold identification and support

c) Identification of custodians, systems, and data sources

d) Forensic and logical collection of ESI

e) Processing and culling of data sets

f) Review support, filtering, and search strategy development

g) Identification of privileged, confidential, and sensitive data

h) Production of disclosure-ready datasets

i) Expert advisory support and reporting

4.2 Out-of-scope activities

4.2.1 Unless agreed separately, the following are out of scope:

a) Provision of legal advice or legal representation

b) Ongoing document review managed services

c) Investigation of systems or data without lawful authority

d) Long-term data hosting beyond agreed retention periods

4.3 Assumptions, Dependencies and Constraints

4.3.1 The service is delivered in alignment with applicable laws and procedural rules, including civil procedure disclosure obligations, data protection legislation, and regulatory guidance. Engagements may be coordinated through external legal counsel to support legally privileged investigations.

4.3.2 Where required, suitably qualified specialists may provide expert witness support, including written statements or testimony, subject to separate agreement.

4.3.3 Service delivery assumes:

a) Lawful authority to access and process in-scope data

b) Timely access to custodians and systems

c) Accurate scoping information provided by the client

4.3.4 Constraints may include data retention limitations, encryption, third-party dependencies, and court or regulatory deadlines.

5. Service Delivery Model

5.1 Engagement Model

5.1.1 The service is delivered on an ad-hoc consultancy basis and tailored to the specific matter. Engagements are initiated following instruction from the organisation or its legal representatives, with scope, timelines, and deliverables agreed at the outset.

5.1.2 Services are primarily delivered remotely using secure processing environments. On-site or hybrid delivery may be provided where required to access local systems, devices, or physical records.

5.2 Delivery Phases

5.2.1 Delivery typically includes:

a) Matter initiation and scoping

b) Legal hold and preservation

c) Data identification and collection

d) Processing and data reduction

e) Review and analysis support

f) Production and reporting

g) Matter closure and offboarding

5.2.2 Phases may be delivered sequentially or in parallel depending on urgency and complexity.

5.3 Reporting and Deliverables

5.3.1 Deliverables may include:

a) Collection and processing logs

b) Chain-of-custody documentation

c) Review-ready datasets

d) Disclosure and production files

e) Executive and legal reporting summaries

6. Support Model

6.1.1 The Corporate Investigation support service is delivered with defined support levels appropriate to the nature, sensitivity, and urgency of each matter. Standard support is provided during normal business hours, with a named engagement lead assigned to coordinate delivery, communications, and issue resolution throughout the engagement.

6.1.2 Hours of operation are typically aligned to standard business hours, with flexibility to support time-critical activities such as preservation actions, urgent collections, or court-mandated deadlines.

6.1.3 Clear escalation paths are established at the outset of each engagement. Issues relating to scope, timelines, access, or risk may be escalated to senior practitioners or service leads to ensure timely resolution and informed decision-making.

6.1.4 Optional enhanced support services may be provided subject to separate agreement, including extended or out-of-hours support, expedited processing and production, high-volume review coordination, and senior advisory or expert witness input for complex or legally sensitive matters.

7. Exit and Offboarding

7.1.1 Upon conclusion, data is securely returned, retained, or destroyed in accordance with agreed instructions and legal obligations. Access is revoked, and formal engagement closure is confirmed.

8. Roles and Responsibilities

8.1 Service Provider Responsibilities

8.1.1 The service provider is responsible for delivering the Corporate Investigation and e-Discovery Service in accordance with agreed scope, applicable laws, and recognised e-discovery and forensic best practice. Responsibilities include supporting matter scoping, implementing defensible preservation and collection processes, processing and preparing electronically stored information, maintaining chain-of-custody records, and producing review- and disclosure-ready datasets. The service provider will provide regular status updates, manage escalations, and ensure secure handling of data throughout the engagement.

8.2 Client Responsibilities

8.2.1 The client is responsible for confirming lawful authority to access and process in-scope data, identifying relevant custodians, systems, and data sources, and providing timely access to information and stakeholders. The client retains responsibility for legal strategy, review decisions, privilege determinations, disclosure obligations, and communications with courts, regulators, or external parties. The client will review and approve outputs where required.

8.3 Joint Responsibilities

8.3.1 Both parties are responsible for effective communication, timely decision-making, and escalation of issues that may impact scope, timelines, or legal obligations. Where external legal counsel is engaged, coordination will be undertaken to ensure consistent, compliant, and legally privileged handling of the investigation and e-discovery activities.

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