e-Discovery Support Service Definition

Document title	e-Discovery Support Service Definition		
Reference No.	IF-SER-022	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Chris De Wit, Senior eDiscovery Analyst		
Issue date	28/01/2026		

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	28/01/2026
1.0	Lisa Washer	Final review and publish	28/01/2026

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

e-Discovery Support Service Definition

Contents

1. E-Discovery Support Service

1.1 Service Overview

1.1.1 The e-Discovery Support Service provides structured, defensible assistance to organisations involved in litigation, regulatory enquiries, public inquiries, arbitration, and internal investigations. The service supports the identification, preservation, collection, processing, review preparation, and production of electronically stored information (ESI) in accordance with applicable legal, regulatory, and procedural requirements.

1.1.2 The service is designed to manage complex, high-volume datasets across multiple custodians and systems while maintaining transparency, auditability, and proportionality.

1.2 Service Objectives

1.2.1 The objectives of the e-Discovery Support Service are to:

a) Enable compliant and defensible handling of ESI

b) Support timely disclosure and production obligations

c) Reduce legal, regulatory, and reputational risk

d) Improve efficiency and cost control in data handling

e) Provide clear audit trails and reporting

2. Service Features

2.1.1 Key features include:

a) **Defensible Workflows** – Aligned to recognised e-discovery best practice

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

c) **Proportionate Data Handling** – Targeted, cost-effective collection and processing

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

e) **Audit-Ready Documentation** – Transparent records of all actions

3. Service Benefits

3.1.1 The service delivers:

a) Reduced risk of disclosure errors

b) Faster access to relevant information

c) Improved cost and scope control

d) Defensible outcomes for legal scrutiny

e) Increased confidence in disclosure decisions

4. Scope of Service

4.1.1 The service is delivered in alignment with applicable civil procedure rules, regulatory requirements, and data protection legislation. Engagements may be coordinated through legal counsel to support legally privileged handling.

4.1.2 Where required, suitably qualified practitioners may provide expert advisory or witness support, subject to separate agreement.

4.2 In-scope activities

4.2.1 The e-Discovery Support Service includes:

a) Matter scoping and e-discovery planning

b) Legal hold and preservation support

c) Identification of custodians, systems, and data sources

d) Forensic and logical data collection

e) Processing, de-duplication, and data reduction

f) Filtering, search, and analytics support

g) Preparation of review-ready datasets

h) Production of disclosure-ready outputs

i) Advisory support and reporting

4.3 Out-of-scope activities

4.3.1 Unless agreed separately, the following are excluded:

a) Provision of legal advice or representation

b) Substantive document review or coding services

c) Continuous managed hosting beyond agreed periods

d) Data access without lawful authority

4.4 Assumptions, Dependencies and Constraints

4.4.1 Delivery of the e-Discovery Support Service is based on the following assumptions:

a) The client has lawful authority and a valid legal basis to identify, preserve, collect, process, and disclose all in-scope electronically stored information (ESI).

b) The scope of the matter, including custodians, systems, date ranges, and relevance criteria, is clearly defined and approved at the outset.

c) Data provided for processing is complete, accurate, and representative of the agreed scope.

d) The client will provide timely access to systems, data sources, custodians, and relevant stakeholders.

e) Legal privilege, confidentiality, and sensitivity considerations are identified by the client and communicated promptly.

f) Instructions provided by the client or its legal representatives are accurate and authoritative.

4.4.2 Service delivery is dependent on the following factors:

a) Availability and timely provision of in-scope data in supported and accessible formats.

b) Cooperation from third-party service providers, custodians, or vendors where data resides outside the client's direct control.

c) Stability of scope, search criteria, and disclosure requirements; material changes may require reprocessing and affect timelines or cost.

d) Timely input and decision-making from client legal, compliance, and investigation teams.

e) Performance, availability, and capacity of secure e-discovery platforms and processing environments.

f) Adherence to agreed communication and escalation processes.

4.4.3 The following constraints may impact delivery, timelines, or outcomes:

a) Data quality issues, including corruption, incomplete metadata, or inconsistent formats, may limit processing accuracy or completeness.

b) Encryption, password protection, proprietary systems, or unsupported file types may restrict access or require additional effort or tools.

c) Statutory deadlines, court directions, or regulatory requirements may constrain processing approaches and sequencing.

d) E-discovery best practice prioritises defensibility, accuracy, and auditability over speed, which may affect turnaround times.

e) Findings and outputs represent a point-in-time assessment based on the data provided and criteria applied.

f) Service delivery is subject to specialist resource availability and agreed commercial terms.

5. Service Delivery Model

5.1.1 Describes how the service is delivered, including engagement approach, delivery phases, and typical timelines. Include whether delivery is on-site, remote, or hybrid.

5.2 Engagement Model

5.2.1 Services are delivered on an ad-hoc or project basis, initiated by the organisation or its legal representatives. Scope, timelines, and deliverables are agreed at the outset.

5.2.2 Services are primarily delivered remotely using secure e-discovery platforms. On-site or hybrid delivery may be provided where access to local systems or secure environments is required.

5.2.3 All data is handled using secure environments, access controls, and confidentiality safeguards. Data is processed solely for the agreed purpose and retained only for the agreed duration.

5.3 Delivery Phases

5.3.1 Typical phases include:

a) Matter initiation and scoping

b) Preservation and legal hold

c) Data identification and collection

d) Processing and data reduction

e) Review preparation and analytics

f) Production and reporting

g) Engagement closure

5.3.2 Phases may run in parallel depending on urgency and complexity.

5.4 Reporting and Deliverables

5.4.1 Deliverables may include:

a) Collection and processing logs

b) Chain-of-custody documentation

c) Data reduction metrics

d) Review-ready and production datasets

e) Status and summary reports

6. Exit and Offboarding

6.1.1 Upon completion, data is securely returned, retained, or destroyed in accordance with agreed instructions and 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 e-Discovery Support Services in accordance with the agreed scope, applicable legal and regulatory requirements, and recognised e-discovery best practice. This includes advising on e-discovery strategy, proportionality, and defensible workflows; supporting matter scoping and planning; and implementing appropriate preservation, collection, processing, and data reduction methodologies.

7.1.2 The service provider will manage the secure handling of all in-scope ESI, including ingestion, processing, de-duplication, filtering, and preparation of review-ready and production-ready datasets. Full audit trails, processing logs, and chain-of-custody records will be maintained throughout the engagement. The provider is responsible for applying agreed technical criteria accurately, conducting quality assurance and validation activities, and promptly escalating risks, data issues, or scope changes that may affect timelines or compliance. Regular status reporting and coordination with client stakeholders will be provided.

7.2 Client Responsibilities

7.2.1 The client is responsible for confirming lawful authority and legal basis to identify, preserve, collect, process, and disclose in-scope ESI. This includes defining the objectives of the matter, identifying relevant custodians, systems, and data sources, issuing legal hold or preservation notices where required, and facilitating timely access to data and personnel.

7.2.2 The client retains responsibility for legal strategy, relevance determinations, privilege decisions, and final disclosure or production decisions. The client will review and approve processing strategies, filtering criteria, and outputs as required and provide timely instructions and decisions to support delivery. The client is also responsible for communications with courts, regulators, opposing parties, or other external stakeholders.

7.3 Legal Counsel Responsibilities (Where Applicable)

7.3.1 Where internal or external legal counsel is engaged, counsel is responsible for providing legal advice, interpreting procedural rules and disclosure obligations, and advising on privilege, confidentiality, and sensitivity. Legal counsel may instruct the service provider directly, approve e-discovery strategies, review outputs prior to disclosure, and oversee legally privileged handling of data and communications.

7.4 Compliance, Privacy, and Investigation Stakeholders (Where Applicable)

7.4.1 Where compliance, privacy, or investigation teams are involved, these stakeholders are responsible for advising on regulatory requirements, data protection obligations, internal policies, and risk tolerance. They may review datasets and reports, advise on handling of personal or sensitive data, and support governance and oversight of the engagement.

7.5 Joint Responsibilities

7.5.1 The service provider and client share responsibility for effective communication, timely decision-making, and proactive escalation of issues that may impact scope, timelines, cost, or legal obligations. All parties are responsible for maintaining confidentiality, supporting transparency and auditability, and ensuring that e-Discovery activities are conducted in a proportionate, defensible, and compliant manner.

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