



Public Enquires – e-Discovery Service Definition



Document title	Public Enquires – e-Discovery Service Definition		
Reference No.	IF-SER-028	Version	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Chris De Wit, Senior e-Discovery		
Issue date	28/01/2026		



Public Enquires – e-Discovery Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Draft Template	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



Public Enquires – e-Discovery Service Definition

Contents

Document Control.....	2
Correlation Chart.....	2
Contents	3
1. Public Enquires – e-Discovery Service	4
1.1 Service Overview	4
1.2 Service Objectives	4
2. Service Features	5
3. Service Benefits	6
4. Scope of Service	7
4.1 In-scope activities	7
4.2 Out-of-scope activities	7
4.3 Assumptions, Dependencies and Constraints	7
5. Service Delivery Model	9
5.1 Engagement Model	9
5.2 Delivery Phases	9
5.3 Reporting and Deliverables	9
6. Exit and Offboarding	10
7. Roles and Responsibilities	11
7.1 Service Provider Responsibilities	11
7.2 Client Responsibilities.....	11
7.3 Legal Counsel Responsibilities (Where Applicable)	11
7.4 Joint Responsibilities.....	12



Public Enquires – e-Discovery Service Definition

1. Public Enquires – e-Discovery Service

1.1 Service Overview

- 1.1.1 The Public Inquiries e-Discovery Support Service provides structured, defensible assistance to organisations participating in statutory public inquiries, inquests, and commissions. The service supports the identification, preservation, collection, review, and production of electronically stored information (ESI) in accordance with inquiry protocols, disclosure directions, and legal obligations.
- 1.1.2 The service is designed to manage large, complex datasets across multiple custodians and systems, ensuring accuracy, transparency, and auditability while supporting strict deadlines and evolving inquiry requirements.

1.2 Service Objectives

- 1.2.1 The objectives of the Public Inquiries e-Discovery Support Service are to:
- a) Enable compliant and timely disclosure to inquiry bodies
 - b) Support accurate identification and preservation of relevant evidence
 - c) Reduce legal, regulatory, and reputational risk
 - d) Provide clear audit trails and defensible processes
 - e) Support legal teams and inquiry response units effectively



Public Enquires – e-Discovery Service Definition

2. Service Features

2.1.1 Key features of the service include:

- a) **Inquiry-Aligned Disclosure** – Processes aligned to inquiry directions and protocols
- b) **Defensible Evidence Handling** – Forensically sound and auditable processes
- c) **High-Volume Data Management** – Scalable handling of complex datasets
- d) **Privacy and Sensitivity Controls** – Controlled handling of sensitive and restricted material
- e) **Transparent Audit Trails** – Clear documentation for inquiry scrutiny



Public Enquires – e-Discovery Service Definition

3. Service Benefits

3.1.1 The service delivers the following benefits:

- a) Confidence in disclosure completeness and accuracy
- b) Reduced risk of non-compliance or adverse findings
- c) Efficient management of large disclosure volumes
- d) Improved coordination with legal and inquiry teams
- e) Clear, defensible evidence handling



Public Enquires – e-Discovery Service Definition

4. Scope of Service

4.1 In-scope activities

4.1.1 The service includes the following activities:

- a) Inquiry scoping and disclosure planning
- b) Support for preservation and legal hold requirements
- c) Identification of custodians, systems, and data repositories
- d) Forensic and logical collection of ESI
- e) Processing, culling, and indexing of datasets
- f) Review support, including relevance, sensitivity, and privilege filtering
- g) Preparation of disclosure and production datasets
- h) Management of inquiry-specific protocols and formats
- i) 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 representation
- b) Ongoing document review managed services
- c) Investigation of systems or data without lawful authority
- d) Long-term hosting beyond agreed retention periods

4.3 Assumptions, Dependencies and Constraints

- 4.3.1 The service is delivered in alignment with statutory inquiry requirements, procedural rules, and applicable data protection legislation.
- 4.3.2 Engagements may be coordinated through external legal counsel to support legally privileged handling where appropriate.
- 4.3.3 Where required, suitably qualified specialists may provide expert advisory or witness support, subject to separate agreement.
- 4.3.4 Service delivery assumes lawful authority to access and process data, timely access to custodians and systems, and clear inquiry directions.
- 4.3.5 Constraints may include statutory deadlines, evolving inquiry scope, third-party dependencies, and data retention or encryption limitations.



Public Enquires – e-Discovery Service Definition

- 4.3.6 All data is handled using secure systems, strict access controls, and confidentiality safeguards. Information is processed solely for inquiry purposes and retained only for the agreed duration.



Public Enquires – e-Discovery Service Definition

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 inquiry. 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 environments. On-site or hybrid delivery may be provided where access to local systems, devices, or secure facilities is required.

5.2 Delivery Phases

- 5.2.1 Delivery typically includes:
- a) Inquiry initiation and disclosure planning
 - b) Preservation and legal hold implementation
 - c) Data identification and collection
 - d) Processing and data reduction
 - e) Review and sensitivity handling
 - f) Disclosure production and submission
 - g) Inquiry support and engagement closure
 - h) Phases may overlap to meet inquiry deadlines and evolving requirements.

5.3 Reporting and Deliverables

- 5.3.1 Deliverables may include:
- a) Collection, processing, and disclosure logs
 - b) Chain-of-custody documentation
 - c) Review-ready and disclosure-ready datasets
 - d) Status and progress reports for inquiry teams
 - e) Summary reporting aligned to inquiry milestones



Public Enquires – e-Discovery Service Definition

6. Exit and Offboarding

- 6.1.1 Upon conclusion, data is securely returned, retained, or destroyed in accordance with inquiry directions and agreed instructions. Access is revoked and formal closure confirmed.



Public Enquires – e-Discovery Service Definition

7. Roles and Responsibilities

7.1 Service Provider Responsibilities

- 7.1.1 The service provider is responsible for delivering the Public Inquiries e-Discovery Support Service in accordance with the inquiry's terms of reference, disclosure protocols, applicable legislation, and recognised e-discovery and forensic best practice. Responsibilities include advising on inquiry-specific disclosure requirements, supporting the development of defensible disclosure strategies, and implementing proportionate preservation and collection processes across identified custodians, systems, and data sources.
- 7.1.2 The service provider will manage the secure collection, processing, indexing, and preparation of electronically stored information, maintaining full chain-of-custody and audit records throughout. The provider will support data reduction, review workflows, sensitivity handling, and production formatting in line with inquiry directions, while ensuring robust security, confidentiality, and access controls. Regular progress reporting will be provided, and issues affecting scope, timelines, or compliance will be escalated promptly to appropriate stakeholders.

7.2 Client Responsibilities

- 7.2.1 The client is responsible for confirming lawful authority to access, process, and disclose in-scope information to the inquiry. This includes identifying relevant custodians, systems, and repositories; issuing legal hold or preservation notices; and facilitating timely access to data, personnel, and subject-matter experts.
- 7.2.2 The client retains responsibility for determining relevance, sensitivity, public interest considerations, legal privilege, and final disclosure decisions. The client is also responsible for communications with the inquiry body, approval of disclosure submissions, and compliance with inquiry deadlines and directions. Where required, the client will coordinate internal governance, legal, and senior leadership oversight.

7.3 Legal Counsel Responsibilities (Where Applicable)

- 7.3.1 Where external or internal legal counsel is engaged, counsel is responsible for providing legal advice, interpreting inquiry directions, advising on privilege, redactions, and disclosure obligations, and overseeing legally sensitive aspects of the process. Counsel may instruct the service provider directly, coordinate legally privileged handling, and review outputs prior to submission to the inquiry.



Public Enquires – e-Discovery Service Definition

7.4 Joint Responsibilities

- 7.4.1 The service provider, client, and legal counsel (where applicable) share responsibility for effective coordination, timely decision-making, and proactive escalation of risks or issues that may impact disclosure completeness, accuracy, or deadlines. All parties are responsible for maintaining confidentiality, supporting transparency and auditability, and ensuring that inquiry obligations are met in a timely, defensible, and proportionate manner.

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