



Digital Disclosure Service Definition



Document title	Digital Disclosure Service Definition		
Reference No.	IF-SER-017	Version	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Carl Osborne, Managing Director		
Issue date	28/01/2026		



Digital Disclosure Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Simon Young	Review and amend or update	28/01/2026
0.3	Carl Osborne	Review and comments	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



Digital Disclosure Service Definition

Contents

Document Control.....	2
Correlation Chart.....	2
Contents	3
1. Digital Disclosure 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
4.2 In-scope activities	7
4.3 Out-of-scope activities	7
4.4 Assumptions, Dependencies and Constraints	7
5. Service Delivery Model	10
5.2 Engagement Approach	10
5.3 Reporting and Deliverables	10
6. Exit and Offboarding	11
7. Roles and Responsibilities	12
7.1 Service Provider Responsibilities	12
7.2 Client Responsibilities.....	12
7.3 Legal Counsel Responsibilities (Where Applicable)	12
7.4 Compliance, Privacy, and Investigation Stakeholders (Where Applicable).....	13
7.5 Joint Responsibilities.....	13



Digital Disclosure Service Definition

1. Digital Disclosure Service

1.1 Service Overview

- 1.1.1 The Digital Disclosure Service provides structured, defensible support to organisations required to identify, review, prepare, and disclose digital material in response to legal proceedings, regulatory enquiries, public inquiries, inquests, or internal investigations. The service supports the management of electronically stored information (ESI) to ensure disclosure obligations are met accurately, proportionately, and transparently.
- 1.1.2 Using established e-discovery and digital forensic methodologies, the service enables controlled handling of digital material while maintaining auditability, evidential integrity, and compliance with applicable procedural and disclosure rules.

1.2 Service Objectives

- 1.2.1 The objectives of the Digital Disclosure Service are to:
- a) Support compliant and timely digital disclosure
 - b) Demonstrate an impartial review of material
 - c) Reduce legal, regulatory, and reputational risk
 - d) Ensure defensible handling of digital material
 - e) Enable proportionate and transparent disclosure decisions
 - f) Provide clear audit trails suitable for scrutiny



Digital Disclosure Service Definition

2. Service Features

2.1.1 Key features of the Digital Disclosure Service include:

- a) **Defensible Disclosure Workflows** – Aligned to recognised e-discovery and disclosure best practice
- b) **Scalable Data Handling** – Suitable for high-volume and complex datasets
- c) **Privacy and Sensitivity Controls** – Structured handling of personal and restricted material
- d) **Audit-Ready Documentation** – Clear records of disclosure processes and decisions
- e) **Impartiality** – provide a service which demonstrates impartiality
- f) **Flexible Engagement Model** – Tailored to litigation, regulatory, inquiry, or internal contexts



Digital Disclosure Service Definition

3. Service Benefits

3.1.1 The service delivers the following benefits:

- a) Increased confidence in disclosure completeness and accuracy
- b) Reduced risk of over- or under-disclosure
- c) Improved efficiency and cost control
- d) Transparent processes suitable for challenge or audit
- e) Strong governance over digital disclosure obligations



Digital Disclosure Service Definition

4. Scope of Service

- 4.1.1 Service delivery assumes lawful authority to process data, timely access to systems and custodians, and clear disclosure requirements. Dependencies may include third-party cooperation and data availability. Constraints may include data quality, encryption, evolving scope, and statutory or court-mandated deadlines.

4.2 In-scope activities

- 4.2.1 The Digital Disclosure Service includes:
- a) Disclosure scoping and planning
 - b) Identification of relevant data sources and custodians
 - c) Collection or ingestion of digital material
 - d) Processing and preparation of datasets for review
 - e) Filtering and search support to identify relevant material
 - f) Review workflow support (non-substantive review)
 - g) Handling of sensitive, personal, or restricted material
 - h) Redaction preparation and management
 - i) Production of disclosure-ready datasets
 - j) Documentation and disclosure reporting

4.3 Out-of-scope activities

- 4.3.1 Unless agreed separately, the following are excluded:
- a) Provision of legal advice or disclosure decisions
 - b) Substantive relevance or privilege review
 - c) Communications with courts, regulators, or opposing parties
 - d) Continuous managed disclosure services

4.4 Assumptions, Dependencies and Constraints

- 4.4.1 Delivery of the Digital Disclosure Service is based on the following assumptions:
- a) The client has lawful authority and a valid legal basis to identify, collect, process, review, and disclose all in-scope digital material, including personal or sensitive data.
 - b) Disclosure obligations, procedural rules, and applicable frameworks (e.g. civil, criminal, regulatory, or inquiry-specific requirements) are clearly defined at the outset or communicated promptly as they arise.



Digital Disclosure Service Definition

- c) The scope of disclosure, including custodians, systems, date ranges, and relevance criteria, is accurately defined and approved by the client or its legal representatives.
- d) Digital material provided for disclosure processing is complete, accurate, and representative of the agreed scope.
- e) Any legal privilege, confidentiality, sensitivity, or restriction requirements are identified and communicated in a timely manner.
- f) The client will provide timely access to systems, data sources, documentation, and subject-matter experts necessary to support disclosure preparation and interpretation.

4.4.2 Service delivery is dependent on the following factors:

- a) Availability and timely provision of in-scope digital material in accessible and supported formats.
- b) Cooperation from internal stakeholders, custodians, and third-party service providers where data is hosted or managed externally.
- c) Timely input, decisions, and approvals from client legal, compliance, investigation, or disclosure teams, particularly where statutory or court-imposed deadlines apply.
- d) Stability of scope and disclosure criteria; material changes may require reprocessing, additional review effort, or revised timelines.
- e) Performance and availability of secure processing and review environments used to support disclosure activities.
- f) Adherence to agreed communication, escalation, and governance processes.

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

- a) Data quality issues, including corruption, missing metadata, or inconsistent formats, may limit processing accuracy or completeness.
- b) Encryption, access restrictions, proprietary platforms, or unsupported file types may restrict access or require additional effort, tools, or third-party assistance.
- c) Statutory deadlines, court directions, or regulatory timetables may constrain processing approaches, sequencing, or prioritisation.
- d) Disclosure best practice prioritises accuracy, proportionality, and auditability over speed, which may affect turnaround times.
- e) Findings and disclosure outputs represent a point-in-time position based on the data provided and criteria applied at the time of preparation.
- f) The service supports disclosure preparation but does not replace legal judgment; final disclosure decisions remain the responsibility of the client or its legal representatives.



Digital Disclosure Service Definition

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



Digital Disclosure Service Definition

5. Service Delivery Model

- 5.1.1 The Digital Disclosure Service is provided on an ad-hoc or project basis. Scope, timelines, service levels, and fees are agreed per engagement.
- 5.1.2 All digital material is handled using secure environments, 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 Digital Disclosure Service is delivered through a structured, phased approach:
- a) **Engagement Initiation and Scoping** – Confirmation of disclosure obligations, scope, and timelines
 - b) **Data Identification and Collection** – Identification and ingestion of in-scope digital material
 - c) **Processing and Preparation** – Normalisation, indexing, and preparation for review
 - d) **Filtering and Review Support** – Application of agreed criteria to identify disclosable material
 - e) **Disclosure Production** – Preparation of disclosure bundles and supporting documentation
 - f) **Closure and Handover** – Secure handover, retention, or disposal of materials
- 5.2.2 Delivery may be remote, on-site, or hybrid depending on security, data location, and engagement requirements.

5.3 Reporting and Deliverables

- 5.3.1 Deliverables may include:
- a) Disclosure logs and audit records
 - b) Review-ready and disclosure-ready datasets
 - c) Redaction and sensitivity handling records
 - d) Disclosure summaries and supporting reports



Digital Disclosure Service Definition

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 formal engagement closure confirmed.



Digital Disclosure Service Definition

7. Roles and Responsibilities

7.1 Service Provider Responsibilities

- 7.1.1 The service provider is responsible for delivering the Digital Disclosure Service in accordance with the agreed scope, applicable procedural rules, and recognised e-discovery and disclosure best practice. This includes advising on disclosure workflows, proportionality, and defensible handling of digital material; supporting disclosure scoping and planning; and implementing structured processes for data identification, processing, filtering, and preparation.
- 7.1.2 The service provider will securely handle all in-scope digital material, maintaining auditability and traceability throughout the disclosure lifecycle. Responsibilities include maintaining processing and disclosure logs, applying agreed technical criteria and workflows consistently, supporting redaction preparation, and producing disclosure-ready datasets and documentation. Quality assurance and validation activities will be performed to ensure accuracy and transparency, and any risks, uncertainties, or limitations affecting disclosure will be promptly escalated.
- 7.1.3 The service provider does not make legal determinations regarding relevance, privilege, or disclosure obligations but ensures that technical handling and preparation of materials supports informed and defensible decision-making by the client and its legal representatives.

7.2 Client Responsibilities

- 7.2.1 The client is responsible for confirming lawful authority and legal basis to collect, process, review, and disclose digital material. This includes defining disclosure obligations, identifying relevant custodians, systems, and data sources, and providing accurate scoping information, documentation, and contextual guidance.
- 7.2.2 The client retains responsibility for legal strategy, relevance assessments, privilege determinations, disclosure decisions, and communications with courts, regulators, inquiry bodies, or opposing parties. The client is also responsible for reviewing and approving disclosure outputs where required and for ensuring that statutory, procedural, or court-mandated deadlines are met.

7.3 Legal Counsel Responsibilities (Where Applicable)

- 7.3.1 Where internal or external legal counsel is engaged, legal counsel is responsible for interpreting disclosure obligations, advising on privilege, confidentiality, and sensitivity, and overseeing legal compliance of disclosure decisions. Legal counsel may instruct the service provider directly, approve disclosure strategies and workflows, review prepared disclosure materials, and coordinate legally privileged handling where appropriate.



Digital Disclosure Service Definition

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 disclosure outputs for compliance considerations, advise on handling of personal or sensitive data, and support governance and oversight of the disclosure process.

7.5 Joint Responsibilities

- 7.5.1 The service provider and client share responsibility for effective communication, timely decision-making, and escalation of issues that may impact scope, timelines, accuracy, or compliance. All parties are responsible for maintaining confidentiality, supporting transparency and auditability, and ensuring that digital disclosure activities are conducted proportionately, defensibly, and in line with applicable legal and regulatory requirements.

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