INTERNATIONAL STANDARD

ISO/IEC 27050-1

First edition
2016-11-01

Information technology — Security techniques — Electronic discovery —

Part 1: Overview and concepts

Technologies de l'information — Techniques de sécurité — Découverte électronique —

Partie 1: Aperçu général et concepts

Reference number
ISO/IEC 27050-1:2016(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

A list of all parts in the ISO/IEC 27050 series can be found on the ISO website.

Introduction

This document provides an overview of electronic discovery and describes related terminology, concepts, and processes that are intended to be leveraged by other parts of ISO/IEC 27050.

Electronic discovery often serves as a driver for investigations as well as evidence acquisition and handling activities (covered in ISO/IEC 27037). In addition, the sensitivity and criticality of the data sometimes necessitate protections like storage security to guard against data breaches (covered in ISO/IEC 27040).

This document is not a reference or normative document for regulatory and legislative security requirements. Although it emphasizes the importance of these influences, it cannot state them specifically, since they are dependent on the country, the type of business, etc.

Information technology — Security techniques — Electronic discovery —

Part 1: Overview and concepts

1 Scope

Electronic discovery is the process of discovering pertinent Electronically Stored Information (ESI) or data by one or more parties involved in an investigation or litigation, or similar proceeding. This document provides an overview of electronic discovery. In addition, it defines related terms and describes the concepts, including, but not limited to, identification, preservation, collection, processing, review, analysis, and production of ESI. This document also identifies other relevant standards (e.g. ISO/IEC 27037) and how they relate to, and interact with, electronic discovery activities.

This document is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities, and it is not intended to contradict or supersede local jurisdictional laws and regulations, so exercise care to ensure compliance with the prevailing jurisdictional requirements.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org.obp

3.1
chain of custody
demonstrable possession, movement, handling, and location of material from one point in time until another

3.2
custodian
person or entity that has custody, control or possession of *Electronically Stored Information* (3.9)

3.3
data breach
compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, *stored* (3.26) or otherwise processed

[SOURCE: ISO/IEC 27040:2015, 3.7]

3.4
discovery
process by which each party obtains information held by another party or non-party concerning a matter

Note 1 to entry: *Discovery* is applicable more broadly than to parties in adversarial disputes.

Note 2 to entry: *Discovery* is also the disclosure of hardcopy documents, *Electronically Stored Information* (3.9) and tangible objects by an adverse party.

Note 3 to entry: In some jurisdictions, the term disclosure is used interchangeably with discovery.

3.5
disposition
range of processes associated with implementing records retention, destruction or transfer decisions which are documented in *disposition authorities* (3.6) or other instruments

[SOURCE: ISO 15489-1:2016, 3.8]

3.6
disposition authority
instrument that defines the *disposition* (3.5) actions that are authorized for specified records

[SOURCE: ISO 15489-1:2016, 3.9]

3.7
electronic archive
long-term repository of *Electronically Stored Information* (3.9)

Note 1 to entry: *Electronic archives* can be online, and therefore accessible, or off-line and not easily accessible.

Note 2 to entry: Backup systems (e.g. tape, virtual tape, etc.) are not intended to be *electronic archives*, but rather data protection systems (i.e. recovery mechanisms for disaster recovery and business continuity).

3.8
electronic discovery
discovery (3.4) that includes the identification, preservation, collection, processing, review, analysis, or production of *Electronically Stored Information* (3.9)

Note 1 to entry: Although *electronic discovery* is often considered a legal process, its use is not limited to the legal domain.

3.9
Electronically Stored Information
ESI
data or information of any kind and from any source, whose temporal existence is evidenced by being *stored* (3.26) in or on any electronic medium

Note 1 to entry: *ESI* includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations and other electronic formats commonly found on a computer. *ESI* also includes system, application and file-associated *metadata* (3.19) such as timestamps, revision history, file type, etc.

Note 2 to entry: Electronic medium can take the form of, but is not limited to, storage devices and storage elements.

[SOURCE: ISO/IEC 27040:2015, 3.16]

3.10
ESI analysis
element of an *electronic discovery* (3.8) process focused on evaluating *Electronically Stored Information* (3.9) for content and context to identify facts, relationships, key patterns, and other features that can lead to improved understanding of an *ESI* (3.9) corpus

Note 1 to entry: Content and context can include key patterns, topics, people and discussions.

3.11
ESI collection
element of an *electronic discovery* (3.8) process focused on gathering *Electronically Stored Information* (3.9) and other related material

3.12
ESI identification
element of an *electronic discovery* (3.8) process focused on locating potential sources and the criteria for selecting potentially relevant *Electronically Stored Information* (3.9)

3.13
ESI preservation
element of an *electronic discovery* (3.8) process focused on maintaining *Electronically Stored Information* (3.9) in its original or existing state

Note 1 to entry: In some matters or jurisdictions, there can be requirements to prevent *spoliation* (3.24) of *Electronically Stored Information* (3.9).

3.14
ESI processing
element of an *electronic discovery* (3.8) process focused on extracting *Electronically Stored Information* (3.9) and converting it, if necessary, to forms more suitable for *ESI review* (3.16) and *ESI analysis* (3.10)

3.15
ESI production
element of an *electronic discovery* (3.8) process focused on delivering or making available *Electronically Stored Information* (3.9)

Note 1 to entry: *ESI production* can also include getting *Electronically Stored Information* (3.9) in appropriate forms and using appropriate delivery mechanisms.

Note 2 to entry: *ESI production* can be to any person or organization.

3.16
ESI review
element of an *electronic discovery* (3.8) process focused on screening *Electronically Stored Information* (3.9) based on specific criteria

Note 1 to entry: In some matters or jurisdictions, *Electronically Stored Information* (3.9) that is considered privileged can be excluded from production.

3.17
investigation
systematic or formal process of inquiring into or researching, and examining facts or materials associated with a matter

Note 1 to entry: Materials can take the form of hardcopy documents or *Electronically Stored Information* (3.9).

3.18
legal hold
process of suspending the normal *disposition* (3.5) or processing of records and *Electronically Stored Information* (3.9) as a result of current or anticipated litigation, audit, government investigation or other such matters

Note 1 to entry: The issued communication that implements the legal hold can also be called a "hold," "preservation order," "preservation notice," "suspension order," "freeze notice," "hold order," or "hold notice."

3.19
metadata
data that defines and describes other data

[SOURCE: ISO/IEC 11179-1:2015, 3.2.16]

3.20
non-volatile storage
storage (3.25) that retains its contents even after power is removed

[SOURCE: ISO/IEC 27040:2015, 3.30]

3.21
production file format
organization and representation of data and *metadata* (3.19) that is presented to a requesting party

3.22
provenance
information that documents the origin or source of *Electronically Stored Information* (3.9), any changes that have taken place since it was originated, and who has had custody of it since it was originated

3.23
sanitize
process to remove information from media such that data recovery is not possible at a given level of effort

[SOURCE: ISO/IEC 27040:2015, 3.38, modified]

Note 1 to entry: Clear, purge, and destruct are actions that can be taken to *sanitize* storage media.

3.24
spoliation
act of making or allowing a change to or destruction of *Electronically Stored Information* (3.9) where there is a requirement to keep it intact

Note 1 to entry: *Spoliation* can take the form of *ESI* (3.9) destruction, corruption, or alteration of the *ESI* (3.9) or associated *metadata* (3.19) as well as rendering *ESI* (3.9) unavailable (e.g. due to encryption with no access to the decryption key, loss of media, under the control of a third party, etc.).

3.25
storage
device, function, or service supporting data entry and retrieval

[SOURCE: ISO/IEC 27040:2015, 3.43]

3.26
store
record data on *volatile storage* (3.27) or *non-volatile storage* (3.20)

[SOURCE: ISO/IEC 27040:2015, 3.50]

3.27
volatile storage
storage (3.25) that fails to retain its contents after power is removed

[SOURCE: ISO/IEC 27040:2015, 3.53]

4 Symbols and abbreviated terms

CD	compact disc
DVD	digital versatile disc
EDMS	electronic document management system
ERMS	electronic records management system

ICT	information and communications technology
NAS	network attached storage
OCR	optical character recognition
PII	personally identifiable information
RAM	random access memory

5 Overall ISO/IEC 27050 structure and overview

5.1 Purpose and structure

ISO/IEC 27050 (all parts) provides requirements and guidance for the process of discovering pertinent Electronically Stored Information (ESI) or data by one or more parties involved in an investigation or litigation, or similar proceeding. Figure 1 provides a notional architecture of ISO/IEC 27050 (all parts).

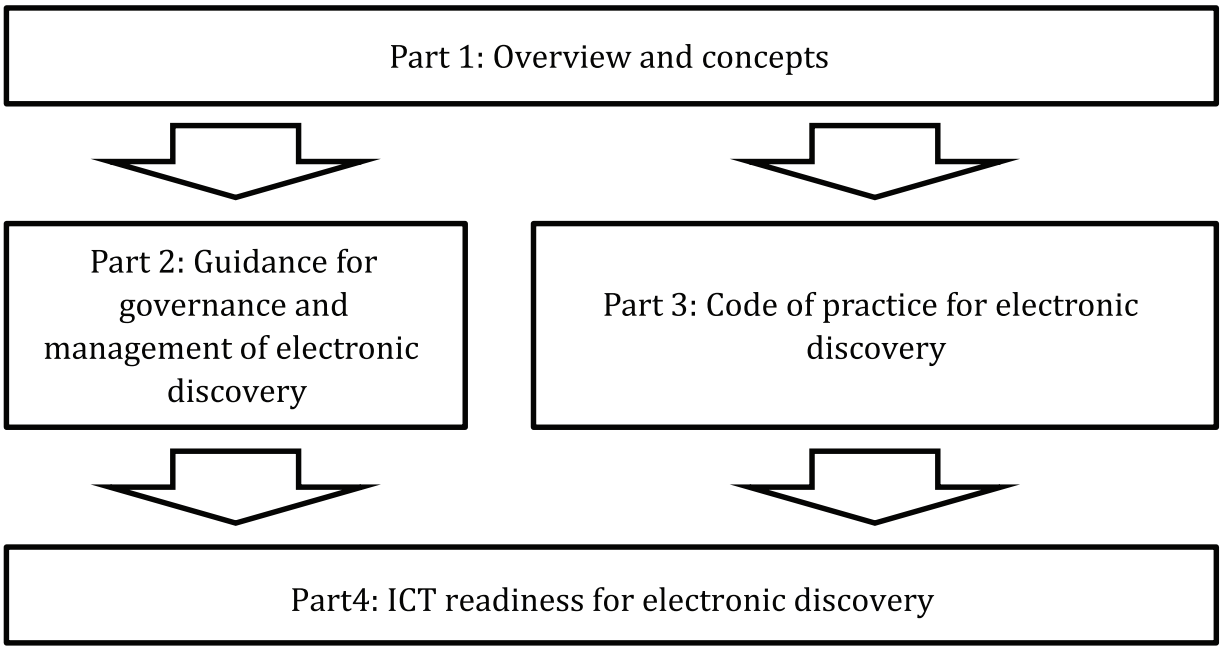

Figure 1 — ISO/IEC 27050 architecture

5.2 Overview of ISO/IEC 27050-1: Overview and concepts

This document provides an overview of electronic discovery, introducing relevant terminology, concepts, and processes. This document is an informative document.

5.3 Overview of ISO/IEC 27050-2: Guidance for governance and management of electronic discovery

This document addresses how personnel at senior levels within an organization can identify and take ownership of risks related to electronic discovery, set policy relating to electronic discovery and achieve compliance with external and internal requirements relating to electronic discovery.

5.4 Overview of ISO/IEC 27050-3: Code of practice for electronic discovery

This document considers each of the distinct elements of the electronic discovery process (ESI identification, ESI preservation, ESI collection, ESI processing, ESI review, ESI analysis, and ESI production) and, for each process element, identifies (i) the objectives, (ii) considerations to avoid failures, and (iii) the specific requirements and guidance for adherence to ISO/IEC 27050 (all parts).

5.5 Overview of ISO/IEC 27050-4: ICT readiness for electronic discovery

This document provides guidance on the ways an organization can be better prepared to address electronic discovery from the perspective of both technology and processes.

6 Overview of electronic discovery

6.1 Background

Electronic discovery is increasingly important, both within organizations and in the legal systems of some jurisdictions. This trend is expected to continue as more and more electronic records and information (or ESI) are created, modified, manipulated, used, and ultimately destroyed without ever taking on a physical form (e.g. a printed document). The emergence of ESI as the preferred representation of information is introducing new challenges associated with locating the ESI, handling massive quantities of data, preservation and retention of ESI, authenticity, data integrity, data confidentiality, data or media sanitization, etc. While electronic discovery needs and responses vary by matter, failure to appropriately handle the electronic discovery process in view of the context of a particular matter can result in rework, unnecessary costs, possible sanctions, and legal liabilities.

ISO/IEC 27050 (all parts) addresses these challenges by

— promoting a common approach, understanding, and language for electronic discovery,

— encouraging practical and cost-effective discovery by those tasked with managing ESI through the process,

— identifying competency areas for those involved in electronic discovery,

— promoting consideration of the proactive use of technology, in reducing costs and risks, while increasing efficiencies throughout the discovery process, and

— suggesting ways of avoiding inadvertent disclosures of potentially privileged, confidential, or sensitive ESI.

The overriding goal is to help organizations plan for and meet their electronic discovery objectives and obligations, if any, commensurate with the needs of each particular matter.

6.2 Basic concepts

It is useful to consider in advance the following electronic discovery issues. The significance of these issues and the need to address them vary by matter and need to be calibrated to the needs of the matter.

— scope of electronic discovery;

— governance and management of electronic discovery;

— establishing responsibilities for each aspect of an electronic discovery project;

— identification of systems holding potentially relevant ESI;

— identification of potentially relevant ESI;

— developing appropriate documentation throughout the electronic discovery process;

— anticipated costs and their proposed allocation;

— preservation of ESI, including the legal hold process;

— disclosure of information on the ESI storage methods, hardware, and software;

— collection/acquisition of ESI;

— processing of ESI;

— review and analysis of ESI;

— production of ESI including the form of production.

Those engaging in electronic discovery have many influencing factors specific to the context. Cost can be significant among these. The primary cost drivers include:

— Collection: finding and retrieving the potentially relevant ESI;

— Volume: the raw quantity of ESI to be collected, processed, or reviewed;

— Number of sources: the number of custodians, enterprise systems, and external systems and applications under the control of the entity involved in the collection of ESI can increase exponentially the amount of time and effort involved;

— Human competencies: the need for qualified people who can perform the functions needed for effective data retrieval, handling, searching, and final review for relevance, privilege, and review for classification (e.g. relevance, privilege, trade secret, confidentiality or special treatment); these competencies can include information technology, computer technology, statistics, search sciences, and law;

— Case complexity: simple cases can require a limited scope and review process, but more complex cases can involve elaborate document review strategies and processes.

The time it takes to find and retrieve ESI, the volume of ESI, the number of sources subject to an ESI investigation and, ultimately, the acceptance of that ESI as reliable in a legal proceeding or ESI investigation are intimately tied to the practices and policies an organization has put in place to address the management of ESI throughout its life cycle in the organization. Organizations that build electronic discovery readiness into their comprehensive information governance structures prior to engaging in electronic discovery are likely to more efficiently and cost-effectively meet the requirements of electronic discovery. ISO/IEC 27050-2 and ISO/IEC 27050-4 provide specific guidance for doing so.

6.3 Objectives of electronic discovery

Objectives of electronic discovery vary by matter. As adjusted for each matter, the objectives can include the following:

— comply with confidentiality, data privacy, and other restrictions on data access, use, handling, or transfer imposed by applicable laws, regulations, rules, and expectations;

— identify potentially relevant sources of ESI;

— properly preserve and retain potentially relevant ESI;

— process relevant ESI into a format that facilitates its efficient searching or review;

— minimize the potential of failing to designate as responsive ESI that is responsive;

— minimize the potential of designating as responsive ESI that is not responsive;

— minimize the potential of failing to designate for withholding or special treatment responsive ESI that qualifies for withholding or special treatment;

— minimize the potential of designating for withholding or special treatment responsive ESI that does not qualify for withholding or special treatment;

— produce responsive ESI in a form that is useable by the requesting party;

— consider the proportionality of the response in the context of the matter and the costs;

— utilize technology in order to reduce risks and costs throughout the project.

6.4 Electronic discovery foundation

6.4.1 General

Electronic discovery often involves parties with conflicting interests and, in a worst-case scenario, they can be adversarial parties. Electronic discovery can be key to resolving a conflict or matter, but only when it is conducted on a foundation that facilitates a measure of trust.

For electronic discovery, this foundation includes adequately addressing competency, candour, cooperation, completeness, and proportionality issues that can require the reconciliation of the requirements of electronic discovery with the requirements of other processes, values or principles.

6.4.2 Competency

Given the complexities associated with electronic discovery, it is important that the individuals engaging in the electronic discovery process have the relevant technical or legal competencies. They potentially need to be able to demonstrate that they are properly trained and have sufficient technical or legal understanding to handle ESI appropriately and to execute the electronic discovery process on behalf of a party.

6.4.3 Candour

The parties conducting electronic discovery are expected to adhere to the applicable standards of professionalism and ethical conduct. In some jurisdictions, this means the parties have an obligation to correct and supplement the record (e.g. additional disclosures or to amend prior responses). In addition, purposeful sluggishness in executing the electronic discovery process needs to be avoided by all parties involved.

6.4.4 Cooperation

Cooperation on issues relating to the preservation, collection, search, review, and production of ESI can be expected in courts of some jurisdictions and, in such courts, cooperation typically does not compromise representation of a client. In addition, in the context of litigation, cooperation in reasonably limiting ESI discovery requests, on the one hand, and in reasonably responding to ESI discovery requests, on the other hand, can reduce costs and delays. Cooperative exchanges of information at the earliest stages of discovery can be useful as appropriate.

6.4.5 Completeness

The objective of a producing party is to retrieve and produce a set of (non-privileged) ESI that represents, under the specific circumstances of the matter, a complete and accurate production.

6.4.6 Proportionality

With the explosive growth of ESI, there are increased concerns over how to best address the costs and burdens associated with the discovery process. One approach to address this problem is to take steps to help ensure that the benefits of discovery be commensurate with the corresponding burdens. The burdens of electronic discovery can be varied including, but not limited to, disruption of business operations, financial cost, or intrusions on individual privacy.

6.5 Governance and electronic discovery

6.5.1 General

ISO/IEC 38500 sets out six principles for good governance of ICT that are associated with responsibility, strategy, acquisition, performance, conformance, and human behaviour. Each principle is expressed as a preferred behaviour to guide decision making (i.e. each principle refers to what is expected to happen, but does not prescribe how, when or by whom the principles would be implemented, as these aspects are dependent on the nature of the organization implementing the principles). Governing bodies are encouraged to require that these principles are applied, and as a result, they can be assisted in managing risks and encouraging the exploitation of opportunities arising from the use of ICT.

According to ISO/IEC 38500, good governance of ICT also assists governing bodies in assuring conformance with obligations (regulatory, legislation, common law, contractual) concerning the acceptable use of ICT.

The general topic of governance, as it relates to electronic discovery, is addressed in ISO/IEC 27050-2, but 6.5 highlights some of the more important elements to help draw attention to the issues.

6.5.2 Risk and environmental factors

Electronic discovery has the potential of exposing an organization or its governing bodies to causes of failure that can have detrimental effects. Governance can help avoid negative consequences that can take the form of

— breaches of privacy, health and safety, record keeping legislation and regulations,

— non-compliance with standards relating to security, social responsibility, and

— matters relating to intellectual property rights including licensing agreements.

Avoiding negative consequences associated with these failures requires awareness and mitigations that cover the electronic discovery process as well as things such as inadequate ICT systems and improper or inappropriate use of ICT.

6.5.3 Compliance and review

Many organizations are faced with compliance issues that originate from statutory, regulatory, legal, or other requirements. These requirements can be the reason that an organization undertakes an electronic discovery activity, but more likely, they have an impact on how the electronic discovery process is carried out. For example, there can be restrictions on who can see the ESI, how the ESI is transmitted or stored, and specific retention or destruction issues. It is important to ensure that the electronic discovery process is executed within the confines of the relevant compliance requirements.

6.5.4 Privacy and data protection

Besides regulatory restrictions and compliance issues as mentioned in 6.5.3, it is important to be aware of some privacy limitations on the use of custodian data (see also ISO/IEC 29100). In particular, there might be some restrictions on personally identifiable information (PII) at custodian data sources that need to be considered as part of ESI management.

When electronic discovery involves PII in some jurisdictions, there can be severe restrictions on what can be done with it (e.g. it cannot be transported across borders). Even without such restrictions, additional data protection measures are often necessary to protect confidentiality and guard against data breaches. ISO/IEC 27050-4, in conjunction with ISO/IEC 27040, provides additional materials that can help deal with these kinds of issues.

6.6 ICT readiness for electronic discovery

6.6.1 General

Throughout the electronic discovery process, the parties involved in a matter are gathering, handling, and manipulating ESI. Often, this ESI has been extracted from a computing or storage environment that is specifically designed to protect it. Similar protections might be needed for the ESI that has been removed or copied from these environments.

ISO/IEC 27050-4 addresses many of these issues within the context of electronic discovery.

6.6.2 Long-term retention of ESI

Electronic discovery is commonly employed early in litigation, audit, government investigation or other such matters. While the matter proceeds, the parties need to retain the associated ESI in such a way that it continues to be available and its integrity is maintained. Adequate disaster recovery and business continuity measures along with common data protection mechanisms (e.g. backups) can be important elements of a retention program for ESI.

It is important to consider the timeframes involved when making decisions about long-term retention of ESI. There are significant differences between the approaches for retaining ESI for a few weeks or months versus retaining ESI for decades (e.g. complex civil litigation that goes through multiple appeals) in electronic archives.

An additional consideration is whether data protection and privacy requirements affect how long personal data may be retained and if the matter requires normal data retention periods to be suspended. This can vary significantly between jurisdictions.

6.6.3 Maintaining ESI confidentiality

ESI often contains proprietary, privileged, and sensitive information that needs to be handled and stored in a way that protects the confidentiality of the information. Failure to adequately control sensitive ESI can result in serious repercussions if there is a data breach.

Depending on the sensitivity of the ESI, security measures such as data in motion and data at rest encryption along with the corresponding key management are likely to be needed.

6.6.4 Destruction of ESI

When ESI is no longer needed, it is important to eliminate it in a way that avoids data breaches. This typically means that the logical storage or the storage media used to retain the ESI has to be properly sanitized (e.g. cleared using overwrite techniques or cryptographic erase).

6.7 Planning and budgeting an electronic discovery project

The varied drivers behind an electronic discovery project make it difficult to plan such a project many months in advance. As such, they are typically managed on an individual basis, which can increase costs significantly. Regardless of the urgency of the request, as with any project, time invested in planning at the outset typically saves significant time and costs later in the project. This is especially so, as many of the steps in a typical electronic discovery project are disproportionately expensive to repeat at a later stage. For example, if the production structure and format are not agreed upon in advance of the review, and families of ESI or hardcopy documents are not marked consistently, then it can cause the review to have to be partially repeated.

An important early step is to establish an electronic discovery project team that, at a minimum, includes a project sponsor and manager from the business/organization, a project manager from the legal or investigative team, and a project manager from the ICT perspective. This triangle of communication between the business/organization, the legal/investigators, and the ICT team is vital to a successful project.

Also, an early step is the establishment of an electronic discovery project plan, with as much detail as possible. As with any project plan, the electronic discovery plan needs to contain the project milestones (e.g. identification, preservation/collection, processing, review, analysis, production, and possibly presentation), the individual steps required at each stage, and the individual assignments at each step.

Given the costs involved in a typical electronic discovery project, preparing and monitoring a detailed budget from the outset are an important consideration. This budget needs to take into account the diverse disciplines on the electronic discovery team and the fact that they can consist of internal and external counsel, as well as internal and external ICT or electronic discovery consultants. It is important to include a budget for each electronic discovery process element of the plan, and in some cases, each step of each process element, so that it is possible to determine if the proposed approach is proportionate to the matter at hand.

NOTE While the description in 6.5 is more oriented towards large enterprises involved in large matters and might not be fully applicable to smaller organizations or smaller matters, the points being made are still relevant for consideration.

7 Electronically Stored Information (ESI)

7.1 Background

ESI is now an integral part of both business and individual environments. Consequently, it forms an increasingly important source of relevant materials in modern disputes or matters.

ESI is worthy of consideration at the earliest stages in a matter. It can be extremely fragile and some of it can be easily lost or modified, even by opening a document. Consideration of the identification, preservation, and possibly the collection process elements in the early days after becoming aware of a matter can enable important decisions and possibly significant time and cost savings in the longer term.

Managing ESI increasingly impacts businesses and individuals; the volume, size, complexity, and range of ESI can often be overwhelming, and the ESI itself can contain confidential, privileged or private information that needs to be considered. ESI management is often not a priority until the true value and cost of locating ESI become apparent as part of a matter. Organizations and individuals frequently

— focus their ESI retention efforts on retention for purely business operational purposes rather than considering the wider context,

— have minimal consideration of their compliance obligations in respect of electronic records,

— have a limited understanding of the evidential value of good business records, and

— do not have a good understanding of the costs and risks associated with poor information management practices.

Poor ESI management can add challenges when it comes to identifying and retrieving ESI in response to a discovery or regulatory request because

— the content is subject to data privacy and similar restrictions to access, and restrictions relating to ownership and control,

— it is more voluminous than expected because it has been stored beyond its required lifespan,

— there is often little knowledge within the organization as to where potentially relevant ESI can be found,

— the volume and complexity are overwhelming even for ICT professionals,

— turnover of staff and organizational changes (e.g. mergers, acquisitions, and divestitures) result in retention of ESI and also the loss of organizational knowledge and context,

— the ICT environment and systems might be poorly documented, and

— ESI can be located in external applications and ICT infrastructure (e.g. social media, cloud computing, etc.).

Depending on the circumstances, these factors can lead to increased costs to locate and handle data that can be relevant to the matter in hand. This can introduce delays and increase the cost of the discovery process, and lead to overlooking potentially relevant ESI.

7.2 Common types of ESI

7.2.1 General

Categorizing ESI sources as readily accessible (or "active") or not-readily accessible (or inactive, residual, or legacy), with a justification for each categorization, is an important activity in the early stages of electronic discovery. In conjunction with budget preparation, this categorization can assist in determining the proportionality of preserving and collecting such sources.

7.2.2 Active data

This type of ESI is "actively" in use and resides on employees' computer hard drives or other storage devices and in the organization's servers, drives and databases. Active data generally can be accessed in a file manager or in the application in which it was created. Users can access it immediately without restoration or reconstruction. With the increasing popularity of cloud computing and Internet-based computing services, it can also reside on the storage devices of outside service providers. Most cases and investigations call primarily for the preservation and production of active files.

Active files can be relatively easy to access and collect, at least compared to other types of ESI. They can also be easily deleted or altered, thus preservation needs to be considered at the earliest possible time.

7.2.3 Inactive data

This type of ESI is related to closed, completed, or concluded activities, including ESI an organization maintains for long-term storage and record keeping purposes, but which is not immediately accessible to the user of a computer system. It can include many of the same sources of data described above in relation to active data.

Archived data are often stored in a compressed format and can be maintained on system drives or off-line devices, including storage tapes or disks and optical media. Some systems allow users to retrieve archival data directly, while other systems require the assistance of an ICT professional. Challenges in preservation and collection include identifying relevant inactive and archived data, locating where and how it is stored, and restoring it from a compressed format.

Another form of inactive data is the ESI stored within data protection systems (e.g. backups). These inactive data can be a source of problems because they tend to be short term (e.g. the backup media are rotated on a regular basis), there might not be any mechanism to determine what is on the media, and stored data might only contain fragments (e.g. only the changes from the last backup). To complicate matters, ICT personnel can make extra backups that fall outside of normal operations (e.g. rotation, documentation, etc.) and it can be extremely difficult to identify these potential sources of ESI. This type of data has all the same challenges as archived data with the additional element of short retention periods, which requires quick action to suspend the automatic destruction of this ESI in the event that preservation is necessary.

7.3.3 provides additional information on backups and archives.

7.2.4 Residual data

This type of ESI is hidden and cannot be viewed in applications (such as system files) or has been erased, fragmented, or damaged. Collecting this type of ESI usually requires an exact, bit-by-bit copy of the entire physical storage media (e.g. hard drive, CD, DVD, tape), including all active and residual data and unallocated or slack space on the media.

Imaging and then extracting the residual data might require a digital evidence specialist (see ISO/IEC 27037) to operate special tools and can be time consuming and expensive. In some cases, however, companies can choose to image the hard drives of particularly important key custodians to ensure that all their data are preserved, including files that the custodian might have unintentionally, or intentionally, deleted or partially overwritten.

7.2.5 Legacy data

This type of ESI is created by software or hardware that is outmoded or has become obsolete (legacy systems). A legacy system might be one that the company still uses but that the hardware or software vendor no longer supports. Alternatively, it might be a system that the company has decommissioned but retains in case its information is needed in the future.

The relevance of legacy data can be difficult to determine without restoration or reconstruction, and it can be costly to do so. If preserving the legacy data is needed, the company might need to retain the legacy hardware and software if there is no other way to view or use the data.

7.3 Common sources of ESI

7.3.1 General

Potentially relevant ESI in litigation and investigations can be found in a wide range of sources. To help identify these sources, it is important to consider systems and resources under the direct control and access of custodians as well as those that are not under the control of custodians.

7.3.2 Custodian data sources

Custodian ESI sources are those sources of ESI over which an individual custodian has direct custody or control. These include, but are not limited to, the following sources:

— Computers: potentially relevant ESI might be present on custodians' desktops, laptops or home computers as well as on removable storage media, such as thumb drives, external hard drives, DVDs or CDs;

— Mobile devices: potentially relevant ESI might be present on custodians' personal devices such as mobile phones, smart phones, tablets, Global Positioning Systems (GPS), etc.

From an enterprise perspective, databases and applications, network storage, backups, and electronic archives, as listed in 7.3.3, can also be considered custodian sources.

7.3.3 Non-custodian data sources

Non-custodian ESI sources are either internal to the organization or external to it.

Internal sources are those to which one or more custodians have access, but over which another custodian, such as an ICT administrator, has control. Non-custodian data sources internal to the organization include, but are not limited to, the following sources:

— Databases and applications: ESI related to dynamic databases can be relevant in some cases, and depending on the issues, a matter might involve an organization's electronic document management systems (EDMS), electronic records management systems (ERMS), or collaborative tools;

— Network storage: ESI might be stored in various places on an organization's internal network (e.g. shared drives, network disk drives, and servers) as well as specialized storage technology such as Network Attached Storage (NAS) and Storage Area Networks (SAN);

— Backups: ESI copied or backed up from information systems onto data protection systems such as tape or other media;

— Electronic archives: ESI contained in electronic or digital archives (data repository) is typically official business records, documents retained for compliance purposes, legacy documents (historical value), etc.

Non-custodian data sources that are external to the organization include, but are not limited to, the following sources:

— Cloud storage: cloud computing solutions are often used for many applications as well as for disaster recovery and business continuity purposes;

— Social media: social media contains ESI that is shared among groups of people mostly for social purposes, but increasingly it has been used for business purposes, which can result in challenges because it tends to reside outside of an organizations immediate control.

7.3.4 Potentially excluded sources of ESI

Not all sources of ESI need to be preserved; the following sources of ESI are potentially not discoverable:

— deleted, slack, or unallocated data on hard drives;

— random access memory (RAM) or other ephemeral data;

— data in metadata fields that are frequently updated automatically, such as last-opened dates;

NOTE Careful consideration and consultation need to be given as to which metadata fields are to be preserved, as it can be difficult, and frequently impossible, to reverse once changed. For example, metadata information such as when a document was first created or last modified can be crucial in filtering ESI later in the process, so it needs to be maintained.

— backup data that are substantially duplicative of data that are more accessible elsewhere;

— test data for temporary use;

— other forms of ESI whose preservation requires extraordinary affirmative measures that are not utilized in the ordinary course of business.

It can be beneficial to attempt to reach an agreement with litigation opponents or investigators that such ESI does not need to be preserved.

7.4 ESI representations

7.4.1 General

The ESI associated with a particular matter can include word processing files, spreadsheets, email, databases, drawings, photographs, data from proprietary applications, website data, voice mail, and much more. The collection and production formats for ESI files can be classified as native, near-native, image (near-paper) and paper.

7.4.2 Native formats

Files in the format they were created and maintained are known as native files. Native format is often recommended for files that were not created for printing, such as spreadsheets and small databases. For some file types, the native format can be the only way to adequately produce the ESI.

Production in native format does not require the producing party to incur the cost of converting the data to a different format; however, the receiving party might need the native application or the producing party's proprietary software to open files.

In the event that a party chooses to convert ESI into a different format, steps to ensure that elements of that ESI, such as metadata, are not unintentionally lost or obscured in the process can be necessary.

7.4.3 Near-native formats

Some files (e.g. email and databases) cannot be reviewed without some form of conversion. For example, most email files have to be extracted and converted into individual files, and as a result, the original format is altered and they are no longer in native format.

Large databases and data compilations are commonly produced in near-native format. Databases can comprise massive amounts of completely undifferentiated tables of data. Enterprise business systems can contain hundreds of tables and thousands of fields of data. The systems can require various database platforms and proprietary software. For these reasons, large databases and data compilations are generally not produced in native format. These databases often need to be analysed by appropriate personnel to identify the responsive data and determine the appropriate near-native format.

Exports from these databases are often produced as text delimited files. In some cases, text files are produced with a database diagram, data dictionary, metadata or software. Data can also be exported to common spreadsheet formats.

7.4.4 Image (near-paper) formats

ESI can also be produced in an image, or near-paper, format. Rendering an image is the process of converting ESI or scanning paper into a non-editable digital file. During this process, a "picture" is taken of the file as it exists or would exist in paper format. Based on the print settings in the document, the printer or the computer, data can be altered or missing from the image. Expertise in the field of electronic discovery and image rendering tools are necessary to minimize these issues.

7.4.5 Hardcopy

Rather than dealing with ESI in its electronic form, it might be reasonable and practical to record the ESI onto some form of hardcopy (e.g. paper printout, photograph, etc.), and then this hardcopy is what is used throughout the matter. As with converting ESI to image formats (see 7.4.4), recording ESI to some form of hardcopy can result in missed or altered data. Consequently, expertise in electronic discovery and image rendering tools might be necessary to minimize these issues during the printing or image rendering process.

7.5 Non-ESI as part of discovery

While most business information is stored in electronic format, a discovery project can involve at least small elements of traditional hardcopy or paper documents (this is different from printed ESI described in 7.4.5). If a determination is made to collect the hardcopy, the more focused the collection is to the matter at hand, the less work is potentially needed to refine the document set to the relevant subset.

With a focused set of hardcopy documents, one choice is to have them scanned into electronic format[1)] and then included in the review process alongside the electronic documents. Consideration may be given to whether they have associated family members. Such documents need to be reviewed, marked, and possibly redacted, before being produced. This can make it more efficient to use the same technologies and processes to manage hardcopy documents that are used for ESI.

1) This process can involve the use of Optical Character Recognition (OCR) technologies to produce searchable results as well as coding by a human reviewer to capture pertinent metadata.

8 Electronic discovery process

8.1 Overview

Electronic discovery is a form of traditional discovery that typically involves identifying, preserving, collecting, processing, reviewing, analysing, or producing Electronically Stored Information (ESI) that is potentially relevant to a particular matter. Potentially relevant ESI is typically

— identified through an iterative process of research and interviews with employees and ICT personnel,

— preserved by taking steps to notify appropriate individuals to refrain from deleting or destroying it or revoking systems that do so automatically,

— collected from an original source, using one or more of several extraction or collection methodologies that preserve data integrity,

— processed using one or more technological tools, indexed to render the text searchable,

— reviewed for relevance, in one or more ways, by legal or subject matter experts assisted by a variety of tools and individuals with the expertise to use them effectively,

— analysed in order to assist in meeting objectives of the matter, and

— produced to the requesting party or parties, in a manner that is reasonably usable or in a form agreed upon by the parties.

Within this document, generic actions such as “identifying” are differentiated from the specific electronic discovery process elements by preceding the names with “ESI” (e.g. ESI identification). Figure 2 shows all of the electronic discovery process elements.

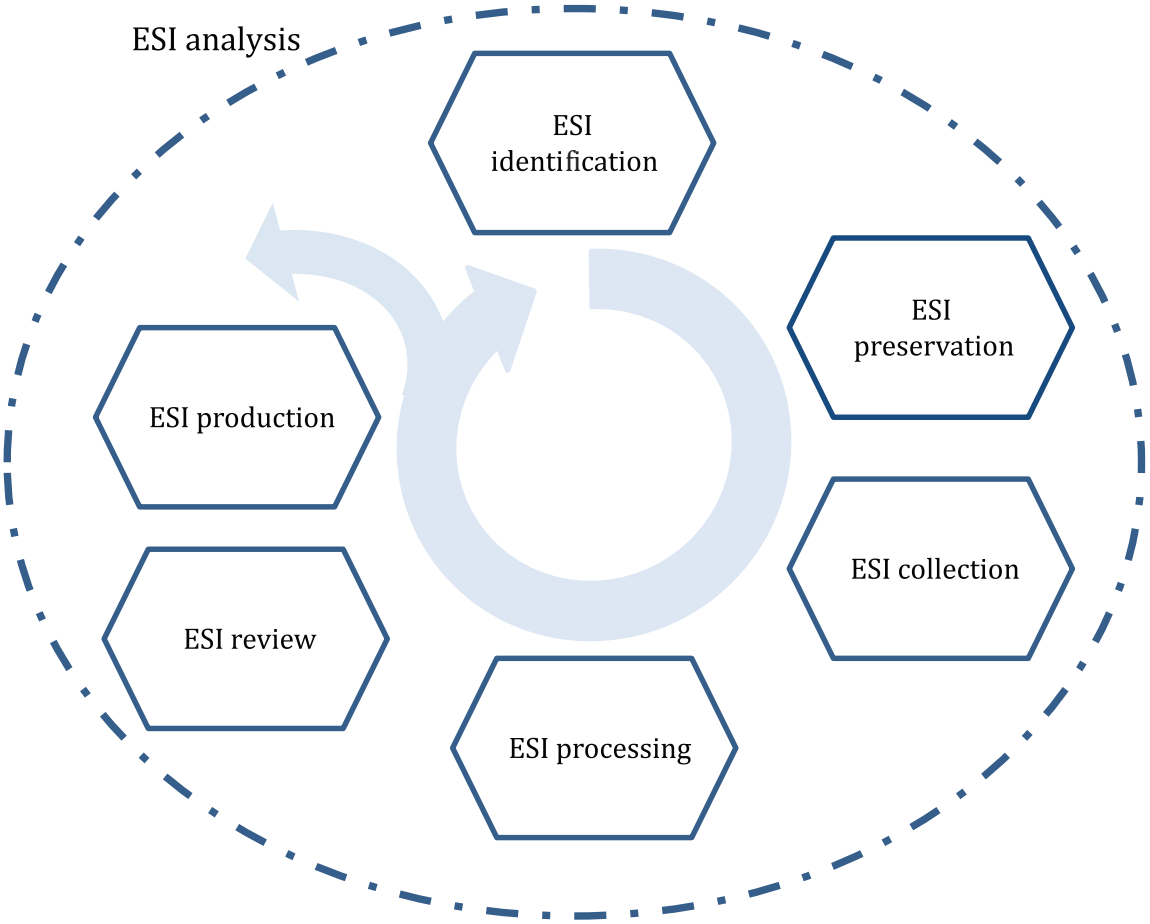

Figure 2 — Electronic discovery process elements

Figure 2 also shows the interrelationship among the electronic discovery process elements. The positioning of ESI analysis as an outer ring is meant to show that analysis can optionally occur in conjunction with each of the other electronic discovery process elements. For example, a possible scenario is one in which ESI identification might require ESI analysis to be performed and then the process returns to ESI identification for additional activity. The process flow can move from one process element, other than ESI analysis, to another and then back to an earlier process element. Lastly, electronic discovery is often an orderly and iterative process undertaken with some or all of the process elements, and this is also shown in Figure 2 with the circular arrows.

This document is intended to serve the interests of multiple stakeholders, large versus small entities, legal versus non-legal, etc. While a robust electronic discovery process is described, there is no intention to impose unneeded processes. Large enterprises with complex electronic discovery issues can use most or all of the process elements described herein, but it can be impractical for small organizations or small matters. A matter may use a subset of the process elements.

Assume a small number of email messages are core to a matter. The activity starts with ESI identification, which then leverages ESI analysis to determine whether additional sources might exist. Upon finding there are none, the email in question is collected (skipping preservation). ESI analysis is then performed to determine whether the ESI collection was adequate as well as to make a reasoned decision to skip the ESI processing and ESI review elements. The email messages relevant to the matter are then produced in native format as part of the ESI production process element.

In some jurisdictions, courts, legislatures, or government regulators have developed rules concerning how organizations identify ESI, particularly for purposes of civil and criminal proceedings, investigations, and audits. In such jurisdictions, organizations might have a duty to take reasonable steps to identify and preserve potentially relevant ESI when a litigation or investigation is reasonably

anticipated or pending against them. Underlying this duty to identify and preserve ESI, an organization has to be able to locate and preserve potentially relevant ESI in a timely manner. Further, organizations might be expected to develop appropriate ESI management protocols and be compliant with those rules.

8.2 ESI identification

ESI identification is the element of the electronic discovery process in which a party, for any number of reasons (e.g. reasonable anticipation of a lawsuit, receipt of a pre-litigation preservation request, a request to inspect, a demand letter, a cease and desist letter, a cure notice, or even a discussion with an opposing party or its counsel), takes steps to identify information that could be potentially relevant to the matter.

ESI identification is essentially an exercise in understanding the relevant subject matter and identifying individuals, departments and ESI sources that could reasonably lead to potentially relevant information related to that subject matter. In the case of electronic information, ESI sources are likely to be varied and complex, potentially encompassing both internal and external ESI locations, various server types, and myriad electronic devices. In addition, due consideration of legacy systems (archives, backups, inactive systems and data) might also be required. Typically, to identify the sources potentially important to a particular matter, individuals potentially involved in the events at issue plus identified members of the ICT department are interviewed to determine if they are in possession of or aware of relevant ESI. These interviews, in turn, can lead to the identification or elimination of other key players or possible locations of relevant ESI.

Having interview templates and tracking mechanisms is ideal for identifying and interviewing individuals and to document their knowledge of the types of data and data locations containing potentially responsive information. There might be different questions in the templates based on the business unit or the role of the individual. This documentation can assist in planning, implementing, and tracking activities and answers in the identification process and can be a point of reference when questions arise regarding additional (or potentially redundant) sources of information. In addition, it can be used to demonstrate that the identification process was appropriate if it comes under question.

8.3 ESI preservation

ESI preservation is the element of the electronic discovery process in which, after a triggering event, efforts are made to keep secure from modification or destruction information that has been identified as relating to the scope of a preservation obligation in a matter. This includes not only potentially relevant ESI within the individual's or organization's possession, but also information outside of the individual's or organization's possession. As a preservation obligation can vary by jurisdiction, there is no single standard that describes how to measure the appropriateness of preservation activities, or a party's exposure or potential liability for failure to fulfil their preservation duties.

Electronic information can be preserved by collecting it (i.e. copying it directly from its source), or by taking steps to ensure its safekeeping where it normally resides (e.g. custodian self-preservation or in-place preservation using technology), after which it might or might not be collected, depending on the needs of the matter and the preservation strategy. The act of collecting a copy of ESI is in itself a form of preservation, and ESI preservation and ESI collection can be carried out together. The key differentiator of ESI preservation is that it involves taking steps to preserve ESI so that it is free from modification. Possible suspension of routine procedures that could delete or alter potentially responsive data (e.g. backup tape rotation or routine records destruction) might be warranted.

8.4 ESI collection

ESI collection is the element of the electronic discovery process in which a data set is created from the ESI and hardcopy documents that have been preserved; the collection is then made available for further processing and eventual review.

Collection is essentially a copying exercise, in which copies or images of the target files are obtained and included in a data set that can then be passed on to downstream processing and review. There is a wide range of tools and methods that can be used for collection, from those that can enable the recovery

of files that a user has deleted to those involving a simple user-created export of the target files. The specific tools and methods appropriate in any given instance can vary with the nature of the device from which the files are being collected (e.g. a desktop computer vs. a smart phone), with the nature of the files being collected (e.g. email vs. a microblog post), with the nature of the proceeding that is the occasion for the collection (e.g. criminal vs. civil), and with the jurisdiction in which the litigation or investigation is conducted.

8.5 ESI processing

ESI processing is the element of the electronic discovery process in which, after data have been preserved and collected, steps are taken to render the data searchable and present them in a reviewable format. This can involve one or more methods. In addition, there can be myriad techniques used to narrow the responsive data volumes beginning by removing system files and other files unlikely to be of interest in the matter. This is often followed by one or more filtering techniques ranging from date-range filtering, to file-type filtering, to basic filtering on metadata or text using search terms, concept or predictive algorithms that run on text-based processed data. Choices regarding deduplication occur in ESI processing as well. The techniques utilized in ESI processing are often agreed to between parties to ensure a common understanding of how the data can be processed and made available in the electronic process elements that follow.

In addition to data reduction, processing data needs to be supported by defensible auditing procedures, quality control measures that include data validation as well as documented chain of custody that includes tracking of file transformations as they move through the ESI processing.

8.6 ESI review

ESI review is the element of the electronic discovery process which focuses on screening ESI based on specific criteria. In essence, documents that meet the production criteria are separated from those that do not.

There is a wide range of approaches to conducting a review, from the long-practiced linear manual review to more recent approaches making extensive use of advanced information retrieval tools and methods. This document is designed to be applicable to all approaches.

8.7 ESI analysis

ESI analysis is the element of the electronic discovery process that refers to the task of applying various tools and methods to the ESI in order to gather information that can be put to use in accomplishing the objectives of each of the distinct electronic discovery process elements. As such, analysis is an activity that can be undertaken in support of any of the iterative steps in the electronic discovery process (identification, preservation, collection, processing, review, and production).

There is a wide range of tools and methods that can be used for purposes of analysis. Which tool or method is appropriate in any given instance can depend on the electronic discovery process element in support of which data analytics are undertaken and on the specific question to which data analytics are being called upon to provide an answer.

8.8 ESI production

ESI production is the element of the electronic discovery process in which a party prepares files for delivery to other parties. The procedures for preparing data for production are typically agreed upon in initial project planning.

Data can be produced in electronic or paper format depending on the agreements made between parties. Production formats can vary to include a combination of native and near-native images derived from scanned paper or physical paper. Considerations need to be made when preparing data for production that include the types of technical intake capabilities that are available by the recipient. This might include

capabilities and tools available to review the production by the recipient. Often, cost considerations are examined based on the volume of data and the production format in order to limit costs.

As in many elements in the electronic discovery process, attention needs to be given to documenting the files produced within production or privilege logs. This documentation serves to provide details on what files were produced and what files were withheld.

9 Additional considerations

9.1 Presentation of ESI

While not considered an element of the electronic discovery process, it is important to understand how ESI can ultimately be used in a matter (e.g. presented in court).

The presentation of ESI can be a challenge for attorneys and paralegals. In the past, exhibits were presented in paper form and still are in many cases today. Technology has developed over the last decade, making it easier to present exhibits in near-paper or "image" format. Due to the nature of Electronically Stored Information and the advent of native and near-native document productions, some cases now require the legal team to present exhibits in native format.

9.2 Chain of custody and provenance

Depending on the matter at hand, it can be important to track or determine information regarding the creation, modification history, influences, ownership, or other provenance or lineage information associated with ESI. Some of this information might be contained in metadata or it might be generated as part of the electronic discovery process. This provenance information can be essential for making informed judgements about ESI quality, integrity, and authenticity.

In some cases, provenance information is not sufficient to demonstrate quality, integrity, and authenticity. In such cases (e.g. criminal investigations or prosecutions), formal chronological documentation that shows the custody, control, transfer, and disposition of ESI is necessary. It is important to recognize when proof of chain of custody is needed and to ensure that the requirements are met.

Bibliography

[1] ISO Guide 73, *Risk management — Vocabulary*

[2] ISO 15489-1:2016, *Information and documentation — Records management*

[3] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[4] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[5] ISO/IEC 27040:2015, *Information technology — Security techniques — Storage security*

[6] ISO/IEC 27041, *Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method*

[7] ISO/IEC 27042, *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*

[8] ISO/IEC 27043, *Information technology — Security techniques — Incident investigation principles and processes*

[9] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[10] ISO/IEC 38500, *Information technology — Governance of IT for the organization*

[11] *Electronic Discovery Reference Model (EDRM)*, http://www.edrm.net

[12] *Good practice guide to eDiscovery in Ireland*, Version 1.0, 16 April 2013, http://www.eDiscoveryGroup.ie

[13] New York Bar Association, *Best Practices in E-Discovery in New York State and Federal Courts*, Version 2.0, December 2012, http://www.nysba.org

[14] *Seventh Circuit Electronic Discovery Pilot Program — Final Report on Phase Two*, May 2012, http://www.discoverypilot.com/sites/default/files/Phase-Two-Final-Report-Appendix.pdf

ICS 35.040
Price based on 21 pages