INTERNATIONAL STANDARD

ISO/IEC 27050-4

First edition
2021-04

Information technology — Electronic discovery —

Part 4:
Technical readiness

Technologies de l'information — Découverte électronique —

Partie 4: Préparation technique

Contents

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.

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) or the IEC list of patent declarations received (see patents.iec.ch).

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

For an explanation of the voluntary nature of standards, 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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Electronic discovery can expose organizations and their stakeholders within and outside those organizations to collective and individual risks, including legal, financial and ethical.

This document is to be read in relation to ISO/IEC 27050-1, ISO/IEC 27050-2, and ISO/IEC 27050-3.

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 electronically stored information (ESI) sometime necessitate protections like storage security to guard against data breaches (covered in ISO/IEC 27040).

Information technology — Electronic discovery —

Part 4:
Technical readiness

1   Scope

This document provides guidance on the ways an organization can plan and prepare for, and implement, electronic discovery from the perspective of both technology and processes. This document provides guidance on proactive measures that can help enable effective and appropriate electronic discovery and processes.

This document is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities.

2   Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 22123-1, *Information technology — Cloud computing — Vocabulary*

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

ISO/IEC 27050-1:2019, *Information technology — Electronic discovery — Part 1: Overview and concepts*

3   Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27050-1, and ISO/IEC 22123-1 and the following apply.

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

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

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

3.1
compliance obligations
legal requirements and other requirements
legal requirements that an organization has to comply with and other requirements that an organization has to or chooses to comply with

Note 1 to entry: Compliance obligations can arise from mandatory requirements, such as applicable laws and regulations, or voluntary commitments, such as organizational and industry standards, contractual relationships, codes of practice and agreements with community groups or non-governmental organizations.

[SOURCE: ISO 14001:2015, 3.2.9, modified — Note 1 to entry has been removed and Note 2 to entry renumbered.]

3.2
technical readiness
state of having the knowledge, skills, processes and technologies needed to address a particular issue or challenge

4   Symbols and abbreviated terms

BCM   business continuity management

CCTV   closed-circuit television

ESI   electronically stored information

ICT   information and communication technology

PBX   private branch exchange

PII   personally identifiable information

RIM   records and information management

SaaS   software as a service

TAR   technology-assisted review

VPN   virtual private network

WORM   write once read many

5   Electronic discovery background

Electronic discovery is an element of traditional discovery or disclosure and it is a process that typically involves identifying, preserving, collecting, processing, reviewing, analysing and producing electronically stored information (ESI) that can be potentially relevant to a particular matter. The requirements and recommendations provided in this document are in accordance with the electronic discovery concepts described in:

— ISO/IEC 27050-1:2019, Clause 3: key electronic discovery terminology;

— ISO/IEC 27050-1:2019, 6.2: electronic discovery issues and primary cost drivers;

— ISO/IEC 27050-1:2019, 6.3: general electronic discovery objectives;

— ISO/IEC 27050-1:2019, Clause 7: common ESI types, common sources, and representations;

— ISO/IEC 27050-1:2019, Clause 8: description of the electronic discovery process and the process elements.

ISO/IEC 27050-1 differentiates between generic actions such as "identifying" from the specific electronic discovery process elements by preceding the names with "ESI" (e.g. ESI identification). Likewise, this document follows this approach. Figure 1, repeated from ISO/IEC 27050-1:2019, shows all the electronic discovery process elements and the interrelationships between them (see ISO/IEC 27050-1:2019, 8.1, for a full description).
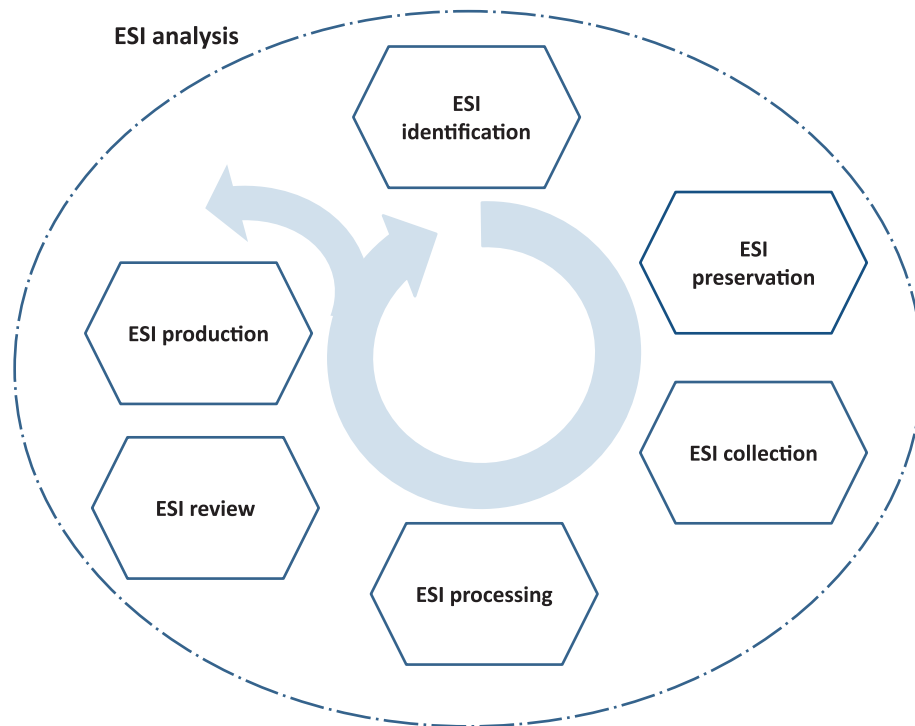
Figure 1 — Electronic discovery process elements

ISO/IEC 27050-2 provides guidance for decision makers and those holding responsible roles to ensure that causes of failure are properly managed and, where possible, minimized while still complying with policy and conformance requirements to enable effective and appropriate electronic discovery and processes. ISO/IEC 27050-3 provides requirements and guidance associated with the electronic discovery process elements shown in Figure 1. While the guidance and requirements provided in ISO/IEC 27050-2 and ISO/IEC 27050-3 cover key aspects of electronic discovery, organization can benefit from additional proactive measures that address a range of related challenges.

The ISO/IEC 27050 series addresses these challenges by:

— promoting common understanding of various concepts and terminology for electronic discovery;

— articulating objectives and risks inherent in the steps in the electronic discovery process;

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

— providing guidance and best practices for those responsible for delivering electronic discovery projects (e.g. legal practitioners, services providers, independent experts, courts, and any other parties engaged in the process);

— identifying competency areas for those involved in electronic discovery;

— promoting the proactive use of technology to reduce costs and risks, while increasing efficiencies throughout the discovery process;

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

The overriding objective is to help organizations meet their electronic discovery goals (e.g. legal obligations, business objectives, regulatory requirements).

While this document has been written with larger electronic discovery projects in mind, and therefore covers aspects encountered in the majority of matters. It is not necessarily the case that all steps are

required or proportionate to every matter. For example, in small matters, it is possible that a single person manages and completes every aspect of the project, whereas larger matters can warrant the use of separate individuals or even teams for each element of the electronic discovery project.

6 Technical readiness

Technical readiness means having the knowledge, skills, processes and technologies needed to address a particular issue or challenge. For an organization, this does not mean that it is all-knowing and able to do everything, but rather it is fit for purpose and ready for the task at hand, including any contingency that can occur.

Within the context of electronic discovery, technical readiness means an organization is well positioned to address the tasks associated with the appropriate electronic discovery process elements. This readiness is also dependent on the type of organization (e.g. legal versus records management) as well as the role the organization plays in the electronic discovery process (e.g. producing party versus receiving party).

The electronic discovery readiness 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;

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

— conduct the electronic discovery process within the time constraints.

Technical readiness in the context of electronic discovery should be based on the information architecture, business processes, and data classification and retention policies of the organization.

Technical readiness is the achievement of the appropriate level of capability by an organization in order for it to be able to identify, preserve, collect, process, review, analyse and produce ESI. It is also important the ESI is protected (for example, backup, business continuity management, or security) and organized so that this material can be used effectively.

Technical readiness implies a proactive effort to better address electronic discovery projects in the future. This effort can require ESI to be organized, participants to be properly trained, protocols to be developed and data retention and disposal practices to be formalized.

This should form part of the electronic discovery plan (see ISO/IEC 27050-2:2018, 6.5).

7 Readiness for electronic discovery

7.1 ESI identification

7.1.1 General

ISO/IEC 27050-3:2020, 6.2, provides both requirements and guidance for ESI identification. Of these, the following can benefit from readiness or proactive activities:

— basic planning associated with determining who executes ESI identification and how it is expected to be performed;

— understanding the organization's ESI landscape, including operational aspects that could impact preservation;

— development of standard templates for interview questions and survey forms;

— create a list or inventory of systems, or possibly a data map to provide a centralized listing of what types of ESI the organization has and where it is stored;

— understand the implications associated with issuing legal holds or preservation orders.

7.1.2   ESI landscape

ISO/IEC 27050-1:2019, Clause 7, provides useful information on the common types of ESI, common sources of ESI, ESI representations and non-ESI as part of the electronic discovery process. This information, when combined with the matter specific requirements, can serve as a useful starting point in identifying potential sources of relevant ESI. These sources can include business units, people, ICT systems and hardcopy.

Identification should be as thorough and comprehensive as possible. The scope of ESI potentially subject to preservation and disclosure can be uncertain in the early phases of a matter. The nature of the matter itself and the individuals involved can change as the matter progresses. The identification team should anticipate change and have a procedure in place for capturing any newly identified ESI. Identification requires diligent investigation and analytical thinking.

7.1.3   Data map

A data map is a comprehensive and defensible inventory of an organization's ICT systems that store ESI. It is important to create a data map to provide a centralized listing of which types of ESI exist within the organization (see ISO/IEC 27050-3:2020, 6.2.5). This should also include details of specific locations of data sets and can include the route data takes when in transit alongside, for example, who has control over a mailbox and where the servers sit including any hardcopy material requirements.

This data map should be designed and managed with the assistance of ICT personnel and should identify all relevant policies (e.g. retention policy, preservation policy, BCM policy) applicable to each item of ESI. Ideally, the data map can also include the locations of hardcopy material. Resource should be assigned to the task and on-going responsibility of creating and managing the data map.

After the triggering event, the electronic discovery team can use the data map to identify where the relevant material is stored (ESI map).

The ESI map can provide sufficient detail around what data repositories are potentially discoverable and how the data within them can be produced to help inform decisions around the electronic discovery system selection process.

Where hardcopy material forms are identified, there should be a decision and process in place to manage the scanning and coding. This should include coding specifications that can be specific to the organizational and project requirements.

See Annex A for assistance with creation of the data map.

The level of security necessary for the ESI, all associated metadata and work product is dependent on business needs and compliance obligations as applicable to the purposes of the electronic discovery process. The security should be commensurate with the controls determined in accordance with 8.2.

7.1.4   Data classification

All ESI should be subject to data classification. This can be according to government standards, market sensitivity, internal governance, privilege, control of data under data protection or privacy legislation, or for the purposes of any matter requiring discovery.

This classification can affect the decisions around the management, traffic and encryption that should be created via the architecture and system design.

7.1.5 Proactive ESI identification

Since ESI identification is crucial to the overall electronic discovery process, proactive measures that help with the ESI identification activities should include, but are not limited to:

— developing a plan template that can be used to guide the identification effort;

— developing and using standard templates for interview questions and survey forms that can be used in multiple matters;

— developing and maintaining report templates for the organization's ESI identification.

7.2 ESI preservation

7.2.1 General

ISO/IEC 27050-3:2020, 6.3, provides both requirements and guidance for ESI preservation. Of these, the following can benefit from readiness or proactive activities:

— ensuring that appropriate preservation notices are issued;

— procedures for suspending destruction of ESI or ESI resources;

— testing of technical preservation controls to verify the effectiveness of the controls.

7.2.2 Assessing preservation needs

It is important to establish preservation procedures covering employees, ICT, legal and former and departing employees. Based on the procedures, the team can assess the needs for preservation with regard to where the relevant ESI is stored and technical implications of collection. The scope of preservation should be determined. The number of subjects affected, who are required to act, who can control ESI, and the time period for preservation are among the first decisions. The team should consider the potential for third-party preservation requirements. A preservation notice should be issued to all relevant parties, including steps to be taken to ensure appropriate preservation. The team should put in place a process for continued preservation throughout the relevant time period, i.e. the life of the case or project.

7.2.3 Preservation obligations

The duty to preserve ESI, sometimes referred to as the trigger to preserve, can begin when a party knows of or has a reasonable anticipation of future litigation or action associated with a matter. The important thing to remember here is that the duty to preserve can be triggered before a lawsuit has been filed or preservation notice has been received. Consequently, organizations should understand preservation triggers within their jurisdictions.

The duty to preserve ESI for electronic discovery is often not described in a law or even explicitly defined in other requirements that are relevant to a matter. In addition, preservation expectations can vary significantly in different jurisdictions.

Another important aspect of preservation is the scope of what needs to be preserved. Again, specific requirements can be vague and be described in terms of "reasonableness" and "proportionality". When preservation has been triggered, the organization should take appropriate information security steps to ensure the integrity of relevant ESI.

7.2.4 Hold/preservation notices

A preservation notice is an internal instruction issued by an organization to its employees directing them to identify, locate and preserve hardcopy and ESI that are potentially relevant to a particular matter. In addition to preventing the deletion, destruction or modification of ESI and information

by individuals, a preservation notice should also include the suspension of any routine document destruction pursuant to an organization's document retention policies or otherwise.

An important step in the legal hold process is deciding who should receive the instruction to preserve ESI. This should include someone in charge of data storage or technology issues to ensure the organization's routine destruction procedures are suspended.

After issuing a preservation notice, responsible individuals should periodically follow up with the individuals and organizations who received the notice to make sure they implemented it as instructed. As the matter progresses, consideration should be given as to whether additional individuals or organizations should receive the litigation hold and whether the scope of the original preservation notice is still sufficient. If claims or issues are added or the nature of the matter changes, it can be necessary to issue a new or amended preservation notice to ensure all potentially relevant ESI is preserved. In addition, as personnel decisions are made, organizations should consider whether new employees should be added to the legal hold and whether departing employees' ESI should be preserved.

7.2.5   Proactive ESI preservation

Since ESI preservation is crucial to the overall electronic discovery process, proactive measures that help with the ESI preservation activities should include, but are not limited to:

— retention policies;

— understanding preservation triggers;

— developing and maintaining legal hold materials and processes for the organization.

7.3   ESI collection

7.3.1   General

ISO/IEC 27050-3:2020, 6.4, provides both requirements and guidance for ESI collection. Of these, the following can benefit from readiness or proactive activities:

— selection of tools and methods appropriate to ESI collection;

— complying with data protection, privacy, or security obligations (see 8.2).

7.3.2   Methods of ESI collection

The specific reasons for collection can affect the method used to obtain the ESI. For example, if the ESI is for discovery in a criminal matter, the methods for obtaining the material should maintain integrity of the metadata so the material can be used as evidence where required.

It is strongly recommended that the guidance given in ISO/IEC 27037, ISO/IEC 27041 and ISO/IEC 27042 is followed when creating and deploying ESI collection processes.

7.3.3   Proactive ESI collection

ESI collection is critical in preparing the preserved ESI as a data set for further electronic discovery operations, so proactive measures that help with the ESI collection activities should include, but are not limited to:

— understanding the technologies the organization uses to protect sensitive data (e.g. encryption);

— identifying defensibility measures (e.g. chain of custody, hashing, audit trails) that can be used is situations where there is contention or controversy;

— having provisions for outside resources that include agreements/contracts with preferred vendors.

7.4   ESI processing

7.4.1   General

ISO/IEC 27050-3:2020, 6.5, states that ESI processing is further broken into four main sub-processes, namely: assessment, preparation, selection and output. Assessment can allow for a determination that certain ESI need not move forward. Preparation involves performing activities against the ESI which can later allow for specific item-level selection to occur (extraction, indexing, hashing, etc.). Selection involves de-duplication, searching and analytical methods for choosing specific items which can be moved forward. Output allows for transport of reviewable items to the subsequent elements of the electronic discovery process. Of the ISO/IEC 27050-3:2020, 6.5, requirements and guidance, the following can benefit from readiness or proactive activities:

— ESI processing tools should be tested for the data types expected to be handled;

— data reductions techniques should be appropriately vetted.

7.4.2   Tools for ESI processing

ESI can arrive at the ESI processing stage in various formats which then need to be restored before subsequent work can be done (tapes, backups, etc.). It is possible that individual files and e-mail need to be extracted from container files (PST, NSF, zip, rar, etc.). If the ESI cannot be used in its native format, it can be necessary to convert certain types of ESI to facilitate further processing (legacy mail formats, legacy file formats). This means that tools are typically needed to retrieve the ESI from the collected sources (e.g. tapes), to ingest the various formats, and to convert the native ESI to a more usable form.

Organizations should:

— catalogue the ESI, capturing details on the sources and formats;

— record the accessibility details (e.g. passwords, encryption keys, etc.) that are necessary to use the ESI;

— address any requirements to capture metadata that can be loss in a format conversion;

— explicitly identify the target format to be used, so that multiple conversions can be avoided (it is possible that this target format can be an element of negotiation as part of ESI production).

7.4.3   Reduction of ESI

Rarely is it necessary to review all items that are submitted for ESI processing, so some form of data reduction is employed. The tools and techniques used to accomplish such reductions should not be a source of issue.

Organizations should:

— document the specific tools and techniques used for all reductions;

— use processes that are repeatable and provide consistent results.

7.4.4   Proactive ESI processing

ESI processing is instrumental in preparing the ESI for further electronic discover operations, so proactive measures that help with the ESI processing activities should include, but are not limited to:

— as an ESI producing party, having a clear understanding of the potential sources and formats of ESI used within the organization;

— as an ESI receiving party, having a clear understanding of types of ESI sources and formats that can be handled and document this information so that it can be used in requests;

— documenting the tools that are available for using during ESI processing;

— identifying ICT resources that can be used for restorations and culling of ESI.

7.5 ESI review

7.5.1 General

ISO/IEC 27050-3:2020, 6.6, provides both requirements and guidance for ESI review. Of these, the following can benefit from readiness or proactive activities:

— the organization should have provisions to use manual review, the use of technology-assisted review and the use of combination methods which use both human review and automated tools to accomplish the ESI review;

— the organization should canvas the availability of the various technologies for technology-assisted review, bearing in mind that each tool can have its own strengths and weaknesses.

7.5.2 Technology-assisted review

Technology-assisted review (TAR) is a process for prioritizing or coding a collection of ESI using a computerized system that harnesses human judgments of one or more subject matter experts on a smaller set of documents and then extrapolates those judgments to the remaining document collection. The objective is to distinguish relevant from non-relevant ESI.

Organizations should:

— understand the TAR statistical models or sampling techniques and the implications associated with the approach;

— ensure the seed set or initial training set is appropriate for the matter.

7.5.3 Proactive ESI review

ESI review is the aspect of the electronic discovery process that determines relevant from non-relevant ESI, so proactive measures that help with the ESI review activities should include, but are not limited to:

— documenting the tools that are available for using during ESI review;

— identifying the review platform that can be used for determining responsive ESI.

7.6 ESI analysis

7.6.1 General

ISO/IEC 27050-3:2020, 6.7, provides both requirements and guidance for ESI analysis. Of these, the following can benefit from readiness or proactive activities:

— identify tools or methods that are appropriate to the ESI to potentially be analysed;

— identify common tasks relevant to ESI analysis to determine relationships and patterns among the data, make predictions, present visualizations of the data, or create reports to exercise judgement regarding the data.

7.6.2 Tools and tasks for ESI analysis

There are many tools that can be used during the initial analysis and identification of documents to be collected that can track the types and locations of ESI within an organization. In addition, many tools today provide content and visual analytic capabilities that can help identify gaps through sampling and review of collected or preserved data sets. For example, social networking visualizations can quickly provide an overview of other custodians of interest based on interactions with key custodians in a

given matter. Important information about the case can also be obtained at an early stage from e-mail string analysis, duplication and near-duplication analysis and concept clustering and related tools.

Organizations should use analysis to:

— determine the provenance of the ESI (e.g. harvesting embedded metadata);

— make it easier to cull documents.

7.6.3   Proactive ESI analysis

ESI analysis is used throughout the electronic discovery process, so proactive measures that help with the ESI analysis activities should include, but are not limited to:

— information management systems should be designed to accommodate legal holds or preservation orders, as well as identification, preservation and collection requirements;

— content analytics, traditionally used during discovery, should be used as a filter when cataloguing ESI for destruction, inclusion in or exclusion from archive systems in an effort to reduce the number of retained business records that are to subject electronic discovery;

— electronic discovery planning and implementation should be followed by vigorous and periodic auditing.

7.7   ESI production

7.7.1   General

ISO/IEC 27050-3:2020, 6.8, provides both requirements and guidance for ESI production. Of these, the following can benefit from readiness or proactive activities:

— identification of tools or methods to be used;

— measures needed to protect the sensitivity of ESI while it is in transit and at rest;

— specification of the preferred forms of ESI to be produced or received and to have appropriate conversion tools;

— identification of storage or transmittal options for different volumes of ESI.

In addition, there can be significant differences in the needs of an organization, depending on whether it is the producing party or a receiving party in a matter, so both are addressed.

7.7.2   Producing parties

Much of the electronic discovery process is focused on the producing parties. As such, extensive requirements and guidance can be found in ISO/IEC 27050-2 and ISO/IEC 27050-3. From a readiness perspective, the following should be addressed:

— allocate sufficient storage space for ESI production such that the ESI data sets can be staged;

— understand the organization's preferred form of production;

— have available tools that allow for the conversion of ESI from native format to near-image or image formats (see ISO/IEC 27050-1:2019, 7.4);

— track the sensitive ESI and ensure that it is adequately protected on any staging platforms used and notify the receiving party of their obligations associated with this ESI.

7.7.3 Receiving parties

As a receiving party, the organization is likely to be involved in various negotiations that can culminate in ESI being made available. To deal with this situation, the receiving party should:

— deploy sufficient ICT resources to be able to receive the ESI data sets produced for the organization;

— clearly understand the forms of ESI that the organization can currently handle;

— establish contractual arrangements that can be used to address ESI volumes and types that are not compatible with existing ICT infrastructure;

— engage internal and external personnel on the appropriate handling procedures for different types of ESI.

7.7.4 Proactive ESI production

Since ESI production is often the final activity in the overall electronic discovery process, proactive measures that help with the ESI production activities should include, but are not limited to:

— ensuring that sensitive ESI is protected in transit and at rest;

— understanding the costs and benefits of different forms of production for their particular ESI data set before agreeing to or finally determining a form of production.

8 Additional considerations

8.1 General

Electronic discovery is just one facet of information management and has many dependencies and potential impacts that need to be addressed. This clause identifies some of the more important issues that need to be considered.

8.2 Privacy and data protection

ISO/IEC 27000 defines confidentiality as the "property that information is not made available or disclosed to unauthorized individuals, entities, or processes." ISO/IEC 27040:2015, 6.8.2.1, points out that "within storage infrastructures, data confidentiality is typically maintained using some method of encryption. These methods are most often associated with protecting data while it is transferred (sometime referred to as in flight or in motion) within the storage infrastructure or as it is stored (or at rest) within a device or on storage media."

While cryptographic mechanisms are one of the strongest ways to provide confidentiality, additional mechanisms can also be required to assure data confidentiality:

— authentication processes;

— authorization and access controls;

— data classifications and policy;

— proof of controls and audit logging.

From a data protection perspective, maintaining data confidentiality is one of the most important aspects of ensuring protection of personal data.

Organization should:

— have a data classification scheme that is documented in policy and that applies to ESI associated with electronic discovery activities;

— clearly identify the privacy and data protection requirements associated ESI that is retained;

— implement adequate security controls to protect the organization's ESI and all copies;

— ensure that the security controls are robust enough that they do not become a source of problem (e.g. loss of data encryption key, which would render the ESI unusable).

8.3 Long-term retention of ESI

8.3.1 Retention and preservation

There are many instances in which the terms "retention" and "preservation" are used interchangeably and incorrectly. This can result in different and conflicting requirements that govern how the same information is maintained, how long it should be kept, and whether and how it is protected and secured.

ISO/TR 18492 notes that electronic document-based information constitutes the "business memory" of daily business actions or events and enables entities to later review, analyse or document these actions and events. As such, this electronic document-based information is evidence of business transactions that enable entities to support current and future management decisions, satisfy customers, achieve regulatory compliance and protect against adverse litigation. To achieve this goal, this electronic document-based information should be retained and appropriately preserved (e.g. addressing evidentiary requirements, which includes authenticity).

In addition to compliance obligations, preservation requirements can take on a legal usability focus. Usability preservation addresses "the processes and operations involved in ensuring the ability to read, interpret, authenticate, secure and protect against the loss of data or information throughout its lifecycle."[1] Usability preservation can also involve transformation of data (e.g. either conversion of files written by obsolete word processors or preservation of the associated ecosystem).

An organization should have a records management policy that defines what is a record[2] and how records can be managed. In addition, the organization should have a retention schedule that classifies its records into record series, with associated retention periods and metadata. It is important to note that not all documented information in the possession, custody or control of the organization should have record status. Instead, only documented information regarding the operation of the organization's business that it is required to keep (e.g. compliance obligations) or which has business value should be a record.

At any given moment, the same information can exist in multiple "states," meaning the purpose for which the information is kept, rather than its physical location or medium. Recognizing these various states as well as using consistent language when describing these states is critical to ensuring applicable retention and preservation requirements are identified.

8.3.2 General data retention

Record-quality information should be retained in the ordinary course of business pursuant to the retention schedule, regardless of the medium of the record (such as paper, digital data or micrographics). Retention periods should be codified in policy and determined based on compliance obligations, and also by considering the business value and business need for the information.

NOTE   Different legal requirements for retention can exist in different countries.

Compliance and business considerations can also dictate the way the records are retained, including how they are protected and secured. And once, in the ordinary course of business, a record has been retained for the length of time that the retention schedule indicates, it should properly be disposed of

---

1)   The Storage Networking Industry Association (SNIA) Online Dictionary definition for "preservation."

2)   An example of a definition for a record is: "A record is broadly defined as documentary material, in any media, that is created or received in the normal course of business, is worth preserving, either temporarily or permanently, because it provides evidence of the organization's policies, procedures, activities, and decisions and has technical, administrative, historical, or legal value."

because its compliance and business value has expired. While it can seem contradictory that retention schedules should include a data disposition policy, organizations that keep everything are exposing themselves to considerable risk.

ISO/IEC 27040:2015, 7.4, approaches data retention from the perspective of long-term versus short/medium-term retention with the latter being driven by legal, regulatory or statutory requirements that are shorter than traditional archives (less than 10 years). The evidentiary nature of the short/medium-term retention is thought to have noteworthy differences that can impact security.

8.3.3 Archive

ISO 14721 points out that the term "archive" has come to be used to refer to a wide variety of storage and preservation functions and systems, and further, that traditional archives are understood as facilities or organizations which preserve records, originally generated by or for a government organization, institution, or corporation, for access by public or private communities. The archive accomplishes this task by taking ownership of the records, ensuring that they are understandable to the accessing community, and managing them so as to preserve their information content and authenticity.

An archive as a collection of data objects that represent an official working copy of the data, but is managed separately from more active production data, for such purposes as long-term preservation and better cost economics. Further, archives are often used for storing data sets that need to meet specific compliance obligations, and they are normally used for auditing or analysis rather than for application recovery. In addition, the retention requirements can vary (e.g. short-, medium- and long-term), but the archive should ensure proper integrity, immutability, authenticity, confidentiality and provenance.

ISO/TR 18492 defines "long-term preservation" as the "period of time that electronic document-based information is maintained as accessible and authentic evidence" and further notes:

> "This period of time can range between a few years to hundreds of years, depending on the needs and requirements of the organization. For some organizations, this period of time would be determined by regulatory compliance, legal requirements and business needs. For other organizations, such as archival repositories holding public records, the period of time required to retain electronic document-based information is usually thought to be hundreds of years."

ISO/TR 18492 also identifies six key issues that storage repositories should consider when they are developing a long-term preservation strategy.

— *Readable electronic document-based information* – the bit stream comprising electronic document-based information should be accessible on the computer system or device that initially created it, currently stores it, currently accesses it, or can be used to store it in the future; media obsolescence and data formatting are also considerations.

— *Intelligible electronic document-based information* – intelligibility of electronic document-based information is a function of information about what the bit stream in fact represents and the processing software's capacity to take appropriate action based on this information.

— *Identifiable electronic document-based information* – document-based information should be organized, classified and described in such a way that it is possible for users and information systems to distinguish between information objects based on a unique attribute such as name or ID number; facilitating search and retrieval is a consideration.

— *Retrievable document-based information* – discrete information objects (or parts of them) can be retrieved and displayed. Retrievability is typically software-dependent in that it requires keys or pointers that link the logical structure of information objects (e.g. data fields or text strings) to their physical storage location.

— *Understandable document-based information* – conveying information to both computers and humans beyond the document contents, including context of creation and use (i.e. metadata) as well as relationships among other documents.

13

— *Authentic electronic document-based information* – ensure the information is what it purports to be (i.e. information that over time has not been altered, changed or otherwise corrupted); focusses on a) transfer and custody, b) the storage environment, and c) access and protection.

The potential evidentiary nature of archives and the need to address data authenticity, provenance and chain of custody are noteworthy because it is possible that the archive needs to retain, protect and maintain significant amounts of metadata. This means that the following security services identified by ISO 14721 apply to both the information and metadata.

— *Identification/authentication service* confirms the identities of requesters for use of information system resources. In addition, authentication can apply to providers of data. The authentication service should occur at the initiation of a session or during a session.

— *Access control service* prevents the unauthorized use of information system resources. This service also prevents the use of a resource in an unauthorized way. This service should be applied to various aspects of access to a resource (e.g. access to communications to the resource, the reading, writing or deletion of an information/data resource, the execution of a processing resource) or to all accesses to a resource.

— *Data integrity service* ensures that data is not altered or destroyed in an unauthorized manner. This service applies to data in permanent data stores and to data in communications messages.

— *Data confidentiality service* ensures that data is not made available or disclosed to unauthorized individuals or computer processes. This service can be applied to devices that permit human interaction with the information system. In addition, this service can ensure that observation of usage patterns of communications resources is not possible.

— *Non-repudiation service* ensures that entities engaging in an information exchange cannot deny being involved in it. This service can take one or both of two forms. First, the recipient of data is provided with proof of the origin of the data. This protects against any attempt by the sender to falsely deny sending the data or its contents. Second, the sender of data is provided with proof of delivery of data. This protects against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.

These security services should be applied during the storage and transfer of the data and metadata to and from the archive. Equally important, care should be exercised when the security services/controls are being adjusted/replaced to avoid exposing the archived data to attack or disclosure (i.e. risk).

In many of the standards and publications, privacy is often not directly addressed in the context of archives. However, with the increase in privacy (protection of PII) regulations around the world, this is something that should be addressed.

Provenance and authenticity are essential elements of most archives, which means that proper metadata handling is required. Chain of custody measures can be necessary as well to address evidentiary requirements and this can complicate the nature of the archive solutions used (e.g. cloud computing-based storage can be unable to provide the needed details).

Many archives are concerned with "proving" data has not been changed (authenticity), but an alternate strategy is to employ immutability measures (e.g. WORM storage) instead of integrity verification approaches.

8.4   Destruction of ESI

Within common records and information management (RIM) frameworks[3], disposition is the last stage of a record's life cycle. Within these frameworks disposition does not necessarily mean destruction, but rather, transfer to archives. In the latter case, this can simply delay when destruction occurs for most records (few records outside of government should be retained indefinitely). When records (data) are no longer needed, the destruction of the data becomes a critical, and often required, component of an

---

3)   ISO 15489-1 is one of many frameworks for planning and implementing a records management program.

effective data governance program. Data destruction is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable[4)] (for digital records).

A record is not ready for final disposition until confirmation can be given that the information it contains is no longer required for operational, legal, governmental, or professional association compliance reasons. In addition, it is the organization's responsibility to demonstrate compliance with all electronic records disposal regulations governing operations and the organization's records retention policies.

In today's world, removing all traces of data from digital and electronic records may not be enough. Increasing concerns about privacy and security means electronic data disposal should be carefully and systematically handled to minimize the risk of illegal or unauthorized access to information. Proper sanitization of media as well as maintaining proof of sanitization records (see ISO/IEC 27040) can be required to meet compliance obligations.

Within the context of data protection, data disposition, specifically data destruction, can be a major source of risk for an organization. Destroying data that should be retained as well as failing to properly destroy data using sanitization techniques or failing to destroy data that should be eliminated can result in significant risk exposures.

ISO/IEC 27040 provides extensive guidance on storage-oriented sanitization (both logical and media-aligned). However, this guidance can be insufficient for ESI that is retained within applications or cloud computing resources where there is no easy way to get at the underlying storage for sanitization operations.

Organizations should:

— have documented retention policies for ESI that are implemented consistently;

— use logical or media sanitization to eliminate ESI that is no longer required (see ISO/IEC 27040);

— avoid using third-party resources (e.g. copiers, printers, cloud computing-based storage, etc.) for which they have no verifiable way of sanitizing the storage;

— record details as recommended by ISO/IEC 27040 associated with ESI destruction (e.g. media sanitization).

8.5 Business continuity management

Risks to continuing normal business operations during an electronic discovery project should be addressed by the organization's business continuity management (BCM) system (see ISO/IEC 22301) and relevant BCM strategy (see ISO/IEC 22331). The electronic discovery process itself can be subject to risks which fall outside the scope of the BCM plan. Therefore, the BCM plan should be adjusted appropriately before an electronic discovery activity is undertaken.

Engagement in an electronic discovery process can have a detrimental effect on normal business processes (e.g. through certain data sources being unavailable during initial processing for electronic discovery). The organization's BCM plan should include mitigation for the potential adverse effects of electronic discovery.

The organization should have an BCM plan in place to mitigate an event causing interrupted access to the electronic discovery system or unwarranted destruction of the ESI. This plan should account for failure of the system at any point and should trigger a mitigation process. Elements of the electronic discovery system which are hosted or managed by third parties should be included in the BCM plan and the third parties' BCM plan should be sufficient to satisfy the requirements of the BCM system.

In addition, organizations should:

— ensure ESI associated with electronic discovery activities are protected with adequate data protection mechanisms (e.g. backups, replications, etc.)

---

4) In the digital world, making data irretrievable is caveated to a specified level of effort to retrieve it.

— have up-to-date malware protections to guard against ESI corruption or destruction as well as loss of availability due to ransomware

— adjust the BCM processes and technology to reflect the sensitivity of the ESI (e.g. PII).

9 Electronic discovery cross-cutting aspects

9.1 General

ISO/IEC 27050-3:2020, 6.1.2, identifies cross-cutting aspects (i.e. behaviours or activities that span multiple electronic discovery process elements and need to be coordinated across the process elements), which are then factored into the requirements and guidance provided in ISO/IEC 27050-3. Some of these cross-cutting aspects can benefit from readiness activities. This clause provides additional information and guidance on the planning, documentation, expertise and use of technology cross-cutting aspects.

Prior to commencing any electronic discovery project, a comprehensive set of technical and non-technical requirements and constraints should be produced. These should include budget considerations and an ESI map.

Appropriate consideration should be given to local compliance obligations and procedural requirements and constraints or the underlying requirements for the discovery of the matter.

The ESI used to reach the produced conclusions should be available in form(s) which allow it to be used for any proceedings (court, tribunals, internal disciplinary or any matter as required). In order to allow provenance to be established where the ESI is required for evidential purposes, it should be possible to present the ESI in its native form or a form as close as possible to its original native form.

9.2 Planning

9.2.1 Configuration and preparation

There are various models of electronic discovery systems which can be vendor specific. All are configurable according to requirements. It is the requirements that should drive the selection process. Hosted services and cloud computing-based services (e.g. leveraging the software as a service model) use a software distribution model in which an application is made accessible, typically over the Internet by a third-party provider. Such a service also includes but is not limited to, full software support and covers the maintenance of IT infrastructure, software licensing and software updates.

There are certain classifications of technology starting from commercial off-the-shelf software which requires little or no configuration prior to roll-out and use by the organization.

Electronic discovery systems to be administered internally by the organization require detailed work to design and roll out. Business requirements should be documented and the system should be designed to meet those requirements. It is possible that some requirements relate to the functionality of the system, and others do not, such as requirements related to a BCM plan. This is dependent on the model purchased from the vendor and if the ESI is hosted by the vendor or not.

Aspects of the system that are usually configurable include workflow, case templates, tag options, dashboards, roles and permissions, and fields to make metadata available.

9.2.2 Budgeting and cost control

At the start of the process, the team should identify potential costs involved. At all stages, the cost of the process should be reviewed and reassessed to ensure proportionality of all actions taken. Regular internal team engagement should be organized as proportionate and appropriate in the current circumstances.

9.2.3 Monitoring and reassessment

Following initial steps, preservation and stakeholder engagement, strategies should be revisited as necessary. Legal issues can evolve, and the scope, form and time of productions can change. The timetable followed by the plan should itself plan for change and schedule in regular stakeholder engagement and reassessment.

9.2.4 End of project considerations

In order to securely manage the ESI, the organization and team should have an agreed exit strategy. This refers to both the technical considerations and financial cost of retrieving the ESI. At the contract negotiation stage, at the beginning of the project, steps should be taken to ensure that the exit strategy is included in the terms and conditions. In order to do this, clear requirements for how the various classifications of ESI that are subject to different retention periods, should be managed. Retention periods are adhered to so that a) ESI that should be retained is not disposed of prematurely and b) ESI that can be disposed of is not stored unnecessarily.

For a purely hosted solution, it can be preferable to migrate the ESI to a cheaper storage facility, and continue to have it managed by the supplier, or the organization's retention policy and method can be triggered. The latter can be to have the ESI extracted to a longer term and affordable media that can be stored more easily, for example, backup tape.

In order to retrieve the ESI, there should be a plan which caters for the technical extraction, copying to alternative media, physical transportation, disposal/destruction methods and details of relevant responsibilities held by parties.

9.3 Documentation

Supporting documentation to manage the process flow of all ESI should be drafted, agreed to and accepted by all relevant parties. The business process documentation should assist the organization to manage the end-to-end solution.

For example, commercial off-the-shelf technology is relatively simple to set up and install and is typically cheaper. However, it is also less configurable and has more demands on the in-house team to manage the system including all associated aspects such as hardware, software, security and backups.

Documentation setting out the requirements for the format of ESI upon collection is beneficial for the processing the ESI into the system. It can help the organization plan for the time and technical resources needed for this stage of the electronic discovery process. For example, some systems are not able to ingest the particular proprietary formats so the system can require native format instead of a structured load.

The archiving process that is used should be clearly documented, as well as the retrieval process, if necessary. The retention plan should also include the form and process for the destruction of material.

9.4 Expertise

9.4.1 Support and maintenance

A support model and service level agreements should be agreed on prior to the roll out of the system. This can include a training package which is an essential element of an electronic discovery process.

9.4.2 Assembling the team

Prior to a triggering incident relevant expertise should be organized into an electronic discovery team with all roles and responsibilities clearly set out as required for an electronic discovery project. Following the triggering incident, the team should be assembled to kick off the coordination process for the management of the project throughout its life. The team can review the details of the trigger event to assess and develop task lists and strategies. Further, the team can assess any need for the

outsourcing of roles and responsibilities, such as if the project is particularly onerous, includes legal complexities or involves additional resource requirements outside the current team structure.

Any organization responsible for the management of large volumes of ESI particularly in relation to litigation, regulation or any form of dispute or adversarial circumstances involving two or more parties should have the requisite roles in place. Each role should have the appropriate level of experience and training required to fulfil this role accordingly. The roles and responsibilities should be on-going and all actions recorded and repeatable. Teamwork is the key to the effectiveness of the electronic discovery process and resulting costs. The team should all have input with expertise to ensure best outcome adhering to all legal requirements, deadlines and issues. The team as a whole is responsible to have a process in place to avoid the need to define the process for each trigger event rather the team should understand their roles and responsibilities within the document process. This process should include on-going responsibilities to ensure smooth running of any electronic discovery requirements. For example the ICT personnel should have an ESI map that should be regularly reviewed to ensure relative ease of access when needed.

The following list is indicative but not exhaustive, of the roles the team should include to ensure the appropriate expertise is engaged.

— Information security officer – responsible for overseeing the security measures satisfying the requirements identified in accordance with 8.2.

— Senior manager – responsible for decision making and rule setting for the policies surrounding ESI management, retention and destruction. This should include final sign off for policies relating to ICT readiness within the organization including but not limited to BCM plans, retention policies and process for collection of ESI. The senior manager has ultimate responsibility for the ICT and also the management of cost of the whole process and sign off at relevant stages as required.

— Subject matter experts – the areas of expertise for example, business process or change management can be identified at the outset of the project and throughout as required. They should be available on an ad hoc basis.

— Counsel – Legal counsel can be an integral part of the team to ensure legal issues are identified and reassessed on an on-going basis throughout the life of the project. Depending on the nature of the project, potential legal issues to be addressed are legal privilege, evidence requirements, court processes, court orders, and agreements between the parties. The project can require specific forensic collection techniques and the managing of ESI in a particular manner.

— Electronic discovery lawyers – not in use in all jurisdictions – should be appointed as experts understanding the legal implications of an electronic discovery project, e.g. implications of using technology-assisted review and how this can be managed and explained to, for example a court of law

— Litigation support personnel – consultation and support services to lawyers/counsel on current and pending cases often called paralegals. Litigation support in relation to electronic discovery can include knowledge and experience in using electronic discovery technology and processes. Litigation support personnel manage technology and should have broad depth of knowledge of the system, what can and cannot be achieved using this technology. They should also work with ICT specialists to ensure the regular assessment of the technology available and industry developments to optimize the process from functional and financial angles.

— ICT specialists – they should have the knowledge of all of the organization systems used, e.g. email and document management systems. The knowledge of the systems, how they work, and their limitations is required to properly feed ESI into the review platform.

— Records managers – lead for each electronic discovery project – policy development/management/ adherence/records managers – information governance experts – have an overall view and management of the preservation, retention and destruction policies. All these individuals/teams should be advised by this on how material should be managed.

— Digital forensic experts – should advise on preservation and collection where integrity of ESI should be maintained, e.g. for a legal reason.

9.4.3 Competency and training

The competency and training requirements of teams working on all areas of the system should be clearly agreed and documented. Some of the training requirements can be driven by the vendor to enable the client/end-users to benefit from the functionality of the system. The teams of people can include, for example technical specialists, reviewers, policy managers, information security specialists and business analysts.

The appropriate individual should create plans for the management and review process. This can include, for example drafting a user guide, glossary, a privileged ESI management policy and an evidence continuity policy.

9.4.4 Stakeholder engagement

Beyond the core team, there can inevitably be stakeholders to engage, such as opposing counsel or the judicial decision maker in a litigation matter, or employees in an internal audit. In virtually every electronic discovery matter, it can be necessary to consult technical personnel on the capabilities and limitations of systems and tools. Stakeholder engagement should be built into the business process for electronic discovery.

9.5 Use of technology

9.5.1 Platform selection/system architecture

The system architecture is primarily dependent on the vendor, but the organization should ensure that any system considered satisfactory, meets as closely as possible, the requirements and constraints already identified. The business can have requirements, for example, for security considerations for the traffic of specific ESI.

Documents setting out the detailed design should include solution architecture design and technical specification documentation.

Hosted services and cloud computing-based services offer an alternative where the vendor provides access to service to the client. The end-user does not have to design and administer the ICT infrastructure. There can be no internal technical personnel required for this type of service as the vendor can provide this as part of the support.

9.5.2 Retiral or migration of systems

When the project has completed and there is no longer a need to pay for the hosting of the ESI or to do further work on the ESI, consideration should be given to what the next steps are for the closure of the electronic discovery project. These considerations can be different depending on how the technology and the service has been designed and managed.

As described in 9.2.4, the exit plan should be triggered to retrieve the ESI in accordance with retention and disposal policies. It is good practice to have a plan in place for how a subsequent electronic discovery project can be managed, if the need arises. It is also good practice to analyse and record lessons learnt during the project to include these in the plan for any future electronic discovery project.

If the system, hosted or on-site, has reached end of life and it is desirable or necessary to move the ESI to a new system, all parties should comply with the terms and conditions for the migration process and procedure as stated in any existing and new contracts. These can set out the responsibilities and methods that can be used to ensure a smooth migration. Primarily, the term migration should be defined and agreement reached about exactly what this entails. All responsibilities for each party involved should be clearly set out. Each part of this plan should feed into the project setting up the new replacement system involving a new contract for goods and services, new supplier service level agreements (or new service level agreements with existing supplier) and any revised requirements as developed following the experience of the previous system.

The configuration and functionality of the new system should also be considered including different technical formats for ESI ingestion and storage as required by the new technology as this can impact on the exit strategy in 9.2.4.

Annex A
(informative)

ESI storage questionnaire

A.1 General

This annex should be used as the ESI data map for the organization management of the data to be used for an electronic discovery project.

A.2 Key contacts

Contact details

— Name

— Role

— Telephone

— E-mail address

— Notes

Considerations

— Record the contact details for key individuals not involved with ICT within your organization

    — Data owners

    — Compliance and legal

— Record the contact details for key individuals involved with ICT within your organization

    — Head of ICT

    — Information security

    — System administrators

    — Authentication service administrators

    — Directory service administrators

— Establish who within ICT is responsible for backup policies and BCM

A.3 Assets

Considerations

Identify if the organization stores/maintains central/remote logs of assets assigned to staff

— Log any resources that shared within a unit

Questions that should be logged:

— Department name responsible for maintenance of a central log of assets

— List devices for new starters

— List additional devices used by employees working in a specified team

— List shared assets on which a user can be able to store data

A.4 ICT infrastructure (internal/third parties)

Considerations

— Details of external organizations that host the organization's ICT infrastructure

    — Backup management company

    — Off-site storage

    — Cloud computing-based data

Questions that should be logged:

— Log if ICT is managed by an external party

— Log if systems are managed by an external party

— The details of any third-party companies

    — Company

    — Details of data hosted

    — Key contact

    — Telephone

    — E-mail

    — Notes

A.5 Authentication services and directory services

Considerations

— Identifying assets, a user on the domain has used

— Restricting access to individuals on domain if they are not present/working remotely

— Identifying access to shares on file server

Questions that should be logged:

— Do you use an authentication server to authenticate users on the network?

— Is your authentication server administered locally? If no, from where and by whom is it administrated?

— Do you log/monitor staff logins and activity? Specifically, do you record which workstations a member of staff has used?

— What are your password policies for users?

— Do all users have home directories on the network?

— What is your naming convention for usernames?

A.6 Workstations – laptops/desktops

Considerations

— What does an employee use to conduct their day to day business on?

— How are their workstations identified on the network?

— What security features do the workstations have (encryption/biometric/card)?

— What can an employee store data on their organization computer?

Questions that should be logged:

— Are computers assigned to individual users, or are they shared?

— Do you have an encryption policy for organization computers? (full disk/file system/etc.)?

   — Are you able to issue decryption certificates?

   — If no, who can? (contact details)

— What is your naming convention for computers?

— What is your policy on users saving files on their local workstation?

— Can an employee install applications on their workstation?

— Can an employee run executables on their workstation?

— Are files stored on a user's profile synchronized/backed up on the file server?

— What can an employee connect to their workstation in order to transfer files on/off?

   — Are portable device connections logged centrally?

— What (if anything) is an employee prevented from connecting to their workstation?

— Are mailboxes stored locally on the workstation? (OST/PST/NSF/etc.)

   — Is it different on laptops vs. desktops?

— What happens to an employee's computer if they leave/terminated (policy)?

— In the case of repaired/re-issued computers, what happens to the existing data? (migration/backed-up/deleted)

A.7 Email servers

Considerations

— Where is the mail server located and is it administered locally/globally/by third party?

— Are any compliance software/filtering/journaling features activated?

— Identify backup policy/regime

— Identify what happens to terminated employees' e-mails.

Questions that should be logged:

— How is email managed:

   — in-house?

— cloud computing-based?

— third party?

— What type of email system is currently used?

— What version is installed?

— In the last five years, have you used any other email system?

— Were the emails migrated/archived?

— How many email servers are there globally?

— Are they on separate domains?

— Do you have different domains for email?

— Where are the email servers geographically located?

— Are the retention and archiving policies the same among all domains?

— Are emails stored locally on individual's computers (PSTs, NSFs)?

— Do you retain deleted messages on the email server?

— Is there an auto-delete system?

— If so, can it be turned off for preservation purposes?

— If not, what is the work around?

— Is there a limit imposed on individual mailboxes?

— If so, what is that limit and what happens when it is reached?

— What software is used to back up email servers?

— Are email backups block level or individual mailboxes?

— Do you use an archive? If so, please describe.

— What type of backup system do you use? Tape or digital? Local or remote?

— If tape, what tapes do you use?

— How are your tapes catalogued and inventoried?

— Are tapes sets clearly identified?

— How often are backups performed?

— What is your retention policy?

— What is your rotation schedule?

— What do you do with an e-mail account when employment is terminated?

A.8 File servers

Considerations

— Understand where employees (individuals, teams) are able to store data

— List folder level permissions/logging

— File servers used for local backups

— Applications that make use of file server to store transactional information (databases)

Questions that should be logged:

— What type of files severs are in use?

— How many file servers do you have globally/locally?

— Where are they located geographically?

— Are there any archived/historical file servers?

— What were they used for?

— When were they decommissioned?

— Was the data migrated/archived

— Are they still available?

— What are names of file server?

— What type of files can users store on file servers?

    — Any proprietary?

— E-mail? What are the locations?

— Is a user's profile synchronized with the file servers? (client-side caching)

— Is file/folder access on the file servers logged?

— Do you have group directories or public shares?

— Can employees delete permanently from the file servers?

    — Prevent that or allow for backup and retrieval if needed?

— What type of backup system do you use? Tape or digital?

— What software is used to back up file servers?

— If tapes, what type of tapes do you use? By location?

— How are tapes catalogued and inventoried?

— Are tape sets clearly identified?

— How often are backups performed?

— What is your rotation schedule?

— What is your retention policy?

— Is there replication in place?

— Where are the replication servers/storage located?

— How often does replication occur?

— What do you do with a user's home drive when employment is terminated?

— What do you do with a user's files in public locations when employment is terminated?

A.9   Print servers/scanners

Considerations

— Logs of all printing and scanning activity

— Tie in with active directory that shows when a user printed/scanned

— Any leasing company additional logging activation for billing purposes

Questions that should be logged:

— Are your printers/scanners organization owned or leased?

— Contact details for lease organization

— What logs are recorded for these devices?

— Are print/scan jobs cached? If yes, how long for?

— Does a user have to authenticate prior to use? If yes, how can a user authenticate?

A.10 Backups/off-site media/storage

Considerations

— Identify if there are any potential issues with preservation and whether or not any relevant data is currently scheduled for destruction.

— Remember to record any third-party arrangements in place for backups and ensure they have been contacted by the firm

Questions that should be logged:

— What type of backup system is used?

    — Tape?

    — Digital?

— What software do you use?

— Where are backups stored?

— How often are backups performed?

— What is your rotation schedule?

— What is your retention policy?

— How are backups catalogued and inventoried?

— Is there a replication in place?

— What is the name of the off-site storage vendor?

— What is the address and telephone of the facility?

— Who is the contact?

— What type of data do they store?

— Does the vendor have relevant data that is not accessible from your current systems?

— Is there a current inventory of the material in storage?

A.11 Applications (local/web-based/cloud computing) – laptops/desktops

Considerations

— Identify which applications does an employee within the specific team have access to and where the transactional, temporary, cached files stored

Questions that should be logged:

— What systems do the individuals/team have access to?

— Do you keep a central register of which applications have been installed on which corporate device?

— Do the applications log user activity?

— Where do the applications store data (file servers/local)?

— Is the system locked down or can employees install/use applications without your knowledge?

— If systems are not maintained by you behind your firewall, where is this information stored?

— Is access to public blog sites allowed (Facebook, Twitter, etc.)

— What type of web-based systems do you use that can have relevant data?

  — SharePoint?

  — Intranet?

  — Extranets?

  — Social media?

  — Collaboration sites?

  — Software as a service?

  — Management systems or databases?

— Do you use any cloud computing-based applications?

— Who is the administrator for cloud computing-based applications?

— Are you able to block user access on cloud computing-based applications?

— Is the cloud computing-based applications backed up?

A.12 Cell phones/tablets/portable devices

Considerations

— Identify which communication devices the company use and give to employees

— Identify organization policy and infrastructure on personal devices and what is synchronized with their servers

— Identify what logs, records the organization maintains

Questions that should be logged:

— What cell phone models (if any) are issued by the organization

— Are the devices issued by or owned by the organization?

— Are employees able to join their personal devices to the network/enterprise services, e.g. bring your own device?

— Are emails sent by a user on their device synched with the organization's e-mail server?

— Are text messages captured by your server?

— Is voicemail stored on your server?

— What type of data is stored on the device that is not on the server?

— Is the security policy on smart phones the same as internet settings on the computers?

— If not, can users access any kind of site from the smartphone?

A.13 Remote access/VPN

Questions that should be logged:

— Are users able to work remotely?

— How do they join/access the organization's services? (VPN, TeamViewer, etc)?

— Where does a user store their files when connected remotely?

— Are users able to use their own devices to connect to the organization?

— Are remote sessions logged?

A.14 Communication applications

Questions that should be logged:

— Do you use or have unified messaging applications within the organization (e-mail, SMS, fax, voicemail, video calling)?

— Do you use instant messaging applications?

— Are conversations/chats logged centrally?

— Do you make use of a PBX (Private Branch Exchange) telephone system?

— What is the retention period for call logs, voicemails?

— Do you log internal-to-internal calls?

— Is voice mail stored on your systems? What is the retention?

A.15 Other questions

Questions that should be logged:

— Do you have security-controlled building entry/exit systems?

— Do you have CCTV?

— What is your retention/turnover period?

— When was the last security or vulnerability assessment conducted (i.e. penetration testing)?

Bibliography

[1] ISO 14721, *Space data and information transfer systems — Open archival information system (OAIS) — Reference model*

[2] ISO/TR 18492, *Long-term preservation of electronic document-based information*

[3] ISO/IEC 22301, *Security and resilience — Business continuity management systems — Requirements*

[4] ISO/IEC 27002, *Security and resilience — Business continuity management systems — Guidelines for business continuity strategy*

[5] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[6] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

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

[8] ISO/IEC 27040, *Information technology — Security techniques — Storage security*

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

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

[11] ISO/IEC 27050-2, *Information technology — Electronic discovery — Part 2: Guidance for governance and management of electronic discovery*

[12] ISO/IEC 27050-3, *Information technology — Electronic discovery — Part 3: Code of practice for electronic discovery*

[13] ISO 15489:2016, *Information and documentation — Records management*

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

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

[16] STORAGE NETWORKING INDUSTRY ASSOCIATION (SNIA) TECHNICAL WHITE PAPER *Data Protection Best Practices*, Version 1.0, 23 October 2017, https://www.snia.org/education/whitepapers

[17] STORAGE NETWORKING INDUSTRY ASSOCIATION (SNIA) ONLINE DICTIONARY https://www.snia.org/education/online-dictionary