FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
27050-4**

ISO/IEC JTC **1**/SC **27**

Secretariat: DIN

Voting begins on:
2021-01-27

Voting terminates on:
2021-03-24

Information technology — Electronic discovery —

Part 4:
Technical readiness

Reference number
ISO/IEC FDIS 27050-4:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.

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).

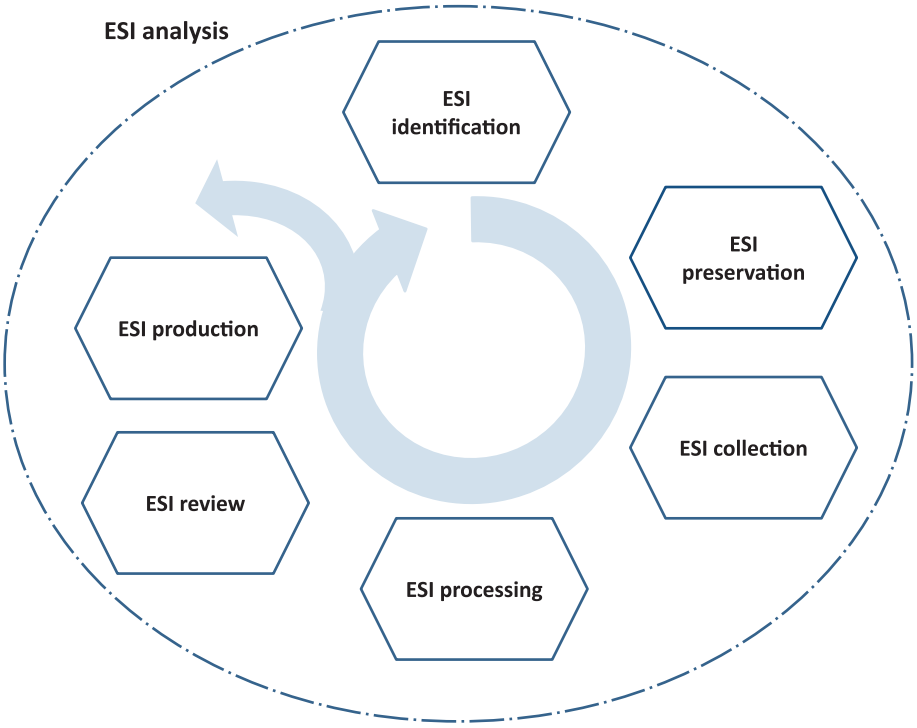

Figure 1 — Electronic discovery process elements

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

