

---

---

**Information technology — Electronic  
discovery —**

**Part 1:  
Overview and concepts**

*Technologies de l'information — Découverte électronique —*

*Partie 1: Aperçu général et concepts*

*ITeH Standards*  
**(<https://standards.iteh.ai>)**  
**Document Preview**

[ISO/IEC 27050-1:2019](https://standards.iteh.ai/catalog/standards/iso/5048dbd0-41b6-4f78-819b-b990942154d0/iso-iec-27050-1-2019)

<https://standards.iteh.ai/catalog/standards/iso/5048dbd0-41b6-4f78-819b-b990942154d0/iso-iec-27050-1-2019>



iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

[ISO/IEC 27050-1:2019](https://standards.iteh.ai/catalog/standards/iso/5048dbd0-41b6-4f78-819b-b990942154d0/iso-iec-27050-1-2019)

<https://standards.iteh.ai/catalog/standards/iso/5048dbd0-41b6-4f78-819b-b990942154d0/iso-iec-27050-1-2019>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Fax: +41 22 749 09 47  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

|                                                                           | Page      |
|---------------------------------------------------------------------------|-----------|
| <b>Foreword</b> .....                                                     | <b>v</b>  |
| <b>Introduction</b> .....                                                 | <b>vi</b> |
| <b>1 Scope</b> .....                                                      | <b>1</b>  |
| <b>2 Normative references</b> .....                                       | <b>1</b>  |
| <b>3 Terms and definitions</b> .....                                      | <b>1</b>  |
| <b>4 Symbols and abbreviated terms</b> .....                              | <b>4</b>  |
| <b>5 Overall structure and overview of the ISO/IEC 27050 series</b> ..... | <b>4</b>  |
| <b>6 Overview of electronic discovery</b> .....                           | <b>5</b>  |
| 6.1 Background.....                                                       | 5         |
| 6.2 Basic concepts.....                                                   | 5         |
| 6.3 Objectives of electronic discovery.....                               | 6         |
| 6.4 Electronic discovery foundation.....                                  | 7         |
| 6.4.1 General.....                                                        | 7         |
| 6.4.2 Competency.....                                                     | 7         |
| 6.4.3 Candour.....                                                        | 7         |
| 6.4.4 Cooperation.....                                                    | 7         |
| 6.4.5 Completeness.....                                                   | 7         |
| 6.4.6 Proportionality.....                                                | 7         |
| 6.5 Governance and electronic discovery.....                              | 8         |
| 6.5.1 General.....                                                        | 8         |
| 6.5.2 Risk and environmental factors.....                                 | 8         |
| 6.5.3 Compliance and review.....                                          | 8         |
| 6.5.4 Privacy and data protection.....                                    | 8         |
| 6.6 ICT readiness for electronic discovery.....                           | 9         |
| 6.6.1 General.....                                                        | 9         |
| 6.6.2 Long-term retention of ESI.....                                     | 9         |
| 6.6.3 Maintaining ESI confidentiality.....                                | 9         |
| 6.6.4 Destruction of ESI.....                                             | 9         |
| 6.7 Planning and budgeting an electronic discovery project.....           | 9         |
| <b>7 Electronically Stored Information (ESI)</b> .....                    | <b>10</b> |
| 7.1 Background.....                                                       | 10        |
| 7.2 Common types of ESI.....                                              | 11        |
| 7.2.1 General.....                                                        | 11        |
| 7.2.2 Active data.....                                                    | 11        |
| 7.2.3 Inactive data.....                                                  | 11        |
| 7.2.4 Residual data.....                                                  | 11        |
| 7.2.5 Legacy data.....                                                    | 12        |
| 7.3 Common sources of ESI.....                                            | 12        |
| 7.3.1 General.....                                                        | 12        |
| 7.3.2 Custodian data sources.....                                         | 12        |
| 7.3.3 Non-custodian data sources.....                                     | 12        |
| 7.3.4 Potentially excluded sources of ESI.....                            | 13        |
| 7.4 ESI representations.....                                              | 13        |
| 7.4.1 General.....                                                        | 13        |
| 7.4.2 Native formats.....                                                 | 13        |
| 7.4.3 Near-native formats.....                                            | 14        |
| 7.4.4 Image (near-paper) formats.....                                     | 14        |
| 7.4.5 Hardcopy.....                                                       | 14        |
| 7.5 Non-ESI as part of discovery.....                                     | 14        |
| <b>8 Electronic discovery process</b> .....                               | <b>15</b> |
| 8.1 Overview.....                                                         | 15        |

## ISO/IEC 27050-1:2019(E)

|          |                                       |           |
|----------|---------------------------------------|-----------|
| 8.2      | ESI identification.....               | 17        |
| 8.3      | ESI preservation.....                 | 17        |
| 8.4      | ESI collection.....                   | 17        |
| 8.5      | ESI processing.....                   | 18        |
| 8.6      | ESI review.....                       | 18        |
| 8.7      | ESI analysis.....                     | 18        |
| 8.8      | ESI production.....                   | 18        |
| <b>9</b> | <b>Additional considerations.....</b> | <b>19</b> |
| 9.1      | Presentation of ESI.....              | 19        |
| 9.2      | Chain of custody and provenance.....  | 19        |
|          | <b>Bibliography.....</b>              | <b>20</b> |

# iTeh Standards (<https://standards.iteh.ai>) Document Preview

[ISO/IEC 27050-1:2019](https://standards.iteh.ai/catalog/standards/iso/5048dbd0-41b6-4f78-819b-b990942154d0/iso-iec-27050-1-2019)

<https://standards.iteh.ai/catalog/standards/iso/5048dbd0-41b6-4f78-819b-b990942154d0/iso-iec-27050-1-2019>

## 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](http://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](http://www.iso.org/patents)) or the IEC list of patent declarations received (see <http://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](http://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*.

This second edition cancels and replaces the first edition (ISO/IEC 27050-1:2016), which has been technically revised.

The main changes compared to the previous edition are as follows:

- the titles of different parts of the ISO/IEC series have been updated;
- [Clause 3](#) has been aligned to the Directives, Part 2.

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](http://www.iso.org/members.html).

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

## Introduction

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

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

**iTeh Standards**  
**(<https://standards.itih.ai>)**  
**Document Preview**

[ISO/IEC 27050-1:2019](https://standards.itih.ai/catalog/standards/iso/5048dbd0-41b6-4f78-819b-b990942154d0/iso-iec-27050-1-2019)

<https://standards.itih.ai/catalog/standards/iso/5048dbd0-41b6-4f78-819b-b990942154d0/iso-iec-27050-1-2019>

# Information technology — Electronic discovery —

## Part 1: Overview and concepts

### 1 Scope

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

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

### 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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

### 3 Terms and definitions

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

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

#### 3.1

##### **chain of custody**

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

#### 3.2

##### **custodian**

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

#### 3.3

##### **data breach**

compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed

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

### 3.4 discovery

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

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

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

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

### 3.5 disposition

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

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

### 3.6 electronic archive

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

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

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

### 3.7 electronic discovery

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

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

### 3.8 Electronically Stored Information ESI

data or information of any kind and from any source, whose temporal existence is evidenced by being stored in or on any electronic medium

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

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

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

### 3.9 ESI analysis

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

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

### 3.10 ESI collection

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



**3.11****ESI identification**

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

**3.12****ESI preservation**

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

Note 1 to entry: In some matters or jurisdictions, there can be requirements to prevent *spoliation* (3.21) of *Electronically Stored Information* (3.9).

**3.13****ESI processing**

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

**3.14****ESI production**

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

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

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

**3.15****ESI review**

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

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

**3.16****investigation**

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

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

**3.17****legal hold**

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

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

**3.18****metadata**

data that defines and describes other data

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

**3.19****provenance**

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

**3.20  
sanitize**

render access to target data on storage media infeasible for a given level of effort

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

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

**3.21  
storage**

device, function, or service supporting data entry and retrieval

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

**3.22  
spoliation**

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

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

**3.23  
store**

record data on volatile storage or non-volatile storage

Note 1 to entry: Non-volatile storage refers to storage that retains its contents even after power is removed, while volatile storage refers to storage that fails to retain its contents after power is removed.

[SOURCE: ISO/IEC 27040:2015, 3.50, modified — Note 1 to entry has been added.]

## 4 Symbols and abbreviated terms

| <a href="https://standards.iso.org/standards/catalog/standards/iso/5048dbd0-41b6-4f78-819b-b990942154d0/iso-iec-27050-1-2019">ISO/IEC 27050-1:2019</a> |                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| CD                                                                                                                                                     | compact disc                              |
| DVD                                                                                                                                                    | digital versatile disc                    |
| EDMS                                                                                                                                                   | electronic document management system     |
| ERMS                                                                                                                                                   | electronic records management system      |
| ICT                                                                                                                                                    | information and communications technology |
| NAS                                                                                                                                                    | network attached storage                  |
| OCR                                                                                                                                                    | optical character recognition             |
| PII                                                                                                                                                    | personally identifiable information       |
| RAM                                                                                                                                                    | random access memory                      |

## 5 Overall structure and overview of the ISO/IEC 27050 series

The ISO/IEC 27050 series is organized to address various stakeholders' needs with regards to electronic discovery. The initial structure of the ISO/IEC 27050 series is as follows:

- This document addresses general ESI and electronic discovery terminology and concepts as well as describing the electronic discovery process elements. It is intended to serve a broad audience and