INTERNATIONAL STANDARD

ISO/IEC 27050-1

First edition
2016-11-01

Information technology — Security techniques — Electronic discovery —

Part 1: Overview and concepts

Technologies de l'information — Techniques de sécurité — Découverte électronique —
Partie 1: Aperçu général et concepts

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

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

Contents

Page

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

7.4.4 Image (near-paper) formats 15
7.4.5 Hardcopy 15
7.5 Non-ESI as part of discovery 15
8 Electronic discovery process 16
8.1 Overview 16
8.2 ESI identification 18
8.3 ESI preservation 18
8.4 ESI collection 18
8.5 ESI processing 19
8.6 ESI review 19
8.7 ESI analysis 19
8.8 ESI production 19
9 Additional considerations 20
9.1 Presentation of ESI 20
9.2 Chain of custody and provenance 20
Bibliography 21

Foreword

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

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

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

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

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

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

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

Introduction

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

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

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

Information technology — Security techniques — Electronic discovery —

Part 1: Overview and concepts

1 Scope

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

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

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.19
metadata
data that defines and describes other data

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4 Symbols and abbreviated terms

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

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

5 Overall ISO/IEC 27050 structure and overview

5.1 Purpose and structure

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

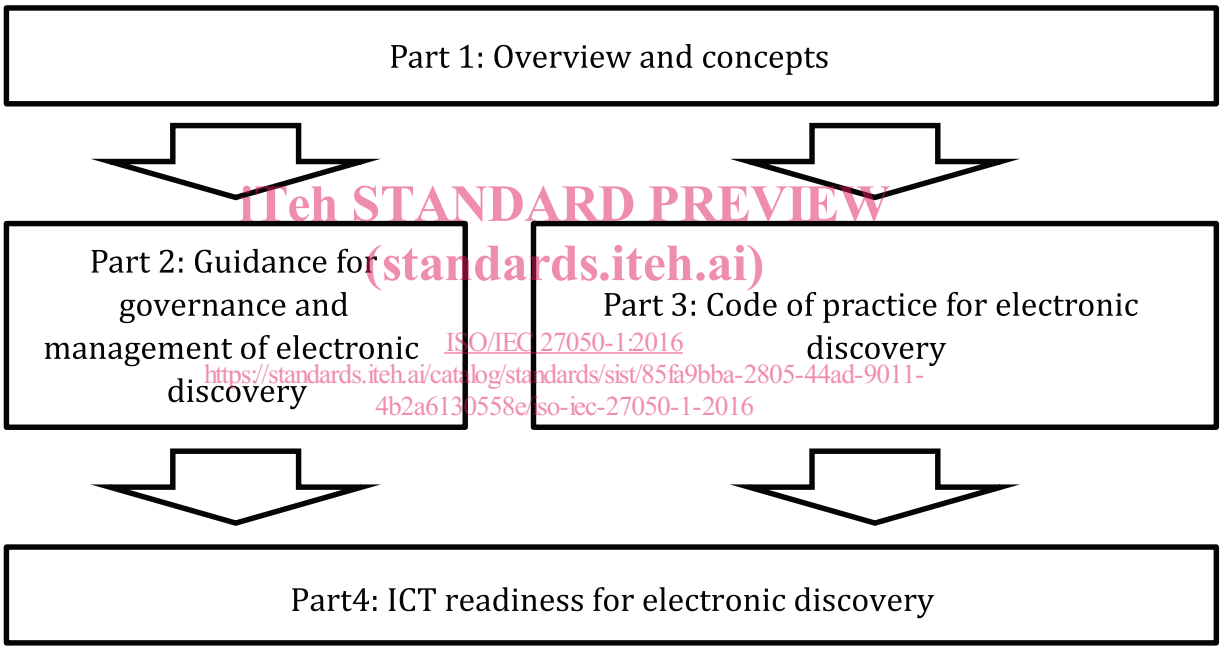

Figure 1 — ISO/IEC 27050 architecture

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

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

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

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