INTERNATIONAL STANDARD

ISO/IEC 27050-1

Second edition
2019-11

Information technology — Electronic discovery —

Part 1: Overview and concepts

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

This document is a preview generated by EVS

Reference number
ISO/IEC 27050-1:2019(E)

© ISO/IEC 2019

This document is a preview generated by EVS

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
Website: www.iso.org

Published in Switzerland

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 structure and overview of the ISO/IEC 27050 series **4**
6 Overview of electronic discovery **5**
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
7 Electronically Stored Information (ESI) **10**
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
8 Electronic discovery process **15**
8.1 Overview 15

This document is a preview generated by EVS

© ISO/IEC 2019 – All rights reserved

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
9 Additional considerations 19
9.1 Presentation of ESI 19
9.2 Chain of custody and provenance 19
Bibliography 20

This document is a preview generated by EVS

 © ISO/IEC 2019 – All rights reserved

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 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.

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.

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

This document is a preview generated by EVS

© ISO/IEC 2019 – All rights reserved

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).

This document is a preview generated by EVS

 © ISO/IEC 2019 – All rights reserved

Information technology — Electronic discovery —

Part 1:
Overview and concepts

This document is a preview generated by EVS

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]

© ISO/IEC 2019 – All rights reserved