INTERNATIONAL STANDARD

ISO/IEC 27050-2

First edition
2018-09

Information technology — Electronic discovery —

Part 2: Guidance for governance and management of electronic discovery

Technologies de l'information — Découverte électronique —

Partie 2: Lignes directrices pour la gouvernance et le management de l'investigation informatique

This document is a preview generated by EVS

Reference number
ISO/IEC 27050-2:2018(E)

© ISO/IEC 2018

This document is a preview generated by EVS

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols and abbreviated terms **1**
5 Electronic discovery background **2**
6 Governance of electronic discovery **4**
6.1 Context and principles 4
6.2 Mandate and establishment 4
6.3 Evaluate 4
6.4 Direct 4
6.5 Monitor 5
7 Management of electronic discovery **5**
7.1 Context and controls 5
7.2 Archival policies 5
7.3 Discovery policies 5
7.4 Disclosure policies 5
7.5 Capability policies 5
7.6 Risk compliance policies 6
7.7 Monitoring and reporting policies 6
8 Risks and environmental factors **6**
8.1 Overview 6
8.2 Privacy 6
8.3 Detection of other serious issues 7
8.4 Adverse effects on organizational activities 7
8.5 Damage to staff morale 7
8.6 Damage to organizational reputation 7
9 Compliance and review **7**
9.1 Overview 7
9.2 Structural requirements for process delivery 7
9.3 Process control and monitoring 8
9.4 Communication mechanisms and disclosure 8
9.5 Consistency to policy and duty to perform 8
9.6 Effectiveness review 8
9.7 Vendor management 8
Bibliography **9**

This document is a preview generated by EVS

© ISO/IEC 2018 – 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. 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 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 Technical Committee 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.

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.

This document is a preview generated by EVS

 © ISO/IEC 2018 – All rights reserved

Introduction

Engagement in electronic discovery and processes can expose organizations and the stakeholders within and outside those organizations to collective and individual risks, including legal, financial and ethical. This document aims to provide 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.

This document is to be read in relation to ISO/IEC 27050-1 and ISO/IEC 27050-3. Common responsibilities of a governing body is to provide strategic direction in all matters of relevance to electronic discovery and to take ownership of the risks related to electronic discovery. The responsibility of management is to develop and implement the policies, plans and strategies for electronic discovery set by the governing body. The inherent causes of failure and environmental issues associated with electronic discovery governance and management impact the viability of a coherent system that delivers optimal business value. Consequently, the structures, processes and communication requirements of electronic discovery needs to be compliant and open to review.

The measure of success for the investment in the use of electronic discovery services is the benefit that it brings to the organization making the investment. Proper foresight, oversight and direction allow the full scope of the effort required to derive the expected benefits and an appropriate framework for governance, risk and value to be determined. This document addresses the concerns of electronic discovery governance by identifying the risk and the risk owners of potential points of failure in electronic discovery processes.

This document is to provide guidance for the governance and management of electronic discovery.

This document is a preview generated by EVS

© ISO/IEC 2018 – All rights reserved

This document is a preview generated by EVS

Information technology — Electronic discovery —

Part 2: Guidance for governance and management of electronic discovery

This document is a preview generated by EVS

1 Scope

This document provides guidance for technical and non-technical personnel at senior management levels within an organization, including those with responsibility for compliance with statuary and regulatory requirements, and industry standards.

It describes how such personnel can identify and take ownership of risks related to electronic discovery, set policy and achieve compliance with corresponding external and internal requirements. It also suggests how to produce such policies in a form which can inform process control. Furthermore, it provides guidance on how to implement and control electronic discovery in accordance with the policies.

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*

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

ISO/IEC 38500, *Information technology — Governance of IT for the organization*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27050-1, ISO/IEC 38500 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/

4 Symbols and abbreviated terms

ICT	Information and Communication Technology
OCR	Optical Character Recognition
ESI	Electronically Stored Information

© ISO/IEC 2018 – All rights reserved