

BS ISO/IEC 27050-1:2019 — **Tracked Changes**

compares BS ISO/IEC 27050-1:2019
with BS ISO/IEC 27050-1:2016



BSI Standards Publication

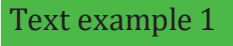
Information technology — Electronic discovery

Part 1: Overview and concepts



IMPORTANT — PLEASE NOTE

This is a tracked changes copy and uses the following colour coding:

-  — indicates added text (in green)
- ~~Text example 2~~ — indicates removed text (in red)
-  — indicates added graphic figure or table
-  — indicates removed graphic figure or table

About Tracked Changes

This document is a PDF containing a Tracked Changes version of BS ISO/IEC 27050-1, which compares BS ISO/IEC 27050-1:2019 with BS ISO/IEC 27050-1:2016.

The original version of BS ISO/IEC 27050-1:2019, appended at the end of this document, should be considered the version of record for this publication.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 14859 6

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

National foreword

This British Standard is the UK implementation of ~~ISO/IEC 27050-1:2016~~ ISO/IEC 27050-1:2019. It supersedes BS ISO/IEC 27050-1:2016, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/~~4, Security Controls, Services~~ Information security, cybersecurity and privacy protection.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution ~~2016~~2020
Published by BSI Standards Limited ~~2016~~2020

ISBN ~~978-0-580-83829-3~~ 978 0 539 05253 4

ICS ~~35.040~~35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on ~~30 November 2016~~29 February 2020.

Amendments/corrigenda issued since publication

Date	Text affected

INTERNATIONAL STANDARD

ISO/IEC
27050-1

~~First~~ **Second** edition
~~2016-11-01~~ **2019-11-14**

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~~ **2019** (E)

© ISO/IEC ~~2016~~ **2019**



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC ~~2016~~ 2019, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
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	5
5 Overall structure and overview of the ISO/IEC 27050 series	5
6 Overview of electronic discovery	7
6.1 Background	7
6.2 Basic concepts	7
6.3 Objectives of electronic discovery	8
6.4 Electronic discovery foundation	9
6.4.1 General	9
6.4.2 Competency	9
6.4.3 Candour	9
6.4.4 Cooperation	9
6.4.5 Completeness	9
6.4.6 Proportionality	9
6.5 Governance and electronic discovery	10
6.5.1 General	10
6.5.2 Risk and environmental factors	10
6.5.3 Compliance and review	10
6.5.4 Privacy and data protection	10
6.6 ICT readiness for electronic discovery	11
6.6.1 General	11
6.6.2 Long-term retention of ESI	11
6.6.3 Maintaining ESI confidentiality	11
6.6.4 Destruction of ESI	11
6.7 Planning and budgeting an electronic discovery project	11
7 Electronically Stored Information (ESI)	12
7.1 Background	12
7.2 Common types of ESI	13
7.2.1 General	13
7.2.2 Active data	13
7.2.3 Inactive data	13
7.2.4 Residual data	14
7.2.5 Legacy data	14
7.3 Common sources of ESI	14
7.3.1 General	14
7.3.2 Custodian data sources	14
7.3.3 Non-custodian data sources	14
7.3.4 Potentially excluded sources of ESI	15
7.4 ESI representations	15
7.4.1 General	15
7.4.2 Native formats	16
7.4.3 Near-native formats	16
7.4.4 Image (near-paper) formats	16
7.4.5 Hardcopy	16

- 7.5 Non - ESI as part of discovery 16
- 8 **Electronic discovery process 17**
 - 8.1 Overview 17
 - 8.2 ESI identification 18
 - 8.3 ESI preservation 19
 - 8.4 ESI collection 19
 - 8.5 ESI processing 19
 - 8.6 ESI review 20
 - 8.7 ESI analysis 20
 - 8.8 ESI production 20
- 9 **Additional considerations 20**
 - 9.1 Presentation of ESI 20
 - 9.2 Chain of custody and provenance 21
- Bibliography 22**

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) 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 ~~on~~ 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 ~~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.~~

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.

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 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.~~

INTERNATIONAL STANDARD

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.~~

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 ~~(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~~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).

~~3.8~~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.

~~3.9~~3.8

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~~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.

~~3.11~~3.10

ESI collection

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

~~3.12~~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)

~~3.13~~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* (~~3.24~~3.21) of *Electronically Stored Information* (3.9).

~~3.14~~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)

~~3.15~~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.

~~3.16~~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* (~~3.9~~)—that is considered privileged can be excluded from production.

~~3.17~~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).

~~3.18~~ **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.”

~~3.19~~ **3.18**

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~~ **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

~~3.23~~ **3.20**

sanitize

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

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, ~~modified~~]

3.21

storage

device, function, or service supporting data entry and retrieval

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

~~3.24~~ **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.).

3.25**storage**

device, function, or service supporting data entry and retrieval

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

3.26 **3.23****store**

record data on volatile storage ~~(3.27)~~ or non-volatile storage ~~(3.20)~~

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.]

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 of the ISO/IEC 27050 series

~~5.1 Purpose and structure~~

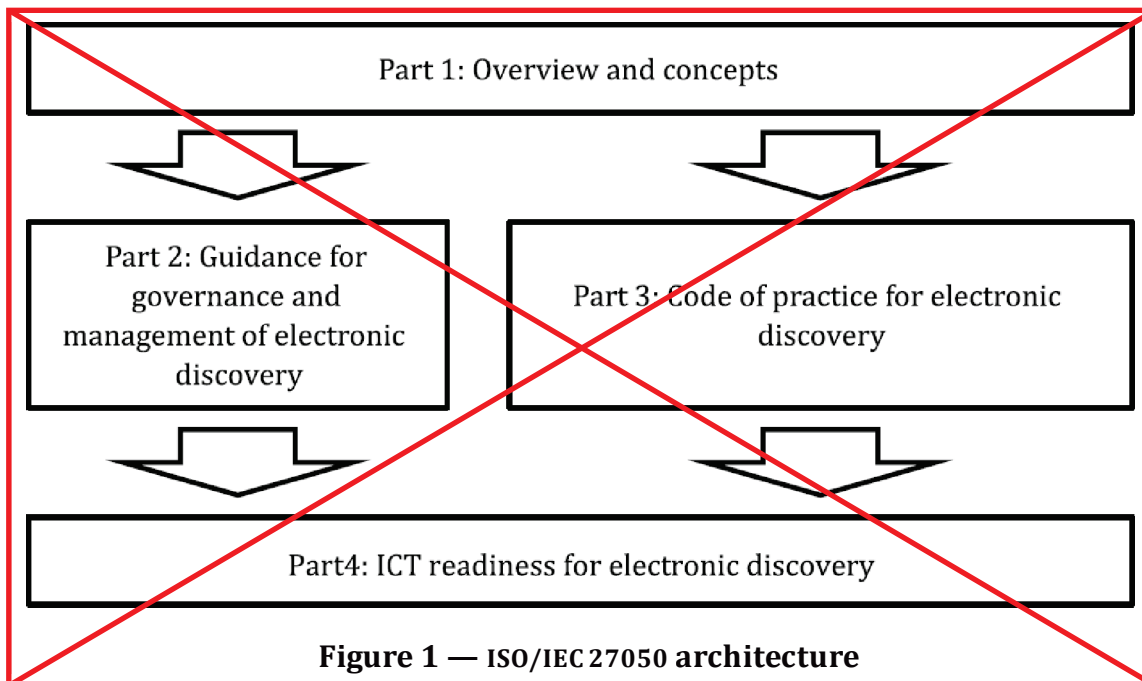
~~ISO/IEC 27050 (all parts) provides requirements and guidance for the process of discovering pertinent Electronically Stored Information (ESI) or data by one or more parties involved in an investigation or litigation, or similar proceeding. Figure 1 provides a notional architecture of ISO/IEC 27050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

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 to be a foundational source of information on electronic discovery. It does not include any guidance or requirements.
- ISO/IEC 27050-2 focuses on the governance and management aspects of electronic discovery that are relevant to the governing body or senior management of an organization. The provided guidance can help an organization align its electronic discovery process with the six principles of good governance described in ISO/IEC 38500.

- ISO/IEC 27050-3 provides requirements and guidance for personnel involved in some or all of the electronic discovery activities. Supplemental materials are included to help practitioners understand the objectives of each electronic discovery process element and the associated considerations, which can help these individuals determine the relevance of each process element and to assist in avoid failures that can increase risks and expenses.

NOTE Additional parts can be added to the ISO/IEC 27050 series as necessary.



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.

5.4 — Overview of ISO/IEC 27050-3: Code of practice for electronic discovery

This document considers each of the distinct elements of the electronic discovery process (ESI identification, ESI preservation, ESI collection, ESI processing, ESI review, ESI analysis, and ESI production) and, for each process element, identifies (i) the objectives, (ii) considerations to avoid failures, and (iii) the specific requirements and guidance for adherence to ISO/IEC 27050 (all parts).

5.5 — Overview of ISO/IEC 27050-4: ICT readiness for electronic discovery

This document provides guidance on the ways an organization can be better prepared to address electronic discovery from the perspective of both technology and processes.

6 Overview of electronic discovery

6.1 Background

Electronic discovery is increasingly important, both within organizations and in the legal systems of some jurisdictions. This trend is expected to continue as more and more electronic records and information (or ESI) are created, modified, manipulated, used, and ultimately destroyed without ever taking on a physical form (e.g. a printed document). The emergence of ESI as the preferred representation of information is introducing new challenges associated with locating the ESI, handling massive quantities of data, preservation and retention of ESI, authenticity, data integrity, data confidentiality, data or media sanitization, etc. While electronic discovery needs and responses vary by matter, failure to appropriately handle the electronic discovery process in view of the context of a particular matter can result in rework, unnecessary costs, possible sanctions, and legal liabilities.

ISO/IEC 27050 (all parts) addresses these challenges by:

- promoting a common approach, understanding, and language for electronic discovery;
- encouraging practical and cost-effective discovery by those tasked with managing ESI through the process;
- identifying competency areas for those involved in electronic discovery;
- promoting consideration of the proactive use of technology, in reducing costs and risks, while increasing efficiencies throughout the discovery process; and
- suggesting ways of avoiding inadvertent disclosures of potentially privileged, confidential, or sensitive ESI.

The overriding goal is to help organizations plan for and meet their electronic discovery objectives and obligations, if any, commensurate with the needs of each particular matter.

6.2 Basic concepts

It is useful to consider in advance the following electronic discovery issues. The significance of these issues and the need to address them vary by matter and need to be calibrated to the needs of the matter:

- scope of electronic discovery;
- governance and management of electronic discovery;
- establishing responsibilities for each aspect of an electronic discovery project;
- identification of systems holding potentially relevant ESI;
- identification of potentially relevant ESI;
- developing appropriate documentation throughout the electronic discovery process;
- anticipated costs and their proposed allocation;
- preservation of ESI, including the legal hold process;
- disclosure of information on the ESI storage methods, hardware, and software;
- collection/acquisition of ESI;

- processing of ESI;
- review and analysis of ESI;
- production of ESI including the form of production.

Those engaging in electronic discovery have many influencing factors specific to the context. Cost can be significant among these. The primary cost drivers include:

- ~~Collection~~collection: finding and retrieving the potentially relevant ESI;
- ~~Volume~~volume: the raw quantity of ESI to be collected, processed, or reviewed;
- ~~Number~~number of sources: the number of custodians, enterprise systems, and external systems and applications under the control of the entity involved in the collection of ESI can increase exponentially the amount of time and effort involved;
- ~~Human~~human competencies: the need for qualified people who can perform the functions needed for effective data retrieval, handling, searching, and final review for relevance, privilege, and review for classification (e.g. relevance, privilege, trade secret, confidentiality or special treatment); these competencies can include information technology, computer technology, statistics, search sciences, and law;
- ~~Case~~case complexity: simple cases can require a limited scope and review process, but more complex cases can involve elaborate document review strategies and processes.

The time it takes to find and retrieve ESI, the volume of ESI, the number of sources subject to an ESI investigation and, ultimately, the acceptance of that ESI as reliable in a legal proceeding or ESI investigation, are intimately tied to the practices and policies an organization has put in place to address the management of ESI throughout its life cycle in the organization. Organizations that build electronic discovery readiness into their comprehensive information governance structures prior to engaging in electronic discovery are likely to more efficiently and cost-effectively meet the requirements of electronic discovery. ISO/IEC 27050-2 ~~and ISO/IEC 27050-4~~ provide specific guidance for doing so.

6.3 Objectives of electronic discovery

Objectives of electronic discovery vary by matter. As adjusted for each matter, the 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;
- process relevant ESI into a format that facilitates its efficient searching or review;
- minimize the potential of failing to designate as responsive ESI that is responsive;
- minimize the potential of designating as responsive ESI that is not responsive;
- minimize the potential of failing to designate for withholding or special treatment responsive ESI that qualifies for withholding or special treatment;
- minimize the potential of designating for withholding or special treatment responsive ESI that does not qualify for withholding or special treatment;

- produce responsive ESI in a form that is useable by the requesting party;
- consider the proportionality of the response in the context of the matter and the costs;
- utilize technology in order to reduce risks and costs throughout the project.

6.4 Electronic discovery foundation

6.4.1 General

Electronic discovery often involves parties with conflicting interests and, in a worst-case scenario, they can be adversarial parties. Electronic discovery can be key to resolving a conflict or matter, but only when it is conducted on a foundation that facilitates a measure of trust.

For electronic discovery, this foundation includes adequately addressing competency, candour, cooperation, completeness, and proportionality issues that can require the reconciliation of the requirements of electronic discovery with the requirements of other processes, values or principles.

6.4.2 Competency

Given the complexities associated with electronic discovery, it is important that the individuals engaging in the electronic discovery process have the relevant technical or legal competencies. They potentially need to be able to demonstrate that they are properly trained and have sufficient technical or legal understanding to handle ESI appropriately and to execute the electronic discovery process on behalf of a party.

6.4.3 Candour

The parties conducting electronic discovery are expected to adhere to the applicable standards of professionalism and ethical conduct. In some jurisdictions, this means the parties have an obligation to correct and supplement the record (e.g. additional disclosures or to amend prior responses). In addition, purposeful sluggishness in executing the electronic discovery process needs to be avoided by all parties involved.

6.4.4 Cooperation

Cooperation on issues relating to the preservation, collection, search, review, and production of ESI can be expected in courts of some jurisdictions and, in such courts, cooperation typically does not compromise representation of a client. In addition, in the context of litigation, cooperation in reasonably limiting ESI discovery requests, on the one hand, and in reasonably responding to ESI discovery requests, on the other hand, can reduce costs and delays. Cooperative exchanges of information at the earliest stages of discovery can be useful as appropriate.

6.4.5 Completeness

The objective of a producing party is to retrieve and produce a set of (non-privileged) ESI that represents, under the specific circumstances of the matter, a complete and accurate production.

6.4.6 Proportionality

With the explosive growth of ESI, there are increased concerns over how to best address the costs and burdens associated with the discovery process. One approach to address this problem is to take steps to help ensure that the benefits of discovery be commensurate with the corresponding burdens.

The burdens of electronic discovery can be varied including, but not limited to, disruption of business operations, financial cost, or intrusions on individual privacy.

6.5 Governance and electronic discovery

6.5.1 General

ISO/IEC 38500 sets out six principles for good governance of ICT that are associated with responsibility, strategy, acquisition, performance, conformance, and human behaviour. Each principle is expressed as a preferred behaviour to guide decision making (i.e. each principle refers to what is expected to happen, but does not prescribe how, when or by whom the principles would be implemented, as these aspects are dependent on the nature of the organization implementing the principles). Governing bodies are encouraged to require that these principles are applied, and as a result, they can be assisted in managing risks and encouraging the exploitation of opportunities arising from the use of ICT.

According to ISO/IEC 38500, good governance of ICT also assists governing bodies in assuring conformance with obligations (regulatory, legislation, common law, contractual) concerning the acceptable use of ICT.

The general topic of governance, as it relates to electronic discovery, is addressed in ISO/IEC 27050-2, but [6.5](#) highlights some of the more important elements to help draw attention to the issues.

6.5.2 Risk and environmental factors

Electronic discovery has the potential of exposing an organization or its governing bodies to causes of failure that can have detrimental effects. Governance can help avoid negative consequences that can take the form of:

- breaches of privacy, health and safety, record keeping legislation and regulations;
- non-compliance with standards relating to security, social responsibility; and
- matters relating to intellectual property rights including licensing agreements.

Avoiding negative consequences associated with these failures requires awareness and mitigations that cover the electronic discovery process as well as things such as inadequate ICT systems and improper or inappropriate use of ICT.

6.5.3 Compliance and review

Many organizations are faced with compliance issues that originate from statutory, regulatory, legal, or other requirements. These requirements can be the reason that an organization undertakes an electronic discovery activity, but more likely, they have an impact on how the electronic discovery process is carried out. For example, there can be restrictions on who can see the ESI, how the ESI is transmitted or stored, and specific retention or destruction issues. It is important to ensure that the electronic discovery process ~~is executed within the confines of~~ **takes into account** the relevant compliance requirements.

6.5.4 Privacy and data protection

Besides regulatory restrictions and compliance issues as mentioned in [6.5.3](#), it is important to be aware of some privacy limitations on the use of custodian data (see also ISO/IEC 29100). In particular, there ~~might~~ **can** be some restrictions on personally identifiable information (PII) at custodian data sources that need to be considered as part of ESI management.

When electronic discovery involves PII in some jurisdictions, there can be severe restrictions on what can be done with it (e.g. it cannot be transported across borders). Even without such restrictions, additional data protection measures are often necessary to protect confidentiality and guard against data breaches. ~~ISO/IEC 27050-4, in conjunction with ISO/IEC 27040, provides additional materials that can help deal with these kinds of issues.~~