International Standard

ISO/IEC 38505-1

Information technology — Governance of data —

Part 1: Application of ISO/IEC 38500 to the governance of data

Technologies de l'information — Gouvernance des données —

Partie 1: Application de l'ISO/IEC 38500 à la gouvernance des données

Second edition
2026-08

Reference number
ISO/IEC 38505-1:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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
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 Good governance of data ... **4**
4.1 General ... 4
4.2 Effective performance ... 4
4.3 Responsible stewardship ... 4
4.4 Ethical behaviour ... 4
4.5 Benefits of good governance of data ... 4
4.6 Responsibilities of the governing body ... 6
4.7 Governing body and oversight mechanisms ... 6
5 Principles, model and aspects for good governance of data ... **6**
6 Data accountability ... **7**
6.1 General ... 7
6.2 Collect ... 8
6.3 Store ... 9
6.4 Report ... 9
6.5 Decide ... 10
6.6 Distribute ... 10
6.7 Dispose ... 10
7 Guidance for the governance of data — Principles ... **11**
8 Guidance for the governance of data — Model ... **12**
8.1 General ... 12
8.2 Model for the governance of data ... 13
8.3 Engage stakeholders ... 13
8.4 Evaluate ... 14
8.5 Direct ... 14
8.6 Monitor ... 15
9 Guidance for the governance of data — Data-specific aspects ... **15**
9.1 General ... 15
9.2 Value ... 16
9.2.1 General ... 16
9.2.2 Quality ... 16
9.2.3 Timeliness ... 16
9.2.4 Context ... 16
9.2.5 Volume ... 16
9.3 Risk ... 17
9.3.1 General ... 17
9.3.2 Management ... 17
9.3.3 Data classification schemes ... 17
9.3.4 Security ... 17
9.4 Constraints ... 18
9.4.1 General ... 18
9.4.2 Regulation and legislation ... 18
9.4.3 Societal ... 18
9.4.4 Organizational policy ... 18
10 Application of the data accountability map ... **18**
Bibliography ... **20**

© ISO/IEC 2026 – 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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC/JTC 1, *Information technology*, Subcommittee SC 40, *IT service management and IT governance*.

This second edition cancels and replaces the first edition (ISO/IEC 38505-1:2017), which has been technically revised.

The main changes are as follows:

— alignment with ISO/IEC 38500:2024, which is itself aligned to ISO 37000.

A list of all parts in the ISO/IEC 38505 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

Introduction

The objective of this document is to provide principles, definitions and a model for governing bodies to use when evaluating, directing and monitoring the handling and use of data in their organizations.

This document is high-level, principles-based and advisory. In addition to providing broad guidance on the role of a governing body, it encourages organizations to use appropriate standards to underpin their governance of data.

All organizations use data; and the major proportion of the data is stored electronically across IT systems. With the advent of cloud computing, the realization of the potential of the "internet of things" and the increasing use of "big data" analytics and artificial intelligence (AI), data have become easier to generate, gather, store and mine for useful information. This flood of data brings with it an urgent requirement and responsibility for governing bodies to ensure that valuable opportunities are leveraged, and sensitive data are protected and secured.

Governance of data plays a critical role in ensuring the responsible, innovative, sustainable, and ethical use of data.

Governance of data is an ongoing practice, adapting to the evolving data landscape.

This document has been prepared to provide guidance to the members of governing bodies to apply a principles-based approach to the governance of data to increase the value of the data while preventing the risks associated with the data. ISO/IEC 38500 provides principles, model, and framework for the governing bodies of organizations to guide their current use and to plan for their future use of Information technology (IT), and this document concerns the application of ISO/IEC 38500. While this document describes the governance of data and its use within an organization, guidance on the implementation arrangement for the effective governance of IT in general is found in ISO/IEC/TS 38501. The constructs in ISO/IEC/TS 38501 can help to identify internal and external factors relating to the governance of IT and help to define beneficial outcomes and identify evidence of success.

The use of AI and the growth of data have created extensive opportunities for the analysis and use of data in decision making. Because legal regulations sometimes lag behind or are not developed, it is up to an organization to ensure the ethical use of data.

As with ISO/IEC 38500, this document is addressed primarily to the governing body of an organization and applies equally regardless of the size of the organization or its industry or sector. The principles of this document can be relevant for the governing bodies of data exchange networks, platforms, spaces and for other inter-organizational data governance contexts. However, the inter-organizational aspects of data governance are outside the scope of this document.

Governance is distinct from management and concerns evaluating, directing and monitoring the use of data, rather than the mechanics of storing, retrieving or managing the data. This document outlines an understanding of various data management and techniques to enunciate the strategies and policies that can be directed by the governing body.

© ISO/IEC 2026 – All rights reserved

Information technology — Governance of data —

Part 1:
Application of ISO/IEC 38500 to the governance of data

1 Scope

This document provides principles for governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient and acceptable use of data within their organizations by:

— applying the governance principles and model of ISO/IEC 38500 to the governance of data;

— assuring stakeholders that, if the principles and practices proposed by this document are followed, they can have confidence in the organization's governance of data;

— informing and guiding governing bodies in the use and protection of data in their organizations.

This document can also provide guidance to a wider community, including:

— executive managers;

— external businesses or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies;

— internal and external service providers (including consultants);

— auditors.

This document applies to the governance of the current and future use of data that is created, collected, stored, secured, protected, or controlled by IT systems, and impacts the management processes and decisions relating to data.

This document defines the governance of data as a subset or domain of the governance of IT, which itself is a subset or domain of organizational, or in the case of a corporation, corporate governance.

This document is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. This document is applicable to organizations of all sizes, regardless of the extent of their dependence on data.

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 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 38500 and the following apply.

© ISO/IEC 2026 – All rights reserved

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

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

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

3.1
anonymization
process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

[SOURCE: ISO/IEC 29100:2024, 3.2]

3.2
big data
extensive datasets — primarily in the data characteristics of volume, variety, velocity, and/or variability — that require a scalable technology for efficient storage, manipulation, management, and analysis

Note 1 to entry: Big data is commonly used in many different ways, for example as the name of the scalable technology used to handle big data extensive datasets.

[SOURCE: ISO/IEC 20546:2019, 3.1.2]

3.3
cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

Note 2 to entry: Self-service provisioning refers to the provisioning of resources provided to cloud services performed by cloud service customers through automated means.

[SOURCE: ISO/IEC 22123-1:2023, 3.1.1]

3.4
data accountability
property that ensures that the actions of an entity can be traced uniquely to the entity

Note 1 to entry: The “use” of data includes all activities associated with data.

3.5
de-identification
general term for any process of removing the association between a set of identifying data and the data subject

[SOURCE: ISO 25237:2017, 3.20]

3.6
governance of data
system by which current and future data is collected, stored, secured, protected or controlled by IT systems, and impacts the management processes and decisions relating to data

© ISO/IEC 2026 – All rights reserved

3.7
internet of things
IoT
global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies

Note 1 to entry: Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

Note 2 to entry: In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

[SOURCE: Rec. ITU-T Y.2060]

3.8
machine learning
ML
process of optimizing model parameters through computational techniques, such that the model's behaviour reflects the data or experience

[SOURCE: ISO/IEC 22989:2022, 3.3.5]

3.9
pseudonymization
process applied to *personally identifiable information (PII)* (3.10) which replaces identifying information with an alias

Note 1 to entry: Pseudonymization can be performed either by PII principals themselves or by PII controllers. Pseudonymization can be used by PII principals to consistently use a resource or service without disclosing their identity to this resource or service (or between services), while still being held accountable for that use.

Note 2 to entry: Pseudonymization does not rule out the possibility that there can be (a restricted set of) privacy stakeholders other than the PII controller of the pseudonymized data which are able to determine the PII principal's identity based on the alias and data linked to it.

[SOURCE: ISO/IEC 29100:2024, 3.22]

3.10
personally identifiable information
PII
information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the PII principal. To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2024, 3.7]

3.11
PII principal
data subject
natural person to whom the *personally identifiable information (PII)* (3.10) relates

[SOURCE: ISO/IEC 29100:2024, 3.9]

3.12
risk management
coordinated activities to direct and control an organization with regard to risk

[SOURCE: ISO 31000:2018, 3.2]

© ISO/IEC 2026 – All rights reserved