INTERNATIONAL STANDARD

ISO/IEC 38505-1

First edition
2017-04

Information technology — Governance of IT — Governance of data —

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

Technologies de l'information — Gouvernance des technologies de l'information — Gouvernance des données —
Partie 1: Application de l'ISO/IEC 38500 à la gouvernance des données

Reference number
ISO/IEC 38505-1:2017(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

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.

This document was prepared by Technical Committee ISO/IEC/JTC 1, *Information technology*, Subcommittee SC 40, *IT Service Management and IT Governance*.

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 a high level, principles-based advisory standard. 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 this 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, data is becoming 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 is protected and secured.

This document has been prepared to provide guidelines to the members of governing bodies to apply a principles-based approach to the governance of data so as to increase the value of the data while decreasing the risks associated with this data. ISO/IEC 38500 provides principles and model for the governing bodies of organizations to guide their current use and to plan for their future use of Information technology (IT), and it is that document that is applied here.

As with ISO/IEC 38500, this document is addressed primarily to the governing body of an organization, and will equally apply regardless of the size of the organization or its industry or sector. Governance is distinct from management and thus we are concerned with evaluating, directing and monitoring the use of data, rather than the mechanics of storing, retrieving or managing the data. That being said, an understanding of some data management and techniques is outlined in order to enunciate the possible strategies and policies that could be directed by the governing body.

Information technology — Governance of IT — Governance of data —

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

1 Scope

This document provides guiding principles for members of 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 organization, and

— establishing a vocabulary for the governance of data.

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), and

— auditors.

While this document looks at 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.

This document applies to the governance of the current and future use of data that is created, collected, stored 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 from the smallest to the largest, 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 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
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 29100:2011, 2.2]

3.2
big data
data set(s) with characteristics (e.g. volume, velocity, variety, variability, veracity, etc.) that for a particular problem domain at a given point in time cannot be efficiently processed using current/existing/established/traditional technologies and techniques in order to extract value

Note 1 to entry: The term 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:—[1)], 3.2.1]

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.

[SOURCE: ISO/IEC 17788:2014, 3.2.5]

3.4
data accountability
accountability for data and its use

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/TS 25237:2008, 3.18]

1) Under preparation.

3.6
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]

3.7
machine learning
process using algorithms rather than procedural coding that enables learning from existing data in order to predict future outcomes

3.8
pseudonymization
process applied to personally identifiable information (PII) 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 might 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 29100:2011, 2.24]

3.9
personally identifiable information
PII
any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

Note 1 to entry: 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 identify that natural person.

[SOURCE: ISO/IEC 29100:2011, 2.9]

3.10
PII principal
natural person to whom the personally identifiable information (PII) relates

Note 1 to entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2011, 2.11]

4 Good governance of data

4.1 Benefits of good governance of data

Good governance of data assists governing bodies in ensuring that the use of data throughout an organization contributes positively to the performance of the organization through:

— innovation in services, markets and business;

— appropriate implementation and operation of data assets;

— clarity of responsibility and accountability for both the protection and potential to add value;

— minimization of adverse or unintended consequences.

Organizations with good governance of data should be expected to be:

— trustworthy organizations for data owners and data users to transact with;

— able to provide reliable data for sharing;

— protectors of intellectual property and other value derived from data;

— organizations with policy and practice in place to deter hackers and fraudulent activity;

— prepared to minimize the impact of data breaches;

— aware of when and how data can be reused;

— able to demonstrate good data handling practices.

This document establishes principles for the effective, efficient and acceptable use of data. Governing bodies, by ensuring that their organizations follow these principles, will be assisted in managing risks and encouraging the exploitation of opportunities arising from the safe handling and accurate interpretation of quality data.

Good governance of data also assists governing bodies in assuring conformance with obligations (regulatory, legislation, contractual) concerning the acceptable use and handling of data.

This document establishes a model for the governance of data. The risk of governing bodies not fulfilling their obligation is mitigated by giving due attention to the model in appropriately applying the principles.

Inadequate provision for the governance of data can expose an organization to several risks including:

— penalties of not complying with legislation, especially legislation relating to required privacy measures;

— loss of confidentiality of business data, e.g. recipes or design specifications;

— loss of trust from stakeholders, including business partners, customers and the public;

— inability to carry out critical organizational functions due to lack of trustworthy or business-relevant data;

— increased competition through the strategic use of data by competitors.

Governing bodies can be held accountable for:

— breaches of privacy, spam, health and safety, record keeping legislation and regulations;

— non-compliance with mandated standards relating to security, social responsibility;

— matters relating to intellectual property rights.

4.2 Responsibilities of the governing body

Members of the governing body are responsible for the governance of data and are accountable for the effective, efficient and acceptable use of data by the organization.

The governing body's authority, responsibility and accountability for the effective, efficient and acceptable use of data arise from its overall responsibility for governance of the organization, and its obligations to its external stakeholders, including regulators.

The key focus of the governing body's role in the governance of data is to ensure that the organization obtains value from investments in data and associated IT, while managing risk and taking constraints into account.

Additionally, the governing body should ensure that there is a clear understanding of what data are being used by the organization and for what purpose, and that there is an effective management system in place to ensure the obligations, such as data protection, privacy and respect for intellectual property, can be met.

4.3 Governing body and oversight mechanisms

The governing body should establish oversight mechanisms for governance of data that are appropriate to the level of business dependency on data.

The governing body should have a clear understanding of the importance of data to the organization's business strategies as well as the potential strategic risk to the organization from the use of that data. The level of attention that a governing body gives to data should be based on these factors.

The governing body should ensure that its members and associated governance mechanisms (such as audit, risk management and related committees) as well as managers have the requisite knowledge and understanding of the importance of data.

The governing body may establish a subcommittee to assist the governing body in overseeing the organization's use of data from a strategic point of view. The need for a subcommittee will depend on the importance of data to the organization and its size.

The governing body should ensure that an appropriate governance framework is established for the governance and management of data.

The governing body should monitor the effectiveness of the mechanisms for the governance and management of data by requiring processes such as audit and independent assessments to gain assurance that governance is effective.

5 Principles, model and aspects for good governance of data

As ISO/IEC 38500 highlights, the governance of IT is a subset or domain of organizational governance, or in the case of a corporation, corporate governance. This standard builds on and extends ISO/IEC 38500 to specifically examine data and its use by the organization.

ISO/IEC 38500 outlines six principles for good governance of IT, as follows:

a) responsibility;

b) strategy;

c) acquisition;

d) performance;

e) conformance;

f) human behaviour.