TECHNICAL REPORT

ISO/IEC TR 38505-2

First edition
2018-06

Information technology — Governance of IT — Governance of data —

Part 2: Implications of ISO/IEC 38505-1 for data management

Technologies de l'information — Gouvernance des technologies de l'information —

Partie 2: Implications de l'ISO/IEC 38505-1 pour la gestion des données

Reference number
ISO/IEC TR 38505-2:2018(E)

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

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 ISO 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 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.

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

A list of all parts in the ISO 38505 series can be found on the ISO website.

Introduction

This document describes what the governing body of an organization expects and requires from the data management team in order to be assured that the governing principles of IT can be implemented and are being upheld for data and its use by the organization.

As the core business processes of nearly all organizations become much more reliant on data, the strategic use of that data makes its governance a priority for the governing bodies of organizations. This governance of data, as part of the overall governance of IT, aims to help the organization extract business value from the data, while operating at an acceptable level of risk and with an appropriate level of accountability of the data and its use.

The governing body is responsible for the strategy of the organization and as ISO/IEC TR 38502 states: “Managers are responsible for achieving organizational strategic objectives within the strategies and policies for use of IT set by the governing body”.

However, management not only accepts the strategy as set by the governing body, it should also provide proposals and plans to assist with the creation of that strategy.

The impact of data to the organization can be highlighted through its many potential uses - including improving operations, altering the nature of products and services, informing and enabling employees, customers and suppliers.

Management can inform the governing body of the existing and required data management capabilities to support such data uses as well as inform them of technologies that enable new data scenarios that can impact strategic plans.

The governing body evaluates such data use options and forms a strategy regarding the use of data and the associated value, risk and constraints so it aligns to and supports the overall organizational purpose.

Utilizing the framework outlined in ISO/IEC 38505-1, this document examines the data management implications of such strategy, showing how the strategy can inform data policy, processes and controls. Those same controls and processes should also be designed to monitor the implementation of the strategy such that the governing body can be assured of the performance and conformance to the strategy.

Information technology — Governance of IT — Governance of data —

Part 2: Implications of ISO/IEC 38505-1 for data management

1 Scope

This document provides guidance to the members of governing bodies of organizations and their executive managers on the implications of ISO/IEC 38505-1 for data management. It assumes understanding of the principles of ISO/IEC 38500 and familiarization with the data accountability map and associated matrix of considerations, as presented in ISO/IEC 38505-1.

This document enables an informed dialogue between the governing body and the senior/executive management team of an organization to ensure that the data use throughout the organization aligns with the strategic direction set by the governing body.

This document covers the following:

— identifying the information that a governing body requires in order to evaluate and direct the strategies and policies relating to a data-driven business;

— identifying the capabilities and potential of measurement systems that can be used to monitor the performance of data and its uses.

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 38500:2015, *Information technology — Governance of IT for the organization*

ISO/IEC 38505-1, *Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 38500 and ISO/IEC 38505-1 apply.

ISO and IEC maintain terminological 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

4 Governance and management roles

4.1 General

This clause covers the linkage between ISO/IEC 38505-1 and this document, by explaining how those responsible for governance and management within an organization should develop policies for data use (including collection, reporting, distributing and so on) that align with the organizational culture, vision, mission and associated goals.

4.2 The governance role

ISO/IEC 38505-1 gives an overall view of key focus areas for data and its use in the organization, through the application of a data accountability map. Assessing the value, risk and constraints related to the elements in the data accountability map (Figure 1), will assist in identifying issues and concerns that can require policies to be defined in order to implement the overall data strategy of the organization.

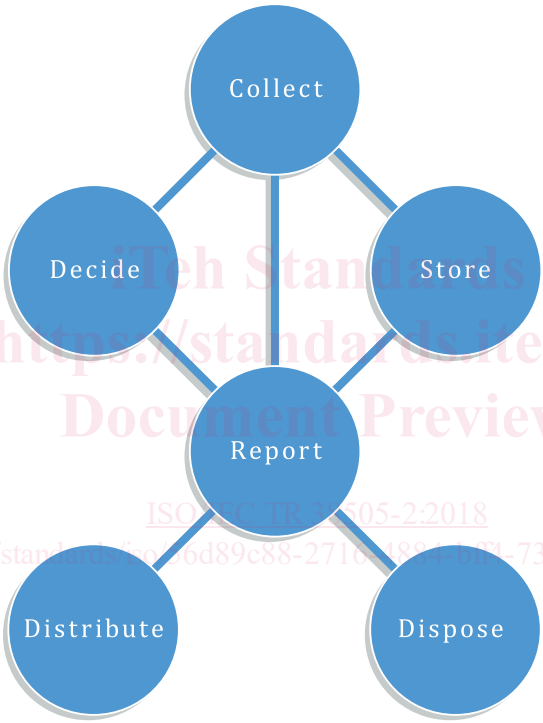

Figure 1 — ISO/IEC 38505-1 data accountability map

As data management technology advances, the ability to process large volumes of data from many sources and then extract value from that data becomes economically viable for an increasing number of organizations. Along with this increased value comes increased risk.

The governing body sets the overall data strategy for the organization which outlines how much the organization is expected to leverage data to extract value for its stakeholders. Closely linked to this strategy, the governing body sets the data risk appetite which describes the level of risk relating to data that the organization is willing to pursue or retain.

No matter what strategy or data risk appetite the governing body establishes, the governing body remains accountable for data and its use by the organization, including all data-related and data-enabled decisions that are made in the organization. The governing body should take into account the constraints of regulation and legislation, societal needs and cultural norms and existing organizational policies that can limit or constrain how data can be collected and used.

ISO/IEC 38505-1 combines these accountability concepts into a checklist of considerations for data strategy and policies. An example checklist is summarized in Table 1 below.

Table 1 — Data areas and data-specific aspects of governance (from ISO/IEC 38505-1)

	Value	Risk	Constraints
Collect	[V1] The governing body should decide the degree to which the organization will leverage or monetize data to achieve its strategic objectives.	[R1] The governing body should recognize the risks associated with the collection and use of data and agree to an acceptable level of their data risk within the overall risk appetite for the organization. This should include an examination of the risks of not collecting and using the data.	[C1] The governing body should approve the policies for data collection, taking into account constraints such as quality, privacy, consent requirements and transparency of use.
Store	[V2] The governing body should approve policies that allocate the appropriate resources for data storage and data subscription such that the potential value of data can be extracted.	[R2] The governing body should direct managers to ensure that an ISMS (Information Security Management System) is in place extending to data and technology suppliers, with adequate resources, controls and trust such that the level of risk appetite is not exceeded.	[C2] The governing body should direct managers to ensure data storage practices (including third-party data subscriptions) support the data collection constraints.
Report	[V3] The governing body should direct managers to use the necessary tools and technologies to ensure that the full value of data can be extracted.	[R3] The governing body should establish the significance of the context of data, including cultural norms and its potential misinterpretation in aggregate.	[C3] The governing body should establish the importance of the relationship between data and its constraints – particularly if the data is aggregated from different datasets.
Decide	[V4] The governing body should ensure that the data culture for the organization aligns with its data strategy including behaviours such as data access practices, data-enabled decision making and the organizational learning from the decision process.	[R4] The appropriate data and format should be delivered in a report for automated or human decision-making. While remaining accountable for these decisions, the governing body should delegate decision-making responsibilities appropriately for the organization and for the acceptable level of data risk.	[C4] The output of the decision-making process, as new data, will have its own value, risk and constraints – and the governing body should set the expectations for the decision process and associated responsibilities.
Distribute	[V5] The governing body should establish a policy for data distribution such that it allows the organization to satisfy the strategic plan of the organization.	[R5] The governing body should ensure that managers have implemented adequate controls to prevent inappropriate distribution.	[C5] The governing body should ensure that the appropriate distribution rights are implemented and that they are respected by third parties.
Dispose	[V6] The governing body should approve policies that allow for the disposal of data when the data is no longer valuable or can no longer be held.	[R6] The governing body should direct managers to implement an appropriate data disposal process that includes such controls as the secure and permanent destruction of the data.	[C6] The governing body should monitor data retention and disposal obligations and ensure that adequate processes have been implemented.

As noted in ISO/IEC 38505-1, "the checklist is not exhaustive and governing bodies should evaluate their organizational situation and add additional actions as required".

There are many data management implications behind each of the considerations in this table. In evaluating any of these, the governing body should be aware of the possible or potential options, and

the current and future capabilities of the organization. The governing body will want to evaluate these options and their implications for data use in the context of the overall strategy of the organization.

The concepts in Table 1 can be used to describe the resulting strategies and policies to be implemented. In many cases, metrics should also be associated with each element — and monitoring processes should be established to measure progress.

For these reasons, Table 1 is used as a checklist for this document.

4.3 The management role

Once the governing body has set the direction for data strategy in alignment with the overall organizational strategy, data policies or data components of existing organizational policies should be established. In the case of data, where the governing body can be unaware of the capabilities of those responsible for data management, neither the governing body nor the management team should create policy in isolation of the other party.

The management team and the governing body should agree on the current capability and desired future capability of the organization for data management. It can be advantageous to take advantage of new markets or products that can be made possible through diligent data collection and use.

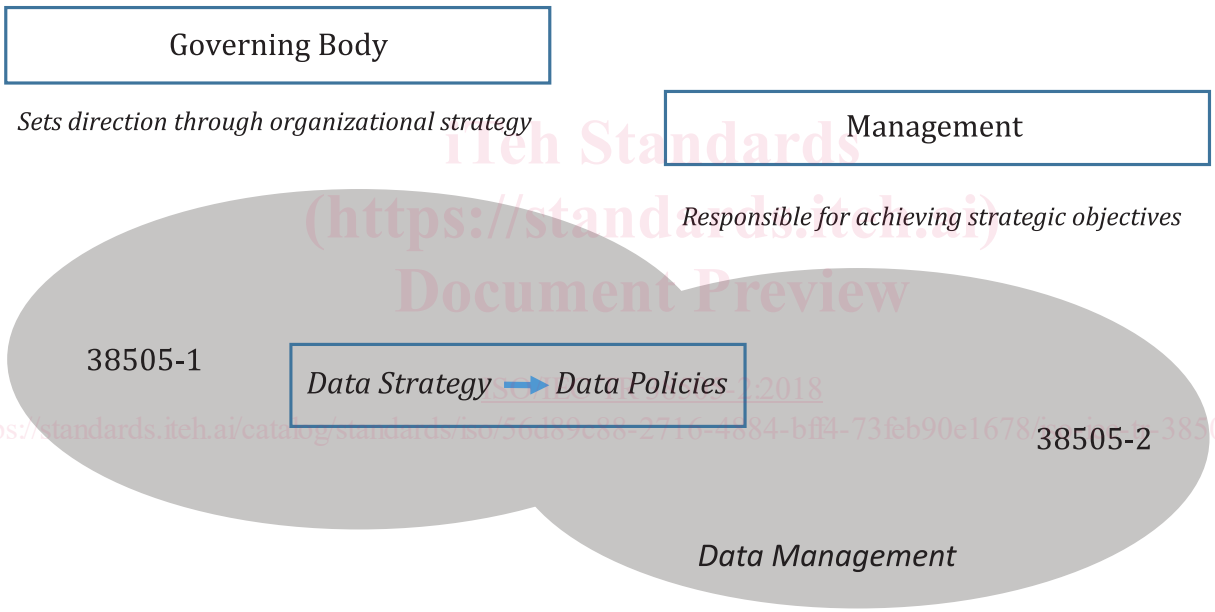

Figure 2 — Data strategy and data policies

Figure 2 shows that the governing body is responsible for the data strategy and data policies for the organization and for ensuring that these align with the overall organizational strategy. It is the management team that is responsible, within their delegated authority, for the implementation of these policies.

Please note that Figure 2 does not show other nuances of the relationship between the governing body and the management team, such as how they can work together to establish the organizational strategy through considerations of stakeholders, risk analysis, market pressures, compliance and other factors. Another important element not shown here is the impact of the culture of the organization and how that would permeate all aspects of the accountability and implementation of the strategy.

As outlined in ISO/IEC TR 38502, “Managers are responsible for ensuring the achievement of the objectives of the organization within the strategies and policies established by the governing body”.

ISO/IEC 38505-1 describes a "checklist of considerations for a governing body to take into account when developing a governance framework for data" as shown in Table 1. This document demonstrates how this checklist can be used to establish data policies.

5 Connecting business strategy to data management

This clause describes the implementation of business strategy through the development of policy, processes and controls. The focus of this document is on the development of policy as an activity carried out by members of the governing body in discussion with the members of the management team responsible for implementing the strategy.

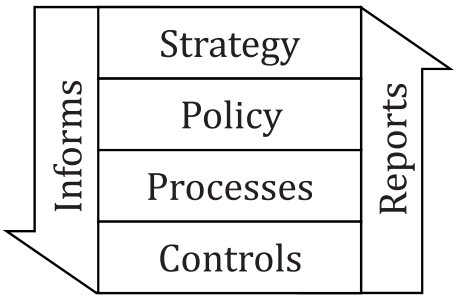

Figure 3 — Cascade mechanism

Figure 3 shows a possible cascade mechanism with data strategy developed by the governing body informing policy, policy developed by the governing body with the management team, guiding and influencing the development of suitable processes, and then controls that enable the processes to match the strategy. Unless these four activities are aligned, the data strategy, a subset of the organizational strategy, developed by the governing body cannot be delivered.

Note the cascade is bi-directional and is important to ensure there is a feedback mechanism from controls up to strategy. The governing body can monitor the performance and conformance according to the reports and alerts produced by controls and be assured that there is alignment from strategy to implementation.

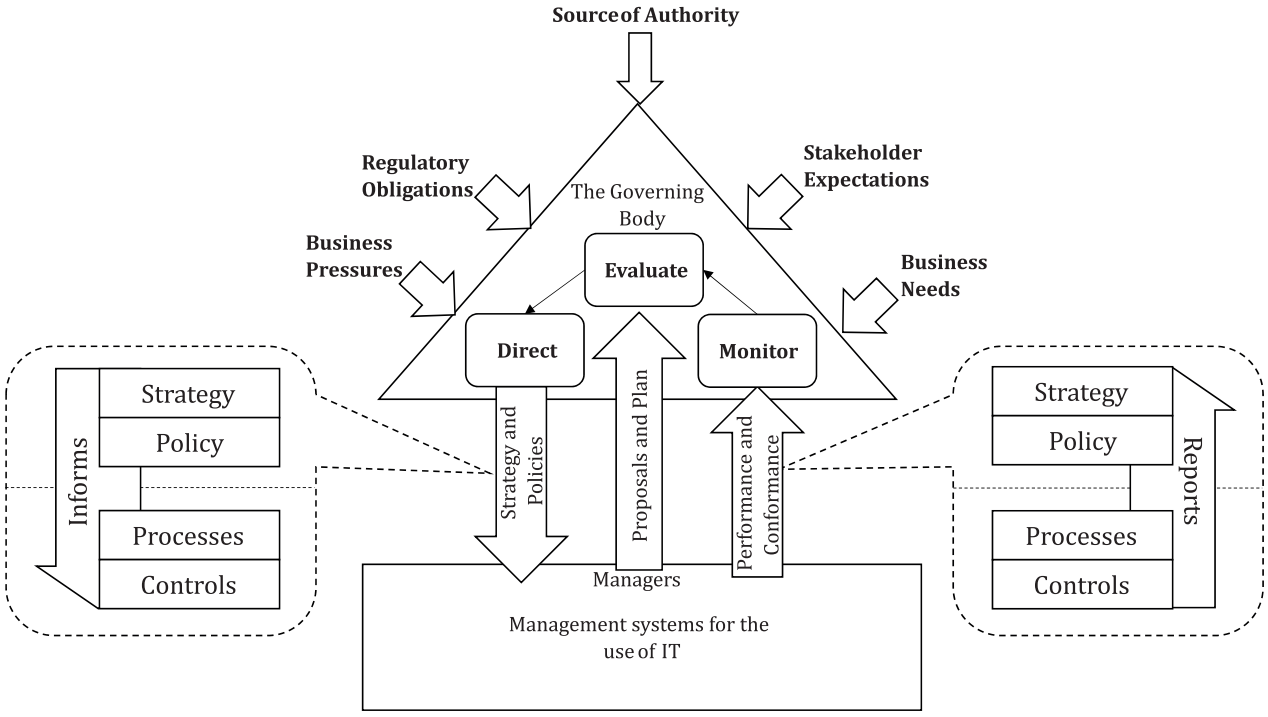

Figure 4 — Connecting the governance of data to data management (adapted from ISO/IEC 38500:2015)

Figure 4 shows how the governing body and management teams work together to implement policy to support the organizational strategy, and specifically, the strategy for data. As shown in Figure 3, the governing and management bodies are connected through the cascade mechanism which includes — amongst other mechanisms — elements of strategy, policy, processes and controls. These connections are developed and maintained through the EDM (Evaluate, Direct, Monitor) model, as follows:

— **Evaluate**. It is the responsibility of the management body to design proposals and plans for the implementation and evaluation of activities to fulfil the organizational strategy developed by the governing body. The plans and proposals should take into account the introduction of new technology which can improve the utility of data such as big data technology. It should also take into consideration the current and future capabilities of infrastructure critical for performing data management activities. The technology and capabilities should be described in the management processes, which is the expression of management activities. Using the management proposals and plans, along with other sources of information, the governing body will be able to evaluate a suitable data strategy.

— **Direct**. The governing body formulates data strategies and policies for the governance of data and assigns responsibilities and accountabilities to build the governance structure. The governing body directs the development of data strategy and policies according to the aspect-accountability mapping introduced in ISO/IEC 38505-1. Activities to be considered include data classification and the organization's risk appetite with respect to data. The mapping assists with the development of policy for managers to implement, taking into account aspects of value, risk and constraints.

— **Monitor**. The governing body should monitor the performance and conformance of management activities against the set directions. The reports and alerts provided by the management body will assist in this task. These reports should include status reports on alignment with legislation and regulation and notification of the occurrence of specific identified high-risk events. Alerts should be activated on the occurrence of key risk, security and privacy events identified in the mapping process.

A data strategy deals primarily with environmental constraints and opportunities to reach the organizational goals and objectives, but data policy refers to a set of rules made by the organization

