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)

COPYRIGHT PROTECTED DOCUMENT

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 **2**

4 Good governance of data **4**
4.1 Benefits of good governance of data 4
4.2 Responsibilities of the governing body 5
4.3 Governing body and oversight mechanisms 5

5 Principles, model and aspects for good governance of data **5**

6 Data accountability **6**
6.1 General 6
6.2 Collect 7
6.3 Store 8
6.4 Report 8
6.5 Decide 9
6.6 Distribute 9
6.7 Dispose 10

7 Guidance for the governance of data — Principles **10**
7.1 General 10
7.2 Principle 1 — Responsibility 10
7.3 Principle 2 — Strategy 11
7.4 Principle 3 — Acquisition 11
7.5 Principle 4 — Performance 11
7.6 Principle 5 — Conformance 11
7.7 Principle 6 — Human behaviour 12

8 Guidance for the governance of data — Model **12**
8.1 Applying the model 12
8.2 Internal requirements 13
8.3 External pressures 13
8.4 Evaluate 13
8.5 Direct 14
8.6 Monitor 14

9 Guidance for the governance of data — Data-specific aspects **15**
9.1 General 15
9.2 Value 15
9.2.1 General 15
9.2.2 Quality 15
9.2.3 Timeliness 16
9.2.4 Context 16
9.2.5 Volume 16
9.3 Risk 16
9.3.1 General 16
9.3.2 Management 16
9.3.3 Data classification schemes 17
9.3.4 Security 17
9.4 Constraints 17
9.4.1 General 17
9.4.2 Regulation and legislation 17
9.4.3 Societal 17
9.4.4 Organizational policy 18

10 Application of the data accountability map **18**
Bibliography **20**

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.

ISO/IEC 38500 also introduces a model for the governance of IT that establishes a cycle of "Evaluate-Direct-Monitor". This "EDM" model describes the three main tasks for governing IT and reminds us that "Authority for specific aspects of IT may be delegated to managers within the organization. However, accountability for the effective, efficient and acceptable use of IT by an organization remains with the governing body and cannot be delegated."

The broad areas of accountability as they relate to data are shown in Clause 6, along with the data flow and "gating" process where strategy and policies are in place to support this accountability.

To apply the principles and model to the governance of data, it is necessary to examine data-specific aspects of governance to the guidance. These aspects apply to all data and should be considered in understanding data and its impact across the organization. They also highlight the opportunities that the use of data (particularly with emerging technologies) provide to the organization, as well as the extra accountabilities that data brings to the governing body.

The data-specific aspects of governance that are introduced in this document are the following.

— **Value**: Data is the raw material for useful knowledge. Some data may not be very useful, while other data is extremely valuable to the organization. However, this value is not known until it is used by the organization and therefore all data is of interest to the governing body that is ultimately accountable for it. The term "Value" in this case also includes the quality and quantity of the data, its timeliness, the context (which is in itself data) and the cost of its storage, maintenance, use and disposal.

— **Risk:** Different classes of data bring different levels of risk and the governing body should understand the risks of data and how to direct managers to manage these risks. The risks not only manifest in data breaches, but also in the misuse of data as well as the competitive risks involved in not properly utilizing data.

— **Constraints**: Most data comes with constraints on its use. Some of these are imposed externally on the organization through legislation, regulation or contractual obligations and include issues of privacy, copyright, commercial interests and so on. Other constraints on data include ethical or societal obligations or organizational policies that restrict the use of the data. Strategies and policies are required to account for these constraints in any use of the data by the organization.

Data and its use by organizations is becoming increasingly important for all organizations and their stakeholders. By applying the principles, model and data-specific aspects of governance outlined in this document, governing bodies should be able to take actions that maximize their investment in data use, manage the risks involved and provide good governance for their organization.

6 Data accountability

6.1 General

Data is a key asset to any organization. It is used to keep track of the business (such as people, accounting, inventory and so on) and as a raw material for knowledge, innovation and insight. The accountability for data and its use rests with the governing body of the organization.

NOTE Like any model, this diagram is simplified in order to highlight specific concepts relating to items of interest for the governing body. The titles of the elements give an indication of the activity and are further explained below.

Figure 1 — Data accountability map

Figure 1 shows the areas of data accountability within an organization. The elements of the map are further described below.

For any organization and for any business type, the map identifies the topics that are of interest from a governance perspective. While the actual processes and implementations are the responsibility of management, the lines indicate both data flow and gating mechanism where it is necessary to ensure governance policies and strategies are in place and accountabilities can be met. The data-specific aspects of governance in the context of these accountabilities are discussed further in Clause 9.

The focus of this document is the governance of data which should not be confused with the management of data. Whereas the governing body is concerned with applying the principles of governance as outlined in Clause 7, the field of data management has well-defined methods for the processing of data as well as mechanisms for ensuring the confidentiality, integrity and availability of that data. An example data management lifecycle is shown in Figure 2.

Figure 2 — Example data management lifecycle

6.2 Collect

The Collect activity includes the data acquisition, gathering and creation process, learning from previous decisions made and additional context extracted from other data sets (internal or external).

Data exists in many forms and can be created and collected for use by the organization in a number of different ways, including the following.

— **Data entry**: Data entry is achieved using applications either within the organization [for example, in an Enterprise Resource Planning (ERP) system or email application] or externally via a website, mobile application or similar application.

— **Transactions from other systems**: Data entry or updating done on other systems can flow through to the organization's system through Electronic Data Interchange (EDI) or other interfacing processes.

— **Sensors**: An increasing amount of data is ingested into the organization through machine systems such as sensors. Sensors cover a wide range of data acquisition devices including web site logs, social media sources and "internet of things" devices which include everyday devices from simple temperature sensors to TVs, cars, traffic lights and buildings. Data from sensors can also include potentially urgent signals such as alerts and alarms.

— **New context**: Data from reports can be combined with other data to provide additional information, which is itself fed back into the data of the organization. In many cases, this additional data gives new context to the original data and may need to be treated differently from the original data. New contextual data can come from decisions which may give relevance or value to existing data.

— **Subscription**: Data may become available to the organization through a subscription to a data feed or virtual data store.

6.3 Store

The Store activity includes locating the data where it can be physically or logically retrieved. This includes data stored on devices owned and operated by the organization, devices external to the organization and also virtual stores such as data feeds where the data is only collated when needed. In each case, the stored data can be retained for reporting purposes pending a decision to dispose.

As data is collected through the above actions, it is ingested into a data store where it is secured and managed and possibly archived. The amount of data that organizations control is increasing rapidly due to new technologies such as the internet of things that use sensors to collect data, and big data that uses large amounts of data to look for trends and make predictions using machine learning. Many of these new technologies run in public cloud computing environments where the economies of scale enable large storage and processing capabilities at much lower cost.

In some cases, the organization will use a data store that is outside its location. Traditionally, this has been through offsite hosting operations where the storage is outsourced. Cloud computing takes this to the next stage where the operation of the store is not visible to the client organization. Furthermore, the organization may use a "virtual store" where data is provided only as a data feed which can flow directly into reports or analysis.

It should also be noted that even though the organization may control the data in its store, it may not "own" that data because of intellectual property rights such as copyright or other legal issues including personal or health information handling laws. Special care may also be necessary where the storage and use of data cross jurisdictional boundaries. In any case, the stewardship of the data remains with the governing body.

6.4 Report

The Report activity includes manual or automated extraction and analysis of data for the purpose of supporting decision making, distribution or disposal.

An important capability of an information system is to extract data from the data store in the form of a data feed. This feed should have associated properties such as quality and currency of the data so that the business can determine its usefulness to the reports they produce from that data.

During the extraction and reporting process, many data feeds may be used and these can come from a data store within the organization or may come from a virtual data store outside the organization. The combination of these data feeds may give a new context to the data. This new context is in itself new data and this should be fed back into the data creation and collection process, where the normal collection process occurs.

Applications can also produce reports as well as update the existing data and again, this new data follows the creation process.

Other extraction and analysis techniques such as data mining and machine learning can be applied to data to gain further insight, predict future outcomes and to make decisions automatically. Again, this is new data being created and collected.

Reports can also be used to filter data to increase its usefulness, or to enable distribution and disposal. For example, data from sensors can be aggregated to extract trends while removing personally identifiable information through techniques such as anonymization and pseudonymization. The original data can then be similarly extracted and disposed of.

6.5 Decide

The Decide activity occurs when a decision is made based on the report examination. The decisions will be made by people within the organization or by automated means.

The main reason for having data is to make decisions, and the value of data is how it improves the decisions that are made. Reports (including on screen reporting) are examined to provide information upon which decisions are made.

Through a process of delegation, the governing body ensures that the decisions made are appropriate for the level of responsibility of those decisions. This is of particular importance when decisions are made automatically through simple data flow processes or more complex machine learning algorithms. In any case, the governing body remains accountable for all decisions and should ensure that they have the appropriate controls and, where necessary, apply human intervention to deal with any biases, discrimination or profiling in the decision making process.

Because the decision making process values the data, that information (the “usefulness” of the data) can be fed back into the data collection and creation process. By creating this data maintenance and feedback loop, it is possible to fine tune the reports that are created, the data feeds that are used and ultimately, the data that is fed into the system. Together, this loop increases the value of the decisions made and that in turn can improve the business.

6.6 Distribute

The Distribute activity involves extraction or copying of data via the Report activity for circulation to external parties.

Data may be extracted from the store and distributed outside the organization. This can occur for a number of reasons, such as:

— external reporting is required for example to a government authority;

— it is part of a business-to-business (B2B) data exchange, customer use or similar activity;

— the data is being sold for example to an advertising agency or survey company;

— the data is part of the publishing business of the organization, for example business data (in other words, the data is the product);

— the distribution was not authorized, in which case this would be classified as a data breach.

6.7 Dispose

The Dispose activity usually involves identifying data for disposal via the Report activity and then permanently removing that data and any duplicates from the data store. In the case of a data feed, this would be the permanent disconnection to that feed.

The increasing sophistication of data analysis, mining and learning tools increases the value of existing data because more information can be extracted from more data. This fact, combined with the reduced cost of keeping data reduces the necessity to dispose of data.

But there are still a number of reasons why some data should be extracted from the store (via the Report activity) and securely disposed of.

— To reduce the risk of data leakage. If the data no longer exists, it cannot be inappropriately distributed or used.

— To remove irrelevant or incorrect data. Although older data may be used for trend analysis, it may no longer be relevant. Also, it may no longer be correct.

— To apply the right to be forgotten. Customers may ask to have their data removed.

— To comply with contractual arrangements with customers or suppliers.

— To comply with legal or regulatory requirements.

Similarly, there may be reasons such as health related regulations or legislation that require the retention of data.

7 Guidance for the governance of data — Principles

7.1 General

ISO/IEC 38500 provides six principles for the good governance of IT. The following subclauses provide guidance on how these principles can be applied to the governance of data.

The practices described are not exhaustive but provide a starting point for discussion of the responsibilities of the governing body for the governance of data. That is, the practices described are suggested guidance.

It is the responsibility of each organization, individually, to identify the specific actions required to implement the principles, giving due consideration to the nature of the organization, and applying appropriate analysis of the data-specific aspects referred to in Clause 9.

7.2 Principle 1 — Responsibility

The governing body is accountable for the responsibilities associated with the organization's use of data, and should ensure that those within the organization understand and accept their responsibilities. These responsibilities:

— extend across the organization and beyond the IT function or department, or IT initiated activities;

— include key data related to business activities such as marketing, where data is used to inform product plans, and product development, where data is collected to guide the design and build of new products;

— include situations where the data itself is the product or service that the organization provides. Such situations include content such as music or movies and information such as weather or stock market reports;

— cover the whole lifecycle of the data.

7.3 Principle 2 — Strategy

The governing body is accountable for a data strategy that aligns with the organization's overall strategy, including current and future capabilities. This data strategy should:

— include plans for data use that address current and future overall strategic objectives;

— allow for technology advances and market expectations;

— cover all parts of the data accountability map;

— account for the data-specific aspects of governance (value, risk, constraints);

— set an expectation that it may require a revision of the overall strategy to account for new opportunities or risks.

7.4 Principle 3 — Acquisition

The governing body is accountable for acquisition (by collection or purchase or as a by-product of business activity) of data and should ensure such acquisitions are appropriate by considering whether:

— the acquisition is consistent with its intended and/or stated use within the organization as well as external use if the data is so distributed;

— the assessment of the value, risks and constraints associated with the proposed use and management of acquired data sets or data streams aligns with the data strategy.

7.5 Principle 4 — Performance

The governing body should identify the relevant performance metrics, ensure they receive appropriate attention and remedial action if necessary.

Performance metrics should include:

— how well data use supports decision making within the organization;

— where data is shared with suppliers or customers, how well data use supports their decision making;

— the adoption rate of new data sets and data streams within the organization;

— the return on investment for data, including data that has been distributed;

— the overall value of data leveraged by the organization against the value leveraged by competitor or comparative organizations.

7.6 Principle 5 — Conformance

The governing body should ensure that the organization knows and conforms to external obligations and properly defines, implements and ensures compliance to appropriate internal policies. Such obligations and policies should include:

— all data sets and data streams be secured according to security policies that meet the organization's needs and obligations;

— the correct handling of PII;

— the appropriate implementation of data retention policy and practice across the organization;

— an understanding of all legal obligations relating to data, and the assurance that these obligations have been met across the organization.

7.7 Principle 6 — Human behaviour

The governing body is accountable for the use of data across the organization such that human behaviours are identified and appropriately considered. This respect for human behaviour should include:

— policy to govern the acceptable use of data and devices across the organization;

— an organizational data culture to encourage the appropriate sharing, protection and interpretation of data;

— the impact and requirements of the human behaviour of stakeholders.

8 Guidance for the governance of data — Model

8.1 Applying the model

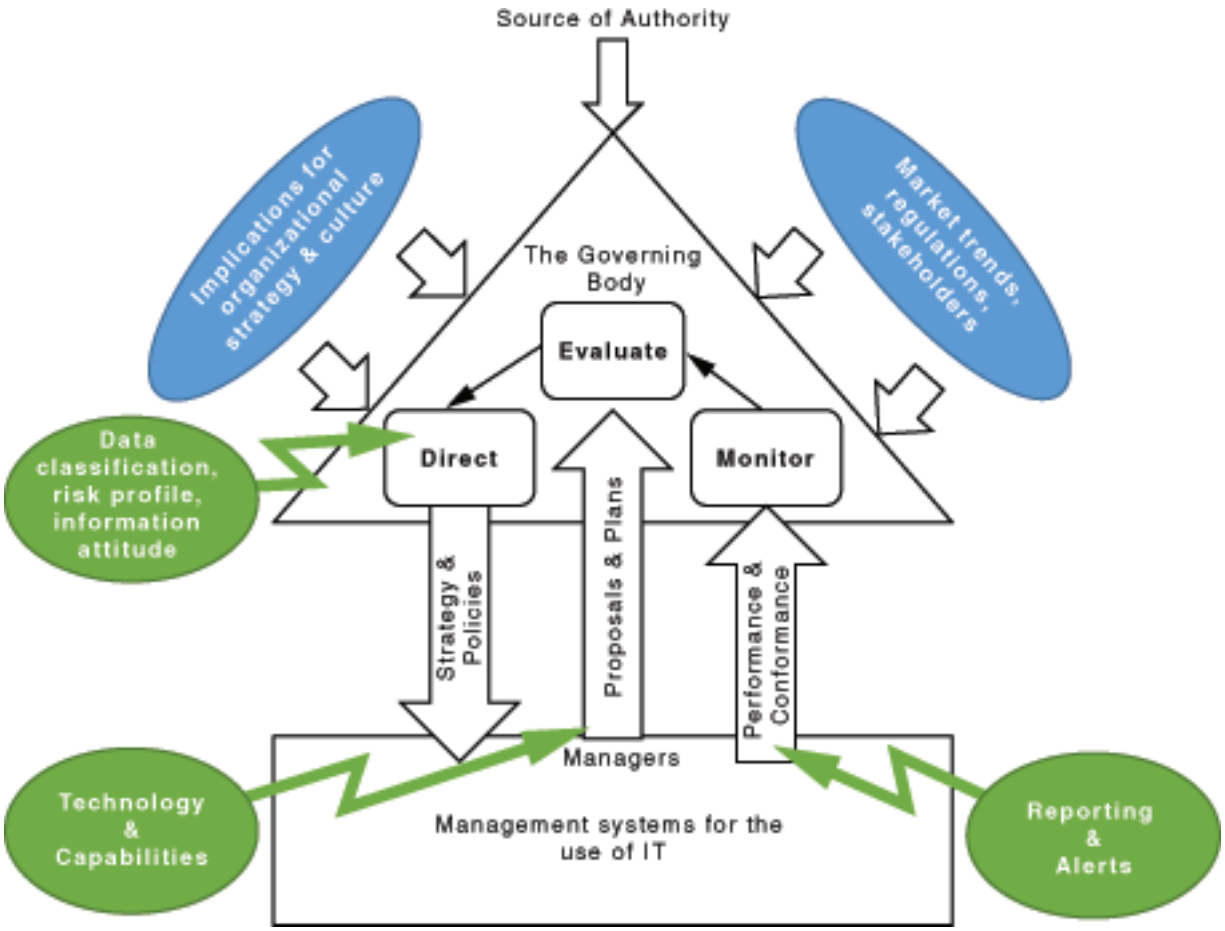

Figure 3 — Governance of IT model — Application to the governance of data

Governing bodies should govern data through three main tasks:

a) evaluate the current and future use of data;

b) direct preparation and implementation of strategies and policies to ensure that use of data meets business objectives;

c) monitor conformance to policies and performance against the strategies.

Authority for specific facets of data may be delegated to managers within the organization. However, accountability for the effective, efficient and acceptable use of data by an organization remains with the governing body and cannot be delegated.

Figure 3 shows specific pressures on the governing body in relation to data and its use by the organization. Stakeholders, including customers, employees and regulators all have an interest in this domain. The figure also shows the type of inputs that are required in the EDM cycle as it relates to data. Areas where management input could assist the governing body in the Direct, Evaluate and Monitor activities are shown in the diagram.

8.2 Internal requirements

The governing body will have established an overall strategy for the business. However, the use of data is much more significant across all industries and government to the point that, in order to fulfil their obligations to their stakeholders, the governing body should examine the use of data as part of their overall strategy.

This requires the governing body to examine the potential uses of data, either by the organization itself or by its competitors, and to adapt the strategic direction to support the desired outcomes. This may include buying and selling data.

The business will have a culture surrounding the use of data by the organization. The governing body should shape that data culture to ensure that it aligns to the data strategy required to reach its overall objectives. Because data is only as valuable as the decisions that are made from it, this data culture could result in organizational behaviours pertaining to data access, good data handling practices and decision processes at all levels that rely on reports in the relevant context.

8.3 External pressures

The organization may need to adjust its strategies and policies to ensure it complies with the pressures of the market forces in which it operates. Such market forces include:

— customer expectations regarding the availability, quality and interaction with the available data, and

— competitors using data to improve or expand their products, services or processes.

Laws and regulations as well as stakeholder requirements may vary between markets and the governing body will need to ensure that the strategies and policies applying to its current and future use of data can apply broadly across these markets. Such constraints and obligations may apply across different data accountability activities including:

— how data is able to be collected, including privacy notification and consent requirements around the collection and use of personal information,

— the data retention and disposal requirements,

— decision making obligations to appropriately deal with biases, discrimination and profiling, and

— the intellectual property issues regarding the sharing or reuse of data.

8.4 Evaluate

In evaluating the governance of data for the organization, the governing body should take into account the internal requirements and external pressures placed on the organization.

Additionally, the governing body should examine and make judgement on the current and future use of data. This includes:

— the internal use of data and associated technologies and processes,

— the use of data by competitors, other organizations, governments and individuals,

— evaluating the evolving set of legislation, regulation, societal expectations, and

— other factors that control and influence the use of data.

The technologies of data management are rapidly changing and the governing body should solicit proposals from managers to explain these technologies and their potential impact on the organization. Such technologies can have a significant effect on all data aspects including cost, insight and privacy. In many cases, these effects can go beyond the management of the data and can provide new business opportunities for the organization, and potentially greater risk. By not availing themselves of these opportunities, the governing body could subject the organization to increased risk from competitors, changing market expectations and increased compliance issues.

The governing body should also be aware of the data management capabilities of the organization. For example:

— to what extent the organization can recover from a data breach;

— how easily the correct information can be delivered in the right format to assist decision making at all levels;

— whether the organization leverages new technologies such as cloud computing to augment its own capabilities.

The governance of data strategies and policies can only be implemented if the organization has the necessary resources and capabilities to implement such policies.

8.5 Direct

Governing bodies should assign responsibility for and direct preparation and implementation of strategies and policies.

The strategies and policies of the current and future use of data for the organization should be aimed at:

— **Maximizing the value from the organization's investment in data**: Data, like any asset within the organization, requires an investment. This is true whether the data is collected from outside the organization, is stored at a third party or is used as a service. And like any investment, the organization will want to ensure it is getting a good return on the data. The ultimate value of data is how its use improves decision making, but an organization may also be able to sell data for others to use.

— **Managing the risk associated with the data in line with the data risk appetite**: Some data, such as product research or undisclosed stock market ambitions, has a high business value and appropriate resources need to be applied to leverage and protect this data. The value and risk associated with managing this data is higher than other types of data and the strategies and policies should reflect this through the adoption of a data classification scheme for the data.

— **Ensuring the correct level of data stewardship:** The governing body is accountable for data and its use, including the decisions that are made from this data. Therefore, the data accountability activities should be delegated appropriately within the organization.

These elements all contribute to the "information attitude" of the organization and its effectiveness in applying data to the business goals of the organization. This reflects the data culture of an organization, its overall strategy, its risk appetite, its perceived security levels, the amount of knowledge-based work it does and the metrics and value it places on data and its use.

8.6 Monitor

Governing bodies should monitor, through appropriate measurement systems, the performance of data use of the organization. They should be able to reassure themselves that the strategies relating to data are being correctly implemented and that the use and management of the data conforms to internal policies and external requirements such as regulations and data stewardship requirements.

The use of reporting and analysis tools in decision making should be measured in order to understand the value of the data and to improve the decision making processes.

Other areas where oversight from the governing body may be of high importance due to strategy or regulations include:

— the use of PII including privacy concerns, consent requirements and transparency of data use (see ISO/IEC 29100);

— the use of an effective Information Security Management system (such as described in ISO/IEC 27001) that reflects the strategic importance of data. This should extend to include third party data feeds and data management in cloud computing services (for example, ISO/IEC 27017). These International Standards provide guidelines for information security controls, but in some cases, such controls will be insufficient and the governing body will need to rely on trust and verification;

— data retention and disposal requirements;

— the reuse, sharing or selling of data and its associated rights, licensing or copyright;

— appropriately accounting for cultural norms, bias, discrimination or profiling in decision making.

9 Guidance for the governance of data — Data-specific aspects

9.1 General

In many organizations, the volume of data in use is increasing exponentially. This is as a result of recent changes in technology that make it economically viable to process large datasets.

This capability means that data use is becoming a core business for many organizations, regardless of their industry.

Whenever data is used by an organization (whether it is stored outside the organization, copyrighted by others or "owned" by a customer) it brings with it the potential to create new value in the organization by providing better decision making or additional information. It also imposes a number of accountabilities on the organization.

Data is a non-consumable asset with many associated attributes and aspects. These require consideration by the governing body of an organization as items that may have significant strategic impact on the organization as a whole.

9.2 Value

9.2.1 General

Data, as a raw material for useful information, can be distributed and sold. That sale, via a subscription, a data feed such as a publication or website, assigns a monetary value to the data.

The business value in data is the measure of how it improves the decisions that are derived from the information it contains. To extract the information from the data requires the data to have quality, timeliness, context, volume and potentially other attributes that together match the requirements of the decision process.

9.2.2 Quality

The quality of data is the measure of how accurately it encapsulates the facts it is trying to represent.

The value which can be derived from data depends in part on the quality of the data matching the accuracy required by different decision scenarios.

In some cases, such as financial information, a dataset of high quality data that is up to date and in the right format is necessary for decision makers (e.g. investors). However, in other cases, a dataset of lower quality may be adequate to derive good decisions, for example, in the case of trend analysis.

9.2.3 Timeliness

Data provides information for improved decision making and most decisions are time dependent and therefore an important property of data is its timeliness or currency.

As with all elements of data quality, the timeliness of the data depends on the decisions being made. For example, automated decision making in an anti-lock braking system relies on up-to-date data collected and analysed over a short time period. This is a very different time span than that required to analyse an annual income statement.

9.2.4 Context

Applying context to data allows information to be obtained from it. This context, in the form of additional data, may affect the policies that are applied to the new information that is obtained. For example, combining sales data with postal information may reveal PII which may require different handling of the data.

Context is an important factor in decision making because it could invoke cultural norms and bias and lead to a different interpretation of the data, resulting in a potentially different decision.

9.2.5 Volume

The volume of data may affect its value. A large amount of consistent data may increase the confidence of a trend or prediction, but different techniques may be required to extract this confidence.

9.3 Risk

9.3.1 General

Because data has value, it also brings with it risk. However, unlike other assets, some aspects of data means that it has different risk profiles. For example, stealing data usually involves unauthorized copying of the data and not moving it.

Additionally, the use of data such as PII or healthcare data carries with it additional responsibilities and therefore increased risk to the organization. A way to reduce this risk is by removing PII attributes through de-identification techniques such as described in ISO/IEC 20889[2)].

The overall risk appetite for the organization is established by the governing body. As data becomes strategically, operationally and financially important to the organization, the risks associated with data itself should be examined by the governing body to ensure an appropriate level of "data risk" is set that aligns with the overall risk appetite.

The risk of not using available data for the benefit of the organization should also be considered. It may be detrimental to the organization when it could be reasonably known that such data is available but was not acted upon. This could relate to operational risks such as safety data, financial risks regarding investments or strategic risks such as allowing new types of customer interactions.

9.3.2 Management

Risk management is described in ISO 31000:2009, 2.2 as the "coordinated activities to direct and control an organization with regard to risk" and includes a framework and structured process for dealing with risk.

---

2) Under preparation.

The main risk associated with data is losing control of it; however, there are also risks to the organization in the misuse of data across the spectrum of the activities in the data accountability map.

To change the risk management processes to account for data risk (or any change to the risk profile or risk appetite), ISO/TR 31004:2013, 3.2 advises that "The organization should determine whether changes are needed to its existing framework for the management of risk, before planning and implementing those changes, and then monitoring the ongoing effectiveness of the amended framework."

9.3.3 Data classification schemes

The governing body should allocate resources to leverage and protect data, with an emphasis on high value and high risk data. Some data, such as research data may have a high business value because that data represents a significant business advantage. And some data that is used by the organization will be freely available on the internet.

As part of an Information Security Management system (ISMS), managers should identify different types of data through a data classification scheme. Such a scheme allows the organization to apply different levels of resourcing to different classes of data. ISO/IEC 27002:2013, 8.2.1 states that "Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification".

9.3.4 Security

Security is an element of risk management. The governing body should have a strong oversight of security of data within the context of the security of the organization.

When evaluating strategies and approving policies for security of data, the following protection measures could be considered, amongst others, as appropriate:

— an overarching IT security framework such as the "Framework for Improving Critical Infrastructure Cybersecurity" from NIST uses business drivers to guide cybersecurity activities as part of an overall risk management framework;

— an ISMS such as the ISO/IEC 27000 series which includes specifics security controls;

— where PII is being processed by a cloud service provider, ISO/IEC 27018 provides controls that ensure data protection for such data.

9.4 Constraints

9.4.1 General

Data used by the organization may come with constraints. Such constraints may limit the potential value (use and distribution) of the data, including how the data can be combined or aggregated with other data. Such data may require a different classification (e.g. high business value, confidential or PII) and need to be handled accordingly throughout the organization.

9.4.2 Regulation and legislation

Regulation and legislation, including common law and contractual law, may apply to the access, use, storage or distribution of data and will need to be considered in the formulation of data strategies and policies.

9.4.3 Societal

From a strategic perspective, this aspect concerns the "implied contract" with society. For example, the main goal of a public health service would be to protect the health of the population as a whole, not only the individual. The governing body being more explicit about the "implied contract" can help clarify the data strategy, including how the data is used and how decisions are made from that data.

9.4.4 Organizational policy

In addition to the external requirements imposed on the use of data, the organization may impose its own policy on data in order to increase its value, decrease the cost of managing the data, to reduce the risks associated with the data or to meet other requirements.

10 Application of the data accountability map

The governance of data requires the governing body to evaluate, direct and monitor activities relating to the use of data, across the organization; whilst taking into account external factors and obligations.

Applying the principles of governance of IT from ISO/IEC 38500, the governance framework for IT from ISO/IEC/TR 38502, and taking an implementation approach from ISO/IEC/TS 38501, provides a foundation for the development of policy and practice relating to data.

An approach in applying the principles and model to the governance of data, is to examine the data-specific aspects of governance. These aspects apply to all data and should be considered in understanding data and its impact across the organization. They also highlight the opportunities that the use of data (particularly with emerging technologies) provide to the organization, as well as the extra accountabilities that data brings to the governing body.

Building on this foundation, the data accountability map from Clause 6, when used in conjunction with the data aspects of value, risk, and constraints, provides guidance for a comprehensive checklist of considerations for a governing body to take into account when developing a governance framework for data appropriate for their organization. The specific actions required to implement the principles will vary according to the nature of the organization and its circumstances.

Table 1 should be used by the governing body as a guide to evaluate, monitor and direct the organizational activities for the governance of data overall, and for particular classes of data as appropriate. For each data accountability activity, the data-specific aspects should be examined to indicate required actions, noting that higher levels of control and more stringent policy will be required for data collections of greater value or sensitivity.

The value, risks and constraints associated with particular data sets will vary over time, at a frequency dependent on many factors including organizational size, sector and jurisdiction. It is the responsibility of the governing body to determine an appropriate review cycle for their organization.

This checklist will provide guidance for governing bodies seeking to develop a governance framework that supports the leveraging of the maximum value from data within their data risk appetite and taking into account external and internal constraints.

The checklist is not exhaustive and governing bodies should evaluate their situation and add additional actions as required.

Table 1 — Data areas and data-specific aspects of governance

	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 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 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.

Bibliography

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

[2] ISO/IEC/TS 38501, *Information technology — Governance of IT — Implementation Guide*

[3] ISO/IEC/TR 38502, *Information technology — Governance of IT — Framework and model*

[4] ISO 31000:2009, *Risk management — Principles and guidelines*

[5] ISO/TR 31004:2013, *Risk management — Guidance for the implementation of ISO 31000*

[6] ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

[7] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[8] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[9] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[10] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[11] ISO/IEC 20546:—[3)], *Information technology — Big data — Definition and vocabulary*

[12] ISO/IEC 20889:—[4)], *Information technology — Security techniques — Privacy enhancing data de-identification techniques*

[13] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

[14] "Framework for Improving Critical Infrastructure Cybersecurity" by National Institute of Standards and Technology, USA. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

3) Under preparation.

4) Under preparation.

ICS 35.020
Price based on 20 pages