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.

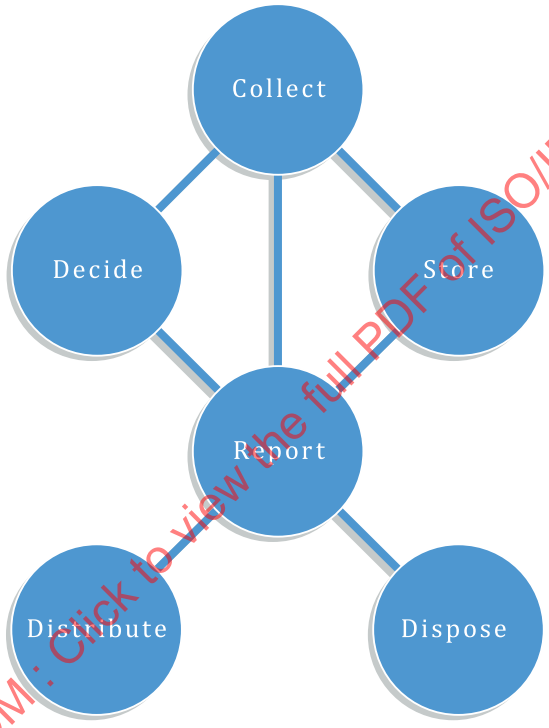


Figure 1 — ISO/IEC 38505-1 data accountability map

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.

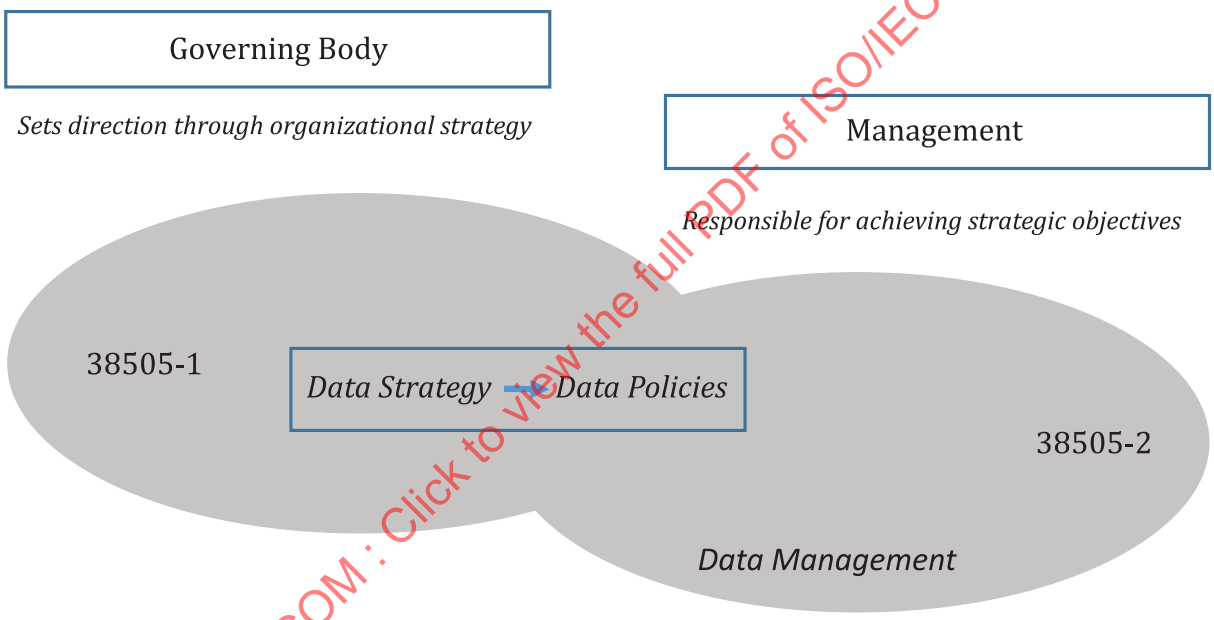


Figure 2 — Data strategy and data policies

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.

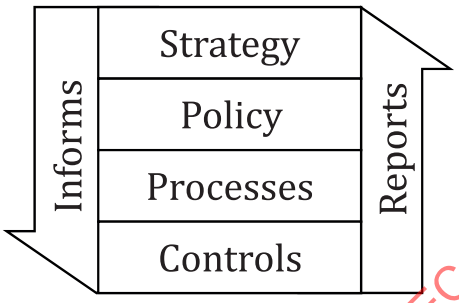


Figure 3 — Cascade mechanism

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.

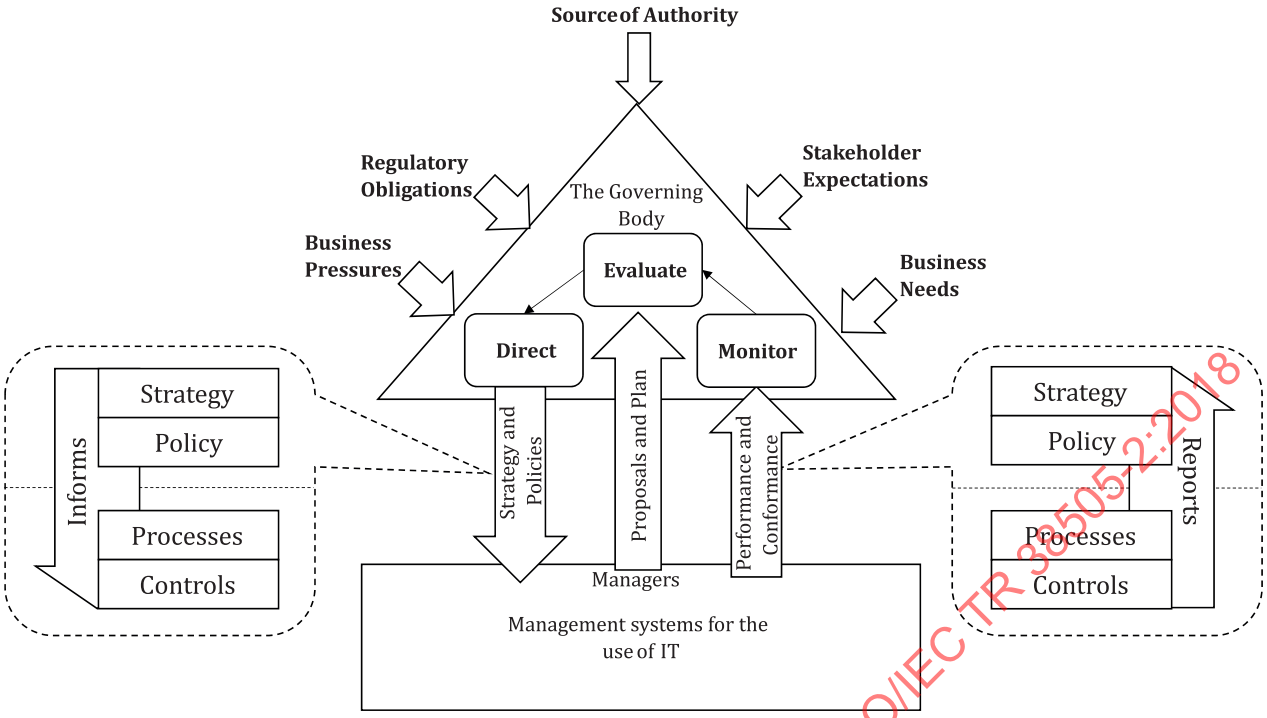


Figure 4 — Connecting the governance of data to data management (adapted from ISO/IEC 38500:2015)

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

for rational decision-making. Strategy and policy are both set at the governing level of an organization, with the governing body establishing policies, in conjunction with the management team, that help the management team to operate in alignment with the strategy, serve as a guideline for operational decision-making and drive expected behaviours within the organization.

Governance of data policy produced by a governing body should

— align with strategy and the organizational goals and objectives,

— be consistent with other organizational policy, and

— include mechanisms for policy implementation and revision.

Policy development within a data governance framework is likely to be an ongoing process, so the governing body should ensure that the following tasks are addressed by management:

— Identify and define:
  — Identify new regulatory requirements, technology developments, operational needs and current issues or gaps;
  — Identify sponsors, stakeholders and determine their relevant roles;
  — Identify different business activities;
  — Formulate a method to define the policies;
  — Obtain approval to proceed with draft policy.
— Develop:
  — Develop and draft initial set of policies;
  — Distribute draft policy to stakeholders for review and input;
  — Review and, where appropriate, incorporate feedback;
  — Obtain approval.
— Implement and maintain:
  — Post and announce policy;
  — Conduct educational and communication activities;
  — Coordinate and support the operation of policy.
— Monitor and improve:
  — Document the effect and result of the operation;
  — Monitor compliance and effectiveness of implemented policy;
  — Review modifications on an annual review cycle;
  — Design a continual improvement process for the set of policies.

6 Establishing policies through the checklist of considerations

This clause demonstrates how the data accountability map and associated considerations matrix from ISO/IEC 38505-1, as shown in Table 1, can be applied to assist with the development of organizational policy that aligns with and informs the data strategy of the organization. The data accountability map provides six areas of focus for governance activities across an organization, and therefore six

distinct areas where policy should applied. The associated considerations of value, risk and constraints prompt discussion and decisions around the appetite of an organization to deliver business value and opportunities through data, and also to inform how this value and these opportunities can be delivered in a way that meets the compliance needs of the organization.

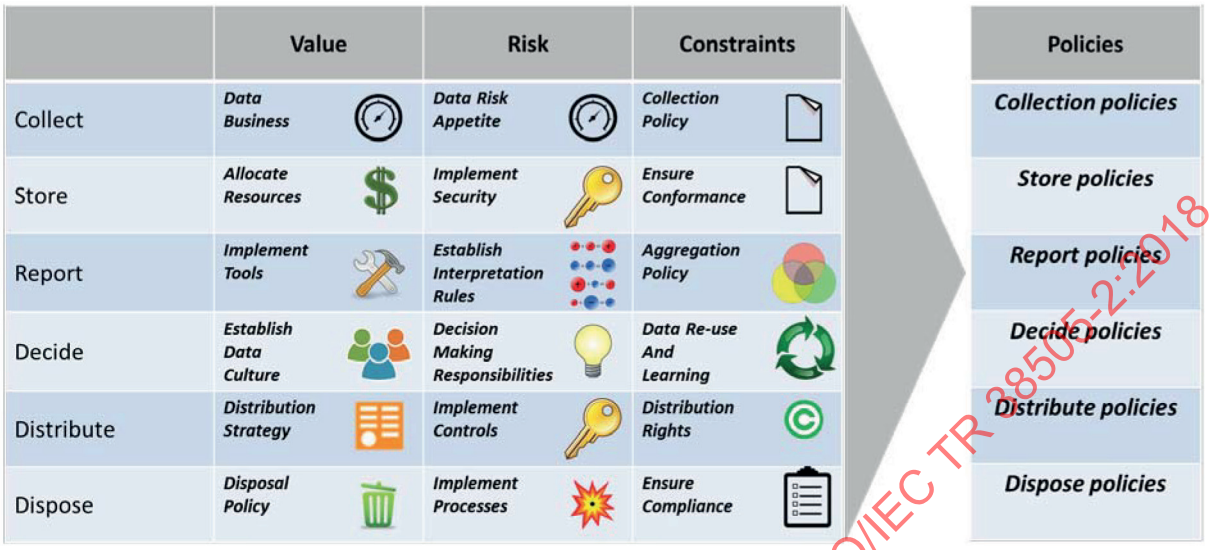


Figure 5 — Data management schema for deriving policy

As shown in Figure 5, by taking each area from the ISO/IEC 38505-1 data accountability map, as represented in Figure 1, (i.e. collect, store, report, decide, distribute and dispose), and considering the aspects of value, risk and constraints for each accountability area, the governing body will be prompted to consider data activities across the organization.

The Annexes provide examples of how the matrix of map areas and considerations can be applied and demonstrate the type and range of policy statements that can result from asking questions around each cell of the matrix. The examples demonstrate how these resulting policy statements can be added to existing organizational policies or set aside in a separate data policy.

Annex A provides a set of worksheets that can be used as the basis for developing policy statements to help implement a data strategy and associated governance framework.

Annex B demonstrates how applying the matrix can assist with the development of sound governance practices and good policy to underpin the development of new data-driven services and products within an organization. The example organization introduced in Annex B is a fictional organization, but the resulting questions and example policy statements are generic.

Annex C provides a mapping of the guidance provided in this document to an exemplar Chinese travel service company, to demonstrate the relationship between developing good governance practices and completing the matrix of map areas and considerations.

Annex D gives an overview of data governance policy development for a large and complex industry.

Annex E describes data governance at an air transport IT and communications specialist.

Table 2 below shows an example approach to the collect activity on the data accountability map. It is envisaged that representatives of the governing body and the management team would work through each cell and consider the data collection activities required to support the delivery of the organizational data strategy and over-arching organizational strategy. These considerations should result in the development of policy to direct management activities and performance and conformance measures along with a reporting structure to enable the governing body to monitor the delivery of the strategy.

Table 2 — Collect activity

	Value	Risk	Constraints
Collect considerations	Identify the value to be obtained from collecting data. This assists in determining the quality, quantity and sources of the data required.	Identify the risks associated with the collection of data such that the data strategy and the overarching organizational strategy can be met.	Identify the constraints that apply to the types and sources of data to be collected. These constraints range from legislation and regulation to existing internal policy.
Policy	Once there is an understanding of the types and sources of data to be collected and the associated risks and constraints, a policy can be set to ensure that the collection of data throughout the organization meets the requirements of the data strategy. This policy in turn can be used to determine appropriate measurements and reporting mechanisms to enable the governing body to monitor the delivery of the organizational data strategy.		

Annex A
(informative)

Example worksheets

The set of tables below provide a set of example worksheets for setting policy and understanding existing standards and guidance that can support the successful delivery of the data strategy. Each table in the set takes into considerations the guidance from ISO 38505-1 for each different point on the data accountability map and proposes a suitable policy focus, some data management options, suggestions for monitoring the performance and conformance and related standards and guidance to assist with the implementation of policy. The examples shown are not exhaustive and it is expected that organizations use these worksheets and extend them as required for their organization.

The codes “V1, R1, C1” and so on represent “Value row 1, Risk row 1, Constraints row 1” and are only to simplify cell references in the table.

Table A.1 — Collect

Value		Risk		Constraints	
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.**
Policy focus	The degree of being a "data business". e.g.: *Our focus is always on delivering a product that meets customer expectations including quality, timeliness and reliability of the service. Data use will support that goal.*		Acceptable level of data risk. The governing body decides the level of risk that the organization is prepared to take in order to achieve the strategic goals. e.g.: *We will only collect detailed data, such as location data or address, from our paying customers.*		V1 + R1. Using the value/risk balance, the governing body sets the boundaries for the use of data. *e.g.: Company policy will include the regulations of the regional markets, and in those regions, we will adopt the most restrictive requirements (e.g. in Western Europe we will default to German law unless otherwise stated).*
Data management options	Ways to collect data of value: — Buying/subscribing to data — Collecting Big Data — Internet of Things/sensors — "Real-time" data feeds (Really Simple Syndication (RSS), OData…)		Data collection risks and risk management considerations: — Quality of data collected — Different data quality dimensions including completeness, consistency, uniqueness, validity and accuracy — Input verification — Avoidance of input scripts — Man-in-the-middle attacks — Address validation — Fraud detection		Data Collection constraints management considerations: — Privacy – notice and consent — Data use and transparency — Consolidating and updating personal information — Policy enforcement in email
Monitoring performance and conformance	Ensuring valuable data is being collected: — Recording which data collections are being used for decision-making — Recording data-enabled decisions — Data classification		Ensuring data risk is managed: — Submitting responsibilities for approval — Submitting collection process for approval		Ensuring data constraints are being managed: — Allocating collecting resources — Making a list of regulation and legislation

Table A.1 *(continued)*

Value		Risk		Constraints	
Related standards		ISO 31000, on principles and guidelines for risk management; ISO TS 8000, on data quality; ISO TR 31004, on guidance for risk management.		ISO/IEC 29100, on privacy framework; ISO/IEC 19944, on data flow, data categories and data use.	

Table A.2 — Store

Value		Risk		Constraints	
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.**
Policy focus	Resource allocation. e.g.: *It is essential that we know what data is being used by the organization. Therefore, data storage and data subscription services must be approved (but not necessarily managed) by the IT department.*		Adequate controls and levels of trust based on V1 + R1 + V2. e.g.: *Our organization will be 27001 certified – and this certification should be maintained.*		V2 + R2 + C1 e.g.: *Customer identified data must be stored within the customer region. Anonymized data can be stored at corporate headquarters.*
Data management options	Value in Storage — Cloud computing — Data subscriptions — Virtualization (Servers, Disks, networks)		ISMS — ISO/IEC 27000 series — NIST Cybersecurity framework — Security Incident Management Cloud computing risk management — Service level agreements — Portability and Interoperability — Data flows and use statements		Constraints and metadata — Metadata for constraints, ensuring constraints stay with the data
Monitoring performance and conformance	Ensuring appropriate data storage is being allocated: — Data storage is ready for data store		Ensuring valuable and sensitive data is stored securely: — Data security policy has been implemented		Ensuring data is stored in compliance with internal policy and the legislative and regulatory environment: — Evaluation reporting for data storing.
Related standards	ISO/IEC 17788, on overview and vocabulary for cloud computing; ISO/IEC 17789, on reference architecture for cloud computing; ISO/IEC 19941, on interoperability and portability; ISO/IEC 20000, on service management.		ISO/IEC 27000, on information security management systems; ISO/IEC 27002, on information security controls; ISO/IEC 27017, on cloud services; ISO/IEC 27035-1, on security incident management; ISO/IEC 19086, on cloud computing SLA.		ISO/IEC 27018, on PII processing.

Table A.3 — Report

Value		Risk		Constraints	
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.**
Policy focus	V1 + V2 e.g.: *Reporting tools (that is, tools that extract relevant data for decision-making) should be available to all staff and match their decision-making needs.*		The significance of data in context. e.g.: *Product price reductions must apply to all customers within a region. Exceptions, such as volume sales, to this policy must be approved by the marketing department.*		V1 + R1 + C1 and the importance of the constraints and new constraints in aggregate. e.g.: *Access to data, including its aggregation from any data source(s) is only for legitimate business use.*
Data management options	Extracting value from data — Big Data analysis — Business data from sensors — Machine learning and AI (Artificial Intelligence) — Business intelligence		Delivering information accuracy — Meta data management — Data lineage		Managing data sets — Data aggregation — Combining internal and external datasets
Monitoring performance and conformance	Ensuring analysis of data for the maximum value — Data analysis model is ready and suitable for business		Ensuring reduction of risk related with reporting — Data reporting is aligning with the business target		Ensuring the staff have enough knowledge to reporting — The ability for data reporting
Related standards					ISO/IEC 20889, on privacy enhancing data de-identification techniques.

Table A.4 — Decide

Value		Risk		Constraints	
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.**
Policy focus	V1 + data culture for the organization. e.g.: *Decisions and the data associated with them should be captured to improve the learning cycle.*		V1 + R1 + appropriate delegation. e.g.: *Decisions, whether human or automated, cannot exceed the authority assigned to those responsible for the decisions.*		Expectations for the decision process. e.g.: *To ensure good (and defensible) decisions, they should be made using validated data.*
Data management options	Data for decision-making — Delivering reports and data feeds to end users — AI assistants		Interpreting reports — Biases and discrimination — Automated decision-making		Organizational learning — Closed-loop reporting — Learning systems
Monitoring performance and conformance	Ensuring formulation of a data culture for data-enabled decisions — A decision-making mechanism based on the data culture		Ensuring reduction of risk for data-enabled decisions — The process of decision-making should be monitored		Ensuring the right person makes decisions — The responsibility for decision-making should be recorded
Related standards					

Table A.5 — Distribute

Value		Risk		Constraints	
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.**
Policy focus	V1 + data distribution policy. e.g.: *When customers buy our product, they also receive data associated with the delivery and use of the product.*		Adequate controls. e.g.: *Data that can be shared at no cost will only be available from the "data-sharing" network partition. Paid data subscriptions have a higher value and risk and are distributed only via the "data-subscription" network partition.*		Appropriate distribution rights, including incoming and outgoing. e.g.: *Data can only be shared with suppliers when there is a confidentiality agreement in place.*
Data management options	Data distribution options — Data feeds (RSS, oData, websites, downloads) — Email alerts for customers and suppliers		ISMS — Alerting tools for management		Managing data rights issues — Copyright, licensing — Software asset management
Monitoring performance and conformance	Ensuring the distributed data is valuable to the customer — Distribution is based on appropriate options — The audience needs the distribution		Ensuring data distribution is under control — Monitor and review alert reports regularly		Ensuring data distribution takes legislation into account — All distribution should be made in accordance with privacy policy
Related standards					ISO/IEC 19770, on software asset management.

Table A.6 — Dispose

Value		Risk		Constraints	
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.**
Policy focus	V1 e.g.: *Data that is incorrect or out of date should be corrected or disposed of.*		R2 + appropriate process e.g.: *To reduce the risk of exposure, a customer's personal details should be removed from our systems within 18 months of the customer no longer using our services.*		R2 + C5 + adequate processes e.g.: *The legal department will inform the CEO of changes to data retention laws and regulations. Such reviews should happen at intervals not exceeding yearly.*
Data management options	The value of data disposal — Choose disposal tools		Managing data disposal — People, processes, technologies — Ensuring data disposal in the cloud		Managing data retention and disposal processes — Tracking metadata of data needed for retention
Monitoring performance and conformance	Ensuring an approved procedure for disposal has been implemented — Procedure review		Ensuring the processes of disposal are controlled and aligned with organizational risk policy — Review the evidence of data disposal		Ensuring data disposal satisfies legislative and regulatory requirements — Review related legislation and regulation
Related standards			ISO/IEC 19086, on cloud computing SLA; ISO/IEC 29100, on privacy framework.		

Annex B
(informative)

Applying the guidance — example coffee shop

B.1 General

In the process of developing the guidance presented in the body of this document, it is useful to refer to case study material. This annex presents a fictional case study, developed through considering how the guidance can be applied and how positive strategic outcomes can be supported, by following the guidance presented in this document. This case study provides the opportunity to explore the value that strategic use of data can bring to a business, through enabling the development of new products and services or through delivering existing products and services in a smarter or more efficient way.

B.2 Setting the scene

Consider a fictional business — the Example Coffee Shop Company or ECS. Through good customer service, consistent quality products and a reliable supply chain, this organization has grown to 50 coffee shops spread across the country.

ECS has a governing body consisting of a board of five directors. Recently, two directors, Chi and Lockie, did a routine store visit as "customers" and noticed some opportunities for expansion. It became clear to them that many of the ECS customers walk past similar coffee shops just to get to ECS, where the shop baristas serve their favourite coffee very quickly. These baristas know the names of most of their customers, as well as the coffee they like.

However, the directors know that after the morning rush, there isn't much profit in their business. Virgil, the manager of this particular shop, knows that many of his customers work close by in the city in fairly important jobs. He knows that they like his coffee, but during the day they will use the coffee machines in the office instead of going back to ECS. After discussing this with a few customers, Virgil thinks the problem isn't the time it takes to walk to ECS, or even the time is takes to make their favourite coffee. The biggest problem is that the customers can't risk being in a long line waiting to order.

Virgil knows an easy solution that is to utilize the video feed from the security camera that is already installed in the shop. Simply by feeding that out to the internet, the customers can use their web browsers to access the feed and see for themselves what the length of the order line is. Then when the customers can see the line is short, they'll walk to the shop and get their coffee. Not only is the problem solved for the customers, but also will ECS increase their daily revenue and have a steadier and more manageable flow of customers. Problem solved. Or is it?

The directors see some issues. The first is around security and maybe privacy. Even if Virgil can get each customer to sign a waiver to say that it's ok to video them in the shop (which ECS does for security anyway), putting it out on the internet can be an issue. And of course, it would be unacceptable to ask every potential customer to sign a disclosure statement before they enter the shop.

So Chi and Lockie sit down together and examine the problem and solutions in more detail. They quickly realize that the issue they are dealing with involves a strategic business initiative based on data. In other words, their solution to increase sales made after the morning rush of customers involves giving their customers more information about the status of the coffee shop.

Chi and Lockie gather the board of directors to look at not just this issue, but to think more broadly about the strategic possibilities. The length of the queue in a shop is just one data point that ECS would like to share with their customers. What other data can ECS make available and to whom? Is data the extra ingredient they need in their coffee to drive the business?

Having used ISO/IEC 38500 to ensure the right behaviours around the governance of IT, the board decides to use ISO/IEC 38505-1 to examine the governance of data. ISO/IEC 38505-1 helped them understand that their organizational goals can be delivered through a well-thought-out data strategy and data governance framework (as shown in Table B.1).

Table B.1 — Example organizational goals

Example Coffee Shop *Your community, your coffee*	***ECS Organizational Purpose*** *The purpose of ECS is to create a friendly, feel-at-home environment where our customers can relax, yet achieve their lifestyle goals with healthy food and drink. They feel good about purchasing goods in our stores knowing that we support their values of fair trade, fresh produce and supporting the community and environment.* ***ECS Organizational Strategy*** *The strategy revolves around the following three pillars:* — *Feel-at-home* — *Personalized service* — *Faster food* — *Hyperlocal delivery (ordering and delivering for customers within 200 metres)* — *Common interest meetups (using the shops for social clubs)* — *Lifestyle goals* — *Gamifying health (calories, sugar, goals, balanced meals)* — *Feel good about purchasing* — *Share my meal (a charity initiative)* — *Where's your bean? (an initiative to show the grower-to-drinker journey)* ***ECS Data Strategy*** *The data strategy of ECS supports the organizational purpose and strategy by enabling the "3 pillars" and allowing future initiatives with a low risk to our customers and preferred suppliers.* *The competitive advantage for ECS lies in being the first in the market with a knowledge-based system and processes such that customers are personally welcomed and rewarded for reaching their personal lifestyle goals and for supporting others.*

B.3 Applying the guidance

The guidance to help business owners and directors such as Chi and Lockie develop a data strategy, comes in the form of the ISO/IEC 38500 series, in particular ISO/IEC 38505-1 that deals with the governance of data.

Table B.2 shows the sorts of questions that Chi and Lockie can go through with representatives from their management team, using ISO/IEC 38505-1 and this document, and how this translates into a policy to support the delivery of their new data strategy.

The example works through the policy required to meet the requirements for the data accountability map area Collect, but it is envisaged that this process would be repeated for the other five areas on the data accountability map.

Table B.2 — Example Collect policy worksheet

	Value	Risk	Constraints
Collect	**The governing body should decide the degree to which the organization will leverage or monetize data to achieve its strategic objectives.**	**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.**	**The governing body should approve the policies for data collection, taking into account constraints such as quality, privacy, consent requirements and transparency of use.**
Policy focus	Customer data is a key resource: — Data must be accurate; — Customer can see and update relevant data including preferences and lifestyle goals and interests Product data and supply chain data are key ingredients. Additional data (e.g. weather, traffic, charity) can be acquired if appropriately curated.	Data quality and accuracy should be consistent across datasets. Customer data is a key asset and must be collected securely.	Consent must be obtained from customers before collection. Customer PII will not be sold. We will use our data to partner with, but not profit from approved charity organizations.
Data management options	Data collection options: — Smart device — Application updates — Sensor collection Customer identification options. Aggregation and augmentation options: — Can data be collected? — Can we (and do we want to) identify our customers? — What kinds of data do we need? — How can we collect data effectively?	— What processes and controls are in place to protect data? — Who is responsible for customer data? — What definitions need to be put in place? — What kinds of responsibilities should be approved? — How can we ensure data accuracy?	— Can we correctly identify what is PII? — If we collect PII, what rules do we need to comply with for each market in which we operate? — What kinds of technology should be accepted for data collection? — What other policies do we need to ensure we are acting as a good corporate data curator?

Table B.2 *(continued)*

	Value	Risk	Constraints
Example Coffee Shop policy Statements	**Organizational Structure** The board should ensure the establishment of the organizational structure required for efficient data collection, including departmental responsibilities, individual posts and responsibilities. e.g.: — Identifying which departments are involved in data collection; — Identifying which positions and associated responsibilities should be set up in the data-collection-relevant departments; — Noting that the Privacy Officer is responsible for ensuring that customer consent is obtained before customer data is collected. **Value** The board should decide the degree to which the organization will leverage or monetize data to achieve its strategic objectives. **Risk** The board should recognize the risks associated with the collection of data and agree to an acceptable level of 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. e.g.: — The board decides the level of risk that the organization is prepared to make in order to achieve the strategic goals. — Detailed data, such as location data or address, will only be collected from paying customers. — The appropriate method to prove data accuracy will be used. — A data collection audit will be performed every half year. **Constraints** The board should approve the policies for data collection, taking into account constraints such as quality, privacy, consent requirements and transparency of use. e.g.: — Regulation and legislation, relating to data collection, that must be met by the organization will be identified. For example, for PII collection, specific rules must be in place for data collection to ensure compliance with privacy legislation. — The policy should include the regulations of the regional market and ensure that the most restrictive requirements are adopted in each region (e.g. in Western Europe the organization will default to German law unless otherwise stated). — PII should not be collected from persons under 15 years of age. — All collected data will be encrypted for transmission.		
Monitoring performance and conformance	The board should monitor compliance relating to data collection, including preparation, implementation and completion of data collection. e.g.: — In the preparation stage, the scope, object, method and other tasks of the data collection will be determined. — The collection processes will be established and approved. — The collection procedures and associated responsibilities will be tracked for IT auditing purposes. — The collection procedures will be reviewed each half year.		

Annex C
(informative)

Case study example — travel service company

C.1 General

The content of this case study is given for the convenience of users and does not constitute an endorsement.

This Annex provides a case study example of a travel service company and demonstrates how the company is implementing a data strategy through the development of policies.

The travel service company provides a number of transportation services including taxis, special cars, express transport, car hire, buses and enterprise-level travel services. The company recognizes that their core competitiveness is dependent on how they collect and use data, and how they offer an efficient one-stop travel platform with a diverse range of information for drivers and passengers. To accelerate the implementation of their data strategy, the company introduced multiple policies to cover their operations from data collection to data disposal.

C.2 Collect

The company determines the kind of data to be collected based on the value of data items. They have built a data classification dictionary that divides data into three types. The most important data type is "passenger appetites data" and this includes passenger information, place of departure, destination, payment etc. The second type is "driver data" and this includes information about vehicles, the success rate of order-taking, order-taking time etc. The third type is data that reflects the "external environment" and this includes information about weather, road conditions etc. These three types of data are collected from different channels which have been set up for passenger clients, driver clients and third party data. Risks associated with using this collection service have been considered. Software and data use and privacy policy is agreed at both the passenger and the driver side when the service is used for the first time. Users of the service are informed about the scope of data to be collected and its application. The software use agreement and privacy policy released by the company specifies passenger information, such as ID (identification data) (not limited to name, ID card, address, telephone number and so on). For drivers, in addition to ID information, the details of the working unit, vehicle data, traveling certificate and supervision card information are also collected. The method of data collection and the terms of usage of collection data are specified in the use agreement.

The following data polices relate to data collection:

— Data classification policy;

— Data risk policy;

— Privacy policy.

Monitoring activities are in place to check that:

— The data dictionary is prepared for data collection;

— User validation is in place to meet the requirements of the privacy policy;

— Software use agreement signature collection meets the requirements of the data risk policy.

C.3 Store

The company retains a large volume of personal information, and this is regarded as a core company asset. The company has stipulated strict storage strategies for data, to ensure that business continuity measures are in place and an uninterrupted service to customers can be provided. They have developed a two-site-three-centre disaster-tolerant policy, with a data centre and disaster-tolerant centre in one city and a disaster-tolerant centre at a different city. A multi-channel-based communication policy requiring dedicated communication links has been developed. In parallel, an information security policy has been developed to reduce the risk of unauthorized access to data storage.

The following data policies relate to data storage:

— Two-site-three-centre disaster-tolerant policy;

— Multi-channel-based communication policy;

— Information security policy.

Monitoring activities are in place to check that:

— The main data centre/disaster-tolerant centre and the disaster-tolerant centre at a remote city together meet the requirements for the two-site-three-centre disaster-tolerant policy;

— The contract(s) for dedicated telecommunication links meet the requirements for the multi-channel-based communication policy;

— The access control list meets the requirements of the information security policy.

C.4 Report

The company has developed tools and techniques for data analysis and mining to provide recommendations to customers. For example, the tools can provide recommendations for destinations to customers hiring cars, based on customers' interests and available time. Reports show that 80 % of the recommended destinations, on average, turn out to be the first choice of customers. This feature is realized based on the analysis of user data. It is implemented through creating and analysing the user data view.

The following data policy relates to storage:

— User analysis and modelling policy.

Monitoring activities are in place to check the:

— Percentage of recommended destinations taken up by customers;

— Match of the data view and data analysis.

C.5 Decide

The company adheres to a policy of data-based decision-making to minimise any negative impact of subjective factors. The real-time success rate of order receiving and the waiting time are used to influence subsequent decision-making and this will in turn influence future policy. To boost the success rate of order receiving, the company has implemented an incentives mechanism. Any driver finishing 10 or 20 orders each day will receive a bonus.

The following data policy relates to decision-making:

— Data-based decision-making policy.

Monitoring activities are in place to check the:

— Success rate of order receiving;

— Waiting times for passengers.

C.6 Distribute

The main business of this company requires efficient collection, matching and distribution of data. For the distribution process, the company has developed a strict countersignature policy together with a multi-level approval policy. Data that is intended for automatic release is countersigned by law, business, technology, risk and compliance departments. In addition, ten user representatives participate in the ballot that determines whether the information can be released or not. In the past, data release has resulted in significant issues for passengers. Initially, drivers could see passenger remarks and phone numbers. Occasionally passengers who gave negative feedback to the driver, suffered harassment from the driver.

The following data policies relate to distribution:

— Multi-level approval policy for data distribution;

— Countersignature policy for collection of approval by relevant departments and stockholders.

Monitoring activities are in place to check the:

— Countersignature list, to ensure that it meets the requirements of the countersignature policy for a ballot including all relevant departments and user representatives;

— Trajectory of examination and approval.

C.7 Dispose

To set rules for data disposal, the company has developed a countersignature on data disposal policy, a hierarchical approval policy and a data storage duration policy. For disposal purposes, data is classified as core data, key data or common data, based on the level of importance. To guide the management team, data storage times were specified as follows: core data (permanent), key data (10 years) and common data (6 years). In parallel, the company formulated strict data disposal procedures: key data is submitted by the data administrator, before disposal, to the data manager, the technical manager and the business manager for approval before submission to the CIO (Chief Information Officer) for further auditing and verification and then to the Board of Directors for final approval.

The following data polices relate to disposal:

— Countersignature on data disposal policy;

— Hierarchical approval policy;

— Data storage duration policy.

Monitoring activities are in place to check the:

— Countersignature list;

— Trajectory of examination and approval;

— The record of data disposal.

Annex D
(informative)

Case study example — China financial industry

D.1 General

The content of this case study is given for the convenience of users and does not constitute an endorsement.

With the widespread application of big data technology, more and more organizations realize that data has become the most important asset for the organization or even for the entire industry. This case study example involves a regulator that encompasses the full lifecycle of financial instruments from issuance to transaction, involving around 20 core organizations that are a central and essential part of the market, and more than 2 000 registered business organizations such as securities, futures, funds and private placement. The transactions of the industry's product varieties are in a large volume of 350 million per day and have a comparatively complicated structure where one transaction needs at least to go through 3 to 6 institutions before the process comes to a full closure. Also, there are all kinds of transaction models which are changing fast. With this situation, the data in the industry has the following characteristics: huge volume (by the end of 2016, the total size of the industry's structured data reached 4 petabytes), highly structured data, good quality and high added-value. As large amounts of customer, transactional and financial data are subject to multiple verification and audit procedures, it requires a high frequency of data exchange. The large number of institutions, huge data volume and highly structured and comparatively complicated data exchange environment provide great challenges to data governance in the industry.

The industry regulator has played an important role in the healthy development of the industry and built SDOM-WG (Security Industry Data Model Work Group). In terms of data, the SDOM-WG is promoting a data governance initiative, which is aimed at, by establishing a unified framework, guiding, monitoring and evaluating data application process in the whole industry according to the core ideas of ISO/IEC 38500.

ISO/IEC 38505-1 provides principles, definitions and a model for governing bodies to use when evaluating, directing and monitoring the handling and use of data in their organizations; while ISO/IEC 38505-2 establishes association between data governance and data management through strategy, policy, controls, and processes, and puts forward the development methods of data governance about policies. Combining the securities industry's business characteristics, future needs and data strategy, the SDOM-WG has developed data governance policies specific to the regulator to guide data management activities, including identification, development, implementation and improvement.

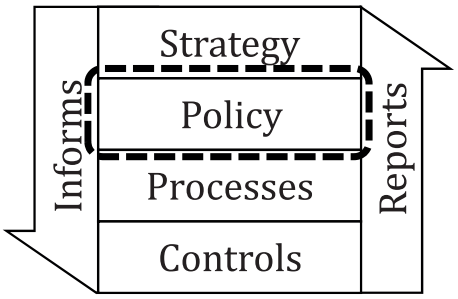


Figure D.1 — Policy development

D.2 Identify

SDOM-WG defines an IBR (Identity, Behaviour, Relevance) methodology which can find out identities such as market participants, objects of transaction, transaction varieties, etc. Then the activities i.e. behaviours in the market are identified, such as account opening, entrusting, closing, liquidating, etc. Next the links among the identities, among the behaviours, and between identities and behaviours are formed from the orthogonal check of the identity tree and behaviour tree (Relevance).

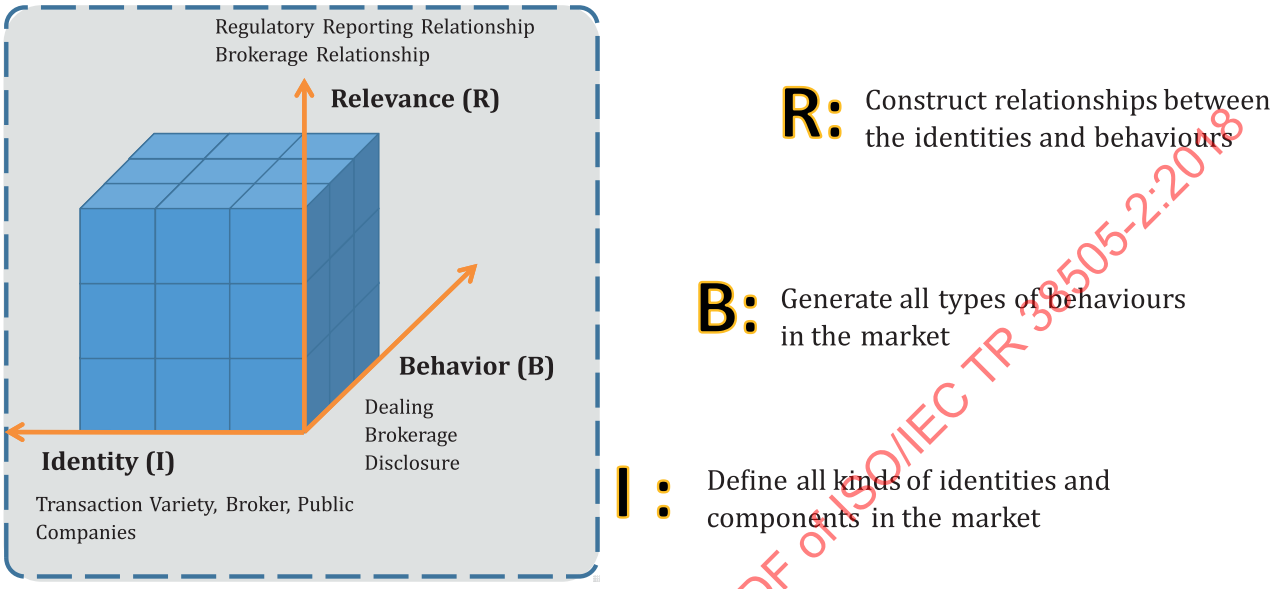
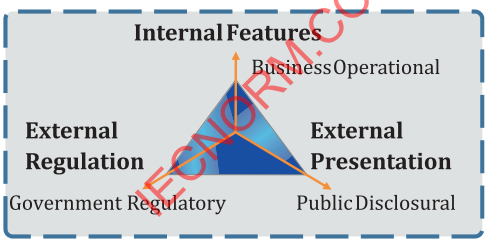


Figure D.2 — Overall methodology of IBR

D.3 Develop

Three major functions are formed by identifying different business activities in the securities and futures industry, i.e. transaction function that is about business operation, information disclosure function that is about public disclosure, and regulatory function that is about government regulation. The IBR methodology is used to analyse related definitions, activities and relationships in each of the three major functions. By considering both data characteristics and compliance requirements, three different methods are used to generate abstract data models.



		Business Operational	Government Regulatory	Public Disclosural
I	Identity	Transaction Varieties	Regulatory Objects	Disclosure Parties, Themes
B	Behaviour	Actions, Processes	Regulatory Themes, Methods	Disclosure
R	Relevance	Business Process	Regulatory and Reporting	Disclosure Catalogue

Figure D.3 — Three business functions

D.4 Implement

These data models are maintained according to the business compliance requirements. Then various industry standards are reviewed through the data models before the standards are certified, so that data semantics can be fully deployed in the industry. Working closely around the deliverables of the industry data modelling, the regulator has developed a set of policies for data governance implementation as follows: develop data governance activities such as industry identity coding specifications, intra-institutional and inter-institutional data exchange, and industry information disclosure; regulate industry standardization based on abstract data models; and guide industry application development based on logical data models. In the process of performing the above policies, the identity classification tree and product tree of the industry are formed, a flow chart of top-level data in the securities and futures industry is prepared, all the to-be-released industry standards are conformed to the models with around 10 000 data definitions in the standards being standardized, and dozens of institutions apply data models and logical models to guide their data application development, involving data in sizes of Petabytes.

D.5 Monitor and Improve

To further promote the implementation of the policies and monitor the actual execution, SDOM-WG built an industry management platform. Abstract models, logical models, industry standards, intra- and inter-institutional data exchange protocols, etc. can all be tracked within the industry's top-level data flow chart, and the relationship with the industry model is also established. The platform conducts regular reviews on the results of the policy execution and performs timely correction and improvement of related issues.

D.6 Conclusion

To conclude, under the framework of international data governance standard, the overall guidance, monitoring and assessment policies of industry data governance are developed. They are successfully implemented in the industry by initial implementations in the following applications.

1) Establish industry-wide data governance practice

The industry data governance method is used to conduct industry data governance practice, generate data policy models for securities companies, and form best practices to guide securities companies to enable their data utilization practice.

2) Integrate industry data resources and enhance data practical value

In the process of establishing industry data governance best practices, various data resources are integrated in the industry with the collective strength of the industry institutions. The best practices built on such integrated data are more general for the industry and better used as industry-wide guidance, therefore the data practical value is effectively enhanced.

3) Strengthen data compliance, risk management and privacy protection

In the process of data governance, comprehensive risk management is considered. Industry models and standards are leveraged to accumulate complete and accurate internal and external data to better serve the purpose of risk identification, measurement, assessment, monitoring and reporting.

4) Build a data governance platform

The overall implementation methodology, rules and final deliverables are integrated into a data practice application platform, which provides a digital and visual presentation of each step of data governance guidance and monitoring. The platform is also used to evaluate the deliverables and conduct tracking of the implementations as shown in Table D.1.

Table D.1 — Governance of data in the industry

	Value	Risk	Constraints	Policy
Collect	The governing body defines the tasks of collection and manages the data as asset.	To protect the completeness and consistency of data, the governing body should guide the management team to standardize the procedure of data management across diverse types of data and institutions. The governing body should guide the managerial team.	The governing body should guide the management team to develop strict format requirements and specifications, taking into account the regulations and legislation specific to the current industry.	All institutions should comply with the data exchange and conversion standard.
Store	The governing body guide the management team to store and manage the data timely, effectively, comprehensively and safely, promote the centralized data storage and protect the feasibility of data application.	To ensure the timely access and backup of data, the governing body should ensure the effective classification of storage and management for different types and massive industrial data.	Effectively and timely monitoring the data by the governing body, sensitive data should be authorized and enciphered by the management team and use different standards for different types of data.	According to the data storage strategy, data storage type and data lifecycle, use different data storage architecture and usage policy.
Report	The governing body should form extraction and analysis rules for industry data, standardize the decision-making procedure based on data and improve the ability of supervision and innovation.	The governing body should supervise the data accuracy in different applied scenarios and ensure the accuracy and timeliness of data analysis for different purposes.	The governing body should guide the management team to ensure that the rules of data extraction are in line with industry logic and the analysis satisfies the industry requirements.	The governing body should meet the corresponding requirements of data extraction and industrial standards.

Table D.1 *(continued)*

	Value	Risk	Constraints	Policy
Decide	The governing body should form extraction and analysis rules for industry data, standardize the decision-making procedure based on data and improve the ability of supervision and innovation.	The governing body should supervise the data accuracy in different applied scenarios and ensure the accuracy and timeliness of data analysis for different purposes.	The governing body should guide the management team to ensure that the rules of data extraction are in line with industry logic and the analysis satisfies the industry requirements.	The governing body should meet the corresponding requirements of data extraction and industrial standards.
Distribute	The governing body should promote data sharing. In order to improve the transparency of relevant information, the governing body should strengthen collaborative work to extract the maximum value of the data.	The governing body should pay attention to data quality attenuation because of internal demand differences, disclosure lag, and deprecated information, all of these will influence the quality of the main data distributing, data security and other risks.	In order to conform, the governing body constraints the format requirements and specifications of data distributing, and the associated process and policy.	The data distributing in the whole industry should conform to the unified template and unified standards of the same information to distribute, while conforming to the regulatory requirements for data distributing.
Dispose	The governing body develops effective systems to reduce costs of data processing and to reduce the risk of data leakage.	The governing body should guide management to avoid losing valuable data.	The governing body should effectively supervise compliance with data health, data security regulations and relevant legislation.	The whole industry in the data processing process should conform to data health, data security and other processes of detailed management restrictions.