International Standard

ISO/IEC 25642

Information technology — Data governance — Data collaboration framework

First edition
2025-10

Reference number
ISO/IEC 25642:2025(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Data collaboration fundamentals **4**
4.1 Decouple data from applications 4
4.2 Access-based collaboration over copy-based integration 4
4.3 Govern and manage data as a product 4
4.4 Enforce controls at the metadata layer 4
4.5 Create metadata-driven experiences 5
4.6 Design for enterprise composability 5
Bibliography **6**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

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

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by DGSI (as CAN/DGSI 100-9:2023 / Rev 1: 2024) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

This is the first revision of the first edition of CAN/DGSI 100-9:2023 / Rev 1:2024, Data governance – Part 9: Data Collaboration Framework.

This revised version incorporates the following amendments:

— Revised title to make it more accessible and add clarity

— Minor updates of terms and definitions to provided added clarity and plain language use

Data collaboration offers a framework for building modular solutions within a controlled data management environment which can be applied either as stand-alone experiences or combined into advanced digital solutions.

This data collaboration framework is designed for an audience of IT professionals facing complex data integration challenges and is intended to accelerate digital transformation projects within organizations.

This document complements the existing International Standards on IT governance (ISO/IEC 38500) and data governance (ISO/IEC 38505-1). It is designed to provide practical guidance for organizations including governing bodies and management to allow them to:

— Build and control new digital capabilities that support universal data access controls.

— Eliminate point-to-point, copy-based data integration from the IT delivery process.

— Support human-to-human, human-to-system, and system-to-system collaboration on operational data. This can include multiple AI systems.

This document is guided by the following core principles:

1. Avoid solution-specific databases (data silos) when building new IT solutions.
2. Adopt a connected or ‘networked’ data management architecture to enable the instant integration of data from legacy and new applications.
3. Make data protection universal by embedding access controls at the *metadata* layer, not the application / code layer.
4. Automate data versioning, recoverability, lineage, and usage reporting.

The sharing and integration of data is crucial to the continued evolution of digital technology, including the effective implementation of artificial intelligence systems.

However, the traditional approach to data sharing is a complex and risky process where information is copied between data silos which often takes the form of application-specific databases and data stores (data warehouses, data lakes).

The result is that control over the access to data is transferred from its rightful owner (e.g., a citizen, team leader, or supply chain partner) to the software that manages the integration process and/or the code that controls individual applications.

This has the following impacts in terms of data governance and data protection:

— The enforcement of uniform access controls is extremely difficult, if not impossible,

— The deletion of data (right to be forgotten/right to erasure) is extremely difficult, if not impossible,

— The porting of customer data between organizations is extremely difficult, and

— The precise reporting (auditability) of data usage is extremely difficult, if not impossible.

These issues pose a significant obstacle to organizations who are required to comply with increasingly strict national and international data privacy, data protection, and AI safety regulations.

This is where the strategic need for modern data governance supported by a data collaboration framework is most notable.

By eliminating copies from the development of new applications, data owners (e.g., customers, team leaders, supply chain partners) can manage a single set of access controls that can be uniformly and universally enforced.

In principle, the reduction of copies and embedding of controls enables organizations to adopt a much more controlled approach to digital innovation that reflects how most societies protect their currency, intellectual property, and identity of citizens.

In addition to the implications for compliance with national and international data protection legal statements, the current copy-based approach to data integration represents a growing “innovation tax” on organizations and a barrier to the productive collaboration on data.

Each new digital solution, whether bought or built, creates a new data silo in the form of an application-specific database. This new silo generally requires some degree of point-to-point integration with pre-existing applications and data stores which in turn creates a complex overhead that grows exponentially over time.

Today, every new application requires organizations to perform more integration which is an increasingly unproductive use of capital and resources.

In contrast, this standard for data collaboration outlines a framework for developing new digital solutions where people and systems (including machine learning, generative AI, and computer vision systems) are able to collaborate on organizational data that is connected across a shared data architecture. This framework leverages modern data management architectures which are based on controlled networks of data capable of reusing data across multiple data models in support of multiple digital solutions rather than requiring application-specific database silos.

For developers, analysts, business users, customers, AI systems, and everyday problem-solvers working within a data collaboration framework, the only barrier to collaboration on operational data is being granted access to it by its rightful owner or their appointed data steward. The access permissions can include the ability to change, delete, add, approve/reject, and query the data.

The major benefit to organizations is that they can use the data collaboration framework to eliminate the escalating cost and compliance risk associated with application-specific databases (aka ‘data silos’ or ‘data fragmentation’) and copy-based data integration.

The impact on the wider economy will also be significant, as access-based collaboration on data is used to accelerate the delivery of innovations in open banking, cleantech, smart cities, and precision healthcare without compromising data protection.

CAN/DGSI 100-9:2023 / Rev 1:2024 was prepared by the Digital Governance Standards Institute Technical Committee 1 (TC 1) on Data Governance, comprised of over 240 thought leaders and experts in data governance and related subjects. This Standard was approved by a Technical Committee formed balloting group, comprised of 5 producers, 2 government / regulator / policymakers, 3 users, and 2 general interests.

All units of measurement expressed in this Standard are in SI units using the International system (SI).

This Standard is subject to technical committee review beginning no later than one year from the date of publication. The completion of the review may result in a new edition, revision, reaffirmation or withdrawal of the Standard. The intended primary application of this Standard is stated in its scope. It is important to note that it remains the responsibility of the user of the Standard to judge its suitability for a particular application.

ICS 35.020; 35.030

Information technology — Data governance — Data collaboration framework

1 Scope

This document specifies minimum recommendations for zero-copy data integration and includes guidance for building modular capabilities within a controlled *data* management environment which can be applied either as stand-alone experiences or combined into advanced solutions.

This document provides a blueprint for IT and other leaders who rely on organizational *data* integrity to perform their functions to support the build of new digital solutions with granular and universally enforced *data* controls.

This document applies to all sectors, including public and private companies, government entities, and not-for-profit *organizations*.

This document is not intended for non-*data* intensive operational roles and does not specify interfaces with other systems or components.

NOTE 1 : This document does not define the specific people or groups who represent the rightful owner of given data – this is to be worked out by individual *organizations.*

NOTE 2 to entry: This document does not force *organizations* into converging on a single *data* ontology, rather, it is intended to support a diversity of *data model*s using the same physical *data*.

NOTE 3 This document does not cover data exchanges or the management of data usage, including potential applications involving artificial intelligence. Guidance for data usage can be found in the following: ISO/IEC 5207 and ISO/IEC 5212.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

3.1
application
product, service or some combination that is specific to the solution of a particular problem

EXAMPLE Customer Relationship Management (CRM), Enterprise Resource, Planning (ERP), Order Management Software (OMS)

Note 1 to entry: *Application* software is computing software designed to carry out a specific task other than one relating to the operation of the computer itself, typically to be used by end-users

3.2
business process
partially ordered set of enterprise activities that can be executed to achieve some desired end-result in pursuit of a given objective of an organization

[SOURCE: ISO/IEC/IEEE 24765:2017]

3.3
collaboration
process of two or more people, groups, *organizations*, or systems working together to complete a task or achieve a goal

Note 1 to entry: *Collaboration* is similar to cooperation but generally involves a greater degree of focus and critically does not require a transfer or degradation of ownership of resources

3.4
conforming application software
application software providing *data* protection conforming to this document

3.5
data
reinterpretable representation of information in a formalized manner suitable for communication, interpretation or processing

Note 1 to entry: *Data* can be processed by humans or by automatic means

[SOURCE: ISO/IEC 2382-1:2015, 2121272, modified.]

3.6
data custodian
party (*person* or *organization*) that has been selected by a *data owner* to be temporarily responsible for managing the associated protection sphere of their *data*

Note 1 to entry: In this document, a *data custodian* is understood to operate in accordance with the requirements set by the authority having jurisdiction.

Note 2 to entry: A *data custodian* may be a trusted advisor e.g., family doctor, a colleague, or a *data steward*.

3.7
data domain
boundaries for one or more sets of data that reside within a *data* management environment

Note 1 to entry: These boundaries are used to identify the organizational users or groups who define access rules and quality parameters for the data stored within the *data domain*

Note 2 to entry: *Data domain*s may be subdivided into one or more *data product*s

3.8
data model
graphical, lexical or combined representation of *data*, specifying their properties, structure, and interrelationships

Note 1 to entry: *data model*s respect the controls set by *data product*s which in turn reflect the access and other controls established by *data domain*s and *data owner*s

[SOURCE: ISO/IEC 11179-1:2022. modified]

3.9
data owner
person having responsibility and authority for the data

[SOURCE: ISO 14292: 2012]

3.10
data product
concept within *data* governance that defines the boundaries for one or more sets of data that reside within a *data domain*

Note 1 to entry: These boundaries identify the people, groups, or some combination who define access rules and quality parameters for the data stored within the *data product*, which itself is hosted within a *data domain*

Note 2 to entry: A *data domain* can also represent a *data product*

3.11
data schema
physical implementation of a *data* model in a specific *data* management system

Note 1 to entry: A data schema can include implementation details such as *data* types, classifications, and access controls

3.12
data silo
storage environment for operational *data* that is specific to an individual *application* or system and not part of an interconnected network of data

3.13
data steward
role within an organization responsible for ensuring that data-related work is performed according to policies and practices as established through data governance

[SOURCE: ISO/IEC 38505:2015]

3.14
governing body
person or group of people who are accountable for the performance and conformance of the organization

[SOURCE: ISO/IEC 38500:2015]

3.15
metadata
data that define and describe other *data*

[SOURCE: ISO/IEC 11179-1:2022]

3.16
modularity
set of characteristics which allow systems to be separated into discrete modules and recombined

[SOURCE: ISO 22166-1:2021]

3.17
organization
person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, nonprofit, charity, or institution, or part or combination thereof, whether incorporated or not, public, or private

[SOURCE: ISO/IEC 38505:2015 modified]

3.18
solution provider
organization involved in the development, deployment, or maintenance of the *application*

3.19
zero-copy application
digital solutions that leverage a shared data architecture and do not incorporate a dedicated database that can exacerbate copy-based data integration. Crucially for data governance, they preserve the data access controls set by data owners as *metadata*

EXAMPLE application-like experiences, workflows, real-time systems, automations, and dashboards

4 Data collaboration fundamentals

4.1 Decouple data from applications

4.1.1 The *governing body* should avoid creation of *application*-specific *data silo*s when adding new *application*s and *application* functionality.

4.1.2 The *governing body* should adopt a shared *data* architecture enabling multiple *application*s to collaborate on a single shared physical copy of *data*.

4.1.3 *The governing body* should continue to support the use of *application*-specific *data schema* without the need to generate *application*-specific *data* copies.

NOTE 1 The governing body may refer to ISO/IEC TS 38505-3, Information technology — Governance of data - Part 3: Guidelines for data classification, for guidance on the use of data classification for its data schema.

4.2 Access-based collaboration over copy-based integration

4.2.1 The *organization* should manage and reuse *data* across *application*s in such a way that *collaboration* on *data* (e.g., create, read, update, delete, query) can take place in real time without the need to create *application*-specific copies of *data*.

4.2.2 The *organization* should use owner-defined access controls to limit who can view, edit, delete, create or query *data* at a granular level (i.e., cell-level, where possible) facilitating controlled sharing of *data* between users and groups.

NOTE 1 The organization may refer to ISO/IEC 29146 for guidance for access management controls.

4.2.3 The *organization* should make access controls and grants interoperable between collaborative environments (i.e., span their digital supply chain) to facilitate secure *collaborationbetween* environments.

NOTE 2 There are environments where zero-copy architecture is technically constrained and may not be viable due to performance, latency, or security segmentation constraints (e.g., edge AI, offline systems).

NOTE 3 Systems may integrate with established security and access control standards, such as OAuth 2.0 for secure authentication and XACML for fine-grained authorization, to ensure interoperability, scalability, and robust protection of resources.

4.3 Govern and manage data as a product

4.3.1 The *governing body* should manage *data owner*ship around aligned *business processes* establishing governance boundaries for one or more sets of data that reside within a *data* management environment. These boundaries identify the people or groups who define access rules and quality parameters for the data stored within the domain.

4.3.2 *Data owner*s should have the ability to assign temporary and revocable control to third-party custodians (i.e., people, intelligent agents) who can control access to their *data*.

4.4 Enforce controls at the metadata layer

4.4.1 *Data owner*s or their designated custodians should have the ability to define granular access policies to manage access for people, groups (or some combination of these) and *application*s and *zero-copy experiences* limiting what they can view, change, delete, approve, reject, or create. Where required, platforms should be designed to support granularity down to a single *data* value, regardless of the *data* management paradigm in use (e.g., tabular, graph, etc.). For example, in a tabular *data* environment, controls should be configurable down to a single *data* cell (i.e., beyond table, row or column-level). Once configured,

access controls should be enabled such that the owner-defined policies are enforced consistently across all *application*s that operationalize the *data*.

NOTE 1 The *governing body* may refer to ISO/IEC 29146 for guidance for access management controls.

NOTE 2 Metadata layer controls are complementary to, not a substitute for, existing layered security approaches. This supports compatibility with enterprise security architectures.

4.4.2 The *governing body* should avoid use of *application* code to determine which users or systems can access or change any particular piece of *data*, instead delegating to the *data*-layer controls to enforce consistency.

4.5 Create metadata-driven experiences

4.5.1 The *organization* should seek to use *metadata* as an operational asset, incorporating it into data models in order to create more controlled, intelligent, and adaptive digital solutions. This approach also helps to minimize complex coding.

4.6 Design for enterprise composability

4.6.1 The *organization* should design for *modularity* where new *application*s can be added, removed, enhanced, fixed, or replaced without requiring *data* copying or migration.

NOTE 1 The organization may refer to ISO/IEC 19941 and ISO/IEC 21838 for test criteria related to interoperability to support the verification and conformance of modular components.

Bibliography

[1] CAN/DGSI 103-1:2024, Digital Trust and Identity – Part 1 – Fundamentals

[2] ISO/IEC 2382:2015, *Information technology — Vocabulary*

[3] ISO/IEC 11179-1:2022, *Information technology — Metadata registries (MDR) - Part 1: Framework*

[4] ISO/IEC 19941:2017, *Information technology — Cloud computing — Interoperability and portability*

[5] ISO/IEC 21838:2021, *Information technology — Top-level ontologies (TLO) Part 1: Requirements*

[6] ISO/IEC 29146:2024, *Information technology — Security techniques — A framework for access management*

[7] ISO/IEC 38500:2024, *Information technology — Governance of IT for the organization*

[8] ISO/IEC/TS 38505-3:2021, *Information technology — Governance of data — Part 3: Guidelines for data classification*

ICS 35.020
Price based on 6 pages

iso.org