DRAFT International Standard

ISO/IEC DIS 15944-19

Information technology — Business operational view —

Part 19: eBusiness, jurisdictional domains, and cross-border data flows (CBDF) requirements

ICS: 35.240.63

ISO/IEC JTC **1**/SC **32**

Secretariat: **ANSI**

Voting begins on:
2026-06-08

Voting terminates on:
2026-08-31

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 15944-19:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **2**

4 Abbreviated terms **26**

5 Fundamental privacy protection principles **28**
5.1 Overview 28
5.2 Primary sources of privacy protection principles 29
5.3 Key eleven (11) privacy protection principles 29
5.4 Link to "consumer protection" and "individual accessibility" requirements (see ISO/IEC 15944-8:2012, 6.3) 30

6 Fundamental Principles and rules governing cross-border data flows (CBDF) of sets of recorded information (SRIs) pertaining to (any type) of business transaction **31**
6.1 Role of a source jurisdictional domain (SJD) as the basis of CBDF external constraints on personal information (PI) in a business transaction and associated rules 31
6.2 Rules governing equivalencies of CBDF requirements on personal information among differing jurisdictional domains in a business transaction context 33
6.3 Rules supporting ILCM "under control of" requirements pertaining to a business transaction in an added CBDF context 34
6.4 Rules governing data residency and data sovereignty requirements applicable to a business transaction 36
6.5 Rules governing cross-border data flow rules (CBDF) pertaining to cloud computing in a business transaction context including CBDF of personal information (PI) 38
6.5.1 Overview and identification of relevancy of earlier CBDF related concerns and related issues already being noted and supported in the development of the multipart ISO/IEC 15944 series of eBusiness standards 38
6.5.2 Open-edi perspective and business transaction rules pertaining to use of a cloud computing service in a CBDF context focusing on personal information 39
6.6 Rules governing privacy protection transactional integrity (PPTI) requirements in a CBDF context 39

7 Summary Rules governing the use of an "agent" or a "third party" in a CBDF related requirements context **40**
7.1 Overview 40
7.2 Summary rules governing the use of an agent in a CBDF related requirements context 41
7.3 Summary rules governing the use of a third party in a CBDF related requirements context 41

Annex A (informative) **Consolidated controlled vocabulary definitions and associated terms, as human interface equivalents (HIEs), English and French language equivalency in the IT standardization context** **43**

Annex B (normative) **Extract of existing Rules (and associated Guidelines stated in parts of ISO/IEC 15944 relevant to cross border data flows (CBDF)** **47**

Annex C (normative) **Business Transaction Model (BTM): Classes of constraints** **89**

Annex D (informative) **Notes on referential integrity and privacy protection transactional integrity in Open-edi among IT-systems** **93**

Annex E (informative) **Introduction to the ISO/IEC 14662: Open-edi reference model** **95**

Annex F (informative) **Link to ISO/IEC 15944-1 Business Operational View (BOV) – Part 1 Operational Aspects of Open-edi for implementation** **97**

Annex G (informative) **Link to ISO/IEC 15944-5 and ISO/IEC 15944-8** **100**

© ISO/IEC 2026 – All rights reserved

Annex H (normative) **List of parts of the ISO/IEC 15944 series of eBusiness standards** **101**
Bibliography **102**

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 documents 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 *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. ISO 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.

This document was prepared by Technical Committee ISO/IEC JTC 1 Information Technology, Subcommittee SC 32, Data Management and Interchange.

A list of all parts in the ISO 15944 series can be found on the ISO website.

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.

© ISO/IEC 2026 – All rights reserved

Introduction

0.1 Purpose and overview

A key aspect in the development of the multipart ISO/IEC 15944 series of eBusiness standard is the recognition of the need for these standards to have the ability to be able support external constraints which apply (or are invoked) based on the nature of the good, service, and/or right (GSR) forming the goal of the business transaction). The primary source of external constraints is legal and regulatory requirements in jurisdictional domains.

Here ISO/IEC 15944-5 focused on the identification and referencing of jurisdictional domains. Part 5 also provides rules governing the same based on the UN system. In addition to identifying levels of regulatory regimes, use of official (or de facto) languages, etc. Part 5 introduces public policy requirements, the three major sub-types of which are consumer protection, privacy protection and individual accessibility. This is because that where the buyer in a business transaction is an "individual", i.e., as differentiated from an organization or public administration, external constraints of a public policy nature apply, i.e., as required by the source jurisdictional domain (SJD) where the business transaction takes place (or is deemed to take place). As such ISO/IEC 15944-8 focuses on the identification governing privacy protection requirements as a set of external constraints on business transactions

The types of external constraints require precise and systematic information/data management of any and all personal information (PI) pertaining to a business transaction. Here ISO/IEC 15944-12 provides the rules and detailed specifications (down to the granular data element level) needed to support privacy protection requirements (PPR) on all stages of information life cycle management (ILCM) and EDI of personal information[1)].

It is in the context of these existing Parts of ISO/IEC 15944, that this document addresses the added layer of external constraints of a cross-border data flow (CBDF) nature and focuses on those pertaining to CBDF of personal information (PI).

As such the propose of this document is two-fold, namely,

— to present the approach to CBDF requirements in a business transaction context while doing so with an (initial) focus on privacy protection requirements (PPR); and,

— to identify those rules (and associated guidelines) already found in existing Parts of ISO/IEC 15944 and explain to relevance of application in the context of meeting I their application to CBDF requirements.

0.2 Use of ISO/IEC 14662 "Open-edi reference model" focus on the Business Operational View and the ISO/IEC 15944 series of e-Business standards[2)]

It is important that readers and users of this document familiarize themselves with the ISO/IEC 14662*"Open-edi reference model"*[3)] One key aspect of this eBusiness reference model is that it introduces two views for modelling a a business transaction, namely,

— the Business Operational View(BOV); and,

— the Functional Services View (FSV).

The purpose of the BOV is that it is designed and has been implanted to capture key common co business requirements in a systematic in a rule-based approach, a.ka., as an axiomatic based ontology and at the same time ensure that external constraints of a legal and regulatory nature can be supported.

(See further below, Annex G for an "*Introduction to the Open-edi reference model*").

1) Although ISO/IEC 15944-12 focuses on ILCM and EDI of personal information, the rules and specifications it contains are of general applicability and deemed to be essential to good data governance not only in an EDI context but also within the organization itself.

2) ISO/IEC 15944 is a multipart eBusiness standard which is based on and focuses on the BOV perspective of the ISO/IEC "*Open-edi reference model"*

3) This is an ISO/IEC JTC1 "no cost available standard

© ISO/IEC 2026 – All rights reserved

There are several Parts of the multipart ISO/IEC 15944 series of eBusiness standards (with the common title of "*Information technology – Business Operational View* " which are of particular relevance to the development of this document. Here ISO/IEC 15944-1 "…*Part 1- Operational aspects of Open-edi for implementation*" serves as a foundational standard for the multipart ISO/IEC 15944 series of standards. All the subsequent parts of ISO/IEC 15944 series of standards are basically "subdivisions" of Part 1 and completely aligned with Part 1. Some key elements of Part 1 are summarized in Annex H.

In addition to the above two foundational standards, ISO/IEC 15944-5, -8, and -12 also serve as a basis for the development of this document. In their context, this document focuses on the CBDF requirements as a specified added set of particular external constraints. (See further below Annex I on the links of this document to these three Parts of ISO/IEC 15944).

Further, it is noted that ISO/IEC 15944-17 which focuses on "Privacy-by-Design" (PbD) contains an Annex C which provides a cross-mapping between the eleven (11) Privacy Protection Principles (PPP) and the seven (7) PbD principles. There is a strong link and complimentarity between PbD standards work (which is consumer protection oriented) and privacy protection requirements (See further Clause 6.32 in Clause in ISO/IEC 15944-5, and Clause 7.2.2 in ISO/IEC 15944-8).

0.3 Importance and role of terms and definitions[4)]

The ISO/IEC 15944 multipart standard sets out the processes for achieving a common understanding of the Business Operational View (BOV) from commercial, legal, ICT, public policy and cross-sectoral perspectives. It is therefore important to check and confirm that a "common understanding" in any one of these domains is also unambiguously understood as identical in the others.

This sub-clause is included in each Part of ISO/IEC 15944 to emphasize that harmonized concepts and definitions (and assigned terms) in its Parts are essential to the continuity of the overall standard..

In order to minimize ambiguity in the definitions and their associated terms, each definition and its associated term has been made available in at least one language other than English in the part in which it is introduced. In this context, it is noted that ISO/IEC 15944-7 eBusiness vocabulary already also contains human interface equivalents (HIEs) in ISO Chinese, ISO French, and ISO Russian.[5)]

0.4 Based on rules and guidelines[6)]

This document is intended to be used within and outside of the ISO and IEC by diverse sets of users having different perspectives and needs with respect to the nature of their business transaction {See below Figure F.1 in Annex F.}

This Business Operational View (BOV) standard, like the others, focuses on providing" precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose"[7)]. The BOV rules have as their basis common business

4) All the terms and definitions of the current editions of the ISO/IEC 14662*Open-edi Reference Model* and the multipart ISO/IEC 15944 eBusiness standard have been consolidated in ISO/IEC 15944-7. A primary reason for having "Terms and definitions" in a standard is because one cannot assume that there exists a common understanding, worldwide, for a specific concept. And even if one assumes that such an understanding exists, then having such a common definition in Clause 3 serves to formally and explicitly affirm (re-affirm) such a common understanding, i.e., ensure that all parties concerned share this common understanding as stated through the text of the definitions in Clause 3.

5) The designation ISO before a natural language refers to the use of that natural language in ISO standards.

6) This introductory clause is primarily based on that found in ISO/IEC 15944-1, Clause 6.1.2 titled "*Standard based on rules and guidelines*". For definition of "standard", see below Clause 3.64.

7) This text n quotes is based on an earlier ISO/IEC definition of a standard. It remains valid for the development of this document.

© ISO/IEC 2026 – All rights reserved

operational practices and functional requirements., i.e., as internal constraints (as found in Parts 1,2 4 9 and 10 of ISO/IEC 15944) as well as external constraints as found) and existing Parts 5,8, 12 of ISO/IEC 15944[8)].

These rules also serve as a common set of understanding bridging the varied perspectives of the commercial framework, the legal framework, the information technology framework, standardisers, consumers, etc.[9)]

The Open-edi based ISO/IEC series of eBusiness standards not only support this rule base approach but in support the same using the following approach

It is essential that all the rules in a ISO/IE 15944 standard are identified and be able to be referenced in a required unique and unambiguous manner using **bold** text in their representation; and are assigned unique sequentially enumerated Rule IDs, i.e., as **Rule nn1**, **Rule nn2**, etc. of the same; and,

in order to provide for the fact that a Rule may have one or more supporting Guidelines, any associated ***Guidelines*** also have their own unambiguous identification and representation, they presented in ***italicized bold text*** with their identification inheriting the Rule ID of which they are part, i.e., ***as Rule nnn/ G1,Rule nn/G2***, etc.

It is noted that these enumerated Rules, and associated Guidelines provide a very systematic approach which is essential to the modelling of business transactions. This approach also supports cross-referencing among the rules, including inter-dependencies among the same

Note Algorithms are by their very nature rule-based. As such this approach by ISO/IEC 15944 facilitates the development of supporting algorithmic implementations as well as associated axiomatic ontologies.

0.5 Development of Part 19 based on existing applicable existing rules (and associated guidelines) found in relevant existing Parts in the multipart eBusiness series of ISO/IEC 15944 standards

On the whole, CBDF requirements represent a set of particular external constraints which are viewed as supplemental to those already identified and specified in existing Parts of ISO/IEC 15944. However only a subset of these rules (and associated guidelines) is impacted by CBDF requirement when and wherever the actualization of a business transaction involve data flows crossing one or more jurisdictional domains. Therefore, in order not to duplicate the set of existing rules and associated normative text, Annex B was developed. It therefore serves as a detailed normative text of this document.

0.6 Use of “Person”, “organization”, “individual” and “party” in the context of business transaction and commitment exchange

Throughout this document:

— the use of Person with a capital "P" represents Person as a defined term, i.e., as the entity within an Open-edi Party that carries the legal responsibility for making commitment(s);

— "individual", "organization", and "public administration" are defined terms representing the three common sub-types of "Person"; and,

— the use of the words “person(s)” and “party (ies)” without a capital “P” indicates their use in a generic context independent of “Person”, as a defined concept in the ISO/IEC 14662 and ISO/IEC 15944 standards. (NOTE: A "party" to a business transaction has the properties and behaviours of a "Person”).

---

8) In addition to this document there are two Parts of ISO/IEC 15944 which are currently under development which are relevant to this Part. They are,
— Part 18 titled “Common principles and rules for the unambiguous identification and assignment of identifiers in business transactions “, and
— Part 22 titled “Framework for types of commitments in support of data interchanges in a business transaction”

9) The working principle is that of "coordinated autonomy", i.e., all parties are autonomous. Therefore, the extent to which they cooperate, agree on common needs, business rules constraints, practices, etc., and reach agreement on the same in form of precise rules, terms and definitions, etc., is a key influence on the creation of necessary standards as well as common scenarios, scenario attributes and scenario components.

© ISO/IEC 2026 – All rights reserved

0.7 Use of "identifier" (in a business transaction) and roles of an individual[10)]

Clause 6.1.4 of ISO/IEC 15944-1 focuses on the requirement for the unambiguous identification of entities in business transactions. "Unambiguous" is a key issue in business transactions because states of ambiguity and uncertainty are an anathema from commercial, legal, consumer and information technology perspectives. Issues of unambiguousness apply to all aspects of a business transaction and even more so to those which are EDI-based. Open-edi transactions anticipate that all entities are fully and clearly identified prior to the instantiation of a business transaction.

0.8 Use of "jurisdictional domain" in the context of privacy protection and related ILCM requirements

The term "jurisdiction" has many possible definitions. Some definitions of "jurisdiction" have accepted international legal status while others do not. It is also common practice to equate "jurisdiction" with "country", although the two are by no means synonymous. It is also common practice to refer to states, provinces, länder, cantons, territories, municipalities, etc., as "jurisdictions", and in contract law it is customary to specify a particular court of law as having jurisdiction or a defined national body, or an international body as having jurisdiction (even if that is not legally enforceable), and so on. Finally, there are differing "legal" definitions of "jurisdiction". Readers should understand that in this document:

— the use of the term "jurisdictional domain" represents its use as a defined term; and,

— the use of the terms "jurisdiction(s)" and/or "country (ies)" represents their use in their generic contexts and do not imply any legal effect per se.

0.9 Application of "privacy protection requirements (PPR) in the context of a business transaction, EDI and any type of commitment exchange

Jurisdictional domains such as UN member states (and/or their administrative sub-divisions), have enacted various "privacy" laws, "data protection" laws, "protection of personal information" laws, etc., (as well as pursuant regulations). Some of these sources of legal requirements focus on the protection of personal information in IT systems only, (e.g., "data protection"), while others focus on the protection of personal information irrespective of the medium[11)] used for the recording of personal information and/or its communication to other Persons.

In the case of personal information, this is currently defined by most jurisdictional domains to be a specific sub-set of recorded information relating to the Person as an "individual" – where the qualities of such type of Person are that they are required to be an identifiable, living individual. So this may only apply to some proportion of the specific role players in a business transaction (including their personae) and not others.

It has to be borne in mind that the delivery of "privacy protection" requires action both at the business operational level (BOV) and functional services view (FSV) (or technology levels). Where human beings interact with recorded information once it has passed through an Open-edi transaction, they may have the potential to compromise technical controls (FSV) that may have been applied. It is essential that business models take into account of the need to establish overarching business processes that address issues that have not been, and/or cannot be resolved by the technical FSV controls applied so as to provide the overall privacy demands of regulation that are required to be applied to personal data, their use, prescribed dissemination and so on. In this regard, the interplay of the BOV and FSV views of all organizations have to be taken into account.

0.10 Use of "set of recorded information" (SRI) and "set of personal information" (SPI) versus record, document, message, data, etc.

The concepts of "record", "document", 'data", "message", etc., are defined and used in ISO standards and in different levels of jurisdictional domains. However, multiple differing definitions exist for each of these terms in ISO, and in standards applicable legislation and related regulations. To address this polysemy issue,

---

10) This is a summary of ISO/IEC 15944-1, Clause 6.1.4 "*Business transactions: Unambiguous identification of entities".* See also Annex C in ISO/IEC 15944-1 titled *Unambiguous Identification of Entities in a Business Transaction* which provides the informative and explanatory text for the rules and definitions in Clause 6.1.4.

11) "Medium" is a defined concept. {See ISO/IEC 15944-1, Clause 6.4 "*Rules governing the data component"*, and its Clause 6.4.1 "*Recorded information*"}.

© ISO/IEC 2026 – All rights reserved

the unifying concept and definition of "set of recorded information" was already introduced and defined in ISO/IEC 15944-5.

In Open-edi, SRIs are modelled as information bundles (IBs) and semantic components (SCs) when they are interchanged among participating parties in a business transaction. Within the IT systems of an organization, and especially within its Decision Making Applications (DMAs), the recorded information pertaining to a business transaction is usually maintained as one or more (linked) SRIs.

In order to maximize linkages between Open-edi (external behaviour) aspects and data management (internal behaviour) aspects of an organization (as well as associated ISO record management and EDIFACT standards), SRI is used as a common higher level concept, which incorporates essential attributes of the concepts of "record", "document", "message", etc. as defined in various ways in existing ISO standards.

Where and when an SRI is of the nature of personal information or contains personal information privacy protection requirements (PPR) apply. Within the context of PPR and with the focus of ILCM the concept and definition of "set of personal information (SPI)" is as follows:

set of personal information (SPI)

set of recorded information (SRI)*which is of the nature of or contains****personal information***

This document focuses on ILCM of personal information in support of PPR and as such "set of personal information (SPI)" is used throughout this document while "set of recorded information (SRI) when referring to the more generic ILCM aspects.

0.11 Aspects currently not addressed

Currently CBDF of personal information have the highest profile and visibility. However, in a business transaction context, there are other categories of CBDF which are relevant to data flows arising from the provisioning of good, services, and/or rights (GSR). They have not yet been addressed in the 1st edition of this document. Here, at a primitive level, at least six other categories has already been identified (there may be more). They include the following,

— "neutral" data flows

— commercial data flows

— economic data flows

— environmental data flows

— socio-economic data flows; and,

— cultural data flows

It is expected that these will be addressed in the 2nd edition of this document (also in the context of external constraints on business transactions).

Note It has always been understood that CBDF requirements of a national security nature, those pertaining to law enforcement, etc. are excluded from the scope of ISO/IEC 15944 and its Parts.

0.12 Organization and description of this document

Clause 1, 2, and 3 are the mandatory clauses of scope, normative references and terms and definitions.

Clause 4 provides the list of abbreviations used in this document.

Clause 5 introduces the fundamental privacy protection principles as specified in other parts of ISO/IEC 15944 and specifies in this clause that these principles apply the context of CBDF which is the focus of this document.

Clause 6 describes fundamental principles and rules governing cross-border data flows of SRIs pertaining to any types of business transactions.

© ISO/IEC 2026 – All rights reserved

Clause 7 includes rules governing the use of an “agent” or a “third party” in a cross-border data flow context.

Annex A provides the consolidated controlled vocabulary definitions and associated terms as human interface equivalents (HIEs) of the terms and definitions listed in this document.

Annex B provides the list of rules and associated guidelines stated in other parts of ISO/IEC 15944 that are relevant to CBDF.

Annex C introduces the business transaction model in more detail for the readers of this document to understand.

Annex D introduces the referential integrity that may be used in privacy protection issues in eBusiness.

Annex E introduces the ISO/IEC 14662 Open-edi reference model in more detail for the readers of this document to understand.

Annex F, G introduces the link of this document to ISO/IEC 15944 part 1, part 5, part 8, and part 17.

Annex H provides the list of parts of the ISO/IEC 15944 series of eBusiness standards.

© ISO/IEC 2026 – All rights reserved

Information technology — Business operational view —

Part 19: eBusiness, jurisdictional domains, and cross-border data flows (CBDF) requirements

1 Scope

This document

a) identifies and specifies the rules governing cross-border data flow (CBDF) requirements which need to be addressed whenever electronic data interchange (EDI) of any kind takes place among participating parties in a business transaction and where such EDI contains (a) personal information(PI); and, (b) in the instantiation of such a business transaction the PI of the individual, in the role of buyer, crosses into one or more jurisdictional domains.; and (c) where the source jurisdictional domain has legal/ regulatory requirements of privacy protection nature;

b) integrates existing normative elements, i.e., rules (and associated guidelines) in support of privacy protection requirements in a business transaction context as are already identified in ISO/IEC 15944-1, ISO/IEC 15944-2, ISO/IEC 15944-4, ISO/IEC 15944-5, ISO/IEC 15944-8, ISO/IEC 15944-9, ISO/IEC 15944-10, ISO/IEC 15944-12, and ISO/IEC 15944-17 (See Annex B below);

c) focuses on privacy protection requirements (PPR) as,

   1) a set of rights of individual with respect to his/her personal information, granted by the jurisdictional domain in which an individual resides and is relevant to its role as a buyer in a business transaction in the role of a buyer; and,

   2) a set of concomitant obligations of an organization or public jurisdictional domain in the role of seller with respect to any personal information forming part of the business transaction, as and where such personal information crosses one or more borders outside that jurisdictional domain; and,

d) supports referential integrity, privacy protection, and transactional integrity in Open-edi among IT systems involving CBDF of personal information among differing jurisdictional domains.

NOTE Privacy protection requirements (PPR) pertaining to cross-border data flows (CBDF) and EDI of personal information as stated in the document serve as a minimum set of CBDF policy and operational requirements, as well as CBDF in any organization in general.

This document does not specify the technical mechanisms, i.e., functional support services (FSV), which are required to support these business operational view (BOV) CBDF identified requirements.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitute 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.[12)].

12) All references in this sub-clause were correct at the time of approval of this document. The provisions of the referenced specifications, as identified in this sub-clause, are valid within the context of this document. The reference to a specification within this document does not give it any further status within ISO/IEC; in particular, it does not give the referenced specification the status of an International Standard.

© ISO/IEC 2026 – All rights reserved

ISO/IEC 14662, *Information technology — Open-edi reference model*

ISO/IEC 15944-1, *Information technology — Business operational view — Part 1: Operational aspects of open-edi for implementation*

ISO/IEC 15944-5, *Information technology — Business Operational View — Part 5: Identification and referencing of requirements of jurisdictional domains as sources external constraints*

ISO/IEC 15944-8, *Information technology — Business operational view — Part 8: Identification of privacy protection requirements as external constraints on business transactions*

ISO/IEC 15944-9, *Information technology — Business operational view — Part 9: Business transaction traceability framework for commitment exchange*

ISO/IEC 15944-12, *Information technology — Business operational view — Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)*

ISO/IEC 15944-17, *Information technology — Business operational view — Part 17: Fundamental principles and rules governing Privacy-by-Design (PbD) requirements in an EDI and collaboration space context*

3 Terms and definitions

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

For the human interface equivalents (HIEs) of each term in Clause 3 in ISO French, Annex A applies.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
agent
Person (3.72) acting for another *Person* in a clearly specified capacity in the context of a *business transaction* (3.5)

Note 1 to entry: Excluded are agents as "automatons" (or robots, bobots, etc.). In ISO/IEC 14662, "automatons" are recognized and provided for but as part of the Functional Service View (FSV) where they are defined as an "Information Processing Domain (IPD)".

[SOURCE: ISO/IEC 15944-1:2025, 3.1]

3.2
back-up copy of data
copy that is any of the following: (a) additional resource or duplicate copy of *data* (3.18) on different a storage *medium* (3.59) stored off-line for emergency purposes; (b) disk, tape or other machine-readable copy of a *data* or program file; (c) *data* or program file recorded and stored off-line for emergency or archival purposes; and, (d) record that preserves the evidence and information it contains if the original is not available

[SOURCE: ISO/IEC 15944-12:2025, 3.6]

3.3
business
series of processes, each having a clearly understood purpose, involving more than one *Person* (3.72), realized through the exchange of *recorded information* (3.89) and directed towards some mutually agreed upon goal, extending over a period of time

[SOURCE: ISO/IEC 14662:2010, 3.2]

© ISO/IEC 2026 – All rights reserved

3.4
business object
unambiguously (3.110) identified, specified, referenceable, registered and re-useable *Open-edi scenario* (3.69) or *Scenario Component* (3.99) of a *business transaction* (3.5)

Note 1 to entry: As an object, a business object exists only in the context of a business transaction.

[SOURCE: ISO/IEC 15944-2:2015, 3.6]

3.5
business transaction
predefined set of activities and/or processes of *Persons* (3.72) which is initiated by a *Person* to accomplish an explicitly shared *business* (3.3) goal and terminated upon recognition of one of the agreed conclusions by all the involved *Persons* although some of the recognition may be implicit

[SOURCE: ISO/IEC 14662:2010, 3.4]

3.6
business transaction audit trail
chronological record of *IT system* (3.37) activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event pertaining to *sets of recorded information (SRIs)* (3.104) in a *business transaction* (3.5) through all its processes, i.e., from planning to the end of post-actualization

Note 1 to entry: The ability to support a business transaction audit trail is required in order to be able to support privacy protection transactional integrity (PPTI) requirements.

[SOURCE: ISO/IEC 15944-12:2025, 3.11]

3.7
business transaction identifier
BTI
identifier assigned by a *seller* (3.100) or a *regulator* (3.93) to an instantiated *business transaction* (3.5) among the *Persons* (3.72)involved

Note 1 to entry: The identifier assigned by the seller or regulator shall have the properties and behaviours of an identifier (in a business transaction).

Note 2 to entry: As an identifier (in a business transaction), a BTI serves as the unique common identifier for all Persons involved for the identification, referencing, retrieval of recorded information, etc. pertaining to the commitments made and the resulting actualization (and post-actualization) of the business transaction agreed to.

Note 3 to entry: A business transaction identifier can be assigned at any time during the planning, identification or negotiation phases but shall be assigned at least prior to the start or during the actualization phase.

Note 4 to entry: As and where required by the applicable jurisdictional domain(s), the recorded information associated with the business transaction identifier (BTI) may well require the seller to include other identifiers, (e.g., from a value-added good or service tax, etc., perspective) as assigned by the applicable jurisdictional domain(s).

[SOURCE: ISO/IEC 15944-5:2017, 3.12]

3.8
buyer
Person (3.72) who aims to get possession of a good, service and/or right through providing an acceptable equivalent value, usually in money, to the *Person* providing such a good, service and/or right

[SOURCE: ISO/IEC 15944-1:2025, 3.8]

© ISO/IEC 2026 – All rights reserved

3.9
character
member of a *set* (3.102) of elements that is used for the representation, organization or control of data

Note 1 to entry: Characters may be categorized as follows: (a) graphic character: (e.g., digit, letter, ideogram, special character); and, (b) control character: (e.g., transmission control, character, format effect or, code extension character, device control character).

[SOURCE: ISO/IEC 2382:2015, 2121335]

3.10
character set
finite set of different *characters* (3.9) that is complete for a given purpose

EXAMPLE The international reference version of the character set of ISO 10646.

[SOURCE: ISO/IEC 2382:2015, 2121547]

3.11
cloud service provider
CSP
party that is acting in a cloud service provider role

[SOURCE: ISO/IEC 22123-1:2023, 3.3.3]

3.12
cloud service provider data
class of data objects, specific to the operation of the cloud service, under the control of the *cloud service provider* (3.11)

[SOURCE: ISO/IEC 22123-1:2023, 3.9.3]

3.12.1
code (in coded domain)
identifier, i.e., an *ID code* (3.38), assigned to an entity as member of a *coded domain* (3.12) according to the pre-established set of *rules* (3.98) governing that *coded domain*

[SOURCE: ISO/IEC 15944-5:2008, 3.19]

3.12.2
coded domain
domain for which (1) the boundaries are defined and explicitly stated as a rulebase of a coded domain Source Authority (cdSA); and, (2) each entity which qualifies as a member of that domain is identified through the assignment of a unique *IDcode* (3.38) in accordance with the applicable Registration Schema *(RS)* of that *Source Authority (SA)* (3.105)

Note 1 to entry: The rules governing the assignment of an ID code to members of a coded domain reside with its Source Authority and form part of the Coded Domain Registration Schema (cdRS) of the Source Authority.

Note 2 to entry: Source Authorities which are jurisdictional domains are the primary source of coded domains.

Note 3 to entry: A coded domain is a data set for which the contents of the data element values are predetermined and defined according to the rulebase of its Source Authority and as such have predefined semantics.

Note 4 to entry: Associated with a code in a coded domain can be: (a) one and/or more equivalent codes; (b) one and/or more equivalent representations especially those in the form of human interface equivalent (HIE) (linguistic) expressions.

Note 5 to entry: In a coded domain the rules for assignment and structuring of the ID codes are required to be specified.

Note 6 to entry: Where an entity as member of a coded domain is allowed to have, i.e., assigned, more than one ID code, i.e., as equivalent ID codes (possibly including names), one of these are required to be specified as the pivot ID code.

© ISO/IEC 2026 – All rights reserved

Note 7 to entry: A coded domain in turn can consist of two or more coded domains, i.e., through the application of the inheritance principle of object classes.

Note 8 to entry: A coded domain may contain an ID code which pertains to predefined conditions other than qualification of membership of entities in the coded domain. Further, the rules governing a coded domain may or may not provide for user extensions.

EXAMPLE 1 (1) The use of ID Code "0" (or "00", etc.) for “Others, (2) the use of ID Code "9" (or "99", etc.) for “Not Applicable”; (3) the use of “8” (or “98”) for “Not Known”; and/or, if required, (4) the pre-reservation of a series of ID codes for use of “user extensions”.

Note 9 to entry: In object methodology, entities which are members of a coded domain are referred to as instances of a class.

EXAMPLE 2 In UML modelling notation, an ID code is viewed as an instance of an object class.

[SOURCE: ISO/IEC 15944-2:2015, 3.13]

3.13
commitment
making or accepting of a right, obligation, liability or responsibility by a *Person* (3.72) that is capable of enforcement in the *jurisdictional domain* (3.52) in which the *commitment* (3.13) is made

[SOURCE: ISO/IEC 14662:2010, 3.5]

3.14
constraint
rule (3.98), explicitly stated, that prescribes, limits, governs or specifies any aspect of a *business transaction* (3.5)

Note 1 to entry: Constraints are specified as rules forming part of components of Open-edi scenarios, i.e., as scenario attributes, roles, and/or information bundles.

Note 2 to entry: For constraints to be registered for implementation in Open-edi, they are required to have unique and unambiguous identifiers.

Note 3 to entry: A constraint may be agreed to among parties, (condition of contract) and is therefore considered an internal constraint. Or a constraint may be imposed on parties, (e.g., laws, regulations, etc.), and is therefore considered an external constraint.

[SOURCE: ISO/IEC 15944-1:2025, 3.11]

3.15
consumer
buyer (3.8) who is an *individual* (3.41) to whom *consumer protection* (3.16) requirements are applied as a set of *external constraints* (3.33) on a *business transaction* (3.5)

Note 1 to entry: Consumer protection is a set of explicitly defined rights and obligations applicable as external constraints on a business transaction.

Note 2 to entry: The assumption is that a consumer protection applies only where a buyer in a business transaction is an individual. If this is not the case in a particular jurisdictional domain, such external constraints should be specified as part of scenario components as applicable.

Note 3 to entry: It is recognized that external constraints on a buyer of the nature of consumer protection may be peculiar to a specified jurisdictional domain.

[SOURCE: ISO/IEC 15944-1:2025, 3.12]

© ISO/IEC 2026 – All rights reserved

3.16
consumer protection
set of *external constraints* (3.33) of a *jurisdictional domain* (3.52) as rights of a *consumer* (3.15) and thus as obligations (and possible liabilities) of a vendor in a *business transaction* (3.5) which apply to the good, service and/or right forming the *object* (3.64) of the *business transaction* including associated information management and interchange requirements including applicable *set(s) of recorded information (SRIs)*

Note 1 to entry: Jurisdictional domains may restrict the application of their consumer protection requirements as applicable only to individuals engaged in a business transaction of a commercial activity undertaken for personal, family or household purposes, i.e., they do not apply to natural persons in their role as organization or organization Person.

Note 2 to entry: Jurisdictional domains may have particular consumer protection requirements which apply specifically to individuals who are considered to be a "child" or a “minor”, (e.g., those individuals who have not reached their thirteenth birthday).

Note 3 to entry: Some jurisdictional domains may have consumer protection requirements which are particular to the nature of the good, service and/or right being part of the goal of a business transaction.

[SOURCE: ISO/IEC 15944-5:2008, 3.33]

3.17
cross border data flows
CBDF
electronic data interchange (EDI) (3.30) generated by or for a *Person* (3.72) which is transmitted across the border of the *jurisdictional domain* (3.52) of that *Person* to a *Person(s)* in another *jurisdictional domain(s)*

Note 1 to entry: External constraints of a jurisdictional domain on any set of recorded information (SRI) may be: (a) generic in nature; (b) be governed by a (set of) rule(s) or which are agreed to be among two or more jurisdictional domains (c) pertain to EDI of any SRIs which specific to the nature of the good, service and/or right which the seller in a business transaction is offering to a (prospective) buyer.

Note 2 to entry: Where personal information (PI) of an individual is involved, i.e., any EDI of a set of personal information (SPI), it is likely that specific CBDF rules of the jurisdictional domain of a privacy protection requirement (PPR) nature apply and need to be supported by the Persons involved before any CBDF can occur.

3.18
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 2382:2015, 2121272]

3.19
data (in a business transaction)
representations of *recorded information* (3.89) that are being prepared or have been prepared in a form suitable for use in a computer system

[SOURCE: ISO/IEC 15944-1:2025, 3.14]

3.20
data back-up
process (3.82) of duplicating and archiving *data* (3.18), often on a different storage *medium* (3.59), so that it may be restored to its original state after a data loss event

Note 1 to entry: The primary purpose of back-up is to recover data be it by data deletion or corruption.

Note 2 to entry: A secondary purpose of back-up is to be able to recover data from an earlier time according to a predefined retention policy.

[SOURCE: ISO/IEC 15944-12:2025, 3.30]

© ISO/IEC 2026 – All rights reserved

3.21
data conversion
process (3.82) of changing *data* (3.18), i.e.,as *set(s) of recorded information (SRI(s)),* from one format or representation to another while maintaining the characteristics of the *SRIs* including the authenticity, integrity, reliability and usability of the *sets of recorded information (SRI(s))* (3.104) as well as relevant *information life cycle management (ILCM)* (3.48)requirements, and especially those of an *external constraints* (3.33) nature including *privacy protection* (3.79) requirements where the *data* involves *personal information* (3.73)

Note 1 to entry: A characteristics of data conversion is a change in the format used for managing and/or representing the contents of the SRI.

EXAMPLE Data conversion resulting from a change in text processing software (e.g. MsWord to HTML), from one database software to another, from a non-data based software to a database based software approach or vice-versa, etc.

Note 2 to entry: A data conversion does not change the content value of the SRI(s).

[SOURCE: Adapted from CAN/CGSB-72.34-2005, 3.16 and ISO 13008:2001, 3.5]

3.22
data element
unit of *data* (3.18) for which the definition, *identification* (3.40), representation and permissible values are specified by means of a set of attributes

[SOURCE: ISO/IEC 15944-1:2017, 3.15]

3.23
data migration
process (3.82) of moving *data* (3.18), i.e., as *sets of recorded information (SRIs)* (3.104) including their existing characteristics from one *IT system* (3.37), (e.g., hardware or software configuration) to another, as required by changes in an *IT system* configuration or as requested by the user, while assuring that the *SRI(s)* will remain addressable and that data authenticity, integrity, reliability and useability of the *SRI(s)*will be maintained in the new environment

Note 1 to entry: Data migration does not change the format or the content of the SRIs.

[SOURCE: Adapted from ISO 13008:2012, 3.12]

3.24
data sovereignty
external constraint (3.33) of the nature of a legal or regulatory requirement of a *jurisdictional domain* (3.52), which is directed at ensuring that sets of recorded information (SRIs)(3.nn) created, collected, managed, processed, used, and/or stored by a *Person* (3.72), in the role of an *organization* (3.70) or a *public administration* (3.85) remains *under the control of* (3.nn) of that *Person* in compliance with the applicable legal or regulatory requirements of the jurisdictional Note to entry 1: A data residency requirement may include prohibition on cross border data flows (CBDF) of specified set(s) of recorded information (SRIs)

Note 1 to entry: A common exercise of data sovereignty by jurisdictional domains is that of restrictions on cross border data flows (CBDF) of personal information (PI) known as personal protection requirements(PPR)>A data residency requirement may be specific to the nature of the SRI

Note 2 to entry: A data sovereignty requirement may be specific to the SRIs associated with the nature of the good, service, and/or rights pertaining to a business transaction

Note 3 to entry: A data sovereignty requirement may be specific to the personal information where the buyer is an individual (e.g. in compliance with applicable consumer protection, privacy protection, individual accessibility, etc. requirements)

© ISO/IEC 2026 – All rights reserved

3.25
Decision Making Application
DMA
model (3.61) of that part of an *Open-edi system* that makes decisions corresponding to the *role(s)(3.97)* that the *Open-edi Party* (3.68) plays as well as the originating, receiving and managing *data* (3.18) values contained in the instantiated *Information Bundles* (3.46*)* which is not required to be visible to the other *Open-edi Parties (OeP)*

[SOURCE: ISO/IEC 14662:2010, 3.6]

3.26
de facto language
natural language (3.63) used in a *jurisdictional domain* (3.52) which has the properties and behaviours of an *official language* (3.65) in that *jurisdictional domain* without having formally been declared as such by that *jurisdictional domain*

Note 1 to entry: A de facto language of a jurisdictional domain is often established through long term use and custom.

Note 2 to entry: Unless explicitly stated otherwise and for the purposes of modelling a business transaction through scenario(s), scenario attributes and/or scenario components, a de facto language of a jurisdictional domain is assumed to have the same properties and behaviours of an official language.

[SOURCE: ISO/IEC 15944-5:2008, 3.42]

3.27
designation
representation of a concept by a sign which denotes it

Note 1 to entry: In terminology work three types of designations are distinguished: symbols, appellations and terms.

[SOURCE: ISO/IEC 15944-2:2015, 3.29. Adapted from ISO 1087:2019, 3.4.1.]

3.28
eBusiness
business transaction (3.5), involving the making of *commitments(3.13)*, in a defined collaboration space, among *Persons* (3.72) using their *IT Systems(3.37)*, according to Open-edi standards

Note 1 to entry: eBusiness can be conducted on both a for-profit and not-for-profit basis.

Note 2 to entry: A key distinguishing aspect of eBusiness is that it involves the making of commitment(s) of any kind among the Persons in support of a mutually agreed upon goal, involving their IT Systems, and doing so through the use of EDI (using a variety of communication networks including the Internet).

Note 3 to entry: eBusiness includes various application areas such as e-commerce, e-administration, e-logistics, e-government, e-medicine, e-learning, etc.

Note 4 to entry: The equivalent French language term for “eBusiness” is always presented in its plural form.

[SOURCE: ISO/IEC 15944-7:2009, 3.06]

3.29
electronic address
address used in a recognized electronic addressing scheme, (e.g., telephone, telex, IP, etc.), to which *recorded information* (3.89) item(s) and/or *business object(s)* (3.4)can be sent to or received from a Contact

[SOURCE: ISO/IEC 15944-2:2015, 3.32]

© ISO/IEC 2026 – All rights reserved

3.30
Electronic Data Interchange
EDI
automated exchange of any predefined and structured *data* (3.18) for *business* (3.3) purposes among information systems of two or more *Persons* (3.72)

Note 1 to entry: This definition includes all categories of electronic business transactions.

[SOURCE: ISO/IEC 14662:2010, 3.8]

3.31
electronic signature
signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with a particular digital/electronic *set of recorded information (SRI)* (3.104)

Note 1 to entry: A Person signature may be in the form of an electronic signature or not.

[SOURCE: Adapted from PIPEDA, Part 2, section 31(1); CAN/CGSB-72.34-2005, 3.28]

3.32
expungement
process (3.82) of ensuring complete elimination, wiping out, destroying, or obliteration of any *recorded information* (3.89) (or *sets of recorded information (SRIs))* (3.104), often including the *medium* (3.59) on which it is recorded, so that there can be no reconstruction of any its contents in whole or in part

[SOURCE: ISO/IEC 15944-12:2025, 3.44]

3.33
external constraint
constraint (3.14) which takes precedence over *internal constraints* (3.50) in a *business transaction* (3.5), i.e., is external to those agreed upon by the parties to a *business transaction*

Note 1 to entry: Normally external constraints are created by law, regulation, orders, treaties, conventions or similar instruments.

Note 2 to entry: Other sources of external constraints are those of a sectoral nature, those which pertain to a particular jurisdictional domain or a mutually agreed to common business conventions, (e.g., INCOTERMS, exchanges, etc.).

Note 3 to entry: External constraints can apply to the nature of the good, service and/or right provided in a business transaction.

Note 4 to entry: External constraints can demand that a party to a business transaction meet specific requirements of a particular role.

EXAMPLE 1 Only a qualified medical doctor may issue a prescription for a controlled drug.

EXAMPLE 2 Only an accredited share dealer may place transactions on the New York Stock Exchange.

EXAMPLE 3 Hazardous wastes may only be conveyed by a licensed enterprise.

Note 5 to entry: Where the Information Bundles (IBs), including their Semantic Components (SCs) of a business transaction are also to form the whole of a business transaction, (e.g., for legal or audit purposes), all constraints are required to be recorded.

EXAMPLE 4 There may be a legal or audit requirement to maintain the complete set of recorded information pertaining to a business transaction, i.e., as the Information Bundles exchanged, as a record.

Note 6 to entry: A minimum external constraint applicable to a business transaction often requires one to differentiate whether the Person, i.e., that is a party to a business transaction, is an individual, organization, or public administration. For example, privacy rights apply only to a Person as an individual.

[SOURCE: ISO/IEC 15944-1:2025, 3.23]

© ISO/IEC 2026 – All rights reserved

3.34
fulfillment
association between an economic *commitment(3.13)*and an economic event where the event executes the promised resource flow from one *Person* (3.72) to another

EXAMPLE A delivery to a customer would fulfill that customer's sale order.

[SOURCE: ISO/IEC 15944-4:2015, 3.34]

3.35
governed
association between an economic agreement and the *business transaction* (3.5) whose conduct and phases are subject to that economic agreement of the *business transaction*

[SOURCE: ISO/IEC 15944-4:2015, 3.35]

3.36
grammatical gender
grammatical category that indicates grammatical relationships between words in sentences

Note 1 to entry: The concept of gender varies from language to language and is not a universal feature of all languages.

EXAMPLE In French, vie (life) is feminine and is used with feminine articles such as la, the feminine pronoun elle, and feminine adjective endings, (e.g. une longue vie).

PERMISSIBLE INSTANCES Types of grammatical gender commonly documented in terminology databases include: (a) masculine; (b) feminine; (c) neuter; (d) other.

[SOURCE: ISO 12620:1999,A.2.2.2]

3.37
Human Interface Equivalent
HIE
representation of the *unambiguous* (3.110) and IT-enabled semantics of an IT interface equivalent (in a *business transaction* (3.5)), often the *ID code* (3.38) of a *coded domain* (3.12) (or a *composite identifier*), in a formalized manner suitable for communication to and understanding by humans

Note 1 to entry: Human interface equivalents can be linguistic or non-linguistic in nature but their semantics remain the same although their representations may vary.

Note 2 to entry: In most cases there will be multiple human interface equivalent representations as required to meet localization requirements, i.e., those of a linguistic, jurisdictional, and/or sectoral nature.

Note 3 to entry: Human interface equivalents include representations in various forms or formats, (e.g., in addition to written text those of an audio, symbol (and icon) nature, glyphs, image, etc.).

[SOURCE: ISO/IEC 15944-2:2015, 3.35]

3.38
ID code
identifier assigned by the coded domain Source Authority (cdSA) to a member of a *coded domain* (3.12) ID

Note 1 to entry: ID codes should be unique within the Registration Schema of that coded domain.

Note 2 to entry: Associated with an ID code in a coded domain can be: (a) one or more equivalent codes; or, (b) one or more equivalent representations, especially those in the form of human equivalent (linguistic) expressions.

Note 3 to entry: Where an entity as a member of a coded domain is allowed to have more than one ID code, i.e., as equivalent codes (possibly including names), one of these should be specified as the pivot ID code.

Note 4 to entry: A coded domain may contain ID codes pertaining to entities which are not members as peer entities, i.e., have the same properties and behaviours, such as ID codes which pertain to predefined conditions other than member entities. If this is the case, the rules governing such exceptions should be predefined and explicitly stated.

© ISO/IEC 2026 – All rights reserved

EXAMPLE (1) The use of an ID code "0" (or "00", etc.), for “Other”; (2) the use of an ID code "9" (or "99") for “Not Applicable”; (3) the use of “8” (or “98”) for “Not Known”; if required, (4) the pre-reservation of a series or set of ID codes for use for user extensions.

Note 5 to entry: In UML modeling notation, an ID codes is viewed as an instance of an object class.

[SOURCE: ISO/IEC 15944-2:2015, 3.37]

3.39
identification
rule-based *process* (3.82), explicitly stated, involving the use of one or more attributes, i.e., *data element(s) (3.22)*, whose value (or combination of values) are used to identify uniquely the occurrence or existence of a specified entity

[SOURCE: ISO/IEC 15944-1:2025, 3.26]

3.40
identifier (in business transaction)
unambiguous (3.110), unique and a linguistically neutral value, resulting from the application of a rule-based *identification* (3.39)*process* (3.82)

Note 1 to entry: Identifiers are required to be unique within the identification scheme of the issuing authority.

Note 2 to entry: An identifier is a linguistically independent sequence of characters capable of uniquely and permanently identifying that with which it is associated. {See ISO 19135:2005 (4.1.5)}

[SOURCE: ISO/IEC 15944-1:2025, 3.27]

3.41
individual
Person (3.72) who is a human being, i.e., a natural person, who acts as a distinct indivisible entity or is considered as such

[SOURCE: ISO/IEC 15944-1:2025, 3.28]

3.42
individual accessibility
set of *external constraints* (3.33) of a *jurisdictional domain* (3.52) as rights of an *individual* (3.41) with disabilities to be able to use *IT Systems* (3.37)at the human, i.e., user, interface and the concomitant obligation of a *seller* (3.100) to provide such adaptive technologies

Note 1 to entry: Although accessibility typically addresses users who have a disability, the concept is not limited to disability issues.

EXAMPLE Disabilities in the form of functional and cognitive limitations include: (a) people who are blind;

(b) people with low vision; (c) people with colour blindness; (d) people who are hard of hearing or deaf, i.e., are hearing impaired; (e) people with physical disabilities; and, (f) people with language or cognitive disabilities.

[SOURCE: ISO/IEC 15944-5:2008, 3.60]

3.43
individual anonymity
state of not knowing the identity or not having any recording of *personal information* (3.73) on or about an *individual* (3.41) as a *buyer* (3.8) by the *seller* (3.100) or *regulator* (3.93), (or any other party) to a *business transaction* (3.5)

[SOURCE: ISO/IEC 15944-8:2025, 3.58]

© ISO/IEC 2026 – All rights reserved

3.44
individual identity
ii
Person identity (Pi) (3.76) of an *individual* (3.41) consisting of the combination of the *persona* (3.77) information and identifier used by an *individual* in a *business transaction* (3.5), i.e., in the making of any kind of *commitment* (3.13)

[SOURCE: ISO/IEC 15944-8:2025, 3.60]

3.45
Information (in information processing)
knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning

[SOURCE: ISO/IEC 2382:2015, 2121271]

3.46
Information Bundle
IB
formal description of the semantics of the *recorded information* (3.89) to be exchanged by *Open-edi parties* (3.68) playing *roles* (3.97)in an *Open-edi scenario* (3.69)

[SOURCE: ISO/IEC 14662:2010, 3.11]

3.47
information law
any law, regulation, policy, or code (or any part thereof) that requires the creation, receipt, collection, description or listing, production, retrieval, submission, retention, storage, preservation or destruction of *recorded information* (3.89), and/or that places conditions on the access and use, confidentiality, privacy, integrity, accountabilities, continuity and availability of the processing, reproduction, distribution, transmission, sale, sharing or other handling of *recorded information*

[SOURCE: ISO/IEC 15944-8:2025, 3.62]

3.48
information life cycle management
ILCM
series of actions and *rules* (3.98) governing the management and its *Electronic Data Interchange (EDI)* (3.30)of *set(s) of recorded information (SRIs)* (3.104) under the control of a *Person* (3.72) from its creation to final disposition, including *expungement* (3.32), in compliance with applicable *information law* (3.47) requirements

Note 1 to entry: The inclusion of information law brings into this definition all the resulting various information management requirements and related activities.

[SOURCE: ISO/IEC 15944-12:2025, 3.58]

3.49
Information Technology System
IT System
set of one or more computers, associated software, peripherals, terminals, human operations, physical processes, information transfer means, that form an autonomous whole, capable of performing information processing and/or information transfer

[SOURCE: ISO/IEC 14662:2010, 3.13]

© ISO/IEC 2026 – All rights reserved

3.50
internal constraint
constraint (3.14) which forms part of the *commitment(s)* (3.13) mutually agreed to among the parties to a *business transaction* (3.5)

Note 1 to entry: Internal constraints are self-imposed. They provide a simplified view for modelling and re-use of scenario components of a business transaction for which there are no external constraints or restrictions to the nature of the conduct of a business transaction other than those mutually agreed to by the buyer and seller.

[SOURCE: ISO/IEC 15944-1:2025, 3.33]

3.51
IT interface equivalent
computer processable *identification* (3.39) of the *unambiguous* (3.110) semantics of a scenario, scenario attribute and/or *scenario component(s)(3.99)* pertaining to a *commitment* (3.13) exchange in a *business transaction* (3.5) which supports computational integrity

Note 1 to entry: IT interface equivalents have the properties of identifiers (in business transaction) and are utilized to support semantic interoperability in commitment exchange.

Note 2 to entry: The value of an IT interface equivalent at times is a composite identifier.

Note 3 to entry: An IT interface equivalent as a composite identifier can consist of the identifier of a coded domain plus an ID code of that coded domain.

Note 4 to entry: An IT interface equivalent is, at times, used as a semantic identifier.

Note 5 to entry: An IT interface equivalent may have associated with it one or more Human Interface Equivalents (HIEs).

Note 6 to entry: The value of an IT interface equivalent is independent of its encoding in programming languages or APIs.

[SOURCE: ISO/IEC 15944-2:2015, 3.45]

3.52
jurisdictional domain
jurisdiction, recognized in law as a distinct legal and/or regulatory framework, which is a source of *external constraints* (3.33) on *Persons* (3.72), their behaviour and the making of *commitments* (3.13) among *Persons* including any aspect of a *business transaction* (3.5)

Note 1 to entry: The pivotal jurisdictional domain is a United Nations (UN) recognized member state. From a legal and sovereignty perspective they are considered peer entities. Each UN member state, (a.k.a. country) may have sub-administrative divisions as recognized jurisdictional domains, (e.g., provinces, territories, cantons, länder, etc.), as decided by that UN member state.

Note 2 to entry: Jurisdictional domains can combine to form new jurisdictional domains, (e.g., through bilateral, multilateral and/or international treaties).

EXAMPLE The European Union (EU), NAFTA, WTO, WCO, ICAO, WHO, Red Cross, the ISO, the IEC, the ITU, etc.

Note 3 to entry: Several levels and categories of jurisdictional domains may exist within a jurisdictional domain.

Note 4 to entry: A jurisdictional domain may impact aspects of the commitment(s) made as part of a business transaction including those pertaining to the making, selling, and transfer of goods, services and/or rights (and resulting liabilities) and associated information. This is independent of whether such an interchange of commitments is conducted on a for-profit or not-for-profit basis and/or includes monetary values.

Note 5 to entry: Laws, regulations, directives, etc., issued by a jurisdictional domain are considered as parts of that jurisdictional domain and are the primary sources of external constraints on business transactions.

[SOURCE: ISO/IEC 15944-5:2008, 3.67]

© ISO/IEC 2026 – All rights reserved

3.53
language
system of signs for communication, usually consisting of a vocabulary and *rules* (3.98)

Note 1 to entry: In this document, language refers to natural languages or special languages, but not "programming languages" or "artificial languages".

[SOURCE: ISO/IEC 15944-2:2015, 3.48]

3.54
language code
combination of *characters* (3.9) used to represent a language or languages

Note 1 to entry: In this standard, the ISO 639-2/T (Terminology) three-alpha code set, shall be used.

[SOURCE: ISO/IEC 15944-5:2017, 3.49. Adapted from ISO 639-2:1998]

3.55
legally recognized language
LRL
natural language (3.63) which has status (other than an *official language* (3.65) or *de facto language* (3.26)) in a *jurisdictional domain* (3.52) as stated in an act, regulation, or other legal instrument, which grants a community of people (or its individuals) the right to use that natural language in the context stipulated by the legal instrument(s)

Note 1 to entry: The LRL can be specified through either: (a) the identification of a language by the name used; or, (b) the identification of a people and thus their language(s).

Note 2 to entry: In addition to acts and regulations, legal instruments include self-government agreements, land claim settlements, court decisions, jurisprudence, etc.

[SOURCE: ISO/IEC 15944-5:2008, 3.71]

3.56
list
ordered set of *data elements* (3.22)

[SOURCE: ISO/IEC 15944-5:2017, 3.73]

3.57
localization
pertaining to or concerned with anything that is not global and is bound through specified sets of *constraints* (3.14) of: (a) a linguistic nature including *natural language* (3.63)and *special languages* and associated multilingual requirements; (b) jurisdictional nature, i.e., legal, regulatory, geopolitical, etc.; (c) a sectoral nature, i.e., industry sector, scientific, professional, etc.; (d) a human rights nature, i.e., privacy, disabled/ handicapped persons, etc.; (e) *consumer* (3.15) behaviour requirements; and/or, (f) safety or health requirements

Note 1 to entry: Within and among "locales", interoperability and harmonization objectives also apply.

[SOURCE: ISO/IEC 15944-5:2008, 3.75]

3.58
location
place, either physical or electronic, that can be defined as an address

[SOURCE: ISO/IEC 15944-2:2015, 3.50]

© ISO/IEC 2026 – All rights reserved

3.59
medium
physical material which serves as a functional unit, in or on which information or *data* (3.18) is normally recorded, in which information or *data* can be retained and carried, from which information or *data* can be retrieved, and which is non-volatile in nature

Note 1 to entry: This definition is independent of the material nature on which the information is recorded and/or technology used to record the information, (e.g., paper, photographic, (chemical), magnetic, optical, ICs (integrated circuits), as well as other categories no longer in common use such as vellum, parchment (and other animal skins), plastics, (e.g., bakelite or vinyl), textiles, (e.g., linen, canvas), metals, etc.).

Note 2 to entry: The inclusion of the "non-volatile in nature" attribute is to cover latency and records retention requirements.

Note 3 to entry: This definition of medium is independent of: (a) the form or format of recorded information; (b) the physical dimension and/or size; and, (c) any container or housing that is physically separate from material being housed and without which the medium can remain a functional unit.

Note 4 to entry: This definition of medium also captures and integrates the following key properties: (a) the property of medium as a material in or on which information or data can be recorded and retrieved; (b) the property of storage; (c) the property of physical carrier; (d) the property of physical manifestation, i.e., material; (e) the property of a functional unit; and, (f) the property of (some degree of) stability of the material in or on which the information or data is recorded.

[SOURCE: ISO/IEC 15944-1:2025, 3.34]

3.60
metadata
data about *data elements* (3.22), including their data descriptions, and data about data ownership, access paths, access rights and data volatility

[SOURCE: ISO/IEC 2382:2015, 2121505]

3.61
model
abstraction of some aspect of reality

[SOURCE: ISO 19115-1:2014, 4.14]

3.62
name
designation (3.27) of an *object* (3.64) by a linguistic expression

[SOURCE: ISO/IEC 15944-1:2025, 3.35. Adapted from ISO 5217:2000 and ISO 1087-1:2000]

3.63
natural language
language (3.53) which is or was in active use in a community of people, and the *rules* (3.98) of which are mainly deduced from the usage

[SOURCE: ISO 5217:2017, 3.1.5.02]

3.64
object
anything perceivable or conceivable

Note 1 to entry: Objects may be material (e.g. engine, a sheet of paper, a diamond), or immaterial (e.g. conversion ratio, a project play) or imagined, (e.g., a unicorn).

[SOURCE: ISO 1087:2019, 3.1.1]

© ISO/IEC 2026 – All rights reserved

3.65
official language
external constraint (3.33) in the form of a *natural language* (3.63) specified by a *jurisdictional domain* (3.52) for official use by *Persons* (3.72) forming part of and/or subject to that *jurisdictional domain* for use in communication(s) either: (a) within that *jurisdictional domain*; and/or, (b) among such *Persons*, where such communications are *recorded information* involving *commitment(s)* (3.13)

Note 1 to entry: Unless official language requirements state otherwise, Persons are free to choose their mutually acceptable natural language and/or special language for communications as well as exchange of commitments.

Note 2 to entry: A jurisdictional domain decides whether or not it has an official language. If not, it will have a de facto language.

Note 3 to entry: An official language(s) can be mandated for formal communications as well as provision of goods and services to Persons subject to that jurisdictional domain and for use in the legal and other conflict resolution system(s) of that jurisdictional domain, etc.

Note 4 to entry: Where applicable, use of an official language may be required in the exercise of rights and obligations of individuals in that jurisdictional domain.

Note 5 to entry: Where an official language of a jurisdictional domain has a controlled vocabulary of the nature of a terminology, it may well have the characteristics of a special language. In such cases, the terminology to be used is required to be specified.

Note 6 to entry: For an official language, the writing system(s) to be used shall be specified, where the spoken use of a natural language has more than one writing system.

EXAMPLE 1 The spoken language of use of an official language may at times have more than one writing system. For example, three writing systems exist for the Inuktitut language. Canada uses two of these writing systems, namely, a Latin-1 based (Roman), the other is syllabic-based. The third is used in Russia and is Cyrillic based.

EXAMPLE 2 Norway has two official writing systems, both Latin-1 based, namely, Bokmål (Dano-Norwegian) and Nynorsk (New Norwegian).

Note 7 to entry: A jurisdictional domain may have more than one official language but these may or may not have equal status.

EXAMPLE 3 Canada has two official languages, Switzerland has three, while the Union of South Africa has eleven official languages.

Note 8 to entry: The BOV requirement of the use of a specified language will place that requirement on any FSV supporting service.

EXAMPLE 4 A BOV requirement of Arabic, Chinese, Russian, Japanese, Korean, etc., as an official language requires the FSV support service to be able to handle the associated character sets.

[SOURCE: ISO/IEC 15944-5:2008, 3.87]

3.66
Open-edi
Electronic Data Interchange(EDI) (3.30) among multiple autonomous *Persons(3.72)* to accomplish an explicit shared *business* (3.3) goal according to Open-edi standards

[SOURCE: ISO/IEC 14662:2010, 3.14]

3.67
Open-edi disposition
process (3.82) governing the implementation of formally approved records retention, destruction (or *expungement* (3.32)) or transfer of *recorded information* (3.89)*under the control of* (3.111) a *Person* (3.72) which are documented in a records scheduling and disposition authority(ies) or similar instrument of the *organization(3.70)*

Note 1 to entry: Within an organization, Open-edi disposition shall be in accordance and compliant with the applicable Open-edi records retention (OeRR) and disposal schedule (RRDS) of the organization.

© ISO/IEC 2026 – All rights reserved

[SOURCE: ISO/IEC 15944-5:2008, 3.90, Adapted from ISO 15489-1, 3.9.]

3.68
Open-edi Party
OeP
Person (3.72) that participates in *Open-edi* (3.66)

Note 1 to entry: Often referred to generically in this and other eBusiness standards, (e.g., parts of ISO/IEC 15944 multipart eBusiness standard) as party or parties for any entity modelled as a Person as playing a role in Open-edi scenarios.

[SOURCE: ISO/IEC 14662:2010, 3.17]

3.69
Open-edi scenario
OeS
formal specification of a class of *business transactions* (3.5)having the same *business* (3.3) goal

[SOURCE: ISO/IEC 14662:2010, 3.18]

3.70
organization
unique framework of authority within which a person or persons act, or are designated to act, towards some purpose

Note 1 to entry: The kinds of organizations covered by this International Standard include the following examples:

EXAMPLE 1 An organization incorporated under law.

EXAMPLE 2 An unincorporated organization or activity providing goods, services and/or rights including: (a) partnerships; (b) social or other non-profit organizations or similar bodies in which ownership or control is vested in a group of individuals; (c) sole proprietorships; and, (d) governmental bodies.

EXAMPLE 3 Groupings of the above types of organizations where there is a need to identify these in information interchange.

[SOURCE: ISO/IEC 15944-1:2025, 3.44. Adapted from ISO/IEC 6523-1: 1998, 3.1]

3.71
organization Person
organization part which has the properties of a *Person* (3.72) and thus is able to make *commitments* (3.13) on behalf of that *organization* (3.70)

Note 1 to entry: An organization can have one or more organization Persons.

Note 2 to entry: An organization Person is deemed to represent and act on behalf of the organization and to do so in a specified capacity.

Note 3 to entry: An organization Person can be a natural person such as an employee or officer of the organization.

Note 4 to entry: An organization Person can be a legal person, i.e., another organization.

[SOURCE: ISO/IEC 15944-1:2025, 3.46]

3.72
Person
entity, i.e., a natural or legal person, recognized by law as having legal rights and duties, able to make *commitment(s)* (3.13), assume and fulfil resulting obligation(s), and able of being held accountable for its action(s)

Note 1 to entry: Synonyms for "legal person" include "artificial person", "body corporate", etc., depending on the terminology used in competent jurisdictional domains.

© ISO/IEC 2026 – All rights reserved

Note 2 to entry: Person is capitalized to indicate that it is being used as formally defined in the standards and to differentiate it from its day-to-day use.

Note 3 to entry: Minimum and common external constraints applicable to a business transaction often require one to differentiate among three common sub-types of Person, namely individual, organization, and public administration.

[SOURCE: ISO/IEC 14662:2010, 3.24]

3.73
personal information
PI
any information on or about an identifiable *individual* (3.41) that is recorded in any form, including electronically or on paper

EXAMPLE Recorded information about an individual's religion, age, financial transactions, medical history, address, or blood type.

[SOURCE: ISO/IEC 15944-5:2008, 3.103]

3.74
personal information controller
PIC
organization Person (3.71) authorized and so formally designated by the *organization* (3.70) to ensure that *personal information* (3.73) remains (fully) under the control of the *organization* and ensures its *privacy protection transactional integrity (PPTI)* (3.81) in compliance with applicable *privacy protection* (3.64) requirements including in any use by the *organization* of *agents* (3.1) and/or *third parties* (3.109) in support of a *business transaction(s)(3.5)*

Note 1 to entry: The primary role and responsibility pertain to and focus on ensuring that: (a) personal information remains under the control of the organization; and, (b) required ILCM aspects are implemented in a verifiable manner. A PIC also bridges the BOV-to-FSV with respect to all aspects of information handling (processing and EDI) of personal information of IT system(s) of an organization.

Note 2 to entry: A PIC has a defined set of responsibilities which can be "outsourced" should a seller decide to use an agent and/or third party based on a contractual agreement to ensure that the privacy protection requirements (rights) of the buyer as an individual are fully supported.

Note 3 to entry: An organization may authorize and designate its privacy protection officer (PPO) to also function in the role of its personal information controller (PIC).

Note 4 to entry: A privacy protection officer (PPO) is a role of an officer in an organization. It may well be that the same organization Person is assigned responsibility for more than one role within an organization including those pertaining to corporate information law compliance, responsibility for corporate internal constraints such as information/records management, security, etc.

[SOURCE: ISO/IEC 15944-12:2025, 3.91]

3.75
personal information profile
PIP
any collection of *personal information (PI)* (3.73)or aggregation of *sets of personal information (SPIs)* (3.103) including associated identifiers, linkages and/or associations, on or about an identifiable *individual* (3.41) being collected, retained, managed, used, etc., by any other *Person* (3.72)and in particular an *organization* (3.70)*or public administration* (3.85) and as such to which *privacy protection* (3.79) requirements apply including those of a *ILCM(3.48)* nature

Note 1 to entry: A personal information profile (PIP) includes any personal information (PI) created by the seller (and parties acting on its behalf such as an agent) in the instantiated business transaction, (e.g., in the post-actualization phase assigning an applicable warranty for the good, service and/or right purchased to another individual where the original buyer (as an individual) "gifts" the good to another individual.

Note 2 to entry: A personal information profile (PIP) often includes personal information (PI) resulting from more than one instantiated business transaction.

© ISO/IEC 2026 – All rights reserved

[SOURCE: ISO/IEC 15944-12:2025, 3.92]

3.76
Person identity
Pi
combination of *persona* (3.77) information and identifier used by a *Person* (3.72) in a *business transaction* (3.5)

[SOURCE: ISO/IEC 15944-1:2025, 3.49]

3.77
persona
set of *data elements* (3.22) and their values by which a *Person* (3.72) wishes to be known and thus identified in a *business transaction* (3.5)

[SOURCE: ISO/IEC15944-1:2025, 3.51]

3.78
principle
fundamental, primary assumption and quality which constitutes a source of action determining particular objectives or results

Note 1 to entry: A principle is usually enforced by rules that affect its boundaries.

Note 2 to entry: A principle is usually supported through one or more rules.

Note 3 to entry: A principle is usually part of a set of principles which together form a unified whole.

EXAMPLE Within a jurisdictional domain, examples of a set of principles include a charter, a constitution, etc.

[SOURCE: ISO/IEC 15944-2:2015, 3.81]

3.79
privacy protection
set of *external constraints* (3.33) of a *jurisdictional domain* (3.52) pertaining to *recorded information* (3.89) on or about an identifiable *individual* (3.41), i.e., *personal information* (3.73), with respect to the creation, collection, management, retention, access and use and/or distribution of such *recorded information* about that *individual* including its accuracy, timeliness, and relevancy

Note 1 to entry: Recorded information collected or created for a specific purpose on an identifiable individual, i.e., the explicitly shared goal of the business transaction involving an individual, shall not be used for another purpose without the explicit and informed consent of the individual to whom the recorded information pertains.

Note 2 to entry: Privacy protection requirements include the right of an individual to be able to view the recorded information about him/herself and to request corrections to the same in order to ensure that such recorded information is accurate and up-to-date.

Note 3 to entry: Where jurisdictional domains have legal requirements which override privacy protection requirements these are required to be specified, (e.g., national security, investigations by law enforcement agencies, etc.).

[SOURCE: ISO/IEC 15944-5:2008, 3.109]

© ISO/IEC 2026 – All rights reserved

3.80
privacy protection officer
PPO
organization Person (3.71) authorized by the *organization* (3.70) to act on behalf of that *organization* (3.55) and entrusted by the *organization* as the officer responsible for the overall governance and implementation of the *privacy protection* (3.79) requirements for *information life cycle management* (3.48) not only within that *organization* but also with respect to any *Electronic Data Interchange* (3.30) of *personal information* (3.73)on the *individual* (3.41) concerned with parties to the *business transaction* (3.5), including a *regulator* (3.93) where required, as well as any *agents* (3.1), *third parties* (3.109) involved in that *business transaction*

[SOURCE: ISO/IEC 15944-8:2017, 3.116]

3.81
privacy protection transactional integrity
PPTI
process (3.82)of ensuringthat the *seller* (3.100)ensures thatdata synchronization (in business transaction) requirements among the *IT systems* (3.37)of all partiesto a *business transaction* (3.5) conform to, and are compliant with, applicable *privacy protection* (3.79)requirements (PPR) of (all) the *jurisdictional domain(s)* (3.52)applicable to that instantiated *business transaction* where and whenever such a *business transaction* involves a *buyer* (3.8)as an *individual* (3.41), i.e., whenever any part of the *recorded information* (3.89) of that *business transaction* involves *personal information (PI)* (3.73)

Note 1 to entry: The concept and requirement of transactional integrity which focuses on EDI among IT systems is based on the requirements for referential integrity within an IT system of an organization.

[SOURCE: ISO/IEC 15944-12:2025, 3.99]

3.82
process
series of actions or events taking place in a defined manner leading to the accomplishment of an expected result

[SOURCE: ISO/IEC 15944-1:2025, 3.53]

3.83
processing of personal information
any operation or set of operations which is performed upon *personal information* (3.73), whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, destruction, or expungement of such personal information.

[SOURCE: ISO/IEC 15944-8:2025, 117]

3.84
pseudonym
use of a *persona* or other identifier by an *individual* (3.41) which is different from that used by the *individual* with the intention that it be not linkable to that *individual*

[SOURCE: ISO/IEC 15944-8:2025, 3.119]

3.85
public administration
entity, i.e., a *Person* (3.72), which is an *organization* (3.70) and has the added attribute of being authorized to act on behalf of a *regulator* (3.93)

[SOURCE: ISO/IEC 15944-1:2025, 3.54]

© ISO/IEC 2026 – All rights reserved

3.86
public policy
category of *external constraints* (3.33) of a *jurisdictional domain* (3.52) specified in the form of a right of an *individual* (3.41) or a requirement of an *organization* (3.70) and/or *public administration* (3.85) with respect to an *individual* pertaining to any exchange of *commitments* (3.13) among the parties concerned involving a good, service and/or right including information management and interchange requirements

Note 1 to entry: Public policy requirements may apply to any one, all or combinations of the fundamental activities comprising a business transaction, i.e., planning, identification, negotiation, actualization and post-actualization. {See further Clause 6.3*"Rules governing the process component"* in ISO/IEC 15944-1}

Note 2 to entry: It is up to each jurisdictional domain to determine whether or not the age of an individual qualifies a public policy requirement, (e.g., those which specifically apply to an individual under the age of thirteen as a child), those which require an individual to have attained the age of adulthood, (e.g., 18 years or 21 years of age) of an individual to be able to make commitments of a certain nature.

Note 3 to entry: Jurisdictional domains may have consumer protection or privacy protection requirements which apply specifically to individuals who are considered to be children, minors, etc., i.e., those who have not reached their 18th or 21st birthday according to the rules of the applicable jurisdictional domain.

[SOURCE: ISO/IEC 15944-5:2008, 3.113]

3.87
publicly available personal information
PAPI
personal information (3.73) about an *individual* (3.41) that the *individual* knowingly makes or permits to be made available to the public, or is legally obtained and accessed from: (1) government records that are available to the public; or, (2) information required by law to be made available to the public

EXAMPLE 1 Personal information which an individual knowingly makes or permits to be made available include public telephone directories, advertisements in newspapers, published materials, postings of this nature on the internet, social media, etc.

EXAMPLE 2 Government records that are publicly available include registers of individuals who are entitled to vote, buy or sell a property, or any other personal information that a jurisdictional domain requires to be publicly available, etc.

[SOURCE: ISO/IEC 15944-8:2025, 3.124]

3.88
recognized Person identity
rPi
Person identity (Pi) (3.76), established to the extent necessary for a specific purpose in a *business transaction* (3.5)

[SOURCE: ISO/IEC 15944-1:2025, 3.56]

3.89
recorded information
information that is recorded on or in a medium irrespective of form, recording *medium* (3.59) or technology used, and in a manner allowing for storage and retrieval

Note 1 to entry: This is a generic definition and is independent of any ontology, (e.g., those of "facts" versus "data" versus "information" versus "intelligence" versus "knowledge", etc.).

Note 2 to entry: Through the use of the term "information," all attributes of this term are inherited in this definition.

Note 3 to entry: This definition covers: (a) any form of recorded information, means of recording, and any medium on which information can be recorded; and, (b) all types of recorded information including all data types, instructions or software, databases, etc.

[SOURCE: ISO/IEC 15944-1:2025, 3.56]

© ISO/IEC 2026 – All rights reserved

3.90
register
set of files containing identifiers assigned to items with descriptions of the associated items

[SOURCE: ISO 19135-1:2015, 4.1.9]

3.91
registration
rule-based *process* (3.82), explicitly stated, involving the use of one or more *dataelements(3.22),* whose value (or combination of values) is used to identify uniquely the results of assigning an Open-edi Registry Item (OeRI)

[SOURCE: ISO/IEC 15944-2:2015, 3.95]

3.92
Registration Authority
RA
Person (3.72) responsible for the maintenance of one or more Registration Schemas(*RS*) including the assignment of a unique identifier for each recognized entity in a Registration Schema (*RS*)

[SOURCE: ISO/IEC 15944-1:2025, 3.57]

3.93
regulator
Person (3.72) who has authority to prescribe *external constraints* (3.33) which serve as *principles(3.78)*, policies or *rules* (3.98) governing or prescribing the behaviour of *Persons* involved in a *business transaction* (3.5)as well as the provisioning of goods, services, and/or rights interchanged

[SOURCE: ISO/IEC 15944-1:2025, 3.59]

3.94
regulatory business transaction
RBT
class of *business transactions* (3.5)for which the explicitly shared goal has been established and specified by a *jurisdictional domain* (3.52), as a *Person* (3.72) in the *role* (3.97) of a *regulator* (3.93)

Note 1 to entry: A regulatory business transaction (RBT) can itself be modelled as a stand-alone business transaction and associated scenario(s).

EXAMPLE The filing of a tax return, the making of a customs declaration, the request for and issuance of a licence, the provision of a specified service of a public administration, a mandatory filing of any kind with a regulator, etc.

Note 2 to entry: A regulatory business transaction (modelled as a scenario) can form part of another business transaction.

Note 3 to entry: A RBT may apply to a seller only, a buyer only or both, as well as any combination of parties to a business transaction.

Note 4 to entry: A RBT may require or prohibit the use of an agent or third party.

Note 5 to entry: A regulatory business transaction (RBT) may be specific to the nature of the good, services and/or right forming part of a business transaction.

[SOURCE: ISO/IEC 15944-5:2008, 3.124]

3.95
responsibility
association between *Persons* (3.72) where one is responsible to the other or between a *Persons* and an organization Person where that *Persons* is assigned

Note 1 to entry: Sub-types of Persons include individuals, organizations, and public administrations. An “individual” is non-divisible but organizations and public administrations are and as such will assign specific responsibilities to organization Persons. {See further Clause 6.2.7 and Figure 17 in ISO/IEC 15944-1}

© ISO/IEC 2026 – All rights reserved

[SOURCE: ISO/IEC 15944-4:2015, 3.59]

3.96
retention period
length of time for which *data* (3.18) on a *data* medium is to be preserved

[SOURCE: ISO/IEC 2382:2015, 2125629]

3.97
role
specification which models an external intended behaviour (as allowed within a scenario) of an *Open-edi Party* (3.68)

[SOURCE: ISO/IEC 14662:2010, 3.25]

3.98
rule
statement governing conduct, procedure, conditions and relations

Note 1 to entry: Rules specify conditions that should be complied with. These may include relations among objects and their attributes.

Note 2 to entry: Rules are of a mandatory or conditional nature.

Note 3 to entry: In Open-edi, rules formally specify the commitment(s) and role(s) of the parties involved, and the expected behaviour(s) of the parties involved as seen by other parties involved in (electronic) business transactions. Such rules are applied to: (a) content of the information flows in the form of precise and computer-processable meaning, i.e., the semantics of data; and, (b) the order and behaviour of the information flows themselves.

Note 4 to entry: Rules should be clear and explicit enough to be understood by all parties to a business transaction. Rules also should be capable of being able to be specified using a using a Formal Description Technique(s) (FDTs).

EXAMPLE A current and widely used FDT is "Unified Modelling Language (UML)".

[SOURCE: ISO/IEC 15944-2:2015, 3.101]

3.99
scenario component
one of the three fundamental elements of a scenario, namely *role* (3.97), *Information Bundle* (3.46), and *Semantic Component* (3.101)

[SOURCE: ISO/IEC 15944-2:2015, 3.104]

3.100
seller
Person (3.72) who aims to hand over voluntarily or in response to a demand, a good, service and/or right to another *Person* and in return receives an acceptable equivalent value, usually in money, for the good, service and/or right provided

[SOURCE: ISO/IEC 15944-1:2025, 3.62]

3.101
Semantic Component
SC
unit of *recorded information* (3.89)*unambiguously* (3.110) defined in the context of the *business* (3.3) goal of the *business transaction* (3.5)

Note 1 to entry: A SC may be atomic or composed of other SCs.

[SOURCE: ISO/IEC 14662:2010, 3.27]

© ISO/IEC 2026 – All rights reserved

3.102
set
assembly of objects or concepts considered as a whole

[SOURCE: ISO 5127:2017, 3.1.1.09]

3.103
set of personal information
SPI
set of recorded information (SRI) (3.104) which is of the nature of, or contains, *personal information* (3.73)

[SOURCE: ISO/IEC 15944-12:2025, 3.127]

3.104
set of recorded information
SRI
recorded information (3.89) of a *Person* (3.72), which is *under the control of* (3.111) the same and which is treated as a unit in its information life cycle

Note 1 to entry: An SRI can be a physical or digital document, a record, a file, etc., that can be read, perceived or heard by a Person or computer system or similar device.

Note 2 to entry: An SRI is a unit of recorded information that is unambiguously defined in the context of the business goals of the organization, i.e., a semantic component.

Note 3 to entry: An SRI can be self-standing (atomic), or a SRI can consist of a bundling of two or more SRIs into another new SRI. Both types can exist simultaneously within the information management systems of an organization.

[SOURCE: ISO/IEC 15944-5:2008, 3.137]

3.105
Source Authority
SA
Person (3.72) recognized by other *Persons* as the authoritative source for a set of *constraints* (3.14)

Note 1 to entry: A Person as a Source Authority for internal constraints may be an individual, organization, or public administration.

Note 2 to entry: A Person as Source Authority for external constraints may be an organization or public administration.

EXAMPLE In the field of air travel and transportation, IATA as a Source Authority, is an organization, while ICAO as a Source Authority, is a public administration.

Note 3 to entry: A Person as an individual shall not be a Source Authority for external constraints.

Note 4 to entry: Source Authorities are often the issuing authority for identifiers (or composite identifiers) for use in business transactions.

Note 5 to entry: A Source Authority can undertake the role of Registration Authority or have this role undertaken on its behalf by another Person.

Note 6 to entry: Where the sets of constraints of a Source Authority control a coded domain, the SA has the role of a coded domain Source Authority.

[SOURCE: ISO/IEC 15944-2:2015, 3.109]

© ISO/IEC 2026 – All rights reserved

3.106
source jurisdictional domain
SJD
jurisdictional domain (3.nn) within which an *individual (3.nn)*, in the *role (3.nn)* of *buyer(3.nn)* in a *business transaction (3.nn)*, initiates the actualization of a *business transaction* and thus serve as the source or primary set of *external constraints* (3.nn) which are of a *public policy* (3.nn)nature

Note 1 to entry: In a federal state, as differentiated from a unitary state, more than one level of jurisdictional domains may apply as public policy rights of an individual (e.g., at both the federal level as well as at their state, provincial, lander, canton, etc. level.

EXAMPLE Within federated states the jurisdictional domain of the province of Quebec is part of the federal jurisdictional domain of Canada. Each has their own privacy protection, consumer protections, human rights, etc. legislation. Brazil Germany, India, Switzerland, United States are but some example of federated UN members.

3.107
standard
documented agreement containing technical specifications or other precise criteria to be used consistently as *rules* (3.98), guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose

Note 1 to entry: This is the generic definition of standard of the ISO and IEC (and now found in the ISO/IEC JTC1 Directives, Part 1, Section 2.5 :1998). {See also ISO/IEC Guide 2:1996 (1.7)}

[SOURCE: ISO/IEC 15944-1:2025, 3.64]

3.108
term
designation (3.27) of a defined concept in a special language by a linguistic expression

Note 1 to entry: A term may consist of one or more words (simple term or complex term) or even contain symbols.

[SOURCE: ISO/IEC 15944-5 :2008, 3.14]

3.109
text
data in the form of *characters* (3.9), symbols, words, phrases, paragraphs, sentences, tables, or other *character* arrangements, intended to convey a meaning and whose interpretation is essentially based upon the reader's knowledge of some natural language or artificial language

EXAMPLE A business letter printed on paper or displayed on a screen.

[SOURCE: ISO/IEC 2382:2015, 2121273]

3.110
third party
Person (3.72) besides the two primarily concerned in a *business transaction* (3.5) who is *agent* (3.1) of neither and who fulfils a specified *role* (3.97) or function as mutually agreed to by the two primary *Persons* or as a result of *external constraints* (3.33)

Note 1 to entry: It is understood that more than two Persons can at times be primary parties in a business transaction.

[SOURCE: ISO/IEC 15944-1:2025, 3.65]

3.111
unambiguous
level of certainty and explicitness required in the completeness of the semantics of the *recorded information* (3.89) interchanged appropriate to the goal of a *business transaction* (3.5)

[SOURCE: ISO/IEC 15944-1:2025, 3.66]

© ISO/IEC 2026 – All rights reserved

3.112
under the control of
set of requirements on an *organization* (3.90), especially those of *external constraint* (3.33) nature, i.e., *privacy protection* (3.79) and related *information law* (3.47) requirements, requiring full and complete *information life cycle management (ILCM)* (3.48)of *personal information* (3.73)as *set(s) of recorded information (SRIs)* (3.104)related to the agreed upon goal of the instantiated *business transaction* (3.5), including state changes to the content of the *SRIs* with respect to their creation/collection, recording processing, organization, storage, use, retrieval, disclosure, retrieval, aggregation, dissemination, *disposition* (including *expungement* (3.32)), *Electronic Data Interchange (EDI)* (3.30), etc., and in particular that of any and all state changes in the *decision making application(DMAs)* (3.25) of the *organization* (3.70)and any of its *agents* (3.1) and/or *third parties* (3.109) (as well as any other parties) to the *business transaction*

Note 1 to entry: The fact that a Person responsible for the control of a SRI(s), especially SPI(s), delegates or contracts out physical custody of the SRI(s) to an agent or third party does not take away from the responsibility of that Person for ensuring ILCM management aspects in support of privacy protection requirements remain fully supported and executed.

Note 2 to entry: If and where a disposition or expungement of SPIs pertaining to a business transaction involves the transfer of the related SPIs to another organization the applicable ILCM requirements of a privacy protection nature continue to apply to the organization to which the SPIs are being transferred to.

[SOURCE: ISO/IEC 15944-12:2025, 3.142]

4 Abbreviated terms

ATI	Access to Information
BOV	Business Operational View
BTI	Business Transaction Identifier
BTM	Business Transaction Model
CBDF	cross border data flows
cdRS	coded domain Registration Schema
cdSA	coded domain Source Authority
CGSB	Canadian General Standards Board
CRPD	(UN) Convention on Rights of Persons with Disabilities
CIP	Consumer Information Profile
CV	controlled vocabulary
DMA	Decision Making Application
EDI	Electronic Data Interchange
FDT	Formal Description Technique
FOI	Freedom of Information
FSV	Functional Service View
FTC	(USA) Federal Trade Commission
HIE	Human Interface Equivalent

© ISO/IEC 2026 – All rights reserved