International Standard

ISO/IEC 15944-8

Second edition
2026-02

Information technology — Business operational view —

Part 8: Identification of privacy protection requirements as external constraints on business transactions

Technologies de l'information — Vue opérationnelle d'affaires —

Partie 8: Identification des exigences de protection de la vie privée en tant que contraintes externes sur les transactions d'affaires

Reference number
ISO/IEC 15944-8:2026(en)

© ISO/IEC 2026

Contents

Page

Foreword ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **2**

4 Abbreviated terms ... **32**

5 Fundamental principles and assumptions governing privacy protection requirements in business transactions involving individuals (external constraints perspective) ... **34**
5.1 General ... 34
5.2 Exceptions to the application of the privacy protection principles ... 36
5.3 Fundamental privacy protection principles ... 36
5.3.1 General ... 36
5.3.2 Privacy protection principle 1: Preventing harm ... 36
5.3.3 Privacy protection principle 2: Accountability ... 37
5.3.4 Privacy protection principle 3: Identifying purposes ... 40
5.3.5 Privacy protection principle 4: Informed Consent ... 40
5.3.6 Privacy protection principle 5: Limiting collection ... 42
5.3.7 Privacy protection principle 6: Limiting use, disclosure and retention ... 43
5.3.8 Privacy Protection Principle 7: Accuracy ... 46
5.3.9 Privacy Protection Principle 8: Safeguards ... 46
5.3.10 Privacy Protection Principle 9: Openness ... 47
5.3.11 Principle Protection Principle 10: Individual Access ... 48
5.3.12 Privacy Protection Principle 11: Challenging compliance ... 50
5.4 Requirement for tagging (or labelling) data elements in support of privacy protection requirements ... 51

6 Collaboration space and privacy protection ... **52**
6.1 General ... 52
6.2 Basic Open-edi collaboration space: Buyer and seller ... 52
6.3 Collaboration space: The role of buyer (as individual), seller and regulator ... 54

7 Public policy requirements of jurisdictional domains ... **55**
7.1 General ... 55
7.2 Jurisdictional domains and public policy requirements ... 55
7.2.1 General ... 55
7.2.2 Privacy protection ... 56
7.2.3 Person and external constraints: Consumer protection ... 58
7.2.4 Individual accessibility ... 59
7.2.5 Human rights ... 60
7.2.6 Privacy as a right of an "individual" and not the right of an organization or public administration ... 60

8 Principles and rules governing the establishment, management and use of identities of an individual ... **61**
8.1 General ... 61
8.2 Rules governing the establishment of personae, identifiers and signatures of an individual ... 62
8.3 Rules governing the assignment of unique identifiers to an individual by Registration Authorities (RAs) ... 67
8.4 Rules governing individual identity, authentication, recognition, and use ... 68
8.5 Legally recognized individual identifies (LRIIs) ... 72

9 Person component — Individual sub-type ... **73**
9.1 General ... 73
9.2 Role qualification of a Person as an individual ... 73

© ISO/IEC 2026 – All rights reserved

9.3 Persona and legally recognized names (LRNs) of an individual 74
9.4 Truncation of legally recognized names of individuals 75
9.5 Rules governing anonymization of individuals in a business transaction 75
9.6 Rules governing pseudonymization of personal information in a business transaction 76

10 Process component 77
10.1 General 77
10.2 Planning 77
10.3 Identification 78
10.4 Negotiation 78
10.5 Actualization 78
10.6 Post-actualization 78

11 Data component 79
11.1 General 79
11.2 Rules governing the role of Business Transaction Identifier (BTI) in support of privacy protection requirements 79
11.3 Rules governing state of change management of business transactions in support of privacy protection requirements 80
11.4 Rules governing records retention of personal information in a business transaction 80
11.5 Rules governing time/date referencing of personal information in a business transaction 81

12 Template for identifying privacy protection requirements on business transactions 82
12.1 Introduction and basic principles 82
12.2 Template structure and contents 82
12.3 Template for specifying the scope of an Open-edi scenario 83
12.4 Consolidated template of attributes of Open-edi scenarios, roles and information bundles 91

13 Conformance statement 94
13.1 General 94
13.2 Conformance to the ISO/IEC 14662 Open-edi Reference Model and the multipart ISO/IEC 15944 eBusiness standard 95
13.3 Conformance to ISO/IEC 15944-8 95

Annex A (normative) **Consolidated controlled vocabulary definitions and associated terms, as human interface equivalents (HIEs), with cultural adaptability: English and French language equivalency in an IT standardization context 96**

Annex B (normative) **Consolidated set of rules in existing parts of ISO/IEC 15944 of particular relevance to privacy protection requirements as external constraints on business transactions 99**

Annex C (normative) **Business Transaction Model (BTM): Classes of constraints 111**

Annex D (normative) **Integrated set of information life cycle management (ILCM) principles in support of information law compliance 115**

Annex E (normative) **Key existing concepts and definitions applicable to the establishment, management, and use of identities of a single individual 118**

Annex F (normative) **Coded domains for specifying state change and record retention management in support of privacy protection requirements 120**

Annex G (informative) **Abstract of ISO/IEC 15944-8 ..... 128**

Annex H (Informative) **Exclusions to the scope of ISO/IEC 15944-8 ..... 129**

Annex I (Informative) **Aspects not currently addressed in this document 130**

Bibliography 132

© ISO/IEC 2026 – All rights reserved

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

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

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

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

This document was prepared by Technical Committee ISO/IEC JTC1, *Information technology*, Subcommittee SC 32, *Data management and interchange*.

This second edition cancels and replaces the first edition (ISO/IEC 15944-8:2012), which has been technically revised.

The main changes are as follows:

— Clause 1 (Scope) has been amended to move the detailed description of "Exclusions" and "Aspects currently not addressed" to two separate informative annexes;

— definitions in Clause 3 have been updated to be aligned with other referenced source definitions;

— clauses and annexes have been aligned to changes in ISO/IEC Directives, Part 2;

— minor edits of Clause 5, Clause 9, Clause 12, all annexes and the bibliography.

A list of all parts in the ISO/IEC 15944 series can be found on the ISO and IEC websites.

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

© ISO/IEC 2026 – All rights reserved

Introduction

0.1 Purpose and overview

0.1.1 General

Modelling business transactions using scenarios and scenario components is done by specifying the applicable constraints on the data content using explicitly stated rules. The *Open-edi Reference Model* identified two basic classes of constraints, "internal constraints" and "external constraints". External constraints apply to most business transactions. (See Clause 0.4 and Annex C.)

Jurisdictional domains are the primary source of external constraints on business transactions. Privacy protection requirements in turn are a common requirement of most jurisdictional domains, although they may also result from explicit scenario demands from, or on, the parties involved in a business transaction.

This document is a BOV-related standard which addresses basic (or primitive) requirements of a privacy protection environment, as legal requirements represented through jurisdictional domains, on business transactions, and also integrates the requirements of the information technology and telecommunications environments.

This document contains a methodology and tool for specifying common classes of external constraints through the construct of "jurisdictional domains". It meets the requirements set in ISO/IEC 15944-1 and ISO/IEC 15944-2 through the use of explicitly stated rules, templates, and Formal Description Techniques (FDTs).

In addition to the existing strategic directions of "portability" and "interoperability", the added strategic direction of ISO/IEC JTC 1 of "cultural adaptability" is also supported in this document. The external constraints of jurisdictional domains as a primary factor in choice and use of language and application of public policy are also addressed.

0.1.2 ISO/IEC 14662

ISO/IEC 14662[1)] states the conceptual architecture and framework necessary for carrying out electronic business transactions among autonomous parties. That architecture identifies and describes the need to have two separate and related views of the business transaction.

The first is the Business Operational View (BOV). The second is the Functional Service View (FSV). ISO/IEC 14662:2010, Figure 1 illustrates the Open-edi environment. (For definitions of the terms used in Figure 1, please see Clause 3.)

1) The ISO/IEC 14462 *Open-edi Reference Model* serves as the basis of the 2000 Memorandum of Understanding (MOU) among ISO, IEC, ITU and the UN/ECE concerning standardization in the field of electronic business. {See https://www.itu.int//ITU-T/e-business/files/mou.pdf }

© ISO/IEC 2026 – All rights reserved

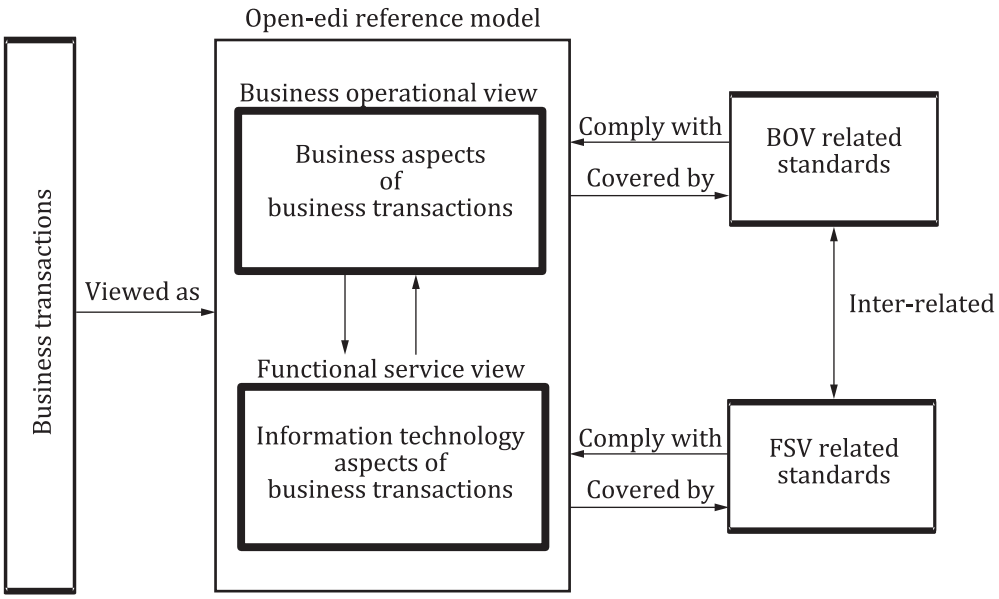

Figure 1 — Open-edi environment — Open-edi Reference Model

ISO/IEC 14662:2010, Clause 5 states:

> *"The intention is that the sending, by an Open-edi Party, of information from a scenario, conforming to Open-edi standards, shall allow the acceptance and processing of that information in the context of that scenario by one or more Open-edi Parties by reference to the scenario and without the need for agreement.*
>
> *However, the legal requirements and/or liabilities resulting from the engagement of an organization in any Open-edi transaction may be conditioned by the competent legal environment(s) of the formation of a legal interchange agreement between the participating organizations. Open-edi Parties need to observe rule-based behaviour and possess the ability to make commitments in Open-edi, (e.g. business, operational, technical, legal, and/or audit perspectives)".*

In addition, ISO/IEC 14662:2010, Figure A.1 illustrates the Relationships of Open-edi standardization areas with other standards and importance of the legal environment. This document is a BOV standard which focuses on the legal environment for the application of privacy protection from an Open-edi perspective, and, as required follow-up standards development in support of the *"Open-edi Reference Model*".

ISO/IEC 15944-5 is used to identify the means by which laws and regulations impacting scenarios and scenario components, as external constraints, may be modelled and represented. The primary source of these external constraints is jurisdictional domains.

ISO/IEC 15944-1 creates rules for creating the specification of external constraints when modelling business transactions through scenarios, scenario attributes and scenario components. Several parts of the ISO/IEC 15944 series are used as input to this document. The rules are consolidated in this document in Annex B.

ISO/IEC 15944-1:2025, 7.1 states:

> "*The approach taken is that of identifying the most primitive common components of a business transaction and then moving from the general to the more detailed, the simplest aspects to the more complex, from no external constraints on a business transaction to those which incorporate external constraints, from no special requirements on functional services to specific requirements, and so on*".

This document focuses on addressing commonly definable aspects of external constraints that relate to privacy protection when the source is a jurisdictional domain. A useful characteristic of external constraints is that, at the sectoral level, national and international levels, etc., focal points and recognized authorities often already exist. The rules and common business practices in many sectoral areas are already known.

© ISO/IEC 2026 – All rights reserved

Use of this document (and related standards) addresses the transformation of these external constraints (business rules) into specified, registered, and re-useable scenarios and scenario components.

0.1.3 ISO/IEC 15944-1"Business Operational View (BOV)"

ISO/IEC 15944-1 states the requirements of the BOV aspects of Open-edi in support of electronic business transactions. They need to be taken into account in the development of business semantic descriptive techniques for modelling e-business transactions and components thereof as re-useable business objects. They include:

— commercial frameworks and associated requirements;

— legal frameworks and associated requirements;

— public policy requirements particularly those of a generic nature such as consumer protection, privacy, accommodation of handicapped/disabled;

— requirements arising from the need to support cultural adaptability. This includes meeting localization and multilingual requirements, (e.g. as may be required by a particular jurisdictional domain or desired to provide a good, service and/or right in a particular market. Here, one needs the ability to distinguish, the specification of scenarios, scenario components, and their semantics, in the context of making commitments, between:

  a) the use of unique, unambiguous and linguistically neutral identifiers (often as composite identifiers) at the information technology (IT) interface level among the IT systems of participation parties on the one hand; on the other;

  b) their multiple human interface equivalent (HIE) expressions in a presentation form appropriate to the Persons involved in the making of the resulting commitments.

Figure 2 shows an integrated view of these business operational requirements. It is based on ISO/IEC 15944-1:2025, Figure 3. Since the focus of this document is that of external constraints for which jurisdictional domains are the primary source, these primary sources have been shaded in Figure 2.

© ISO/IEC 2026 – All rights reserved

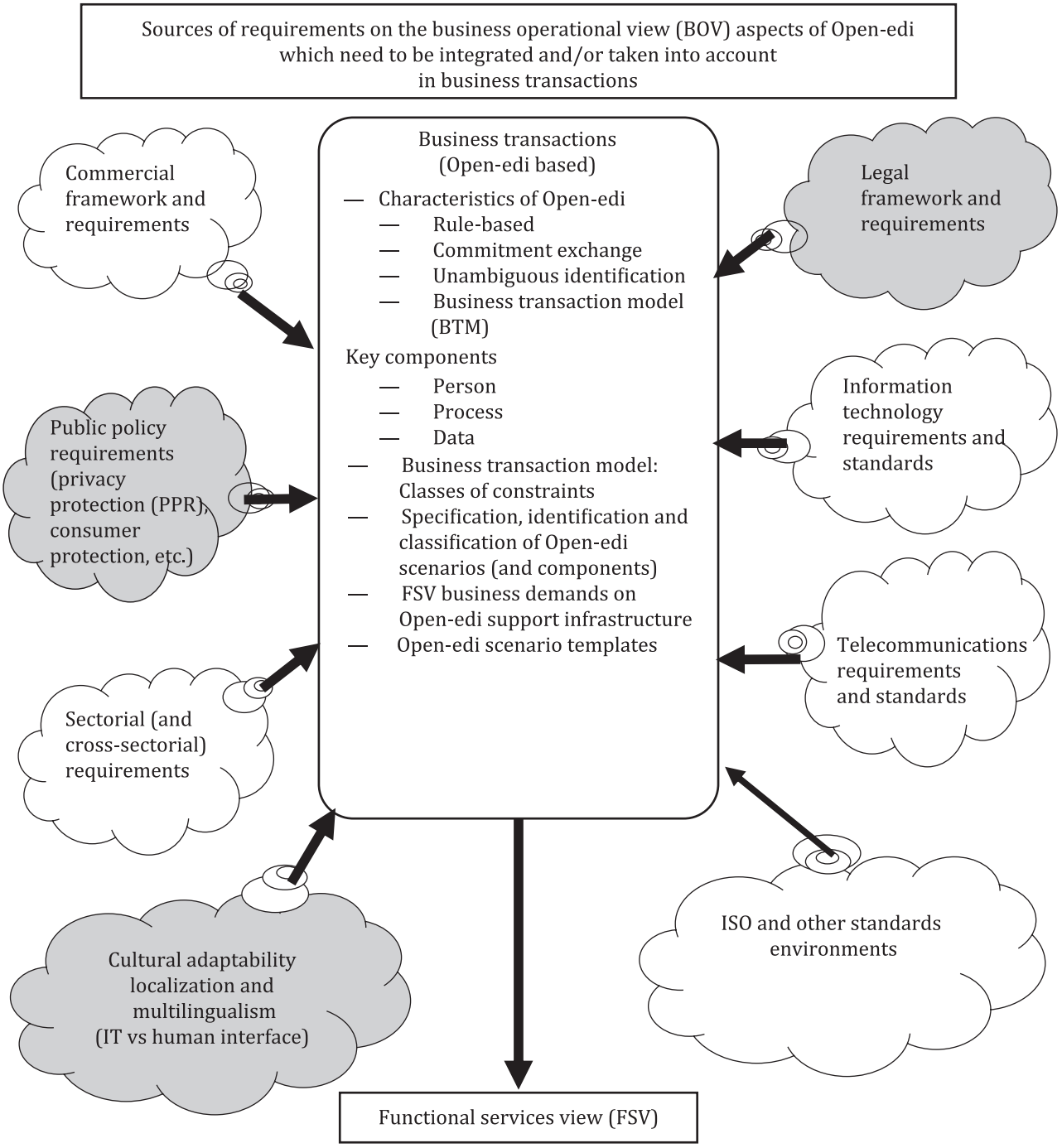

Figure 2 — Integrated view — Business operational requirements: External constraints focus

0.2 Introducing the use of "Person", "organization" and "party" in the context of business transaction and commitment exchange

In electronic business transactions, whether undertaken on a for profit or not-for-profit basis, the key element is commitment exchange among Persons made among their Decision Making Applications (DMAs) of the Information Technology Systems (IT Systems)[2)] acting on behalf of "Persons". "Persons" are the only entities able to make commitments[3)]. ISO/IEC 15944-1:2025, 0.4 states:

2) See further "*Functional Services View*" in ISO/IEC 14662:2010, 5.2.

3) The text in this clause is based on existing text in ISO/IEC 15944-1:2025, 0.3 and ISO/IEC 14662.

© ISO/IEC 2026 – All rights reserved

> "*When the ISO/IEC 14662 Open-edi Reference Model standard was being developed, the "Internet" and "WWW" were in an embryonic stage and their impact on private and public sector organizations was not fully understood*."

The Business Operational View (BOV) was therefore defined as:

> "*perspective of business transactions limited to those aspects regarding the making of business decisions and commitments among organizations which are needed for the description of a business transaction*".

The ISO/IEC 6523-1 definition of "organization" was used in the first edition (1997) of ISO/IEC 14662. The fact that today Open-edi, through the Internet and WWW, also involves "individuals" has been taken into account in the development of the 2nd and subsequent editions. ISO/IEC 15944-1 defines the term "commitment". However, the definition of the term "Open-edi Party" previously used proved not to be specific enough to satisfy scenario specifications, including scenario specification attributes when the legal aspects of commitment were considered. In many instances commitments were noted as being actually among IT systems acting under the direction of those legally capable of making commitment, rather than actual individuals acting in their own capacities. It was also recognized that in some jurisdictional domains a commitment could be made by "artificial" persons such as corporate bodies. Finally, it was noted that there are occasions where agents act, either under the instruction of a principal, or as a result of requirement(s) laid down by a jurisdictional domain, or where an individual is prevented by a relevant jurisdictional domain from being able to make a commitment in their own right (e.g. a minor), and this is incorporated into this document.

To address these extended requirements the additional concept and term of "Person", has been defined. A Person is defined such that they are capable of having the appropriate legal and regulatory constraints applied to them.

There are three categories of Person as a role player in Open-edi, namely: (1) the Person as "individual", (2) the Person as "organization", and (3) the Person as "public administration". There are also three basic (or primitive) roles of Persons in business transactions, namely: "buyer", "seller", and "regulator".

When modelling business transactions, jurisdictional domains prescribe their external constraints in the role of "regulator" and execute them as "public administration". (See further 6.3.)

While "public administration" is one of the three distinct sub-types of Person, most of the rules applicable to "organization" also apply to "public administration". In addition, an unincorporated seller is also deemed to function as an "organization". Consequently, the use of "organization" throughout this document also covers "public administration". Where it is necessary to bring forward specific rules, constraints, properties, etc., which apply specifically to "public administration", this is stated explicitly.

The requirements of jurisdictional domains are specified through the use of sets of "Codes representing X..." Such sets of codes are created and maintained by Source Authorities via a rulebase with resulting coded domains in the form of data elements whose permitted values represent predefined semantics in a structured form, i.e. as a type of semantic component. Jurisdictional domains serve as Source Authorities for such coded domains.

These three categories of Person also identify the possible Source Authorities for coded domains. Source Authorities for coded domains are therefore either "organizations" or "public administrations".

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";

— the words "person(s)" and/or "party(ies)" are used in their generic contexts independent of roles of "Person" as defined in the ISO/IEC 14662 and ISO/IEC 15944-1 standards. A "party" to a business transaction has the properties and behaviours of a "Person".

© ISO/IEC 2026 – All rights reserved

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

The ISO/IEC 15944 series 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 subclause is included in each part of ISO/IEC 15944 to emphasize that harmonized terms and definitions are essential to the continuity of the overall standard. Definitions and their assigned terms need to be established as early as possible in the development process. Comments on any definition/term pair need to address the question of changes needed to avoid possible misinterpretation. Definitions may need to be amended/improved as part of the harmonization of definitions and their assigned terms among the various parts of ISO/IEC 15944.

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 document in which it is introduced. In this context, it is noted that ISO/IEC 15944-7 already also contains human interface equivalents (HIEs) in Chinese, French and Russian[5)].

0.4 Importance of the two classes of constraints of the Business Transaction Model (BTM)

The BTM has two classes of constraints; namely:

1) those which are "self-imposed" and agreed to as commitments among the parties themselves, i.e. "internal constraints";

2) those which are imposed on the parties to a business transaction based on the nature of the good, service and/or right exchanged, the nature of the commitment made among the parties (including ability to make commitments, the location, information identifying the parties as living individuals, and so on), i.e. "external constraints".

This document addresses external constraints. Jurisdictional domains are the primary source of external constraints[6)]. Privacy protection is addressed as a common set of external constraint requirements coming from jurisdictional domains.

ISO/IEC 15944-1:2025, 6.1.6 provides normative text for these two classes of constraints. It is included for convenience in this document as Annex C.

0.5 Need for a standard based on rules and guidelines[7)]

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. {See Figure 2 in Clause 0.2}

This Business Operational View (BOV) standard focuses on "other 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".

---

4) All the terms and definitions of the current editions of the ISO/IEC 14669 *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) For business requirements of the Functional Service View and business demands on the Open-edi support infrastructure with respect to internal constraints, see further ISO/IEC 15944-1:2025, 6.5.2 "*Self-Imposed Constraints*". ISO/IEC 15944-4, which focuses on accounting and economic aspects of business transactions, does so from an "internal constraints" perspective.

7) This introductory clause is primarily based on that found in ISO/IEC 15944-1:2025, 6.1.2 titled "*Standard based on rules and guidelines*".

© ISO/IEC 2026 – All rights reserved

Open-edi is based on rules which are predefined and mutually agreed to. They are precise criteria and agreed upon requirements of business transactions representing common business operational practices and functional requirements.

ISO/IEC 15944-1:2025, Clause 5 defines the "Business Operational View (BOV)" type of Open-edi standards as "rule-based" standards[8]. Of particular relevance is the first key characteristic of Open-edi is that of actions based upon following clear, predefined rules (See further ISO/IEC 15944-1:2025, 5.1). It is useful to quote some key normative text of ISO/IEC 15944-1 so that users of this document have a clear understanding of the nature and purpose of this BOV standard.

> *"Open-edi requires the use of clear and pre-defined rules, principles and guidelines. These rules formally specify the role(s) of the parties involved in Open-edi and the available expected behaviour(s) of the parties as seen by other parties engaging in Open-edi. Open-edi rules are applied to:*
>
> — *the content of information flows;*
> — *the order and behaviour of information flows themselves.*
>
> *The combination of both of these provides a complete definition of the relationships among the parties since it requires them to achieve a common semantic understanding of the information exchanged. They should also have consistent generic procedural views on their interaction. Therefore, rule sets have to be agreed to in advance and captured in Open-edi scenarios. This is a major component of the agreement required among parties."*

NOTE Here and elsewhere where this document speaks of data, information flows, electronic data interchange (EDI), etc. it pertains to data (in a business transaction).

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, standardizers, consumers, etc.[9]

For ease of reference, common rules have been sequentially enumerated, and are presented in **bold** font. Where guidelines associated with a rule are provided, they are numbered sequentially after that rule and are shown in **bold** and *italic* font[10]. Choice of words in the rules, the guidelines and the terms and definitions are governed by maximizing the ability to map, on the one hand, to all the sources of requirements of the Business Operational View (BOV) of any e-business transaction (e.g. commercial, legal, public policy, cultural adaptability, sectoral, etc.), frameworks of the day-to-day world of business, and, on the other hand, those pertaining to the Functional Services View (FSV) in support of BOV requirements, (e.g. that of those providing information technology and communication services in support of commitment exchange of any kind and among all parties involved in a business transaction).

0.6 Use of "jurisdictional domain", and "jurisdiction" (and "country") in the context of business transaction and commitment exchange

The term "jurisdiction" has many possible definitions. Some "jurisdictions" 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

---

8) The key characteristics of Open-edi are (as stated in ISO/IEC 15944-1:2025, Clause 5) are: a) actions based on following predefined rules; b) commitment of the parties involved; c) communications among parties are automated; d) parties control and maintain their states; e) parties act autonomously; f) multiple simultaneous transactions can be supported.

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.

10) For example, "Guideline 5G2" equals the second Guideline under Rule 5.

© ISO/IEC 2026 – All rights reserved

jurisdiction (even if that is not legally enforceable), and so on. Finally, there are differing "legal" definitions of "jurisdiction". Readers of this document need to understand that in this document:

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

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

At the same time, a set of external constraints of a jurisdictional domain lends itself to being modelled through scenarios and semantic components. For example, ISO/IEC 15944-1:2025, Annex H is a scenario of an external constraint of a jurisdictional domain, i.e. the USA, that provides a business process framework for the enterprise process required for a telecommunications service provider. Here, the fact that external constraints of jurisdictional domains are a primary factor in choice of language and application of public policy are also addressed in this document.

0.7 Use of "identifier" as "identifier (in business transaction)" to prevent ambiguity[11)]

ISO/IEC 15944-1:2025, 6.1.4 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 transaction.

The ISO/IEC 15944 series of standards serves as a methodology and tool for the specification and unambiguous identification of Open-edi scenarios, scenario attributes and scenario components as re-useable elements, i.e. as re-useable business objects, in support of common business transactions. These and related objectives of interoperability and re-usability of Open-edi scenarios and scenario components for business transactions require their unambiguous identification.

ISO/IEC 15944-1:2025, 3.66 defines "unambiguous" as *level of certainty and explicitness required in the completeness of the semantics of the recorded information interchanged that is appropriate to the goal of a business transaction.*

ISO/IEC 15944-1:2025, 3.27 defines "identifier (in business transaction)" as *unambiguous, unique and a linguistically neutral value, resulting from the application of a rule-based identification process*.

Thus, readers of this document need to understand that the "identifier" in this document is used as a defined term as "identifier (in a business transaction)"[12)].

0.8 Use of “privacy protection” in the context of business transaction and 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[13)] 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. Therefore, this may only apply

---

11) This is a summary of ISO/IEC 15944-1:2025, 6.1.4 "*Business transactions: Unambiguous identification of entities".* See ISO/IEC 15944-1:2025, Annex C which provides the informative and explanatory text for the rules and definitions in 6.1.4.

12) Identifiers in business transactions can be simple or composite identifiers. This is dependent on (1) the rules governing "identifiers" as a rule-based process; (2) the "registration schema" used (as well as any permitted combinations of the same).

13) “Medium” is a defined concept. {See ISO/IEC 15944-1:2025, 6.4.and6.4.1}.

© ISO/IEC 2026 – All rights reserved

to some proportion of the specific role players in a business transaction (including their personae) and not others.

This document incorporates the common aspects of such laws and regulations as pertaining to privacy protection, applicable at the time of publication only. The concept of "privacy protection" also integrates these various sets of legal and regulatory requirements and does so from a public policy requirements perspective. (See 6.3 and Clause 7)

It needs to be borne in mind that the delivery of "privacy protection" requires action both at the business level (BOV) and technology levels (FSV). 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 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, proscribed dissemination and so on. In this regard, the interplay of the BOV and FSV views of all organizations needs to be taken into account.

0.9 Aspects currently not addressed

There are relevant privacy protection aspects which are currently not addressed in this document, see Annex I.

0.10 Organization and description of this document

This document identifies basic common requirements of privacy protection requirements, as external constraints of jurisdictional domains, on the modelling of a business transaction through scenarios and scenario components.

Following the Introduction and Clauses 1, 2, 3 and 4, which have common content in the ISO/IEC 15944 series, Clause 5 introduces a fundamental set of principles and assumptions governing privacy protection requirements in business transactions involving individuals as Persons. The essential aspects of eleven common privacy protection principles have been identified and their requirements are captured in the form of rules. Also, included in Clause 5 are exclusions and rules for tagging (or labelling) data elements (in organization of data)in support of privacy protection requirements.

The importance of the concept of "collaboration space" introduced in ISO/IEC 15944-4 is carried forward and adapted in the privacy protection context in Clause 6, as the "privacy collaboration space (PCS)". Refer to ISO/IEC 15944-4 in order to understand and use the concept of collaboration space and apply it in an ISO/IEC 15944-8 context. Generic public policy requirements which apply whenever individuals engage in a business transaction, i.e. as a buyer, are summarized in Clause 7, which is based on ISO/IEC 19544-5. Refer to ISO/IEC 15944-5 in order to understand and use of the concept of public policy requirements. (Privacy protection is one of several common public policy requirements; others include consumer protection and individual accessibility.) Clause 7 concludes by noting that privacy protection is a right of an "individual" only and not of an organization or public administration.

The establishment, management and use of the different identities that an individual has, is the focus of Clause 8. The generic principles and rules already stated in ISO/IEC 15944-1 pertaining to Person are used, being placed in a privacy protection requirements context. These include "persona", "identifiers" (and their assignment by Registration Authorities), "signature", "individual identity (ii)", "authentication", recognition, i.e. as a "recognized individual identity (rii)", "recognized individual name (RIN)", etc.

Many aspects of the individual as a sub-type of Person and the resulting link to privacy protection were anticipated in the development of ISO/IEC 15944-1 and ISO/IEC 15944-5. The purpose of Clause 9 is to consolidate those which apply to an individual, and do so in a privacy protection requirements context. Clause 9 addresses role qualifications of an individual, a legally recognized name (LRN), truncation of LRNs, anonymization and use of pseudonyms.

Clause 10 focuses on the process component of the Business Transaction Model (BTM) which is constructed of five fundamental activities: planning, identification, negotiation, actualization and post-actualization. The generic rules in ISO/IEC 15944-1:2025, subclause 6.5 are brought forward, and those which pertain to an individual as a buyer are adapted and applied from a privacy protection perspective.

© ISO/IEC 2026 – All rights reserved

Similarly, Clause 11 focuses on the data component of the BTM and brings forward, in summary form, applicable concepts and rules in ISO/IEC 15944-1 and ISO/IEC 15944-5 in the context of privacy protection requirements. Specific aspects addressed in Clause 11 include the role of the business transaction identifier (BTI), change management and records retention of personal information, and associated data synchronization requirements, for personal information among all parties to a business transaction as well as date/time referencing.

As in ISO/IEC 15944-1, ISO/IEC 15944-2 and ISO/IEC 15944-5, Clause 12 provides a checklist through the use of templates to guide the user through the mechanics of determining the source of the external constraints where these are jurisdictional domains; and of determining the adequacy of a scenario specification as well as of available scenario components.

Finally, annexes are provided for elaboration of points raised in the main body. Annex A introduces the consolidated controlled vocabulary definitions and associated terms, as human interface equivalents (HIEs), with cultural adaptability: English and French language equivalency in an IT standardization context.

Annex B identifies rules stated in the other parts of ISO/IEC 15944 that are applicable to this document. Annex C is common to ISO/IEC 15944-2, ISO/IEC 15944-4 and ISO/IEC 15944-5. It summarizes the Business Transaction Model (BTM). Annex D presents, in summary form, an integrated set of information life cycle (ILCM) principles in support of information law compliance from a jurisdictional domain perspective.

The purpose of Annex E is to bring forward and highlight the key concepts and their definitions applicable to the establishment and management, etc., of the multiple identities of a single individual.

Annex F[14)] provides the primitive and essential set of coded domains whose interworking is required in order to be able to support state changes and record retention requirements in support of privacy protection requirements.

Annex G contains an abstract of ISO/IEC 15944-8.

Annex H provides detailed exclusions to the scope of this document.

Annex I introduces many other relevant privacy protection aspects currently not addressed in this document.

14) The coded domains presented in Annex F are an application in a privacy protection context of those stated in ISO/IEC 15944-5:2008, subclause 6.6.4, which presents a high level generic approach. The reason that this normative text is in an annex is to facilitate its possible use in a new part of ISO/IEC 15944, i.e. new Part 12 and possibly other new parts.

© ISO/IEC 2026 – All rights reserved

Information technology — Business operational view —

Part 8: Identification of privacy protection requirements as external constraints on business transactions

1 Scope

This document:

— provides method(s) for identifying, in Open-edi modelling technologies and development of scenarios, the extra requirements in Business Operational View (BOV) specifications for identifying the additional external constraints to be applied to recorded information in business transactions relating to personal information of an individual, as required by legal and regulatory requirements of applicable jurisdictional domains having governance over the personal information exchanged among parties to a business transaction;

— integrates existing normative elements in support of privacy protection requirements as are already identified in ISO/IEC 14662 and ISO/IEC 15944-1, ISO/IEC 15944-2, ISO/IEC 15944-4 and ISO/IEC 15944-5, which apply to information concerning identifiable living individuals as buyers in a business transaction or whose personal information is used in the business transaction;

— provides overarching operational "best practice" statements for associated (and not necessarily automated) processes, procedures, practices and governance requirements that need to act in support of implementing and enforcing mechanisms needed to support privacy/data protection requirements necessary for the implementation in Open-edi transaction environments;

— identifies and provides a sample scenario and implementation (use case) for one or more use cases of privacy/data protection in business transactions;

— provides guidelines on the need for procedural mechanisms in the event that mandatory disclosure rules of transactional information that needs to be implemented.

This document does not specify the technical mechanisms needed to implement the Functional Services View. Detailed exclusions to the scope of this document are provided in Annex H.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 639:2023, *Code for individual languages and language groups*

ISO/IEC 7501-1:2008, *Identification cards — Machine readable travel documents — Part 1: Machine readable passport*

ISO/IEC 7812 (all parts), *Identification cards — Identification of issuers*

ISO/IEC 14662:2010, *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 2026 – All rights reserved

Bibliography

[1] ISO/IEC Guide 2:2004, *Standardization and related activities — General vocabulary*

[2] ISO 1087:2019, *Terminology work and terminology science — Vocabulary*

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

[4] ISO 3166-1:2020, *Codes for the representation of names of countries and their subdivisions — Part 1: Country code*

[5] ISO 5127:2017, *Information and documentation — Foundation and vocabulary*

[6] ISO/IEC 5218:2022, *Information technology — Codes for the representation of human sexes*

[7] ISO/IEC 6523-1:2023, *Information technology — Structure for the identification of organizations and organization parts — Part 1: Identification of organization identification schemes*

[8] ISO/IEC 6523-2, *Information technology — Structure for the identification of organizations and organization parts — Part 2: Registration of organization identification schemes*

[9] ISO/IEC 7501 (all parts), *Identification cards — Machine readable travel documents*

[10] ISO 8601-1, *Date and time — Representations for information interchange — Part 1: Basic rules*

[11] ISO 8601-2, *Date and time — Representations for information interchange — Part 2: Extensions*

[12] ISO/IEC 9798-1:2010, *Information technology — Security techniques — Entity authentication — Part 1: General*

[13] ISO/IEC 10181-2:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework*

[14] ISO/IEC 11179-1:2023, *Information technology — Metadata registries (MDR) — Part 1: Framework*

[15] ISO 15489-1:2016, *Information and documentation — Records management — Part 1: Concepts and principles*

[16] ISO/IEC TR 15944-6, *Information technology — Business Operational View — Part 6: Technical introduction to eBusiness modelling*

[17] ISO 19108:2002, *Geographic information — Temporal schema*

[18] ISO 19115-1:2014, *Geographic information — Metadata — Part 1: Fundamentals*

[19] ISO 19135-1:2015, *Geographic information — Procedures for item registration — Part 1: Fundamentals*

[20] ISO/IEC 19501, *Information technology — Open Distributed Processing — Unified Modeling Language (UML) Version 1.4.2*[110], *Information technology — Open Distributed Processing — Unified Modeling Language (UML) Version 1.4.2*

[21] ISO 25237:2017, *Health informatics — Pseudonymization*

[22] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

[23] *GS1Global Traceability Standard* (GDSN). Issue 1.3.0. (November, 2012). Available from: https://www.gs1.org/docs/gsmp/traceability/Global_Traceability_Standard.pdf (Accessed 2024-05-22)

[24] *GS1 Global Data* Dictionary: https://apps.gs1.org/gdd/SitePages/Home.aspx(Accessed 2024-05-22)

110) Throughout this document, ISO/IEC 19501:2005 is simply referenced as "UML".

© ISO/IEC 2026 – All rights reserved

[25] Quittner,Joshua. Going Private.[J].Time 153(5):62, 1999.

[26] UN. *International Covenant on Economic, Social and Cultural Rights.* (1966), Available from: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights(Accessed 2024-05-22)

[27] UN. *Universal Declaration of Human Rights* (1948) Available from https://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed 2024-05-22)

[28] UN. *Universal Declaration of Rights of Persons belonging to National or Ethnic, Religious and Linguistic Minorities*. Available from: https://www.ohchr.org/en/instruments-mechanisms/instruments/declaration-rights-persons-belonging-national-or-ethnic (Accessed 2024-05-22)

[29] UNESCO. *Universal Declaration of Cultural Diversity* (Paris, November, 2001). Available from http://portal.unesco.org/en/ev.php-URL_ID=13179&URL_DO=DO_TOPIC&URL_SECTION=201.html (Accessed 2024-05-22)

[30] APEC Privacy Framework. (2005)*

[31] Charter of the United Nations (as signed 1945 and Amended 1965, 1968, and 1973+), United Nations (UN)*

[32] EU General Data Protection Directive (GDPR) (2016)

[33] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)

[34] UN Convention on the Rights of Persons with Disabilities. 2006+

[35] Vienna Convention of the Law of Treaties (1969), United Nations (UN)

© ISO/IEC 2026 – All rights reserved