INTERNATIONAL STANDARD

ISO/IEC 15944-8

First edition
2012-04-01

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 15944-8:2012(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Figures

Page

Tables

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15944-8 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 32, *Data management and interchange*.

ISO/IEC 15944 consists of the following parts, under the general title *Information technology — Business Operational View*:

— *Part 1: Operational aspects of Open-edi for implementation*

— *Part 2: Registration of scenarios and their components as business objects*

— *Part 4: Business transaction scenarios — Accounting and economic ontology*

— *Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints*

— *Part 6: Technical introduction to e-Business modelling* [Technical Report]

— *Part 7: eBusiness vocabulary*

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

— *Part 10: Coded domains*

The following parts are under preparation:

— *Part 3: Open-edi description techniques (OeDTs)*

— *Part 9: Traceability framework*

0 Introduction

0.1 Purpose and overview

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 E}

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. (Requirements for secrecy or confidentiality are not addressed in this part of ISO/IEC 15944, unless they are implicitly needed to apply privacy protection requirements to data).

This part of ISO/IEC 15944 describes the business semantic descriptive techniques needed to support privacy protection requirements when modelling business transactions using the external constraints of jurisdictional domains

In addition to the existing strategic directions of "portability" and "interoperability", the added strategic direction of ISO/IEC JTC1 of "cultural adaptability" is also supported in this part of ISO/IEC 15944. The external constraints of jurisdictional domains as a primary factor in choice and use of language and application of public policy are also addressed.

0.1.1 ISO/IEC 14662 "Open-edi Reference Model"[1]

The ISO/IEC 14662 Open-edi Reference Model[2] states the conceptual architecture 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). Figure 1 from ISO/IEC 14662:2010 illustrates the Open-edi environment. {For definitions of the terms used in Figure 1, please see Clause 3 below}

---

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 http://www.itu.int//ITU-T/e-business/files/mou.pdf }

2 ISO/IEC 14662:2010 (3rd ed. E/F) *"Information technology — Open-edi Reference Model/Technologies de l'information — Modèle de référence EDI-ouvert*".

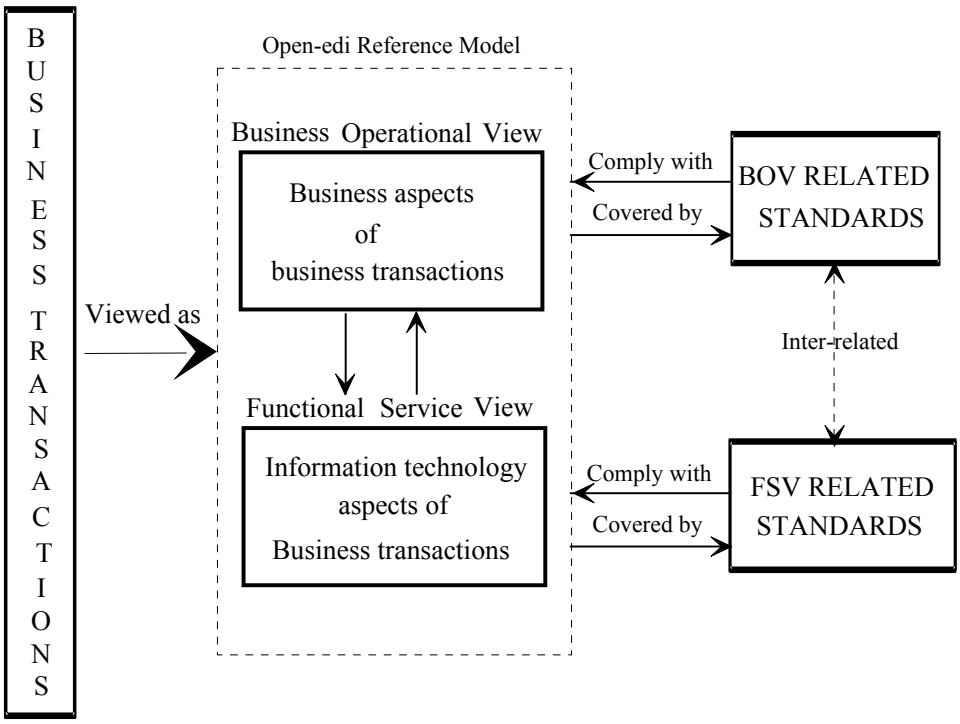


Figure 1 — Open-edi environment – Open-edi Reference Model

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, Annex A of the ISO/IEC 14662:2010 "Open-edi Reference Model" contains Figure A.1 *"Relationships of Open-edi standardization areas with other standards and import of the legal environment"*. This part of ISO/IEC 15944 is a BOV standard which focuses on the legal environment for the application of privacy and/or data 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 ISO/IEC 15944 are used as input to this part. They are consolidated in this part of ISO/IEC 15944 in Annex B.

ISO/IEC 15944-1:2011 in Clause 7 *"Guidelines for scoping Open-edi Scenarios"* states in Clause 7.1:

> *"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 part of ISO/IEC 15944 focuses on addressing commonly definable aspects of external constraints that relate to privacy and data 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. Use of this part of ISO/IEC 15944 (and related standards) addresses the transformation of these external constraints (business rules) into specified, registered, and re-useable scenarios and scenario components.

0.1.2 ISO/IEC 15944-1 "Business Agreement Semantic Descriptive Techniques" ("Business Operational View (BOV")")

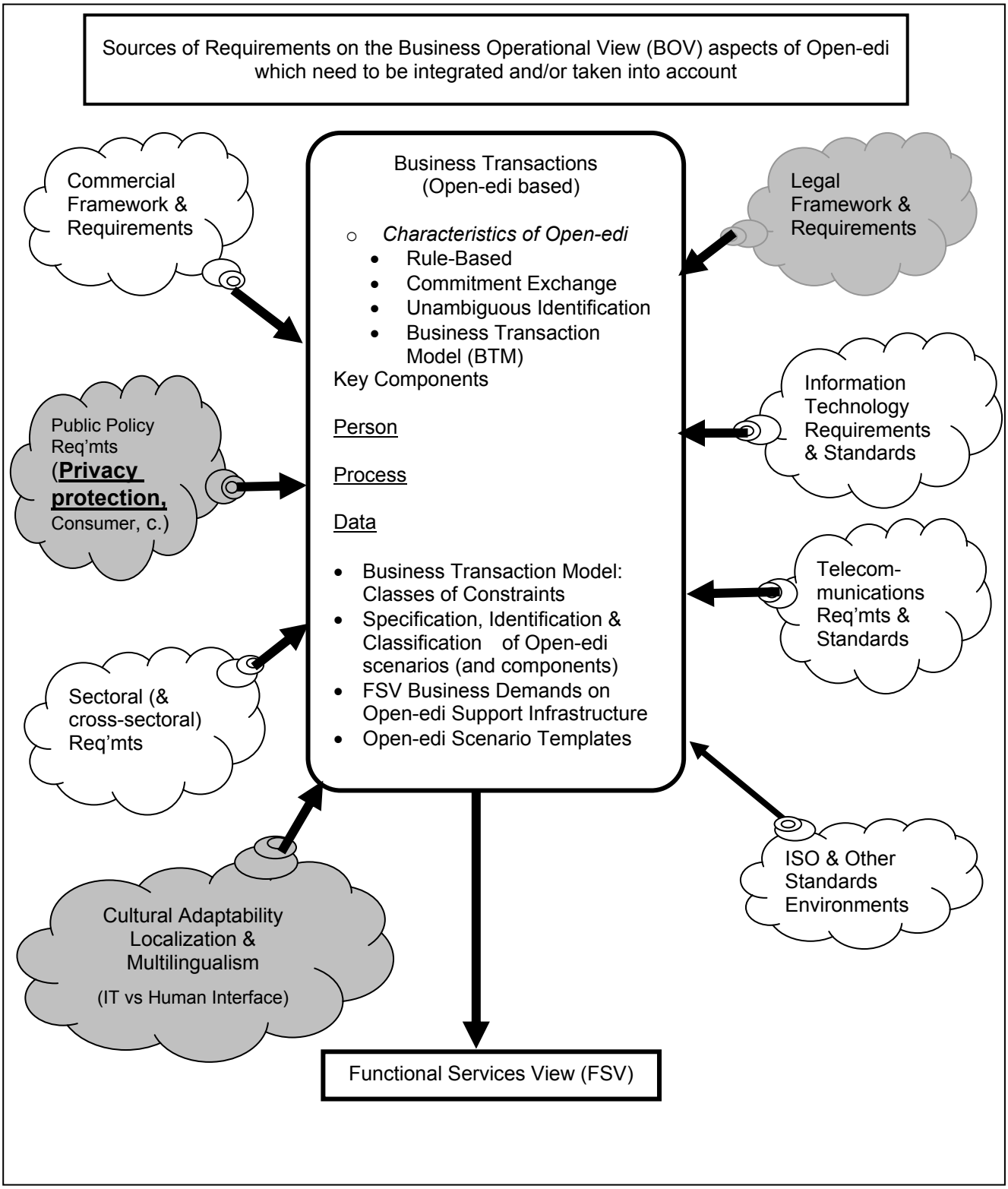
ISO/IEC 15944-1 states the requirements of the BOV aspects of Open-edi in support of electronic business transactions. They shall be taken into account in the development of business semantic descriptive techniques for modelling e-business transactions and components thereof as re-useable business objects. 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; and, 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 Figure 3 from ISO/IEC 15944-1. Since the focus of this part of ISO/IEC 15944 is that of external constraints for which jurisdictional domains are the primary source these primary sources have been shaded in Figure 2 below).



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)[3] acting on behalf of "Persons". "Persons" are the only entities able to make commitments[4]. Clause 0.4 in ISO/IEC 15944-1 states:

> *"When the ISO/IEC 14662 Open-edi Reference Model standard was being developed, the "Internet" and "WWW" were 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 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 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 actually the individuals acting in their own capacities. It was also recognized that in some jurisdictions 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 jurisdiction, or where an individual is prevented by a relevant jurisdiction from being able to make a commitment in their own right, (e.g., a minor), and this must be incorporated into the standard.

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 below Clause 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 part of ISO/IEC 15944 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 part of ISO/IEC 15944:

---

3 See further Clause 5.2 "*Functional Services View*" in ISO/IEC 14662:2010 *"Open-edi Reference Model"* (3rd edition).

4 The text in this section is based on existing text in Section "0.3" in ISO/IEC 15944-1:2011 and ISO/IEC 14662:2010 (3rd edition).

- 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 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".

0.3 Importance and role of terms and definitions[5]

ISO/IEC Directives Part 2 provide for “Terms and definitions” as a “Technical normative element,” necessary for the understanding of certain terms used in the document, where the words have special, extended or technical meaning.

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 terms and definitions are essential to the continuity of the overall standard. Definitions and their assigned terms should be established as early as possible in the development process. Comments on any definition/term pair should 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 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.

Normative Annex A “*Consolidated list of terms and definitions with cultural adaptability: ISO English and ISO French language equivalency*” is derived from Clause 3 of each part of ISO/IEC 15944.[6] Annex A is repeated in each part of ISO/IEC 15944 as a convenient reference. The designation ISO before a natural language refers to the use of that natural language in ISO standards, and has no other meaning.

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"; and,

2) those which are imposed on the parties to a business transaction based on the nature of the good, service and/or rights exchanged, the nature of the commitment made among the parties (including ability to make

5 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 15944-7:2009. 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.

6 Canada has committed to maintain this comprehensive list in a database as the reference file for Annex A. This Annex A reference file will insure the consistency of definitions and their assigned terms among the various parts in the on-going harmonization effort. {See also ISO/IEC 15944-7 *e-Business Vocabulary}*

commitments, the location, information identifying the parties as living individuals, and so on), i.e., "external constraints".

This part of ISO/IEC 15944 addresses external constraints. Jurisdictional domains are the primary source of external constraints.[7] **Privacy protection is addressed as a common set of external constraint requirements coming from of jurisdictional domains.**

ISO/IEC 15944-1:2011, Clause 6.1.6 provides normative text for these two classes of constraints. It is included for convenience in this part of ISO/IEC 15944 as Annex C.

0.5 Need for a standard based on rules and guidelines[8]

This part of ISO/IEC 15944 is intended to be used within and outside of the ISO and IEC by diverse sets of users having different perspectives and needs {See above Figure 2 in Clause 0.2}.

In an ISO, IEC, ISO/IEC JTC1 context, a standard is considered to be a:

> "*documented agreement containing technical specifications or 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*."[9]

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".

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.

Clause 5 "*Characteristics of Open-edi*" in ISO/IEC 15944-1:2011 defines the "Business Operational View (BOV)" type of Open-edi standards as "rule-based" standards[10]. Of particular relevance here is the first key characteristic of Open-edi as stated in Clause 5.1 "*Actions based upon following clear, predefined rules"*. It is useful to quote some key normative text of ISO/IEC 15944-1:2011 so that users of ISO/IEC 15944-5 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:*

---

7 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 15944-1:2011, Clause 6.5.2 "*Self-Imposed Constraints".* ISO/IEC 15944-4:2007, which focuses on accounting and economic aspects of business transactions, does so from an "internal constraints" perspective.

8 This introductory clause is primarily based on that found in ISO/IEC 15944-1:2011, Clause 6.1.2 titled "*Standard based on rules and guidelines*".

9 See entry D252, Annex D, ISO/IEC 15944-7. One can interpret "agreement" in a variety of ways. The ISO/IEC Guide 2:2004 (1.7) uses the term "consensus" which need not imply unanimity but rather "absence of sustained opposition to substantial issues…"

10 The key characteristics of Open-edi are (as stated in Clause 5, ISO/IEC 15944-1:2011, pp.12-14) are:

- actions based on following predefined rules;
- commitment of the parties involved;
- communications among parties are automated;
- parties control and maintain their states;
- parties act autonomously; and,
- multiple transactions can be supported.

The six sub-clauses of Clause 5 of ISO/IEC 15944-1:2011 describe each of these in more detail.

- *the content of information flows; and,*

- *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 must 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."

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.[11]

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[12]. 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 jurisdiction (even if that is not legally enforceable), and so on. Finally, there are differing "legal" definitions of "jurisdiction". Readers of this part of ISO/IEC 15944 should understand that in this part of ISO/IEC 15944:

- 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 that this part of ISO/IEC 15944 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, Annex "I" in ISO/IEC 15944-1:2011, titled, "*Scenario Description Using the Open-Edi Scenario Template, Telecommunications Operations Map Example"* 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 part of ISO/IEC 15944.

---

11 The working principle here 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.

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

0.7 Use of "identifier" as "identifier (in business transaction)" to prevent ambiguity[13]

Clause 6.1.4 of ISO/IEC 15944-1:2011 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 multipart standard 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 defines "unambiguous" as follows:

> ***unambiguous***
>
> *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 15944-1:2011 (3.66)]

and "identifier (in business transaction)" as follows:

> ***identifier (in business transaction)***
>
> ***unambiguous****, unique and a linguistically neutral value, resulting from the application of a* ***rule-based identification process***
>
> *NOTE Identifiers must be unique within the identification scheme of the issuing authority.*
>
> [ISO/IEC 15944-1:2011 (3.27)]

Thus, readers of this part of ISO/IEC 15944 should understand that the "identifier" in this part of ISO/IEC 15944 is used as a defined term as "identifier (in a business transaction)".[14]

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[15] used for the recording of personal information and/or its communication to other Persons.

---

13 This is a summary of ISO/IEC 15944-1:2011, 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.

14 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).

15 “Medium” is a defined concept. {See ISO/IEC 15944-1:2011, Clause 6.4. “*Rules governing the data component”*, and its Clause 6.4.1 “*Recorded informaton*”}.

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 must 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.

This part of ISO/IEC 15944 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 below at Clause 6.3 and Clause 7}

It has 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 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 must 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 must be taken into account.

0.9 Organization and description of this document

This part of ISO/IEC 15944 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 Clauses 0, 1, 2, 3 and 4, which have common content in the multipart standard, 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 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. Here 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. Here the generic rules in Clause 6.5 of ISO/IEC 15944-1:2011 are brought forward, and those which pertain to an individual as a buyer are adapted and applied from a privacy protection perspective.

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 or 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 is a consolidated list of the definitions and their associated terms used in this part of ISO/IEC 15944 in ISO English and ISO French. As stated in the main body of this part of ISO/IEC 15944, the issue of semantics and their importance of identifying the correct interpretation across official aspects is critical.

Annex B identifies rules stated in the other parts of ISO/IEC 15944 that are applicable to this part of ISO/IEC 15944. 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 principles (ILCM) 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 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.[16]

[16] The coded domains presented in this Annex F are an application in a privacy protection context of those stated in Clause 6.6.4 of ISO/IEC 15944-5:2008, which presents a high level generic approach. The reason that this normative text is in an annex is to facilitate its possible future use of a new part of ISO/IEC 15944 which takes these coded domains as new part of ISO/IEC 15944.

Information technology — Business Operational View —

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

1 Scope

1.1 Statement of scope

This part of ISO/IEC 15944:

- provides method(s) for identifying, in Open-edi modelling technologies and development of scenarios, the additional 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 and data protection requirements as are already identified in the current editions of 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[17] in a business transaction or whose personal information is used in the transaction;

- provides overarching operational 'best practice' statements for associated (and not necessarily automated) processes, procedures, practices and governance requirements that must act in support of implementing and enforcing technical 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; and,

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

This part of ISO/IEC 15944 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 part of ISO/IEC 15944 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).

[17] As stated in Clauses 6.2.4 – 6.2.8, and Figure 18 of ISO/IEC 15944-1:2011, a natural person who provides a good, service and/or right is deemed to be an organization. Most jurisdictional domains also view an unincorporated activity providing a good, service and/or right to be an organization. {See further ISO/IEC 6523}

1.2 Exclusions

1.2.1 Functional Services View (FSV)

This part of ISO/IEC 15944 focuses on the BOV aspects of a business transaction, and does not concern itself with the technical mechanisms needed to achieve the business requirements (the FSV aspects, including the specification of requirements of a Functional Services View (FSV) nature which include security techniques and services, communication protocols, etc.). The FSV includes any existing standard (or standards development of an FSV nature), which have been ratified by existing ISO, IEC, UN/ECE and/or ITU standards.

1.2.2 Internal behaviour of organizations (and public administration)

Excluded from the scope of this part of ISO/IEC 15944 is the application of privacy protection requirements within an organization itself. The Open-edi Reference Model, considers these to be internal behaviours of an organization and thus not germane to business transactions (which focus on external behaviours pertaining to electronic data interchange among the autonomous parties to a business transaction). As such, excluded from the scope of this part of ISO/IEC 15944 are any:

1) internal use and management of recorded information pertaining to an identifiable organization Person an organization (or public administration) within an organization; and,

2) implementation of internal information management controls, internal procedural controls or operational controls within an organization or public administration necessary for it to comply with applicable privacy requirements that may be required in observance of their lawful or contractual rights, duties and obligations as a legal entity in the jurisdictional domain(s) of which they are part.

This should not be taken to mean that an organization could not adapt this part of ISO/IEC 15944 in order to model internal behaviour if they so wished, say when moving personal data within the organization.

1.2.3 "organization Person"

From a public policy privacy protection requirements perspective, an "organization Person" is a "natural person" who acts on behalf of and makes commitments on behalf of the organization (or public administration) of which that natural person is an "organization part". But, as an "organization Person, they do not attract inherent rights to privacy. Privacy protection requirements which do apply to an organization Person are placed in an employee-employer context with associated contractual elements. In addition, some jurisdictional domains have privacy protection laws and regulations which apply specifically to employees of their public administrations.

As such, from a business transaction perspective, it is an internal behaviour of an organization, as to who makes commitments on behalf of an organization or public administration. How and why organization Persons make decisions and commitments is not germane to the scope and purpose of this part of ISO/IEC 15944. {See further ISO/IEC 15944-1:2011, Clause 6.2 "*Person and external constraints: Individual, organization, and public administration"* as well as its Figure 17 "*Illustration of commitment exchange versus information exchange for organization, organization part(s) and organization Person(s)*"}

1.2.4 Overlap of and/or conflict among jurisdictional domains as sources of privacy protection requirements

A business transaction requires an exchange of commitments among autonomous parties. Commitment is the making or accepting of a right, an obligation, liability or responsibility by a Person. In the context of a business transaction, the making of commitments pertains to the transfer of a good, service and/or right among the Persons involved.

Consequently, it is not an uncommon occurrence, depending on the goal and nature of the business transaction, that the Persons (and parties associated) are in different jurisdictional domains, and that multiple sets of external constraints apply, and overlap will occur. It is also not an uncommon occurrence that there is overlap among such sets of external constraints and/or conflict among them. This is also the case with respect

to laws and regulations of a privacy protection nature. Resolving issues of this nature is outside the scope of this part of ISO/IEC 15944.

However, modelling business transaction as scenarios and scenario components as re-useable business objects may well serve as a useful methodology for identifying specific overlaps and conflicts (thereby serving as a tool for their harmonization, if only within the context of a specific transaction).

The application of business semantic descriptive techniques to laws, regulations, etc., of jurisdictional domains and their modelling of such sets of external constraints as scenarios and scenario components is an essential step to their application in a systematic manner to (electronic) business transactions (and especially e-government, e-commerce, e-education, etc.).

Open-edi business agreement descriptive techniques methodologies can serve as a tool in the harmonization and simplification of external constraints arising from jurisdictional domains.

NOTE This part of ISO/IEC 15944 is based on the following assumptions:

1) the privacy protection requirements of the individual, as a buyer in a business transaction, are those of the jurisdictional domain in which the individual made the commitments associated with the instantiated business transaction; and,

2) where the seller is in a jurisdictional domain other than that of the individual, as the buyer, this edition of ISO/IEC 15944 incorporates and supports the *"OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data"*.[See further below Clause 2.2]

1.2.5 Publicly available personal information

Excluded from the scope of this part of ISO/IEC 15944 is "publicly available personal information" (PAPI). In a business transaction context, the seller does not collect personal information of this nature from the individual (particularly in the "planning phase" of the business transaction process).

For example, the seller in advertising product to the market may:

1) publish personal information that is publicly available personal information, such as that found in telephone directories;

2) make use of any personal information declared to be of a public information by a regulation based on an law or regulation of the applicable jurisdictional domain; and, or,

3) include that which the individual itself chose to make public, (e.g., via one or more Internet based applications such as "Facebook").

In a privacy protection context, publicly available personal information is defined as follows:

publicly available personal information (PAPI)

personal information about an **individual** that the **individual** knowingly makes or permits to be made available to the public, or is legally obtained and accessed from: (a) government records that are available to the public; or, (b) information required by law to be made available to the public

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

EXAMPLE 2 Examples of 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.

Further, determining whether or not personal information is of a "PAPI" nature is also excluded from the scope of this part of ISO/IEC 15944.

1.3 Aspects currently not addressed

This part of ISO/IEC 15944 focuses on the essential and basic aspects of privacy protection requirements. The purpose of this Clause is to identify aspects not currently addressed. These will be addressed in either:

a) an Amendment to this part of ISO/IEC 15944,

b) new editions of this part of ISO/IEC 15944,

c) through a new part of ISO/IEC 15944,

d) in a new edition of an existing part of ISO/IEC 15944 (as may be applicable),

e) through a new edition of an existing standard of ISO/IEC JTC1, or another existing ISO/IEC JTC1/SC, or ISO, IEC or ITU; and/or,

f) new standard(s) by any of the above noted committees.

ISO/IEC 15944-8 also does yet address the following requirements:

1) differences in equality in the use of official languages by an individual, in being informed and exercising privacy protection rights within a jurisdictional domain[18];

2) interworking between privacy protection and consumer protection requirements as two sets of external constraints applicable to an individual as a buyer in a business transaction;

3) identification and registration of schemas involving the control and management of legally recognized names (LRNs) as personas and associated unique identifiers for the unambiguous identification of an individual and/or the role qualification of an individual in a specific context;

4) more detailed information management and audit requirements pertaining to ensuring privacy protection of personal information that should be enacted by and among organizations and public administrations as parties to a business transaction;

5) more detailed rules and associated text pertaining to the BOV perspective with respect to transborder data flows of personal information;

6) inter-operation between jurisdictional domains where they do not possess defined equivalents to their protection requirements (interoperability) or where protection requirements simply are different;

7) instances in which privacy protection requirements continue to apply to the personal information of an individual after his/her death;

   In addition, from a business transaction perspective, there may be some continuity in privacy protection requirements, (e.g., those pertaining to temporal aspects of post-actualization aspects of an instantiated business transaction, (e.g., health care matters, warranties on products, service contracts, rights (including IP), etc.). Instantiated business transactions may require personal information to be retained and continue to be protected following the death of the individual.

---

[18] This part of ISO/IEC 15944 focuses on the essential basic, i.e. primitive, aspect of jurisdictional domains as sources of external constraints. As such this edition of ISO/IEC 15944-8 does not address differences in status that may exist among official languages within a jurisdictional domain. It is not uncommon that where a jurisdictional domain has three or more official languages that not all of these have equal status. For example, for use of some official language(s) in a jurisdictional domain, there could be criteria such as “where and when numbers warrant”, “there is a significant demand for communication with and services from a public administration in that language”, etc. This impacts both the language in which personal information is recorded by an organization or public administration as well as the language of communications of the individual with the organization in a business transaction.

NOTE 1 This may also include a settlement of wills, probate, investments, etc., pertaining to that individual once proved deceased.

NOTE 2 Tax information filed has 4-6 years record retention requirements in most jurisdictional domains. In some jurisdictional domains, tax matters are confidential and in others they are public. The status of personal information may change as a result of litigation and public hearings.

NOTE 3 Instantiated business transactions may require personal information to be retained and continue to be protected following the death of an individual, (e.g., many credit card agreements exist after the death of the credit card holder).

NOTE 4 One may need to have an added Clause on privacy protection of personal information on individuals consequent upon the death of the individual.

8) personal information found in journalistic reports:

The use of personal information in a business transaction which is found in journalistic reports including news items, public broadcasts, items published by news media about an individual, personal information published and made available by third parties on the internet, (e.g., via Google, Facebook, Twitter, etc.), which in some jurisdictional domains is held to be "in the public interest", is not included in this part of ISO/IEC 15944.

The reasons for exclusion are that a journalistic report containing personal information about an individual:

- may contain inaccurate information, allegations, and thus should not (can not) be used as "personal information";
- may be subject to libel and other legal actions by the individual;
- etc.

Further issues pertaining to privacy protection versus journalistic reports on identified individuals resulting in the publishing of personal information is a "grey area" which courts in various jurisdictional domains are addressing and thus not yet resolved;

9) this part of ISO/IEC 15944 does not address the question of negotiated consent, but rather considers the simplest case, that a scenario may be registered which includes a specific form of consent within it;

10) the use of biological characteristics and attributes of an individual which require the physical presence of an individual and are physically "taken" from an individual in a particular context and for a specified role action of an individual;

These include the use of biometrics, biological (such as hair, blood, DNA samples), dentistry records, etc.

11) the application of the rights of individuals who are disabled as stated in the "UN Convention on the Rights of Persons with Disabilities" (2006)[19];

Of particular importance here is that this UN Convention takes as its basis the need to support individuals with disabilities to be a fully functioning member of society means that information necessary for these individuals to be able to make commitments including the undertaking of business transactions shall be made available in a form and format so that the semantics are fully communicated, the individual is able to have informed consent, etc.

[19] Most, if not all, of the jurisdictional domains of the P-members of ISO/IEC JTC1 are signatories to this UN Convention and are enacting the requirements of this UN Convention into their domestic legislation.

12) this part of ISO/IEC 15944 does not address the role of an “ombudsperson”, “Privacy Commissioner”, a “Data Protection Commissioner”, etc., who serves as an independent adjudicator of complaints and ensures compliance with privacy protection requirements (including of internally of the organization or public administration themselves);

    Many jurisdictional domains provide for the role of an ombudsperson which may be a role similar in application to public administration.

13) detailed rules pertaining to the use of agents and/or third parties by a seller in a business transaction

    This includes their qualification and assurance of compliance with applicable privacy protection requirements for the personal information pertaining to a business transaction.

14) an agent acting on behalf of an individual

    An individual may request an agent to act on its behalf and this may or may not include the individual to require the agent not to reveal the individual identity or any personal information about the individual, i.e., as an anonymous “client” of the agent.

15) detailed rules governing the requirement to tag (or label) at the data elements (or field) level which form part of personal information of an individual generally as is required for as the business transactions(s) and its associated BTI(s);

16) mergers and acquisitions

    It is presumed that when an organization “A” merges with, or is acquired by another organization “B”, that the privacy protection requirements applicable to personal information under the control of organization “A” continue to apply and be enforced. It is also assumed the personal information under the control of organization “A” remains under its control and that a merger with or acquisition by organization “B” does not allow organization “B” to access and/or use personal information held by organization “A” without the express and informed consent of the individuals whose personal information is/was organization “A”.

17) ICT and other service providers

    It is presumed that any ICT (or other) services provider which is under contract to provide ICT services to an organization or public administration (which has personal information under its control) shall not access or use such personal information processed as part of its services offering to that organization, unless it has a formal contractual arrangement to do so, in compliance with applicable privacy protection requirements.

18) data mining

    It is also presumed that an organization shall ensure that any data mining activities undertaken by itself (or via an agent or third party on its behalf) shall be in compliance with applicable privacy protection requirements, and not involve any secondary use or any other use of personal information for which the individual(s) concerned have not provided explicitly informed consent.

19) formal Conformance Statements

    Clause 13 below deals with conformance requirements at the most primitive level only. More detailed conformance statements with associated rules and procedures are required in implementation. It is also necessary to ensure that any such conformance statement, i.e., declaration by an organization or public administration is “verifiable”.

20) linkages and similarities between privacy protection and consumer protection requirements

Many of the external constraints pertaining to personal information of a privacy protection nature in a business transaction are similar to consumer protection requirements. {See further below Clause 7.2.2}

It is anticipated that some or all of these requirements will be addressed in future editions of ISO/IEC 15944-8 or in companion standards or technical reports (including possible new parts of ISO/IEC 15944).

1.4 IT-systems environment neutrality

This part of ISO/IEC 15944 does not assume nor endorse any specific system environment, database management system, database design paradigm, system development methodology, data definition language, command language, system interface, user interface, syntax, computing platform, or any technology required for implementation, i.e., it is information technology neutral. At the same time, this part of ISO/IEC 15944 maximizes an IT-enabled approach to its implementation and maximizes semantic interoperability.

THIS PAGE INTENTIONALLY LEFT BLANK

2 Normative references

The following referenced documents are indispensable for the application 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.

2.1 ISO/IEC, ISO and ITU[20]

ISO 639-2:1998(E/F), *Codes for the representation of names of languages — Part 2: Alpha-3 code/Codes pour la représentation des noms de langue — Partie 2: Code alpha-3*

ISO 1087-1:2000(E/F), *Terminology work — Vocabulary — Part 1: Theory and application/Travaux terminologiques — Vocabulaire — Partie 1: Théorie et application*

ISO/IEC 2382 (all parts) (E/F), *Information technology — Vocabulary/Technologies de l'information — Vocabulaire*

ISO 3166-1:2006(E/F), *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes/Codes pour la représentation des noms de pays et de leur subdivisions — Partie 1: Codes pays*

ISO 3166-2:2007(E/F), *Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code/Codes pour la représentation des noms de pays et de leurs subdivisions — Partie 2: Code pour les subdivisions de pays*

ISO 5127:2001(E), *Information and documentation — Vocabulary*

ISO/IEC 5218:2004(E/F), *Information technology — Codes for the representation of human sexes/ Technologies de l'information — Codes de représentation des sexes humains*

ISO/IEC 6523-1:1998(E/F), *Information technology — Structure for the identification of organizations and organization parts — Part 1: Identification of organization identification schemes/Technologies de l'information — Structures pour l'identification des organisations et des parties d'organisations — Partie 1: Identification des systèmes d'identification d'organisations*

ISO/IEC 6523-2:1998(E/F), *Information technology — Structure for the identification of organizations and organization parts — Part 2: Registration of organization identification schemes/Technologies de l'information — Structures pour l'identification des organisations et des parties d'organisations — Partie 2: Enregistrement des systèmes d'identification d'organisations*

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

ISO/IEC 7501-2:1997(E), *Identification cards — Machine readable travel documents — Part 2: Machine readable visa*

ISO/IEC 7501-3:2005(E), *Identification cards — Machine readable travel documents — Part 3: Machine readable official travel documents*

ISO/IEC 7812-1:2006(E), *Identification cards — Identification of issuers — Part 1: Numbering system*

ISO/IEC 7812-2:2007(E), *Identification cards — Identification of issuers — Part 2: Application and registration procedures*

---

20 For standards referenced for which both English and French versions are available both the English and French language titles are provided. This is independent of whether the English and French language versions of the standard are published as a single document or as separate documents. For those standards which are available in English only, only the English language title is provided.

ISO 8601:2004(E), *Data elements and interchange formats — Information interchange — Representation of dates and times*

ISO/IEC 14662:2010(E/F), *Information technology — Open-edi reference model/Technologies de l'information — Modèle de référence EDI-ouvert*

ISO/IEC 15944-1:2011(E), *Information technology — Business Operational View — Part 1: Operational aspects of Open-edi for implementation*

ISO/IEC 15944-2:2006(E), *Information technology — Business Operational View — Part 2: Registration of scenarios and their components as business objects*

ISO/IEC 15944-4:2007(E), *Information technology — Business Operational View — Part 4: Business transactions and scenarios — Accounting and economic ontology*

ISO/IEC 15944-5:2008(E), *Information technology — Business Operational View — Part 5: Identification and referencing of requirements of jurisdictional domains as sources external constraints*

ISO/IEC 15944-7:2009(E), *Information technology — Business Operational View — Part 7: eBusiness vocabulary*

ISO 19108:2002(E), *Geographic information — Temporal schema*

ISO/IEC 19501:2005(E), *Information technology— Open Distributed Processing — Unified Modeling Language (UML) Version 1.4.2*[21]

ISO 22857:2004(E), *Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health information*

2.2 Referenced specifications[22]

APEC Privacy Framework. (2005)

Charter of the United Nations (as signed 1945 and Amended 1965, 1968, and 1973+), United Nations (UN).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) Directive

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

UN Convention on the Rights of Disabled Persons (2006+)

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

21 Throughout this part of ISO/IEC 15944, ISO/IEC 19501:2005 is simply referenced as “UML”.

22 All references in this sub-clause were correct at the time of approval of this part of ISO/IEC 15944. The provisions of the referenced specifications, as identified in this sub-clause, are valid within the context of this part of ISO/IEC 15944. The reference to a specification within this part of ISO/IEC 15944 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.

3 Terms and definitions

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

3.1
address
set of **data elements** that specifies a **location** to which a **recorded information** item(s), a **business object**(s), a material **object**(s) and/or a person(s) can be sent or from which it can be received

NOTE 1 An address can be specified as either a physical address and/or electronic address.

NOTE 2 In the identification, referencing and retrieving of registered business objects, it is necessary to state whether the pertinent recorded information is available in both physical and virtual forms.

NOTE 3 In the context of Open-edi, a “recorded information item” is modelled and registered as an Open-edi scenario (OeS), Information Bundle (IB) or Semantic Component (SC).

[ISO/IEC 15944-2:2006 (3.1)]

3.2
agent
Person acting for another **Person** in a clearly specified capacity in the context of a **business transaction**

NOTE Excluded here are agents as "automatons" (or robots, bobots, etc.). In ISO/IEC 14662:2009, "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)".

[ISO/IEC 15944-1:2011 (3.1)]

3.3
anonymization
process whereby the association between a **set of recorded information (SRI)** and an identifiable **individual** is removed where such an association may have existed

NOTE Adapted from ISO 25237.

3.4
attribute
characteristic of an **object** or **entity**

[ISO/IEC 11179-3:2003 (3.1.3)]

3.5
authentication
provision of assurance of the claimed identity of an **entity**

[ISO/IEC 10181-2:1996 (3.3)]

3.6
authenticity
property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information

NOTE Authenticity applies to entities such as users, processes, systems and information.

[ISO/IEC TR 13335-1:1996 (3.3)

3.7
business
series of **processes**, each having a clearly understood purpose, involving more than one **Person**, realised through the exchange of **recorded information** and directed towards some mutually agreed upon goal, extending over a period of time

[ISO/IEC 14662:2010 (3.1.2)]

3.8
business event
occurrence in time that **partners** to a **business transaction** wish to monitor or control

NOTE 1 Business events are the workflow tasks that business partners need to accomplish to complete a business transaction among themselves. As business events occur, they cause a business transaction to move through its various phases of planning, identification, negotiation, actualization, and post-actualization.

NOTE 2 Occurrences in time can either be:

(1) internal as mutually agreed to among the parties to a business transaction; and/or,

(2) reference some common publicly available and recognized date/time referencing schema, (e.g., one based on using the ISO 8601 and/or ISO 19135 standards).

[ISO/IEC 15944-4:2007 (3.5)]

3.9
business object
unambiguously identified, specified, referenceable, registered and re-useable **Open-edi scenario** or **scenario component** of a **business transaction**

NOTE As an “object”, a “business object” exists only in the context of a business transaction.

[ISO/IEC 15944-2:2006 (3.6)]

3.10
Business Operational View (BOV)
perspective of **business transactions** limited to those aspects regarding the making of **business** decisions and **commitments** among **Persons**, which are needed for the description of a **business transaction**

[ISO/IEC 14662:2010 (3.1.3)]

3.11
business transaction
predefined set of activities and/or **processes** of **Persons** which is initiated by a **Person** to accomplish an explicitly shared **business** goal and terminated upon recognition of one of the agreed conclusions by all the involved **Persons** although some of the recognition may be implicit

[ISO/IEC 14662:2010 (3.1.4)]

3.12
business transaction identifier (BTI)
identifier assigned by a **seller** or a **regulator** to an instantiated **business transaction** among the **Persons** involved

NOTE 1 The identifier assigned by the seller or regulator shall have the properties and behaviours of an “identifier (in a business transaction)”.

NOTE 2 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 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 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).

[ISO/IEC 15944-5: 2008 (3.12)]

3.13
buyer
Person 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

[ISO/IEC 15944-1:2011 (3.8)]

3.14
characteristic
abstraction of a **property** of an **object** or of a set of **objects**

NOTE Characteristics are used for describing concepts.

[ISO 1087-1:2000 (3.2.4)]

3.15
character set
finite set of different **characters** that is complete for a given purpose

EXAMPLE The international reference version of the character set of ISO 646-1.

[ISO/IEC 2382-4:1999 (04.01.02)]

3.16
classification system
systematic **identification** and arrangement of **business** activities and/or **scenario components** into categories according to logically structured conventions, methods and procedural **rules** as specified in a classification schema

NOTE 1 The classification code or number often serves as a semantic identifier (SI) for which one or more human interface equivalents (HIEs) exist.

NOTE 2 The rules of a classification schema governing the operation of a classification system at times lead to the use of ID codes which have an intelligence built into them, (e.g., in the structure of the ID, the manner in which it can be parsed, etc.). Here the use of block-numeric numbering schemas is an often used convention.

[ISO/IEC 15944-5:2008 (3.17)]

3.17
code
data representation in different forms according to a pre-established set of **rules**

NOTE In this part of ISO/IEC 5944 the "pre-established set of rules" are determined and enacted by a Source Authority and must be explicitly stated.

[ISO 639-2:1998 (3.1)]

3.18
code (in coded domain)
identifier, i.e., an **ID code**, assigned to an **entity** as member of a **coded domain** according to the pre-established set of **rules** governing that **coded domain**

[ISO/IEC 15944-5:2008 (3.19)]

3.19
coded domain
domain for which (1) the boundaries are defined and explicitly stated as a **rulebase** of a **coded domain Source Authority**; and (2) each **entity** which qualifies as a member of that domain is identified through the assignment of a unique **ID code** in accordance with the applicable **Registration Schema** of that **Source Authority**

NOTE 1 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 of the Source Authority.

NOTE 2 Source Authorities which are jurisdictional domains are the primary source of coded domains.

NOTE 3 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 Associated with a code in a coded domain can be:

- one and/or more equivalent codes;
- one and/or more equivalent representations especially those in the form of Human Interface Equivalent (HIE) (linguistic) expressions.

NOTE 5 In a coded domain the rules for assignment and structuring of the ID codes must be specified.

NOTE 6 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 must be specified as the pivot ID code.

NOTE 7 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 A coded domain may contain 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 Common examples include: (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 In object methodology, entities which are members of a coded domain are referred to as instances of a class.

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

[ISO/IEC 15944-2:2006 (3.13)]

3.20
coded Domain Registration Schema (cdRS)
formal **definition** of both (1) the **data** fields contained in the **identification** and specification of an **entity** forming part of the members a **coded domain** including the allowable contents of those fields; and, (2) the **rules** for the assignment of **identifiers**

[ISO/IEC 15944-5:2008 (3.21)]

3.21
coded domain Source Authority (cdSA)
Person, usually an **organization**, as a **Source Authority** which sets the **rules** governing a **coded domain**

NOTE 1 Source Authority is a role of a Person and for widely used coded domains the coded domain Source Authority is often a jurisdictional domain.

NOTE 2 Specific sectors, (e.g., banking, transport, geomatics, agriculture, etc.), may have particular coded domain Source Authority (ies) whose coded domains are used in many other sectors.

NOTE 3 A coded domain Source Authority usually also functions as a Registration Authority but can use an agent, i.e., another Person, to execute the registration function on its behalf.

[ISO/IEC 15944-2:2006 (3.14)]

3.22
collaboration space
business activity space where an economic exchange of valued resources is viewed independently and not from the perspective of any **business** partner

NOTE In collaboration space, an individual partner's view of economic phenomena is de-emphasized. Thus, the common use business and accounting terms like purchase, sale, cash receipt, cash disbursement, raw materials, and finished goods is not allowed because they view resource flows from a participant's perspective.

[ISO/IEC 15944-4:2007 (3.12)]

3.23
commitment
making or accepting of a right, obligation, liability or responsibility by a **Person** that is capable of enforcement in the **jurisdictional domain** in which the **commitment** is made

[ISO/IEC 14662:2010 (3.5)]

3.24
composite identifier
identifier (in a business transaction) functioning as a single unique **identifier** consisting of one or more other **identifiers**, and/or one or more other **data elements**, whose interworkings are **rule**-based

NOTE 1 Identifiers (in business transactions) are for the most part composite identifiers.

NOTE 2 The rules governing the structure and working of a composite identifier should be specified.

NOTE 3 Most widely used composite identifiers consist of the combinations of:

- the ID of the overall identification/numbering schema, (e.g., ISO/IEC 6532, ISO/IEC 7812, ISO/IEC 7506, UPC/EAN, ITU-T E.164, etc.), which is often assumed;
- the ID of the issuing organization (often based on a block numeric numbering schema); and,
- the ID of the entities forming part of members of the coded domain of each issuing organization.

[ISO/IEC 15944-2:2006 (3.16)]

3.25
computational integrity
expression of a **standard** in a form that ensures precise description of behaviour and semantics in a manner that allows for automated processing to occur, and the managed evolution of such **standards** in a way that enables dynamic introduction by the next generation of information systems

NOTE Open-edi standards have been designed to be able to support computational integrity requirements especially from a registration and re-use of business objects perspectives.

[ISO/IEC 15944-2:2006 (3.17)]

3.26
constraint
rule, explicitly stated, that prescribes, limits, governs or specifies any aspect of a **business transaction**

NOTE 1 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 For constraints to be registered for implementation in Open-edi, they must have unique and unambiguous identifiers.

NOTE 3 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".

[ISO/IEC 15944-1:2011 (3.11)]

3.27
consumer
buyer who is an **individual** to whom **consumer protection** requirements are applied as a set of **external constraints** on a **business transaction**

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

NOTE 2 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 jurisdiction, such external constraints should be specified as part of scenario components as applicable.

NOTE 3 It is recognized that external constraints on a buyer of the nature of consumer protection may be peculiar to a specified jurisdiction.

[ISO/IEC 15944-1:2011 (3.12)]

3.28
consumer protection
set of **external constraints** of a **jurisdictional domain** as rights of a **consumer** and thus as obligations (and possible liabilities) of a **vendor** in a **business transaction** which apply to the good, service and/or right forming the **object** of the **business transaction** (including associated information management and interchange requirements including applicable (**sets of**) **recorded information**

NOTE 1 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 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 (13) birthday).

NOTE 3 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.

[ISO/IEC 15944-5:2008 (3.33)]

3.29
controlled vocabulary (CV)
vocabulary for which the entries, i.e., **definition**/**term** pairs, are controlled by a **Source Authority** based on a **rulebase** and **process** for addition/deletion of entries

NOTE 1 In a controlled vocabulary, there is a one-to-one relationship of definition and term.

EXAMPLE The contents "Clause 3 Definitions" in ISO/IEC standards are examples of controlled vocabularies with the entities being identified and referenced through their ID codes, i.e., via their clause numbers.

NOTE 2 In a multilingual controlled vocabulary, the definition/term pairs in the languages used are deemed to be equivalent, i.e., with respect to their semantics.

NOTE 3 The rule-base governing a controlled vocabulary may include a predefined concept system.

[ISO/IEC 15944-5:2008 (3.34)]

3.30
data (in a business transaction)
representations of **recorded information** that are being prepared or have been prepared in a form suitable for use in a **computer system**

[ISO/IEC 15944-1:2011 (3.14)]

3.31
data element
unit of **data** for which the **definition**, **identification**, representation and permissible values are specified by means of a set of **attributes**

[ISO/IEC 11179-1:2004 (3.3.8)]

3.32
data element (in organization of data)
unit of **data** that is considered in context to be indivisible

EXAMPLE The data element "age of a person" with values consisting of all combinations of 3 decimal digits.

NOTE Differs from the entry 17.06.02 in ISO/IEC 2382-17.

[ISO/IEC 2382-04:1998 (04.07.01)]

3.33
dataset
identifiable collection of **data**

NOTE A dataset may be a smaller grouping of data which, though limited by some constraint such as spatial extent or feature type, is located physically within a larger dataset. Theoretically, a dataset may be as small as a single feature or feature attribute contained within a larger dataset. A hardcopy map or chart may be considered a dataset.

[ISO 19115:2003 (4.2)]

3.34
dataset series
collection of **datasets** sharing the same product specification

[ISO 19115:2003 (4.3)]

3.35
data synchronization (in business transaction)
process of continuous harmonization of a **set(s)** of **recorded information** among all the parties to a **business transaction** to ensure that the current state of such a **set(s)** of **recorded information** is the same in the **IT systems** of all the participating parties

NOTE Adapted from GS1 Global Traceability Standard (GDSN) Glossary.

3.36
Decision Making Application (DMA)
model of that part of an **Open-edi system** that makes decisions corresponding to the **role**(s) that the **Open-edi Party** plays as well as the originating, receiving and managing **data** values contained in the instantiated **Information Bundles** which is not required to be visible to the other **Open-edi Parties**

[ISO/IEC 14662:2010 (3.7)]

3.37
de facto language
natural language used in a **jurisdictional domain** which has the properties and behaviours of an **official language** in that **jurisdictional domain** without having formally been declared as such by that **jurisdictional domain**

NOTE 1 A de facto language of a jurisdictional domain is often established through long term use and custom.

NOTE 2 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.

[ISO/IEC 15944-5:2008 (3.42)]

3.38
definition
representation of a concept by a descriptive statement which serves to differentiate it from related concepts

[ISO/IEC 1087-1:2000 (3.3.1)]

3.39
designation
representation of a concept by a sign which denotes it

NOTE In terminology work three types of designations are distinguished: symbols, appellations and terms.

[ISO 1087-1:2000 (3.4.1 adapted)]

3.40
distinguishing identifier
data that **unambiguously** distinguishes an **entity** in the **authentication** process

[ISO/IEC 10181-2:1996]

3.41
eBusiness
business transaction, involving the making of **commitments**, in a defined **collaboration space**, among **Persons** using their **IT systems**, according to **Open-edi standards**

NOTE 1 eBusiness can be conducted on both a for-profit and not-for-profit basis.

NOTE 2 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 eBusiness includes various application areas such as e-commerce, e-administration, e-logistics, e-government, e-medicine, e-learning, etc.

NOTE 4 The equivalent French language term for “eBusiness” is always presented in its plural form.

[ISO/IEC 15944-7:2009 (3.06)]

3.42
electronic address
address used in a recognized electronic addressing scheme, (e.g., telephone, telex, IP, etc.), to which **recorded information** item(s) and/or **business object**(s) can be sent to or received from a **Contact**

[ISO/IEC 15944-2:2006 (3.32)]

3.43
Electronic Data Interchange (EDI)
automated exchange of any predefined and structured **data** for **business** purposes among information systems of two or more **Persons**

NOTE This definition includes all categories of electronic business transactions.

[ISO/IEC 14662:2010 (3.8)]

3.44
entity
any concrete or abstract thing that exists, did exist, or might exist, including associations among these things

EXAMPLE A person, object, event, idea, process, etc.

NOTE An entity exists whether data about it are available or not.

[ISO/IEC 2382-17:1999 (17.02.05)]

3.45
entity authentication
corroboration that the **entity** is the one claimed

[ISO/IEC 9798-1:1997 (3.3.11)

3.46
exchange code set
set of **ID codes** identified in a **coded domain** as being suitable for information exchange as shareable **data**

EXAMPLE The 3-numeric, 2-alpha and 3-alpha code sets in ISO 3166-1.

[ISO/IEC 15944-5:2008 (3.49)]

3.47
external constraint
constraint which takes precedence over **internal constraints** in a **business transaction**, i.e., is external to those agreed upon by the parties to a **business transaction**

NOTE 1 Normally external constraints are created by law, regulation, orders, treaties, conventions or similar instruments.

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

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

NOTE 4 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 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 must be recorded.

EXAMPLE 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 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".

[ISO/IEC 15944-1:2011 (3.23)]

3.48
Formal Description Technique (FDT)
specification method based on a description **language** using rigorous and **unambiguous rules** both with respect to developing expressions in the **language** (formal syntax) and interpreting the meaning of these expressions (formal semantics)

[ISO/IEC 14662:2010 (3.9)]

3.49
Functional Service View (FSV)
perspective of **business transactions** limited to those information technology interoperability aspects of **IT Systems** needed to support the execution of **Open-edi transactions**

[ISO/IEC 14662:2010 (3.10)]

3.50
Human Interface Equivalent (HIE)
representation of the **unambiguous** and **IT-enabled** semantics of an **IT interface equivalent** (in a **business transaction**), often the **ID code** of a **coded domain** (or a **composite identifier**), in a formalized manner suitable for communication to and understanding by humans

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

NOTE 2 In most cases there will be multiple Human Interface Equivalent representations as required to meet localization requirements, i.e., those of a linguistic nature, jurisdictional nature, and/or sectoral nature.

NOTE 3 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.).

[ISO/IEC 15944-2:2006 (3.35)]

3.51
IB Identifier
unique, linguistically neutral, **unambiguous** referenceable **identifier** for an **Information Bundle**

[ISO/IEC 15944-2:2006 (3.36)]

3.52
ID Code
identifier assigned by the **coded domain Source Authority** (**cdSA**) to a member of a **coded domain** ID

NOTE 1 ID codes must be unique within the Registration Schema of that coded domain.

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

NOTE 3 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 must be specified as the pivot ID code.

NOTE 4 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 must be predefined and explicitly stated.

EXAMPLE Common examples include: (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 In UML modeling notation, an ID codes is viewed as an instance of an object class.

[ISO/IEC 15944-2:2006 (3.37)]

3.53
identification
rule-based **process**, explicitly stated, involving the use of one or more **attributes**, i.e., **data elements**, whose value (or combination of values) are used to identify uniquely the occurrence or existence of a specified **entity**

[ISO/IEC 15944-1:2011 (3.26)]

3.54
identifier (in business transaction)
unambiguous, unique and a linguistically neutral value, resulting from the application of a **rule**-based **identification process**

NOTE 1 Identifiers must be unique within the identification scheme of the issuing authority.

NOTE 2 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).

[ISO/IEC 15944-1:2011 (3.27)]

3.55
individual
Person who is a human being, i.e., a natural person, who acts as a distinct indivisible **entity** or is considered as such

[ISO/IEC 15944-1:2011 (3.28)]

3.56
individual accessibility
set of **external constraints** of a **jurisdictional domain** as rights of an **individual** with disabilities to be able to use **IT systems** at the human, i.e., user, interface and the concomitant obligation of a **seller** to provide such adaptive technologies

NOTE Although “accessibility” typically addresses users who have a disability, the concept is not limited to disability issues.

EXAMPLE Examples of disabilities in the form of functional and cognitive limitations include:

- people who are blind;
- people with low vision;
- people with colour blindness;
- people who are hard of hearing or deaf, i.e., are hearing impaired;
- people with physical disabilities;
- people with language or cognitive disabilities.

[ISO/IEC 15944-5:2008 (3.60)]

3.57
individual anonymity
state of not knowing the identity or no having any recording of **personal information** on or about an **individual** as a **buyer** by the **seller** or **regulator**, (or any other party) to a **business transaction**

3.58
individual authentication
provision of the assurance of a **recognized individual identity (rii)** sufficient for the purpose of the **business transaction**

3.59
individual identity (ii)
Person identity of an **individual**, i.e., an individual identity, consisting of the combination of the **persona** information and **identifier** used by an **individual** in a **business transaction**, i.e., the making of any kind of **commitment**

3.60
individual persona Registration Schema (ipRS)
persona Registration Schema (pRS) where the **persona** is, or includes, that of an **individual** being registered

NOTE 1 Where an persona Registration Schema includes persona of sub-types of Persons, i.e., individuals, organizations, and/or, public administrations, those which pertain to individuals shall be identified as such because public policy as external constraints apply including those of a privacy protection requirements nature.

NOTE 2 In an individual persona Registration Schema, one shall state whether or not a truncated name, i.e. registered persona, of the individual, is allowed or mandatory, and if so the ipRS shall explicitly state the rules governing the formation of the same.

3.61
Information Bundle (IB)
formal description of the semantics of the **recorded information** to be exchanged by **Open-edi Parties** playing **roles** in an **Open-edi scenario**

[ISO/IEC 14662:2010 (3.11)]

3.62
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**, 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**

3.63
Information Processing Domain (IPD)
Information Technology System which includes at least either a **Decision Making Application** and/or one of the components of an **Open-edi Support Infrastructure**, and acts/executes on behalf of an **Open-edi Party** (either directly or under a delegated authority)

[ISO/IEC 14662:2010 (3.12)]

3.64
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

[ISO/IEC 14662:2010 (3.12)]

3.65
internal constraint
constraint which forms part of the **commitment**(s) mutually agreed to among the parties to a **business transaction**

NOTE 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.

[ISO/IEC 15944-1:2011 (3.33)]

3.66
IT-enablement
transformation of a current **standard** used in **business transactions**, (e.g., **coded domains**), from a manual to computational perspective so as to be able to support **commitment** exchange and **computational integrity**

[ISO/IEC 15944-5:2008 (3.48)]

3.67
IT-interface equivalent
computer processable **identification** of the **unambiguous** semantics of a scenario, **scenario attribute** and/or **scenario component**(s) pertaining to a **commitment** exchange in a **business transaction** which supports **computational integrity**

NOTE 1 IT interface equivalents have the properties of identifiers (in business transaction) and are used to support semantic interoperability in commitment exchange.

NOTE 2 The value of an IT interface equivalent at times is a composite identifier.

NOTE 3 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 An IT interface equivalent is at times used as a semantic identifier.

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

NOTE 6 The value of an IT Interface is independent of its encoding in programming languages or APIs.

[ISO/IEC 15944-2:2006 (3.45)]

3.68
jurisdictional domain
jurisdiction, recognized in law as a distinct legal and/or regulatory framework, which is a source of **external constraints** on **Persons**, their behaviour and the making of **commitments** among **Persons** including any aspect of a **business transaction**

NOTE 1 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 Jurisdictional domains can combine to form new jurisdictional domains, (e.g., through bilateral, multilateral and/or international treaties).

EXAMPLE Included here, for example, are the European Union (EU), NAFTA, WTO, WCO, ICAO, WHO, Red Cross, the ISO, the IEC, the ITU, etc.

NOTE 3 Several levels and categories of jurisdictional domains may exist within a jurisdictional domain.

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

NOTE 5 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.

[ISO/IEC 15944-5:2008: (3.67)]

3.69
jurisdictional domain identifier
ID code of a **jurisdictional domain** as recognized for use by peer **jurisdictional domains** within a system of mutual recognition

[ISO/IEC 15944-2:2006 (3.47)]

3.70
language
system of signs for communication, usually consisting of a **vocabulary** and **rules**

NOTE In this part of ISO/IEC 15944, language refers to natural languages or special languages, but not "programming languages" or "artificial languages".

[ISO 5127-1:2001 (1.1.2.01)]

3.71
language code
combination of **characters** used to represent a **language** or **languages**

NOTE In this multipart ISO/IEC 15944 standard, the ISO 639-2/T (terminology) three alpha-code, shall be used.

[ISO 639-2:1998 (3.2. adapted)]

3.72
legally recognized language (LRL)
natural language which has status (other than an **official language** or **de facto language**) in a **jurisdictional domain** 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 The LRL can be specified through either:

- the identification of a language by the name used; or,
- the identification of a people and thus their language(s).

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

[ISO/IEC 15944-5:2008 (3.71)]

3.73
legally recognized name (LRN)
persona associated with a **role** of a **Person** recognized as having legal status and so recognized in a **jurisdictional domain** as accepted or assigned in compliance with the **rules** applicable of that **jurisdictional domain**, i.e. as governing the **coded domain** of which the **LRN** is a member

NOTE 1 A LRN may be of a general nature and thus be available for general use in commitment exchange or may arise from the application of a particular law, regulation, program or service of a jurisdictional domain and thus will have a specified use in commitment exchange.

NOTE 2 The process of the establishment of a LRN is usually accompanied by the assignment of a unique identifier.

NOTE 3 A LRN is usually a registry entry in a register established by the jurisdictional domain (usually by a specified public administration within that jurisdictional domain) for the purpose of applying the applicable rules and registering and recording LRNs (and possible accompanying unique identifiers accordingly).

NOTE 4 A Person may have more than one LRN (and associated LRN identifier).

[ISO/IEC 15944-5:2008 (3.72)]

3.74
list
ordered set of **data elements**

[ISO/IEC 2382-4:1999 (04.08.01)]

3.75
localization
pertaining to or concerned with anything that is not global and is bound through specified sets of **constraints** of:

(a) a linguistic nature including natural 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 behaviour requirements; and/or,

(f) safety or health requirements.

Within and among "locales", interoperability and harmonization objectives also apply

[ISO/IEC 15944-5:2008 (3.75)]

3.76
location
place, either physical or electronic, that can be defined as an **address**

[ISO/IEC 15944-2:2006 (3.50)]

3.77
medium
physical material which serves as a functional unit, in or on which information or **data** 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 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 The inclusion of the "non-volatile in nature" attribute is to cover latency and records retention requirements.

NOTE 3 This definition of "medium" is independent of:

i) the form or format of recorded information;

ii) the physical dimension and/or size; and,

iii) any container or housing that is physically separate from material being housed and without which the medium can remain a functional unit.

NOTE 4 This definition of "medium" also captures and integrates the following key properties:

i) the property of medium as a material in or on which information or data can be recorded and retrieved;

ii) the property of storage;

iii) the property of physical carrier;

iv) the property of physical manifestation, i.e., material;

v) the property of a functional unit; and,

vi) the property of (some degree of) stability of the material in or on which the information or data is recorded.

[ISO/IEC 15944-1:2011 (3.34)]

3.78
model
abstraction of some aspect of reality

[ISO 19115:2003 (4.9)]

3.79
multilingualism
ability to support not only **character sets** specific to a (**natural**) **language** (or family of **languages**) and associated **rules** but also **localization** requirements, i.e., use of a **language** from **jurisdictional domain**, sectoral and/or **consumer** marketplace perspectives

[ISO/IEC 15944-5:2008 (3.82)]

3.80
mutually defined - recognized individual identity (md-rii)
recognized individual identity (rii) which is mutually defined and agreed to for use between the **seller** and the i**ndividual**, as **buyer**, in a **business transaction**

NOTE 1 The establishment of a mutually agreed to and recognized individual between a seller and individual, as buyer, does not extinguish the applicable privacy protection rights of that individual.

NOTE 2 A mutually defined recognized individual identity (md-rii) shall be established between the seller and the individual no later than the end of the negotiation phase.

NOTE 3 Use of a mutually defined recognized individual identity (md-rii) may not be permitted where external constraints apply.

3.81
name
designation of an **individual** concept by a linguistic expression

NOTE Adapted from ISO 1087-1:2000.

[ISO 5217:2000 (1.1.2.02)]

3.82
natural language
language which is or was in active use in a community of people, and the **rules** of which are mainly deduced from the usage

[ISO 5217:2000 (1.1.2.02)]

3.83
object
anything perceivable or conceivable.

NOTE 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).

[ISO 1087-1:2000 (3.1.1)]

3.84
object class
set of ideas, abstractions, or things in the real world that can be identified with explicit boundaries and meaning and whose properties and behaviour follow the same **rules**

[ISO/IEC 11179-1:2004 (3.3.22)]

3.85
official language
external constraint in the form of a **natural language** specified by a **jurisdictional domain** for official use by **Persons** forming part of and/or subject to that **jurisdictional domain** for use in communication(s) either:

(1) within that **jurisdictional domain**; and/or,

(2) among such **Persons**, where such communications are **recorded information** involving **commitment**(s)

NOTE 1 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 A jurisdictional domain decides whether or not it has an official language. If not, it will have a de facto language.

NOTE 3 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 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 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 must be specified.

NOTE 6 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 Another example is that of Norway which has two official writing systems, both Latin-1 based, namely, Bokmål (Dano-Norwegian) and Nynorsk (New Norwegian).

NOTE 7 A jurisdictional domain may have more than one official language but these may or may not have equal status.

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

NOTE 8 The BOV requirement of the use of a specified language will place that requirement on any FSV supporting service.

EXAMPLE 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.

[ISO/IEC 15944-5:2008 (3.87)]

3.86
Open-edi
electronic data interchange among multiple autonomous **Persons** to accomplish an explicit shared **business** goal according to Open-edi standards

[ISO/IEC 14662:2010 (3.14)]

3.87
Open-edi Description Technique (OeDT)
specification method such as a **Formal Description Technique**, another methodology having the characteristics of a **Formal Description Technique**, or a combination of such techniques as needed to formally specify **BOV** concepts, in a computer processable form

[ISO/IEC 14662:2010 (3.16)]

3.88
Open-edi disposition
process governing the implementation of formally approved records retention, destruction (or expungement) or transfer of **recorded information** under the control of a **Person** which are documented in disposition authorities or similar instruments

NOTE Adapted from ISO 15489-1.

[ISO/IEC 15944-5:2008: (3.90)]

3.89
Open-edi Party (OeP)
Person that participates in **Open-edi**

NOTE Often in this ISO/IEC 15944-1 standard referred to generically as "party" or "parties" for any entity modelled as a Person as playing a role in Open-edi scenarios.

[ISO/IEC 14662:2010 (3.17)]

3.90
Open-edi Record Retention (OeRR)
specification of a period of time that a **set of recorded information** must be kept by a **Person** in order to meet operational, legal, regulatory, fiscal or other requirements as specified in the **external constraints** (or **internal constraints**) applicable to a **Person** who is a party to a **business transaction**

[ISO/IEC 15944-5:2008 (3.92)]

3.91
Open-edi system
information technology system which enables an **Open-edi Party** to participate in **Open-edi** transactions

[ISO/IEC 14662:2010 (3.22)]

3.92
organization
unique framework of authority within which a person or persons act, or are designated to act, towards some purpose

NOTE 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 and/or services including:

1) partnerships;

2) social or other non-profit organizations or similar bodies in which ownership or control is vested in a group of individuals;

3) sole proprietorships;

4) governmental bodies.

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

[ISO/IEC 6523-1: 1998 (3.1)]

3.93
organization part
any department, service or other **entity** within an **organization**, which needs to be identified for information interchange

[ISO/IEC 6523-1:1998 (3.2)]

3.94
organization Person
organization part which has the properties of a **Person** and thus is able to make **commitments** on behalf of that **organization**

NOTE 1 An organization can have one or more organization Persons.

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

NOTE 3 An organization Person can be a "natural person" such as an employee or officer of the organization.

NOTE 4 An organization Person can be a legal person, i.e., another organization.

[ISO/IEC 15944-1:2011 (3.46)]

3.95
Person
entity, i.e., a natural or legal person, recognized by law as having legal rights and duties, able to make **commitment**(s), assume and fulfil resulting obligation(s), and able of being held accountable for its action(s)

NOTE 1 Synonyms for "legal person" include "artificial person", "body corporate", etc., depending on the terminology used in competent jurisdictions.

NOTE 2 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 Minimum and common external constraints applicable to a business transaction often require one to differentiate among three common subtypes of Person, namely "individual", "organization", and "public administration".

[ISO/IEC 14662:2010 (3.24)]

3.96
Person authentication
provision of the assurance of a **recognized Person identity** (**rPi**) (sufficient for the purpose of the **business transaction**) by corroboration

[ISO/IEC 15944-1:2011 (3.48)]

3.97
persona
set of **data elements** and their values by which a **Person** wishes to be known and thus identified in a **business transaction**

[ISO/IEC 15944-1:2010 (3.51)]

3.98
persona Registration Schema (pRS)
formal **definition** of the **data** fields contained in the specification of a **persona** of a **Person** and the allowable contents of those fields, including the **rules** for the assignment of **identifiers**. (This may also be referred to as a **persona** profile of a **Person**)

[ISO/IEC 15944-1:2011 (3.52)]

3.99
personal information
any information on or about an identifiable **individual** that is recorded in any form, including electronically or on paper

NOTE Some examples would be information about a person's religion, age, financial transactions, medical history, address, or blood type.

[ISO/IEC 15944-5:2008 (3.103)]

3.100
Person identity (Pi)
combination of **persona information** and **identifier** used by a **Person** in a **business transaction**

[ISO/IEC 15944-1:2011 (3.49)]

3.101
Person signature
signature, i.e., a **name** representation, distinguishing mark or usual mark, which is created by and pertains to a **Person**

[ISO/IEC 15944-1:2011 (3.50)]

3.102
personal information filing system
any structured set of personal information which is accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis

3.103
physical address
address that is used/recognized by a postal authority and/or courier service to deliver information item(s), material **object**(s), or **business object**(s) to a **Contact** at either an actual **address** or a pick-up point **address**, (e.g., P.O. Box, rural route, etc.)

[ISO/IEC 15944-2:2006 (3.80)]

3.104
pivot code set
set of **ID codes** in a **coded domain** which is made publicly known and available, the most stable, representing the defined semantics. Most often it is the same as the **ID code**

NOTE 1 The use of the pivot code set as distinguished from the ID code supports the requirement of a Source Authority to maintain internally and on a confidential basis the ID code of its members.

NOTE 2 At times a coded domain has more than one valid code set, (e.g., ISO 639, ISO 3166, etc.).

EXAMPLE In ISO 3166-1 the 3-digit numeric code is the pivot. The 2-alpha and 3-alpha code sets can change when the name of the entity referenced is changed by that entity.

[ISO/IEC 15944-5:2008: (3.104)]

3.105
pivot ID code
most stable **ID code** assigned to identify a member of a **coded domain** where more than one **ID code** may be assigned and/or associated with a member of that **coded domain**

EXAMPLE ISO 3166-1:2006 (E/F) "Codes for the representation of names of countries and their subdivisions — Part 1: Country codes/Codes pour la représentation des noms de pays et de leur subdivisions — Partie 1: Codes pays" contains three code sets:

- a three digit numeric code;
- a two alpha code
- a three alpha code.

Here, the three digit numeric code serves as the pivot ID code. It is the most stable, remains the same even though the two alpha and/or three alpha codes may and do change.

[ISO/IEC 15944-5:2008: (3.105)]

3.106
principle
fundamental, primary assumption and quality which constitutes a source of action determining particular objectives or results

NOTE 1 A principle is usually enforced by rules that affect its boundaries.

NOTE 2 A principle is usually supported through one or more rules.

NOTE 3 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.

[ISO/IEC 15944-2:2006 (3.80)]

3.107
privacy collaboration space (PCS)
modelling or inclusion of an **Open-edi scenario** of a **collaboration space** involving an **individual** as the **buyer** in a potential or actualized **business transaction** where the **buyer** is an **individual** and therefore privacy protection requirements apply to personal information of that individual provided in that **business transaction**

3.108
privacy protection
set of **external constraints** of a **jurisdictional domain** pertaining to **recorded information** on or about an identifiable **individual**, i.e., **personal information**, 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 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 Privacy requirements include the right of an individual to be able to view the recorded information about him/her and to request corrections to the same in order to ensure that such recorded information is accurate and up-to-date, or have it deleted.

NOTE 3 Where jurisdictional domains have legal requirements which override privacy protection requirements these must be specified, (e.g., national security, investigations by law enforcement agencies, etc.).

[ISO/IEC 15944-5:2008 (3.109)]

3.109
privacy protection officer (PPO)
organization Person authorized by the **organization** to act on behalf of that **organization** and entrusted by the **organization** as the officer responsible for the overall governance and implementation of the privacy protection requirements for information life cycle management not only within that **organization** but also with respect to any **electronic data interchange** of **personal information** on the **individual** concerned with parties to the **business transaction**, including a **regulator** where required, as well as any **agents**, **third parties** involved in that **business transaction**

3.110
process
series of actions or events taking place in a defined manner leading to the accomplishment of an expected result

[ISO/IEC 15944-1:2011 (3.53)]

3.111
processing of personal information
any operation or set of operations which is performed upon personal data, 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 or destruction

3.112
property
peculiarity common to all members of an **object class**

[ISO/IEC 11179-1:2004(3.3.29)]

3.113
pseudonym
use of a **persona** or other **identifier** by an **individual** which is different from that used by the **individual** with the intention that it be not linkable to that **individual**

NOTE Adapted from ISO TS 25237.

3.114
pseudonymization
particular type of anonymization that removes the associate with an **individual** and adds an associate between a particular set of **characteristics** relating to the **individual** and one more **pseudonym**

NOTE Adapted from ISO TR 25237.

3.115
public administration
entity, i.e., a **Person**, which is an **organization** and has the added **attribute** of being authorized to act on behalf of a **regulator**

[ISO/IEC 15944-1:2011 (3.54)]

3.116
public policy
category of **external constraints** of a **jurisdictional domain** specified in the form of a right of an **individual** or a requirement of an **organization** and/or **public administration** with respect to an **individual** pertaining to any exchange of **commitments** among the parties concerned involving a good, service and/or right including information management and interchange requirements

NOTE 1 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 15944-1:2010}.

NOTE 2 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 (13) 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 Jurisdictional domains may have consumer protection or privacy requirements which apply specifically to individuals who are considered to be "children", "minors", etc. (e.g. those who have not reached their 18th or 21st birthday according to the rules of the applicable jurisdictional domain).

[ISO/IEC 15944-5:2008 (3.113)]

3.117
publicly available personal information (PAPI):
personal information about an **individual** that the **individual** knowingly makes or permits to be made available to the public, or is legally obtained and accessed from: a) government records that are available to the public; or, b) information required by law to be made available to the public

EXAMPE 1 Examples of 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, etc.

EXAMPLE 2 Examples of 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.

3.118
recognized individual identity (rii)
identity of an **individual,** i.e., **individual identity**, established to the extent necessary for the specific purpose of a business transaction

3.119
recognized individual name (RIN)
persona of an **individual** having the properties of a **legally recognized name** (**LRN**)

NOTE 1 On the whole, a persona presented by an individual should have a basis in law (or recognized jurisdictional domain) in order to be considered as the basis for a recognized individual name (RIN).

NOTE 2 An individual may have more than one RIN and more than one RIN at the same time.

NOTE 3 The establishment of a RIN is usually accompanied by the assignment of a unique identifier, i.e. by the jurisdictional domain (or public administration) which recognizes the persona as a RIN.

[ISO/IEC 15944-5:2008 (3.114)]

3.120
recognized Person identity (rPi)
identity of a **Person**, i.e., **Person identity**, established to the extent necessary for a specific purpose in a **business transaction**

[ISO/IEC 15944-1:2011 (3.55)]

3.121
recorded information
information that is recorded on or in a **medium** irrespective of form, recording **medium** or technology used, and in a manner allowing for storage and retrieval

NOTE 1 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 Through the use of the term "information," all attributes of this term are inherited in this definition.

NOTE 3 This definition covers:

(i) any form of recorded information, means of recording, and any medium on which information can be recorded; and,

(ii) all types of recorded information including all data types, instructions or software, databases, etc.

[ISO/IEC 15944-1:2011 (3.56)]

3.122
register
set of files containing identifiers assigned to items with descriptions of the associated items

[ISO 19135:2005 (4.1.9)]

3.123
registration
rule-based **process**, explicitly stated, involving the use of one or more **data elements,** whose value (or combination of values) is used to identify uniquely the results of assigning an **OeRI**

[ISO/IEC 15944-2:2006 (3.94)]

3.124
Registration Authority (RA)
Person 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**)

[ISO/IEC 15944-1:2011 (3.57)]

3.125
Registration Authority Identifier (RAI)
identifier assigned to a **Registration Authority** (**RA**)

[ISO/IEC 11179-1:2004 (3.3.32)]

3.126
Registration Schema (RS)
formal **definition** of a set of **rules** governing the **data** fields for the description of an **entity** and the allowable contents of those fields, including the **rules** for the assignment of **identifiers**

[ISO/IEC 15944-1:2011 (3.58)]

3.127
Registration Schema (based) –recognized individual identity (RS-rii)
recognized individual identity (rii) for use in a **business transaction**, by the buyer as an **individual**, which is one based on the use by an **individual** as a member of a specified **Registration Schema (RS**) of a particular **Registration Authority (RA)**

3.128
registry
information system on which a **register** is maintained

[ISO/IEC 19135:2005 (4.1.13)]

3.129
regulator
Person who has authority to prescribe **external constraints** which serve as **principles**, policies or **rules** governing or prescribing the behaviour of **Persons** involved in a **business transaction** as well as the provisioning of goods, services, and/or rights interchanged

[ISO/IEC 15944-1:2011 (3.59)]

3.130
regulatory business transaction (RBT)
class of **business transactions** for which the explicitly shared goal has been established and specified by a **jurisdictional domain**, as a **Person** in the **role** of a **regulator**

NOTE 1 A regulatory business transaction (RBT) can itself be modelled as a stand-alone business transaction and associated scenario(s). For example, the filing of a tax return, the making of a customs declaration, the request for and issuance of a license, the provision of a specified service of a public administration, a mandatory filing of any kind with a regulator, etc.

NOTE 2 A regulatory business transaction (modelled as a scenario) can form part of another business transaction.

NOTE 3 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 A RBT may require or prohibit the use of an agent or third party.

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

[ISO/IEC 15944-5:2008 (3.124)]

3.131
retention period
length of time for which **data** on a **data medium** is to be preserved

[ISO/IEC 2382-12:1988 (12.04.11)]

3.132
role
specification which models an external intended behaviour (as allowed within a scenario) of an **Open-edi Party**

[ISO/IEC 14662:2010 (3.25)]

3.133
rule
statement governing conduct, procedure, conditions and relations.

NOTE 1 Rules specify conditions that must be complied with. These may include relations among objects and their attributes.

NOTE 2 Rules are of a mandatory or conditional nature.

NOTE 3 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: -content of the information flows in the form of precise and computer-processable meaning, i.e. the semantics of data; and, -the order and behaviour of the information flows themselves.

NOTE 4 Rules must be clear and explicit enough to be understood by all parties to a business transaction. Rules also must 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)".

NOTE 5 Specification of rules in an Open-edi business transaction should be compliant with the requirements of ISO/IEC 15944-3 "Open-edi Description Techniques (OeDT)".

[ISO/IEC 15944-2:2006 (3.100)]

3.134
rulebase
pre-established set of **rules** which interwork and which together form an autonomous whole

NOTE One considers a rulebase to be to rules as database is to data.

[ISO/IEC 15944-2:2006 (3.101)]

3.135
SC identifier
unique, linguistically neutral, **unambiguous**, referenceable **identifier** of a **Semantic Component**

[ISO/IEC 15944-2:2006 (3.101)]

3.136
scenario attribute
formal specification of information, relevant to an **Open-edi scenario** as a whole, which is neither specific to **roles** nor to **Information Bundles**

[ISO/IEC 14662:2010 (3.26)]

3.137
scenario component
one of the three fundamental elements of a scenario, namely **role**, **Information Bundle**, and **Semantic Component**

[ISO/IEC 15944-2:2006 (3.103)]

3.138
scenario content
set of recorded information containing **registry** entry **identifiers**, labels and their associated **definitions** and related **recorded information** posted (or reposted) in any **registry** for **business objects**

[ISO/IEC 15944-2:2006 (3.104)]

3.139
scenario specification attribute
any **attribute** of a scenario, **role**, **Information Bundle**, and/or **Semantic Component**

[ISO/IEC 15944-2 2006 (3.105)]

3.140
seller
Person 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

[ISO/IEC 15944-1:2011 (3.62)]

3.141
Semantic Component (SC)
unit of **recorded information** unambiguously defined in the context of the **business** goal of the **business transaction**

NOTE A SC may be atomic or composed of other SCs.

[ISO/IEC 14662:2010 (3.27)]

3.142
semantic identifier (SI)
IT-interface identifier for a **semantic component** or other semantic for which (1) the associated context, applicable **rules** and/or possible uses as a semantic are predefined and structured and the **Source Authority** for the applicable **rulebase** is identified and (2) for which more than one or more **Human Interface Equivalents**(**HIEs**) exist

NOTE The identifier for a Semantic Component (SC), an Information Bundle (IB) and/or an ID Code for which one or more Human Interface Equivalents (HIEs) exist are considered to have the properties or behaviours of semantic identifiers.

[ISO/IEC 15944-5:2008 (3.136)]

3.143
set of recorded information (SRI)
recorded information of an **organization** or **public administration**, which is under the control of the same and which is treated as a unit in its information life cycle

NOTE 1 A 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 A 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 A 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.

[ISO/IEC 15944-5:2008 (3.137)]

3.144
Source Authority (SA)
Person recognized by other **Persons** as the authoritative source for a set of **constraints**

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

NOTE 2 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 A Person as an individual shall not be a Source Authority for external constraints.

NOTE 4 Source Authorities are often the issuing authority for identifiers (or composite identifiers) for use in business transactions.

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

NOTE 6 Where the sets of constraints of a Source Authority control a coded domain, the SA have the role of a coded domain Source Authority.

[ISO/IEC 15944-2:2006 (3.108)]

3.145
special language
language for special purposes (LSP), **language** used in a subject field and characterized by the use of specific linguistic means of expression

NOTE The specific linguistic means of expression always include subject-specific terminology and phraseology and also may cover stylistic or syntactic features.

[ISO 1087-1:2000 (3.1.3)]

3.146
standard
documented agreement containing technical specifications or 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

NOTE 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)}.

[ISO/IEC 15944-1:2011 (3.64)]

3.147
term
designation of a defined concept in a **special language** by a linguistic expression

NOTE A term may consist of one or more words i.e. simple term, or complex term or even contain symbols.

[ISO 1087-1:2000 (3.4.3)]

3.148
text
data in the form of **characters**, 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.

[ISO/IEC 2382-23:1994 (23.01.01)]

3.149
third party
Person besides the two primarily concerned in a **business transaction** who is **agent** of neither and who fulfils a specified **role** or function as mutually agreed to by the two primary **Persons** or as a result of **external constraints**

NOTE It is understood that more than two Persons can at times be primary parties in a business transaction.

[ISO/IEC 15944-1:2011 (3.65)]

3.150
treaty
international agreement concluded among **jurisdictional domains** in written form and governed by international law

NOTE 1 On the whole a treaty is concluded among UN member states.

NOTE 2 Treaties among UN member states when coming into force are required to be transmitted to the Secretariat of the United Nations for registration or filing or recording as the case may be and for publication. {See further Article 80 or the Charter of the UN}

NOTE 3 Treaties can also be entered into by jurisdictional domains other than UN member states, i.e. non-members such as international organizations and the rare sub-national units of federations which are constitutionally empowered to do so.

NOTE 4 A treaty can be embodied in a single instrument or in two or more related instruments and whatever its particular designations. However, each treaty is a single entity.

NOTE 5 Jurisdictional domains can make agreements which they do not mean to be legally binding such as for reasons of administrative convenience or expressions of political intent only, (e.g., as a Memorandum of Understanding (MOU)).

NOTE 6 Adapted from the Vienna Convention on the Law of Treaties, 1(a).

[ISO/IEC 15944-5:2008 (3.144)]

3.151
truncated name
short form of a **name** or **persona** of a **Person** resulting from the application of a **rule**-based **truncation process**

[ISO/IEC 15944-5:2008 (3.145)]

3.152
truncated recognized name (TRN)
truncated name, i.e., **persona**, of a **Person** which has the properties of a **legally recognized name** (**LRN**)

NOTE 1 Truncated recognized name(s) may be required for use in machine-readable travel documents, (e.g., passports or visas), identity tokens, drivers' licenses, Medicare cards, etc.).

NOTE 2 The source of a truncated recognized name may be a legally recognized name (LRN).

[ISO/IEC 15944-5:2008 (3.146)]

3.153
truncation
rule-base **process**, explicitly stated, for shortening an existing **name** of an **entity** to fit within a predefined maximum length (of **characters**)

NOTE Truncation may be required for the use of names in IT systems, electronic data interchange (EDI), the use of labels in packaging, in the formation of a Person identity (Pi), etc.

[ISO/IEC 15944-5:2008 (3.147)]

3.154
unambiguous
level of certainty and explicitness required in the completeness of the semantics of the **recorded information** interchanged appropriate to the goal of a **business transaction**

[ISO/IEC 15944-1:2011 (3.66)]

3.155
vendor
seller on whom **consumer protection** requirements are applied as a set of **external constraints** on a **business transaction**

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

NOTE 2 It is recognized that external constraints on a seller of the nature of consumer protection may be peculiar to a specified jurisdiction.

[ISO/IEC 15944-1:2011 (3.67)]

3.156
vocabulary
terminological dictionary which contains **designations** and **definitions** for one or more specific subject fields

NOTE The vocabulary may be monolingual, bilingual or multilingual.

[ISO 1087-1:2000 (3.7.2)]

THIS PAGE INTENTIONALLY LEFT BLANK

4 Symbols and abbreviations

For the purposes of this document, the following symbols and abbreviations apply.

Acronym	Description
API	Application Programming Interface
BOV	Business Operational View
BTI	Business Transaction Identifier
BTM	Business Transaction Model
cdRS	coded domain Registration Schema
cdSA	coded domain Source Authority
CV	controlled vocabulary
DMA	Decision Making Application
DMA Interface	Decision Making Application Interface
EC	European Community
EDI	Electronic Data Interchange
EU	European Union
FDT	Formal Description Technique
FSV	Functional Service View
HIE	Human Interface Equivalent
IB	Information Bundle
IEC	International Electrotechnical Commission
ii	individual identity
IPD	Information Processing Domain
ipRS	individual persona Registration Schema
ISO	International Organization for Standardization
IT System	Information Technology System
ITU	International Telecommunications Union
ITU-R	International Telecommunications Union – Radiocommunications Sector
ITU-T	International Telecommunications Union – Telecommunications Sector
JTC1	Joint Technical Committee 1 “Information Technology” (of the ISO and IEC)
LRL	Legally Recognized Language
LRN	Legally Recognized Name

md-rii	mutually defined – recognized individual identity
OeBTO	Open-edi Business Transaction Ontology
OeDT	Open-edi Descriptive Techniques
OeORI	Open-edi Registration Organization Identifier
OeP	Open-edi Party
OeR	Open-edi Registry
OeRA	Open-edi Registration Authority
OeRI	Open-edi Registry Item
OeRO	Open-edi Registration Organization
OeRR	Open-edi Records Retention
OeS	Open-edi scenario
OeSI	Open-edi Support Infrastructure
PAPI	publicly available personal information
PCS	privacy collaboration space
pRS	persona Registration Schema
RA	Registration Authority
RAI	Registration Authority Identifier
RBT	Regulatory Business Transaction
rii	recognized individual identity
RIN	Recognized Individual Name
rPi	recognized Person identity
RA	Registration Authority
RS	Registration Schema
RS-rii	Registration Schema (based) – recognized individual identity
SA	Source Authority
SC	Semantic Component
SI	Semantic Identifier
SRI	set of recorded information
TRN	truncated recognized name
UML	Unified Modelling Language
UN	United Nations

5 Fundamental principles and assumptions governing privacy protection requirements in business transactions involving individuals (external constraints perspective)

5.1 Introduction

Clause 5 introduces a fundamental set of principles and assumptions based on two primary sources; namely:

1) those already stated in other parts of the ISO/IEC 15944 eBusiness standards which are of relevance to privacy protection requirements; and,

2) those introduced explicitly in this part of ISO/IEC 15944 addressing the BOV aspects of privacy protection.

Whilst there is acknowledgement that information must, of necessity, be exchanged in the furtherance of the goals and actualization of a business transaction, many jurisdictional domains require that where personal information is concerned particular external constraints apply, i.e., where the buyer is an individual as a party to a business transaction.

Although legislation and regulations of a privacy/data protection nature differ among jurisdictional domains, where they exist there are many common elements. A high level review and analysis of privacy/data protection legislation in Australia, Canada, Japan, USA, (and APEC member states), the EU, and Norway as well as Europe (both at the EU level and that of component countries (and within country such as those of länder within Germany), etc., indicates that they have common primitive requirements. These have been captured and integrated below into a single set of common privacy protection principles.

The three most common and international recognized and accepted sources for privacy protection requirements are:

- the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data / Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel[23]
- the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data / Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[24]
- the 2005 APEC Privacy Framework[25]

These three normative references, i.e., as referenced specifications, are indispensable to the understanding and use of this document. As such, they shall be referenced by users and implementers of this document. In addition, the following normative references also apply in a similar nature and shall be referenced.

These are stated in the following referenced specifications which shall apply and must be referenced. These three sources of external constraints indentified are crucial to the understanding and use of this document. They shall be referenced and used by those implementing this part of ISO/IEC 15944. In addition, the following three normative references are also essential to the understanding and use of this part of ISO/IEC 15944 and shall be used; namely:

---

23 http://www.oecd.org/document/53/0,3343,fr_2649_34255_15591797_1_1_1_1,00.html.

24 This 1995 Directive is supplemented by the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) / DIRECTIVE 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 12 JUILLET 2002 CONCERNANT LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL ET LA PROTECTION DE LA VIE PRIVÉE DANS LE SECTEUR DES COMMUNICATIONS ÉLECTRONIQUES DIRECTIVE VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

25 http://publications.apec.org/publication-detail.php?pub_id=390

a) the Charter of the United Nations

b) the UN Convention on the Rights of Persons with Disabilities; and,

c) the Vienna Convention on the Law of the Treaties.

The essential aspects of each of these eleven (11) common privacy protection principles and their requirements are captured below in the form of rules[26]. It is noted that for organizations and public administrations to be able to comply with these rules as external constraints which apply to them, surrounding and overarching business processes and systems may be required to be changed to be able to support external constraints of this nature.

The approach to the development of the 11 principles governing privacy protection requirements is illustrated in the following Figure 3 below.

[26] The development of the Parts of the multipart ISO/IEC 15944 set of eBusiness standards focuses on common primitives which are captured in the form of principles and their rules along with clearly defined concepts, i.e. as a rule-based approach in support of the Business Operational View. This is required to ensure unambiguity in the modelling of business agreement semantic descriptive techniques through Open-edi scenarios and scenario components.

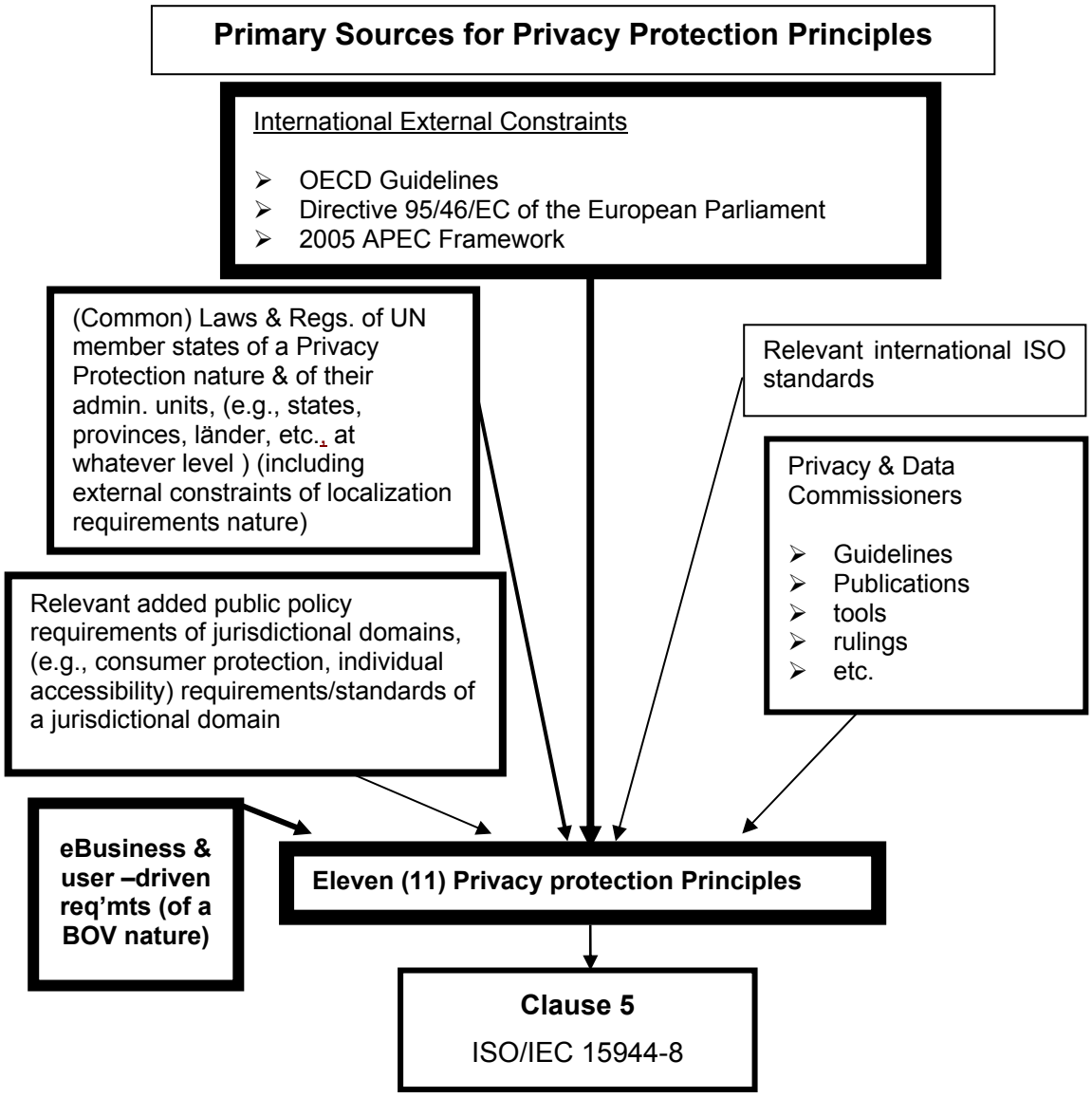


Figure 3 — Primary sources for privacy protection principles

In the text which follows, these eleven (11) Privacy Protection principles are placed in a LET and learning transaction context, i.e. that of the parties making a commitment on a commonly agreed upon goal for a learning transaction.

From a FSV perspective, this includes ensuring that the IT systems of an organization provide the technical implementation measures which must be capable of exchanging the necessary information among the parties to a business transaction. This is necessary to be able to determine when personal information is to be processed as against all other recorded information forming part of the business transaction. This includes ensuring that applicable controls are in place in the Decision Making Applications (DMAs) of the IT systems of organizations (and public administration) where personal information is processed and interchanged among all parties to a business transaction[27].

[27] On Decision Making Applications (DMAs), Information Processing Domain (IPD) and Open-edi Support Infrastructure (OeSI) in IT systems, see further Clause 5.2 *Functional Service View* in ISO/IEC 14662:2010 (3rd edition) and its Figure 3 *Open-edi system relationships*.

Finally, the privacy protection principles enumerated below represent a whole and should be interpreted and implemented as a whole and not piecemeal. Be aware that in subsequent clauses of this part of ISO/IEC 15944, two or more of the privacy protection principles referenced may be instantiated simultaneously.

5.2 Exceptions to the application of the privacy protection principles

Privacy protection requirements of jurisdictional domains may contain exceptions (derogations) to the application of external constraints of this nature. The most common exceptions are those relating to national sovereignty and security, law enforcement, public safety and health.

Exceptions of this nature often requires access to personal information about a particular individual and the tracing of any other personal information pertaining to that individual[28], (e.g., access to personal information by particular Persons other than those who are parties to the business transaction, i.e., qualified and specified public administrations based on predefined criteria).

Rule 001:

Where exceptions to the application of privacy protection principles exist, they shall be:

1) **limited and proportional[29] to meeting the objectives to which these exceptions relate; and,**

2) **a) made known to the public; or,**

   b) in accordance with law.

5.3 Fundamental Privacy Protection Principles[30]

5.3.1 Privacy Protection Principle 1: Preventing Harm

Rule 002:

The protection of personal information shall be designed to prevent the misuse of such personal information.

A primary objective of the preventing harm principle is to prevent misuse of personal information, and consequently harm to individuals[31]. Therefore, the implementation of privacy protection, including self-regulatory efforts, education, and awareness campaigns, as well as enforcement mechanisms, etc., should be a priority governance principle of any organization and public administration which provides a good, service and/or right to an individual by a business transaction using electronic means,

---

28 Traceability issues including those pertaining to individuals are being addressed in the ISO/IEC 15944-9 "Traceability Framework" standard which is under development.

29 In relation to "limited and proportional", the *APEC Privacy Framework*, Clause 13 states that "The Principles contained in Part III of the APEC Privacy Framework should be interpreted as a whole rather than individually, as there is a close relationship among them." It goes on to state that countries implementing the Framework "may adopt suitable exceptions that suit their particular circumstances." Further, "one should take into consideration the impact of these activities," i.e. invocation of an exception, "upon the rights, responsibilities and legitimate interests of individuals."

30 The purpose here is simply to present, in summary form and in a non-technical BOV manner, key common privacy/data protection requirements as promulgated. Other groupings of Privacy/Data Protection Principles have been published elsewhere; and some may have more or fewer than these ten "principles". The same set of requirements can also be grouped differently or have different titles.

31 This privacy protection principle is introduced in the *APEC Privacy Framework*. It can be considered an application of the generic aspect of the human rights of "do no harm", already a well and long established principle in the field of medicine.

This requirement also applies to both the business operational view (BOV) and functional services view (FSV) of the organization (and/or public administration) and especially to the interchange of personal information among parties to a business transaction.

5.3.2 Privacy Protection Principle 2: Accountability

Rule 003:

An organization subject to privacy protection requirements in the jurisdictional domain (at whatever level[32]) in which it delivers a good, service and/or rights, shall have in place implemented, enforceable policies and procedures with the proper accountability controls required to ensure its compliance with applicable privacy protection requirements.

This means that the ability to comply with applicable privacy protection requirements is a precondition for an organization to be able to offer goods, services and/or rights to individuals in that jurisdictional domain.

Rule 004:

An organization[33] is responsible for all personal information under its control and shall designate an organization Person, i.e. a privacy protection officer (PPO), who is accountable for the organization's compliance with established privacy principles which, in turn, are compliant with and support the legal requirements of a privacy protection nature of the applicable jurisdictional domain(s) in which the organization operates.

In practice, this means that at any time, in the process of an individual establishing a business transaction with an organization or public administration, the individual is informed of the presence of a privacy protection officer (PPO) within the organization who has been assigned this role[34]. Most organizations already do so in the 'planning phase' of the process for a business transaction by making such information readily available in their catalogue(s), on their website, etc.

Rule 005:

Any organization to which privacy protection requirements apply shall have in place policies and practices which make it clear as to who (and where), in an enforceable and auditable manner, in their business operations is responsible for compliance with these external constraints as applicable to the conduct of business transactions where the buyer is an individual.

Guideline 005G:

Organizations should ensure that their accountability policies, practices and controls are supported, if not embedded, in the operations of their DMAs in their IT systems to ensure that the personal information of individuals is managed through its information life cycle in compliance with applicable privacy protection requirements.

It is recognized "best practice" that the design and operation of an organization's IT systems in support of its business operations should implement not only the information management polices of the organization but also, and especially, any external constraints which may apply. In this context Privacy protection requirements

---

32 In some jurisdictional domains, privacy protection requirements are found at the UN member state level, an administrative unit of the UN member state, at a municipal level, or at any combination of the same.

33 The use of the term "organization" in these Privacy Protection Principles includes "public administration".

34 Within an organization it is a common and well accepted practice to label any organization Person who has a (legal) responsibility at the organization–wide level as an "officer", i.e., one who has an "official" responsibility on behalf of the organization as a whole. The concept/term "controller" within an organization is usually related to "financial controls".

represent a defined set of external constraints of jurisdictional domains which apply when and where the buyer is an individual.[35]

It is not uncommon that in the "actualization" of a business transaction that the seller may well utilize one or more "agents", now commonly known as "outsourcing". The role of such agents (of whatever nature and role) may range from a simple transport delivery role to one including the undertaking of many other business operational functions which a seller may delegate to an agent (and in some cases also a third party, i.e. where the use of such a designated third party is either mandated by the rules of the applicable jurisdictional domain in which the business transaction is taking place, and/or the seller and buyer, i.e., as an individual agree to such an arrangement (e.g., using a mutually. At the same time, it is also not uncommon that the actualization of the business transaction involves the use of third parties. The use and role of third parties may be mutually consented to by the buyer and seller, i.e. as part of modelling internal constraints, or be mandatory based on the requirements of an applicable regulator, i.e. as external constraints.

Privacy protection requirements which apply to the organization when providing a good, service and/or right to a buyer who is an individual often do not address directly the aspect of delegates (subcontractors) of role or functions in a business transaction delegated to an agent or third party. Commonly, the organization acting as the seller, i.e., as primary party, remains responsible and accountable for ensuring that privacy protection requirements are complied with for that business transaction regardless of how or where it is delivered.

Rule 006:

Where an organization, as a seller, delegates any aspect of a business transaction involving an individual , and interchanges of personal information pertaining to that individual, to an "agent" (and/or "third party"), the organization shall ensure that: (1) in its arrangement with the designated agent (and/or third party), the agent (and/or third party) is fully aware of the applicable privacy protection requirements; and, (2) such parties commit themselves to support the applicable privacy protection requirements pertaining to the business transaction[36].

This rule is consistent with the overall approach that delegation of a BOV or FSV aspects (including scenario components) to an agent (and/or third party) of commitments made by a Person as a seller in a business transaction apply to any combination of agents and/or third parties where the seller may delegate a BOV or FSV aspect to them.

It is noted that should an organization make use of an agent in the instantiation of a business transaction where the buyer is an individual and thus personal information is involved, that the organization remains responsible for ensuring that privacy protection requirements are complied with.

Guideline 006G1:

Prior to an organization delegating part (or all) of the instantiation of a business transaction to an agent, the organization should obtain (written) assurance of the "agent's compliance with privacy protection requirements and particularly in the DMAs in the IT systems of the agent.

With respect to the engagement of a third party in a business transaction, it is already stated in Clause 6.2.5 of ISO/IEC 15944-1, that a third party is not an agent of either the buyer or seller but is one who fulfils a specific role or function in the execution of a business transaction as mutually agreed to by the two primary Persons or as a result of applicable external constraints.

---

35 Privacy protection is but one set of external constraints of a public policy nature which apply when the buyer is an individual. Others include those of a consumer protection, individual accessibility, etc. nature. {See further below, Clause 7 "*Public policy requirements of jurisdictional domains*"}

36 One should note that whether or not the seller in an business transaction, decides to delegate one or more role or functions (if permitted in a scenario) to an agent and/or third party, that this is immaterial to the fact that the seller shall ensure that it maintains control of any and all of the personal information associated with a business transaction where the buyer is an individual.

Guideline 006G2:

Where a third party is involved in a business transaction involving personal information, the seller and buyer should be provided with the (legally binding) assurance of the "third party's compliance with privacy protection requirements and particularly in the DMAs in the IT systems of the third party.

Guideline 006G3:

Where:

1) ***due to the nature of the good, service and/or right of the goal of the business transaction external constraints of a jurisdictional domain, mandate the use of a third party; and,***

2) ***for a business transaction of this nature, the buyer may be an individual, the jurisdictional domain which is the source of such an external constraint should ensure that such a third party is able to comply with privacy protection requirements and particularly in the DMAs in the IT systems of the third party.***

Rule 007:

An agent (and/or third party) which commits itself to act on behalf of a Person acting as a seller in a business transaction, where the buyer is an individual in a *jurisdictional* domain where privacy protection requirements apply, shall ensure that the DMA(s) in its IT system(s) is capable of supporting applicable external constraints requirements.

The purpose of this rule is to ensure that any agent (and/or third party) recognizes the fact that it, as a Person in a jurisdictional domain, is also bound by external constraints of a privacy protection nature which apply to that jurisdictional domain. This applies to any business transaction where the buyer is an individual and privacy protection requirements apply. This also applies to applicable data synchronization requirements between the sellers and its agent(s) and/or third-party (ies).

Rule 008:

An organization shall ensure that in the execution of an (instantiated) business transaction, i.e., as identified by its business transaction identifier (BTI), that where these involve parties, other than the individual as a buyer, that such parties, are capable of and have implemented the requirements of the privacy protection principles[37].

It is recognized that the development of efficient and cost-effective Open-edi scenarios often require EDI among parties with varying business relationships. It is therefore not uncommon that the Persons acting as a seller, in a business transaction, involve other Persons in the instantiation of the business transaction. It is important for an organization acting as a seller in a business transaction to ensure that these other parties to a business transaction are committed to, and do have in place (and have implemented), applicable privacy protection requirements, i.e., where the buyer is an "individual" and the business transaction involves the use of personal information.

Finally, one should note that there is a direct relation here between accountability requirements and requirements here of synchronization of master data among all the parties to a business transaction.

The internal constraint of the general requirement of data synchronization with master data among parties to a business transaction becomes an external constraint based on privacy protection principles where the buyer is an individual and thus requiring data synchronization.

37 A key requirement is the ability for the seller to be able to support data synchronization among the IT systems of all parties participating in a business transaction. This is particularly important where this data is of the nature of personal information.

5.3.3 Privacy Protection Principle 3: Identifying Purposes

Rule 009:

The specified purpose(s) for which personal information is collected with respect to the (the (potential) goal of the business transaction shall be identified by the organization at or before the personal information is collected.

Here the specified purpose is deemed to be the goal of the business transaction, i.e., that mutually agreed to by the individual at the end of the negotiation phase, and prior to the actualization phase.

In an Open-edi context, the purpose for which the personal information is being collected is specified as (part of) the purpose of an Open-edi scenario, i.e., as the OeS purpose. The Clause 7.2 *Rules for scoping Open-edi scenarios* in ISO/IEC 15944-1 already make provision for supporting this rule from a privacy protection requirements perspective.[38]

5.3.4 Privacy Protection Principle 4: Informed Consent

The principle of "informed consent" requires that the individual, as prospective buyer, be fully and explicitly informed by the seller as to why and for what purpose, the individual is requested (or required) to provide (additional) personal information (of various kinds), i.e., in addition to that which may be required with respect to payment aspects.

This principle is clearly a requirement to flag personal information supplied as being for limited use. It is for the surrounding BOV and FSV processes to identify what the use implications are, and how the 'informed consent' status for the transaction has been achieved. However, it is clearly necessary for scenarios to develop the granularity of what the informed consent being given actually is for. It is possible that different data in a single transaction could be of different "informed consent" use; however, this part of ISO/IEC 15944 addresses the simplest case of all of the data to the transaction being subject to the single 'informed consent' agreement.

It is noted that in a substantial number of business transaction, the buyer, as an individual, remains for all practical purposes "anonymous". A good is purchased in a store, payment is made in cash or by credit/debit card (as authorized by the relevant financial institution, etc. and the individual is provided by the seller of a sales receipt which contains the associated business transaction identifier (BTI). As such the only binding between the individual as buyer and the seller might be the BTI[39]. Thus the use of a BTI is mandatory.[40]

Rule 010:

Where in a business transaction, the seller requires the buyer, as an individual, to provide personal information, the seller shall ensure that the collection and use of such personal information shall have the informed and explicit consent of the individual and that the same be directly linked to the specified goal of the business transaction (to be) entered into.

---

38 See further below Clause 12.3 *"Template for specifying an Open-edi scenario*" for privacy protection requirements.

39 In the development of this part of ISO/IEC 15944, it has been taken into account that many organizations, especially small and medium enterprises do not collect or maintain personal information pertaining to the individual as buyer. It is also a common business practice that with respect to any complaint, return of merchandise, invocation of a warranty, that the buyer (or now owner) must have the sales receipt (in hand) and/or be able to provide the BTI pertaining to the business transaction.

40 On the role and importance of business transaction identifier (BTI) and associated rules, see below Clause 11.2 *Business Transaction Identifier*.

The application of this rule also prevents the possible use of "automatic opt-in"[41] by the seller, i.e., collection is not allowed unless expressly consented to be the individual, since that may not be part of the "informed consent" and may violate the principle of "limiting collection" and of limiting use".

This includes the need for a seller to ask for explicit consent from the individual who is the buyer, for the use of any of his/her personal information for any purpose which is different form that originally agreed to, i.e., as the agreed upon goal of the business transaction. As such, privacy protection requirements preclude the use by the seller of an "automatic opt-ins" in EDI and in links (including posting any and use of Internet-based functional services which may be used to identify an individual). The following Guideline supports this privacy requirement.

Guideline 010G1:

In support of privacy protection requirements, the seller shall ensure that there are no "automatic opt-ins" by the seller with respect to aspects of the commitment exchange forming the basis of the business transaction or any secondary use of the personal information of the individual who is the buyer in a business transaction.

Rule 011:

Any secondary use of personal information of the individual in a business transaction requires the explicit and informed consent of the individual.

Here it is understood that the organization in the role of seller will maintain a record (as a SRI) on the individual providing such explicit informed consent, i.e., in compliance with documentary evidence rules of the applicable jurisdictional domain.

The following Guideline represents a "best practice" approach[42].

Guideline 011G1:

Any use of "automatic opt-ins" shall be explicitly agreed to by the individual, i.e., as informed consent, and be recorded as such by the seller, i.e., in compliance with documentary evidentiary rules of the applicable jurisdictional domain.

This Guideline supports the fact that the use of "an automatic op-in" by a seller necessitates use of personal information of the buyer as an individual and therefore requires documented evidence of his/her informed consent.

Rule 012:

Except with the explicit informed consent of the individual, or as required by law, personal information shall not be used or disclosed for purposes other than those for which it was collected, i.e., in the context of the specified goal of the business transaction to which it pertains.

This means that:

- the personal information of the individual as the buyer in the business transaction collected by the seller in that business transaction shall not be disclosed, i.e., communicated to any other party(ies) unless so required for the actualization of that specific business transaction with the individual being fully informed of the same by the seller and having consented to; seller;

41 With respect to rules governing the use of "automatic opt-in" by sellers, there is a link here to external constraints of a privacy protection nature.

42 Rules pertaining to compliance with documentary evidence rules of jurisdictional domains are outside the scope of this part of ISO/IEC 15944.

- unless the individual provides explicitly stated and documented informed consent, none of the personal information created or obtained for one business transaction shall be used for any other business transaction or purpose (such as aggregation);

- once the business transaction has been actualized all personal information shall be deleted unless required for post-actualization purposes and/or other specified external constraints of an information law nature require specific personal information to be retained; and,

- personal information concerning the transaction shall not be retained for longer that is necessary in the relevant jurisdiction for the purpose of satisfying national regulation for record keeping.

5.3.5 Privacy Protection Principle 5: Limiting Collection

Rule 013:

The collection of personal information shall be limited to only that which is necessary and relevant for the identified and specified purpose, i.e., the goal, of the specified business transaction.

Only personal information on the individual as a buyer that is essential, i.e., can be proved to be relevant, for the completion of the business transaction "in hand" shall be collected. This also means that any information that is not essential to the business transaction shall be clearly identified, and the business transaction shall not fail if information that is not fundamental to the transaction is missing.

The implementation of this privacy protection principle requires that at the planning phase, or no later than before completion of the negotiation phase in a business transaction, that the individual is fully informed, not only of the purpose of the business transaction, but also why specific sub-sets or components of personal information are required or optional and that they are clearly and unambiguously identified.

Rule 014:

Any collection of personal information by the seller, or other parties to a business transaction, which pertains to a buyer as an individual in that business transaction, shall be lawful and fair.

This rule recognizes the fact that:

1) laws (and regulations) of jurisdictional domains, i.e., external constraints, may require data to be collected depending on the nature of the good, service and/or right as the goal of the business transaction; and,

2) where the (prospective) buyer is an individual,

then that individual is required to provide specified personal information either as part of the actualization of a business transaction or even during the planning, identification and/or negotiation phase, or at any time prior to the actualization of a business transaction. For example, an external constraint may be of the nature that:

1) only an individual (and not an organization) may purchase a specified good, service and/or right; and,

2) where this is the case the individual may be required to provide additional personal information before making a purchase .This can include, the individual being required to provide proof of age, status (e.g. citizenship, landed immigrant, etc.), credentials (e.g. as a licensed medical doctor, an engineer, qualified technician, etc.).[43]

This principle also provides that collection methods shall be lawful and fair. For example, fraudulent misrepresentation in order to obtain personal information on an individual is considered unlawful in most jurisdictional domains. This includes misrepresentation, via EDI, to deceive individuals, as (potential)

[43] On this matter and for other examples see further, Clause 6.1.6 "*Business model: Classes of External constraints",* Clause 6.3.3 *"Identification"* and Annex F, Clause F.2.3 "*Identification Phase*" in ISO/IEC 15944-1.

consumers to induce them to provide sensitive personal information such as credit/debit card numbers, bank account information, etc.[44]

Rule 015:

An organization collecting personal information shall inform the individual concerned whether or not the personal information collected is:

1) **essential to the intention of the business transaction;**

2) **required to be provided by the individual due to identified and specified constraints of jurisdictional domains applicable to the nature and goal of the business transaction; and/or,**

3) **"optional", i.e., desired to have by the organization, acting as the seller, but not required.**

[44] The use "unfair" means includes of fraudulent means. The use of fraudulent means to obtain personal information on or about an individual (irrespective of how it may be used) is likely subject to sanctions under the Criminal Code (or laws of an equivalent nature) in most jurisdictional domains.

5.3.6 Privacy Protection Principle 6: Limiting Use, Disclosure and Retention

This Privacy Protection Principle consolidates and integrates what are considered "generic, primitive" Information Life Cycle Management (ICLM) principles which apply to any and all types of sets of recorded information (SRIs) within an organization (including public administrations) and among organizations. This addresses the "collaboration space" among all parties, i.e., types of Person, to a business transaction. As such, Annex D below titled *"Integrated set of information life cycle management principles in support of information law compliance"* applies to these privacy protection principles.[45] The integrated set of information life cycle management (ICLM) principles in support of information law compliance, which apply to data management and interchange generally also apply to Open-edi[46] within and among Persons (and their IT systems). In addition, Annex E below titled "*Coded domains for the management and control of state changes, retention and destruction of personal information in commitment exchange, including business transactions*" supports both the implementation of the ICLM principles as well as privacy protection requirements.

Rule 016:

The integrated set of ICLM principles applies to and supports the external constraints of a privacy protection nature for any business transaction involving an individual and its personal information.

Parties to a business transaction are required to be able to support these six Open-edi characteristics as requirements governing the DMAs of the organization in their IT systems[47]. The ICLM principles reflect and support the six key characteristics of Open-edi.

Note that this rule may require that some personal data must be retained specifically for this purpose and that therefore this purpose is implicitly necessary to a transaction involving personal data.

Rule 017:

Personal information shall not be used or disclosed by the seller (or regulator) for purposes other than for those it was originally collected as part of the business transaction, except with the informed consent of the individual, or as required by law. Secondary or derivative uses of personal information are <u>not</u> permitted.

---

45 The focus and scope of ISO/IEC JTC1/SC32 standards development work is *"Data Management and Interchange*" was at first not only within the IT system(s) of a Person of primarily organizations (including public administrations) but now also includes individuals (and their IT systems). As such, Open-edi standards development, which focuses on the collaboration space among Persons and their IT systems, has from it inception supported information life cycle management (ICLM) requirements. The need to reflect and support ICLM requirements is of particular importance where external constraints apply to the modelling of a business transaction. This was reflected and explicitly supported in the development of the existing principles, rules and definitions in ISO/IEC 15944, i.e., its definitions of relevant concept, and rules and include those found in the "Characteristics of Open-edi", those pertaining to state changes, record retention, the specification of the collaboration space, etc., as well as being found in the templates for scoping Open-edi transactions and modelling Open-edi scenarios and their components.

Annex D below brings forward and states explicitly the ILCM principles in support of information law compliance, i.e. external constraints, applicable to the modelling of common business transactions via Open-edi scenarios.

46 While the focus here is on "Electronic data interchange (EDI)", these ICLM principles apply to any internal or external constraints applicable to any. set of recorded information (SRI) of any Person.

47 The six key characteristics by which Open-edi is recognized and defined are:

- actions based upon following rules;
- commitment of the parties involved;
- communications among parties automated;
- parties control and maintain their states;
- parties act autonomously; and,
- multiple simultaneous transactions can be supported.

See further Clause 5 "*Characteristics of Open-edi*" ISO/IEC 15944-1.

This means that the purpose for which personal information was collected or requested from an individual shall be directly related to, if not explicitly stated, in the mutually agreed upon and explicitly stated goal of the business transaction being instantiated.

In scenario definitions, this shall require that the scenario definition identify explicitly all data that are subject to this rule Other BOV processes will be required to enact this rule, so the scenario definition is required in order to identify to the party(ies) subject to this rule that they are liable for non-compliance if they fail to instantiate annual or other separate procedures in compliance with this rule.

Rule 018:

Where the organization, having collected personal information for a specific purpose and goal of the execution of the business transaction, desires to use the relevant personal information for another purpose, it is necessary to obtain revised/new "informed consent" directly from the individual concerned.

This rule requires not only that:

1) the individual may refuse consent for a secondary, derivative or new use of its personal information; but also;

2) where an organization is not able to contact the individual concerned to make request for another use of that individual's personal information, then such a proposed "new" use is not permitted.

Rule 019:

Personal information shall be retained by the seller only for as long as is necessary for the fulfillment of those purposes as specified as part of the business transaction.

Personal information must be identified as having a specific 'life' of time of existence if this is to be other than that demanded for the purposes of national record keeping. This retention time period shall form part of the scenario definition and the time period will be explicit.

This also means that organizations shall have in place auditable rules and procedures as are necessary to ensure that personal information no longer required for the post-actualization phase of a business transaction shall be destroyed (expunged) by the organization, or its agents where applicable, and in a manner which can be verified via audit procedures.

For most, if not all, instantiated business transactions, external constraints of the applicable jurisdictional domain(s) require that specific sets of recorded information (SRIs) pertaining to any business transaction be retained by the seller for a specified period of time.

It is recognized that, depending on the nature of the good, service and/or right which is the goal of the business transaction, specified additional records retentions requirements of applicable jurisdictional domains may apply to all or specified subsets of all the recorded information pertaining to a business transaction.

It is also recognized that where the purchase of a good, service and/or right involves "post-actualization" aspects of a temporal nature that these will also impact record retention requirements and obligations resulting from an actualized business transaction. A primary example here of an internal constraint nature is

that of a "warranty" for "n" number of years[48]. This includes the possibility that the individual who made the purchase may not be the "warranty holder"[49].

The following rules summarize these requirements from a BOV perspective:

Rule 020:

The seller shall identify to the buyer, especially where the buyer is an individual, any and all record retention requirements pertaining the resulting sets of recorded information forming part of the specified goal of a business transaction as a result of applicable external constraints of jurisdictional domain(s) as a result of the actualization of the business transaction.

Rule 021:

Where the seller offers a warranty, or extended warranty, as part of the business transaction, the seller shall inform the buyer, when the buyer is an individual, of the associated added records retention requirements for the personal information associated with the warranty (including the purchase by the individual of an extended warranty).

The sale of many types of goods or services, require the seller to inform the buyer of possible safety and health considerations with respect to whatever was purchased. These include product recalls, repairs, verifications checks or testing of specific function or components, etc.

Rule 022:

Where the buyer in a business transaction is an individual, the seller shall inform the individual of any and all records retention requirements of personal information which is recorded as the result of the actualization of the business transaction, including:

1) **personal information which is required to actualize the business transaction and the time period(s) for which such sets of personal information are to be retained;**

2) **additional personal information, i.e., in addition to (1), which is required to be collected and retained as a result of applicable external constraints, of whatever nature, of relevant jurisdictional domain(s); and/or,**

3) **additional personal information, i.e. in addition to (1) or (2), which is required to be collected and retained as a results of the invocation of an associated warranty, purchase of an extended warranty, or any other personal information which is required to be collected or retained as part of the post-actualization phase of an instantiated business transaction.**

From a customer service, many sellers, i.e. organizations (including public administrations), wish to stay in contact with their customers for a variety of reasons. These include providing catalogues of their offerings, possible associated goods or services, etc., as well as obtaining client feedback, surveys, new product announcements, etc.

Rule 023:

Where the buyer in business transaction is an individual, the seller shall inform that individual of the applicable record retention conditions where these pertain to personal information.

---

[48] Here it is noted that in order to be able to support a "warranty" of whatever nature, the seller will need to maintain personal information for a time period other, i.e. longer, than that required by law, i.e. as part of the applicable external constraints of the relevant jurisdictional domain(s). This is especially so where consumers purchase an "extended warranty".

[49] For example, where the good or service purchased as a gift. Here the recipient of the gift, as an individual, would become the owner and also would complete the warranty information including personal information required for the warranty to be invoked.

It is important that when the buyer is an individual that, prior to and at the actualization phase in a business transaction, that the buyer is fully informed of the records retention requirements and practices of the seller particularly as these pertain to the personal information forming part of the set(s) of recorded information. Here it may well occur, depending on the nature of the business transaction, that certain types of personal information may be subject to differing records retention periods.

It is noted that where the business transaction is one of the nature of the provision of a service or a right, (such as a license or authority of some kind) that the seller needs to retains a specified set(s) of personal information for as long as a business transaction of this nature remains active.

Rule 024:

Where a business transaction does not reach the actualization phase, any personal information collected by the organization in support of that transaction shall be deleted by the organization (unless the individual concerned explicitly consents to the prospective seller to the retention of such personal information for a defined period of time).

An individual may have provided personal information to a seller as part of the identification or negotiation phase. However, in this case the individual decides not to commit to the actualization of the business transaction. As such the personal information provided by the individual to the seller is no longer relevant, and therefore the organization concerned shall delete the personal information pertaining to that individual.

It is noted that this rule makes provision for the possibility that the individual, as a prospective buyer, may consent to be kept informed by the seller about product information (e.g. via a catalogue), special sales, new offerings, etc. Such a decision by the individual is of the nature of obtaining "informed consent".

Particular care must be taken to avoid collecting or providing data that are not actually necessary for the purpose(s) of the transaction itself. By way of example, in the transaction given in section 6 of a purchase and payment it may not be necessary for the seller to know the actual personal identity of the buyer, but to have an identifier by which that buyer may be uniquely identified to the seller. It may be sufficient that the seller is certain of payment because the seller has an authority from a third party such as a bank that the transaction will be paid. Thus the bank may need to know the identity of the buyer and seller in order to fulfill its requirements in the transaction (but not the content of the transaction), whilst the seller does not need to know the identity of the buyer. The same is true when agents are used, or when a public administration is a supervisor to a transaction, where the other parties need to know and perhaps be able to prove that the public administration was involved, but not be able to identify the individual within the public administration actually involved (although the internal functions of the public administration may need that information for their own supervisory purposes).

5.3.7 Privacy Protection Principle 7: Accuracy

It is to the mutual benefit of all parties to a business transaction, and also a good business practice, to ensure that any and all recorded information pertaining to a business transaction be as timely, accurate, complete, up-to-date, etc., as possible. Accuracy of recorded information is an essential component of "integrity[50]" which is a major asset of any organization. No organization should keep recorded information on its business transaction or its clients which is not accurate or out-of-date, especially in the DMAs of its IT systems. As such for this generally accepted set of internal constraint on recorded information applicable to all parties to a business transaction, organizations concluding business transactions with buyers as individuals, should have no difficulties in support the external constraint of "accuracy" of a privacy protection nature (including in the DMAs of their IT systems).

50 It is noted that an organization which does not have policies and auditable procedures in place, as part of its overall governance, to ensure that the recorded information on which its decisions and commitments are made, does not have the required level of "integrity" (e.g. timeliness, accuracy, being-up-to data, etc.) and ensures that all its recorded information which does not meet these criteria is expunged (unless required to be retained due to applicable external constraints), may find itself (and particular its officers) being subject to legal action for not exercising stewardship, due diligence, damages, etc., for not implementing these requirements (which in turn form part of the implementation of ILCM principles).

Rule 025:

Personal information shall be as accurate, complete and up-to-date as is necessary for the specified purposes for which it was collected in support of the business transaction.

Here, the scenario definition shall make it clear that the data identified shall subsequently be capable of amendment (including deletion). It may be that there are other data for which alteration may be forbidden, either by automatic or manually inspired processes.

One should consider the implementation of this principle to be of the nature of good corporate governance and best practices. For a variety of reasons, organization should not retain personal information, or retain the same in its IT systems, if such personal information is not accurate, complete and up-to-date.

Guideline 025G1:

In order to support the privacy principle of accuracy, organizations should consider informing their clients, who are individuals, of the personal information retained on that individual, and do so on a cyclical basis in order to ascertain whether such personal information, collected earlier and still maintained by the organization, is still accurate.

5.3.8 Privacy Protection Principle 8: Safeguards

This Privacy Protection Principle pertains to ensuring that the organization has in place policies and operational controls and practices to ensure its policies for the retention, storage, preservation or destruction, confidentiality, integrity, continuity and availability of the processing, reproduction, distribution, sharing or other handling of its recorded information is "safeguarded" in compliance with applicable "information law" requirements[51].

This principle is of the nature of an external constraint which makes such existing best practices from a business operational view perspective mandatory from an external constraints privacy protection requirements perspective.

Recognized international standards for "safeguards" exist not only with respect to those pertaining to Open-edi but also in the fields of:

- records/information management (including records retention and archiving as well as supporting IT systems and their DMAs));
- audit controls;
- security services;
- "quality" of communication services;
- evidentiary aspects of paper, microform and/or electronic based document;
- database management.

International standards support and provide guidance to organizations for addressing address and implementing most of the accountability, information managements, and "safeguard" requirements of a privacy protection nature. Many organizations already have in place officers, mechanisms, procedures, etc., required to provide safeguard measures in support of the implementation of this principle either directly or as an integrated aspect of its overall approach to information management.

---

[51] For a generic "information law" requirement from a BOV perspective, see further below Annex D *(Normative) Integrated set of information lifecycle management (ILCM) principles in support of information law compliance.*

Rule 026:

Personal information shall be protected by operational procedures and safeguards and safeguards appropriate to the level of sensitivity of such recorded information and shall have in place (and tested) measures in support of compliance of compliance with privacy protection requirements of applicable jurisdictional domains, as well as any other external constraints which may apply such measures as are appropriate to ensure that all applicable legal requirements are supported.

Guideline 026G1:

Where an organization does not have a single designated focal point and "officer, i.e., a "privacy protection officer (PPO)" responsible for ensuring the identification and implementation of safeguard requirements applicable to all of its recorded information, it should ensure that all of its personal information meets privacy protection requirements.

This principle also introduces the concept of protection. Protection involves one or more constraints that are to be applied to specific data that are expected to provide the safeguard that is appropriate. It should be noted that the actual sensitivity of the data to be protected may be of national or cultural expectation, and need not be consistent. It should also be noted that in modelling, specific data fields are labelled with the type of privacy protection that is to be provided, but that it is for the FSV implementation to determine how such privacy protection requirements are given technical effect. In this part of ISO/IEC 15944 only the means of determining the agreed (or required) privacy protection that is attaching to specified individual data elements (fields and records) is addressed.

5.3.9 Privacy Protection Principle 9: Openness

The principle of "openness" pertains to the privacy protection requirement that any organization which collect and uses personal information shall be fully transparent in its use of personal information. This means that all of its policies and business practices pertaining to the collection, use and management of any personal information shall be made readily and publicly available, free of charge, and via various means and media of communication.

Rule 027:

An organization shall have and make readily available to any Person[52] specific information about its policies and practices pertaining to the management and interchange of personal information under its control.

In support of this principle the organization will have explicitly stated such information:

(i) on its website; and,

(ii) have a policy in place to provide printed materials of this nature for free and upon request from anyone.

It is expected that in support of this principle the organization will have explicitly stated such information.

In addition, any agents and/or third parties that the organization may wish to involve in the business transaction shall be fully cognizant of and able to comply with and support the privacy protection policies and practices of the organization to which they are an agent or third party to.

Where protection scenarios are recorded for the purpose of Open-edi this principle is met by publishing the agreed scenario constraints, together with any external manual processes that have been used or providing references to them in an external source.

52 "Person" is used here, instead of individual so that other (potential) parties to a business transaction, (e.g., organizations and public administrations) need to have access to an organization's privacy protection policies, practices and related information.

5.3.10 Principle Protection Principle 10: Individual Access

A key component of privacy protection requirements is that an individual shall be able to enquire of any organization (private or public sector) whether or not that organization has and maintain personal information about that individual anywhere in its record/information management systems. From a business transaction and Open-edi perspective, this principle applies in particular to the DMAs in the IT systems of an organization.

It is anticipated that this principle will be enacted not through this part of ISO/IEC 15944 but through laws and regulations of the applicable jurisdictional domain(s) pertaining to the business transaction where the individual is the buyer.

Rule 028:

An individual has the right to know whether or not an organization has personal information under its control[53] on or about that individual.

Rule 029:

An organization, subject to privacy protection requirements, upon receiving a request from an individual shall inform that individual of the existence, use and disclosure of his or her personal information in any and all records management/information systems and in particular the DMAs of the IT systems which support the business transactions of that organization.

Where this principle is implemented through Open-edi, the scenario, i.e., model, shall show the protection labels that are applied to the fields of data as part of the implementation of the scenario. It must be noted that this may be met by other means, such as the publishing of contact information for the point at which this information may be requested since there will be a need for the individual to prove they have the correct identity before a disclosure can be made.

Guideline 029G1:

Upon receiving a request of this nature, the organization may request the individual to provide personal information which will assist the organization in ascertaining whether or not it has under its control personal information on that individual. Personal information of this nature requested by the organization may include provision by the individual making the request for access (any combination of the following, in no particular order):

- ***one or more personae by which the individual may represent itself[54];***
- ***the provision of a temporal period which may be applicable;***
- ***the provision of one or more physical addresses which may be applicable;***
- ***the provision of one or more electronic addresses including telephone numbers, e-mails addresses, etc.;***
- ***the Business transaction identifier (BTI) pertaining to the business transaction which led to the organization collecting and maintaining personal information about the individual making the request; and/or,***

---

53 The use of "under its control" covers the fact that the organization may engage agents, third parties, other parties to a business transaction and thus provide them with personal information. However, the seller organization retains control of all its recorded information including personal information. This is already stated in Clause 6.4 *"Data component*" in ISO/IEC 15944-1 and emphasized in Clause 6.4 *"Data component"* below in this document.

54 It is a fact that an individual has and uses many differing personae. The organization receiving the request for "individual access" can only assume that the name that the individual uses is the same (or 95%+) the same as the one that it maintains in its IT systems. If not there may be no match. Thus, it is up to the individual to provide alternative personae to be used in any search/discovery.

- ***any other personal information, i.e. as data elements, which the organization receiving the request may require to ensure that its search for the existence of personal information relating to the requesting individual is as complete and thorough as possible.***

Rule 030:

Where an organization discovers that it has personal information on the individual who made the request, that individual shall be given full and complete access to any and all personal information which the organization maintains on that individual (unless there exist specified and referenced external constraints of the applicable jurisdictional domain(s) which prohibit access to one or more sets of such personal information).

The qualification on access to personal information in the above rule is necessary as this document applies to both private and public organizations as well as regulators.

The cost effective and efficient implementation of these privacy protection principles requires that the organization/public administration shall make publicly available its accessible fax or phone numbers, website URL, and where relevant, the name of its privacy protection officer (PPO) as to:

1) where and how an individual is able to obtain a complete record of its personal information; and,

2) how and where such personal information is used and interchanged with other parties to a business transaction.

The overall purpose of this principle is to ensure that the personal information which a Person retains on a specified individual is as accurate and complete at all times as possible. This means that where and whenever personal information on a particular individual which an organization has or retains for business transactional reasons (or related legal "upon request" requirements) shall provide (be able to provide) a complete transcript of any and all personal information to the individual concerned about his/her personal information.

Guideline 030G1:

On the whole, based both on requirements of jurisdictional domains as well as "best practices" organizations should ensure that:

1) such information and documentation is available without charge;

2) no costs are charged to an individual making a privacy protection request;

3) no costs are charged to the individual by the organization in providing the personal information it has on or about that individual

4) such information and documentation is made available in the official language(s) of the jurisdictional domain in which the good, service, and/or right is being offered for sale.

Note: Users of this document shall refer to the ISO 639-2/T set of 3-alpha codes in order to understand the use of codes representing official (and de facto) languages.

5) such information and documentation is made available to individuals in accordance with consumer protection and individual accessibility requirements.

Rule 031:

Where an organization has and maintains personal information on the individual making the request for access to his/her personal information and such personal information does exist, the organization shall provide access to the personal information in a manner which is convenient to that individual.

Guideline 031G1:

While it is up to the organization and the individual concerned to agree on the most effective and efficient way to provide access to the personal information requested, it is up to the individual to decide as to what is the most convenient means for providing the personal identification identified.

Guidelines 31G2:

In cases where there is a difference of opinion between an organization and an individual about the accuracy of that individual's personal information held by the organization, it is advisable for the organization to maintain both (1) the personal organization which the organization considers to be accurate; and, (2) the personal information which the individual considers to be accurate.

This guideline supports a pragmatic approach in support of the fact that not all requesters use the Internet or have e-mail address or fax machines, etc. which support the provision of access to the identified personal information via attachments to an e-mail or via fax. That is, the organization may well have to send hardcopy or printout of the personal information requested to the individual.

5.3.11 Privacy Protection Principle 11: Challenging Compliance

Challenging compliance is a key privacy protection principle. It pertains to the right of an individual to question and thus challenge whether or not: (1) an organization has under its control (or maintains on behalf of other organizations) personal information on the individual; and, (2) if it does, that such personal information is accurate, timely, and relevant to the nature of the informed consent provided by that individual.

Depending on the privacy protection requirements of the applicable jurisdictional domain, an individual may have the right to:

(a) challenge compliance directly with the organization to whom the challenge is directed;

(b) direct such a challenge, (e.g., complaint) to a privacy or data protection commissioner/ombudsman as provide for in the jurisdictional domain; or,

(c) various combinations of (a) or (b) above".

It is anticipated that this principle will be enacted not through this part of ISO/IEC 15944 but through laws and regulations of the applicable jurisdictional domain(s) pertaining to the business transaction where the individual is the buyer.

Rule 032:

An individual shall be able to challenge the accuracy and completeness of his or her personal information held by an organization with respect to a business transaction (and/or part of a general client file) and have it amended or deleted as appropriate[55]

It is to no one's benefit to maintain or make decisions on personal information which is not accurate. As such, one practical solution might be for the organization to maintain in its records both (1) the personal information which it considers to be accurate; and, (2) the personal information which the individual considers to be accurate. At the same time it may well be that the organization as the seller and the buyer, as individual, in a business transaction may not agree as to the accuracy of the personal information pertaining to that individual with respect to the business transaction(s) entered into.

55 This rule requires an organization to tack its master data and have data synchronization. These and related matters of traceability, including those pertaining to individuals are being addressed in the ISO/IEC 15944-9 "*Traceability Framework*" standard which is under development.

Guideline 032G1:

In cases where there is a difference of opinion between an organization and an individual about the accuracy of that individual's personal information, it is advisable for the organization to maintain both (1) that of the organization; and (2) the personal information that the individual considers to be accurate.

For example, an organization which maintains "credit information" on an individual may not be in a position to, or even want to adjudicate, where there exist differences between an organization reporting personal information on an individual and that individual questioning its accuracy.

Rule 033:

An individual shall be able to challenge an organization concerning its compliance with the above privacy protection principles 1 through 10, including assurance of privacy protection for any personal information that is interchanged with other organizations as agents or third parties (as well as secondary or derivative uses of personal information).

In effect, this means that any organization, to which privacy protection requirements apply, shall have:

a) in place the identification of a public contact, if other than that of its Privacy Protection Office (PPO), and physical address (e-mail optional) to which an individual can direct and challenge compliance of that organization with respect to personal information which that organization currents has on that individual (as well as secondary or derivative uses of that individual's personal information);

b) available a document which states clearly and explicitly the procedures the procedures the organization has in place to address a challenge to compliance with privacy protection requirements.

5.4 Requirement for tagging (or labelling) data elements in support of privacy protection requirements

The application of the general privacy protection principles, as stated in Clause 5.3 above, requires an organization to be able to identify and tag any and all personal information when it is created or collected in its IT systems. Such tagging is required enable an organization's compliance with specific privacy protection requirements. (It also assists the organization in meeting general ICLM requirements). An organization can do such tagging of sets of recorded information at the records level (e.g. client file level) down to the more granular data element level.

Rule 034:

An organization shall have in place policies and procedures in order to identify and tag (or label) all sets of recorded information (SRIs) which contain personal information and do so at the appropriate level of granularity to facilitate compliance with specific privacy protection requirements.

An SRI can be any scenario component such as semantic component (SC), an Information Bundle (IB) or scenario attribute.

Further from data interchange perspective, among parties to a business transaction, there are additional privacy protection requirements which apply.

Rule 035:

For a field or data element comprising the recorded information pertaining to a business transaction, for personal information the following requirements apply from a data interchange perspective, the need to ensure the provision of a tag(s) to note that the personal information:

1) **shall not be communicated with other parties;**
2) **may be communicated to other parties but with restrictions; or,**
3) **may be communicated to other parties with no restrictions.**

Rule 036:

For a field or data element comprising the recorded information pertaining to a business transaction, for personal information the following requirements apply from a data interchange perspective, i.e., the need to ensure the provision of a tag(s) to note that the personal information is subject to mandatory disclosure is:

1) **the actual information;**

2) **anonymous information that represents the actual information; or,**

3) **pseudonyms that represents the actual information.**

6 Collaboration space and privacy protection[56]

6.1 Introduction

The focus of these Open-edi and eBusiness standards is modelling the collaboration space among the primary parties to a business transaction. For modelling purposes a business transaction requires at the least the roles of a "buyer" and a "seller", based on "internal constraints" only. Depending on the nature of the good, service and/or right (or combination of the same) one or more sets of "external constraints" may apply. These are modelled through the introduction of the role of a "regulator".

This section summarizes "collaboration space", as already defined along with applicable rules in ISO/IEC 15944-4 and ISO/IEC 15944-5 but does so from a Privacy Protection requirements perspective. As such, users of this document shall use and reference these two standards in their use of this document.

6.2 Basic Open-edi collaboration space: Buyer and seller

The primary purpose of collaboration space is to avoid having the same commitment exchanges comprising a business transaction modelled multiple times, i.e., as mirror images views of the same sets of recorded information being interchanged among "Persons" in their roles of "buyer" and "seller" as information bundles (IBs) (and their semantic components (SCs)), as part of the scenario governing a business transaction.

By way of example, the "receipt of a sale" between a buyer and seller always contains the same information with respect to:

- the business transaction identifier (BTI);
- date (and time) of sale, i.e., the date of the instantiated business transaction;
- the price paid (often before and then including applicable taxes);
- identification (at various levels of granularity) of what was purchased/sold;
- the means and mode of payment;
- conditions, warranties, rebates, etc., as applicable; and,
- any other documentation provided (including that as part of the packaging, recorded information in the packaging, or "online" via the Internet, including where it is a "virtual" good, service and/or right being transacted).

The purpose of business process modelling in an Open-edi context is to model the recorded information exchanged among the two primary Persons to a business transaction (and any others). In this context, there are two roles of Person, one assuming the role of "buyer" and the other the role of "seller", and the focus is on the information bundles that are being interchanged among these two primary partners in the business transaction.

From an Open-edi perspective, the collaboration space is a view of transactions that take place outside the internal control space of the Persons who are parties to a business transaction. This view sees both interchanges of information, from seller to buyer and buyer to seller, as conceptually similar. Such a perspective is quite different from that of the view taken inside an organization.

In Open-edi collaboration modelling, internal processes are not relevant until a resource, as an information flow (or represented by it via a reference tag) crosses an organization's logical boundaries. This independent

[56] In order to obtain a clear understanding of this Clause 6, users of this part of ISO/IEC 15944 should familiarize themselves with Clauses 0.1-0.4 of ISO/IEC 15944-4 and Clauses 5.22 and 5.23 in ISO/IEC 15944-5.

perspective is the focus of Open-edi and is represented by collaboration space, where values in the form of sets of recorded information (SRIs) are interchanged among the parties to a business transaction.

This is illustrated in Figure 4 below (taken from Figure 3 "Concept of a Business Collaboration" in ISO/IEC 15944-4).

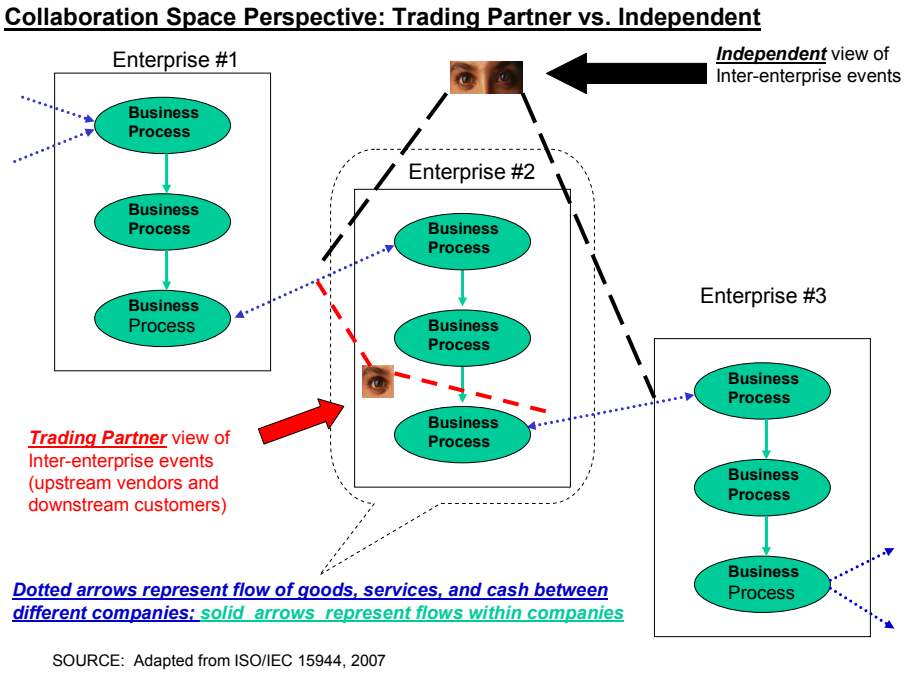


Figure 4 — Concept of a business collaboration

6.3 Collaboration space: The role of buyer (as individual), seller and regulator[57]

The collaboration space, introduced and defined in ISO/IEC 15944-4 of this multipart standard, focuses on collaboration space from an internal constraints perspective only. ISO/IEC 15944-5 {Clause 5.2.2} focuses on adding external constraints from the perspective of the requirements of jurisdictional domains[58]. They are modelled by adding (1) a regulator" (as already introduced and provided for in Clause 6.2.6 in ISO/IEC 15944-1 titled *"Person and external constraints: the "regulator";* and, (2) the three sub-types of Person (see Clause 6.2.7 in ISO/IEC 15944-1 titled *"Person and external constraints "individual", "organization", and "public administration"*).

Where a Person is acting as (1) an individual; and, (2) in the role of a buyer the external constraints identified in Clause 5.3 in this Part of ISO/IEC 15944 may be required. Thus, when modeling a scenario, two possible approaches may be used. In the first it will be necessary to identify different scenario components in the model when addressing scenarios which involve privacy from those that do not. In the second the privacy constraints must be included in the model with an option to switch them off for the scenarios where privacy requirements are absent. Either approach is valid.

There may therefore be more than one role fulfilled by the regulator (or regulators) in the transaction, since the regulator may act to supervise that the information constraint(s) have been applied, or may act to provide an anonymous or pseudonymous identity for one or more of the parties to the transaction (which may include the regulator).

---

57 This Clause is based on Clauses 5.2.2 and 5.2.3 in ISO/IEC 15944-5.

58 See further ISO/IEC 15944-5.

The regulator is the source of external constraints in a privacy collaboration space (PCS), defined as:

> ***privacy collaboration space (PCS)***
>
> *modelling or inclusion in an **Open-edi scenario** of a **collaboration space** involving an **individual** as the **buyer** in a potential or actualized **business transaction** where the **buyer** is an **individual** and therefore privacy protection requirements apply to personal information of that individual provided in that* **business *transaction***

The overall business transaction being modelled (as a scenario or scenario component) involves (1) a "buyer" who is an individual; and, (2) the jurisdictional domain(s) involved have external constraints of a privacy protection nature.

Rule 037:

For any business transaction (or part thereof) which involves external constraint(s) of a privacy protection nature, the Open-edi model shall include:

1) **the Person in the role of buyer as an individual;**

2) **the role of the regulator(s) representing the source of privacy protection requirements for modelling as part of a scenario and scenario components;**

3) **the role of the regulator(s) providing proof of identity of the individual without necessarily disclosing the actual identity of the individual.**

This is illustrated in Figure 5 below (as adapted from Figure 5 in ISO/IEC 15944-5.

It is noted that in some business transactions the seller as well as the buyer may be both making use of an agent or a third party supplier for the purpose(s) of concluding a business transaction.

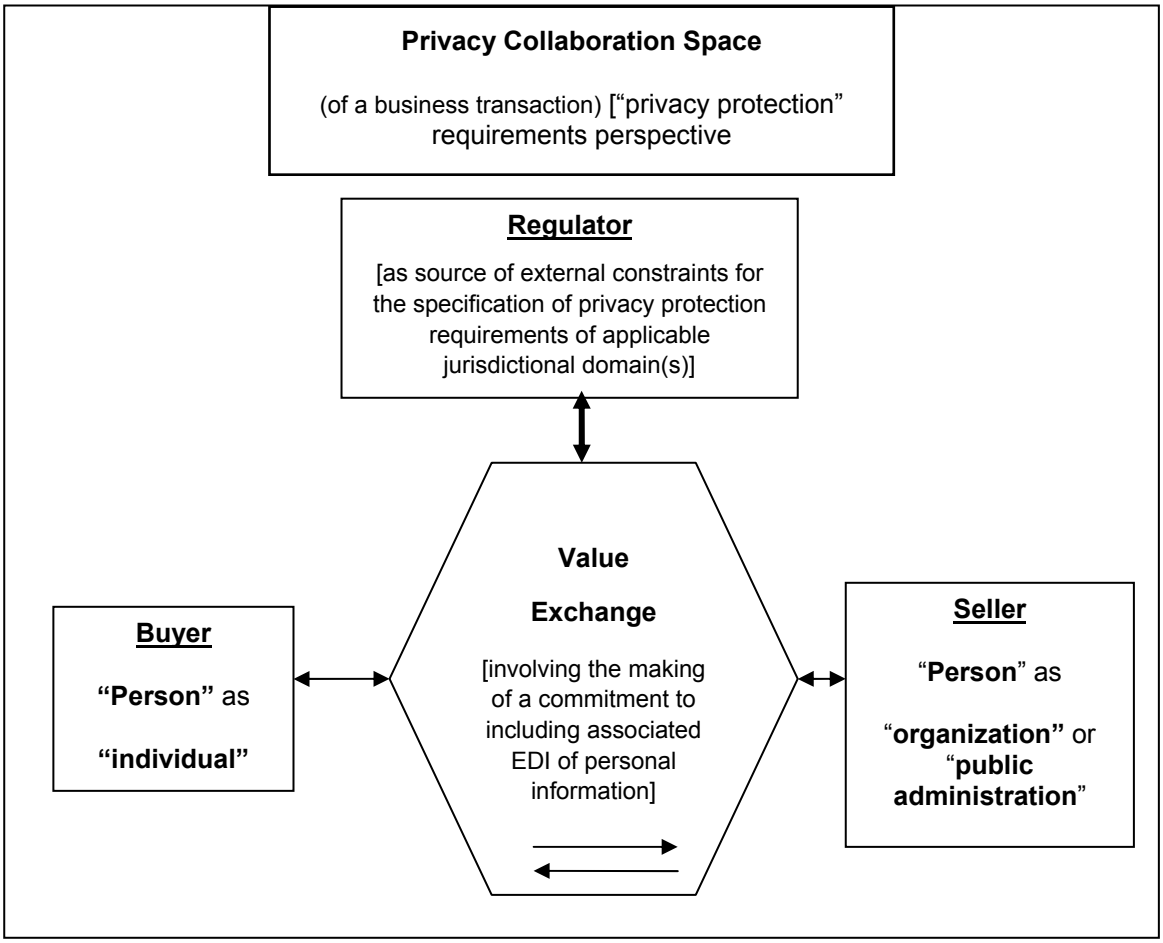


Figure 5 — Privacy collaboration space (of a business transaction) including the role of a regulator

7 Public policy requirements of jurisdictional domains

7.1 Introduction

Clause 7 relates privacy protection in the context of public policy requirements, i.e., the overall legal and regulatory requirements which apply to an “individual” as a “buyer”. The focus here is the fact that when the buyer is an individual then the (legal) rights, which the individual has, must be supported and modelled in scenarios and scenario components.

Clause 6.3 of ISO/IEC 15944-5 sets out the overall approach and key rules. They are summarized here, and expanded with respect to the privacy protection perspective.

7.2 Jurisdictional domains and public policy requirements

Increasingly jurisdictional domains require those providing a good, service and/or right in making such offers, and those executing resulting (electronic) business transactions, to comply with requirements expressed as rights of natural persons in their role as individuals.[59] Clause 0.2 and Figure 3 in ISO/IEC 15944-1:identified these as "public policy" requirements. “Public policy” is defined in ISO/IEC 15944-5. (For text see above Clause 3)

Clause 6.2.8 in ISO/IEC 15944-1 titled "*Person and external constraints: constraints: consumer and vendor"* introduced "consumer protection" as a minimum external constraint which needs to be taken into account in modelling business transactions, involving an individual as “buyer”, but doing so in a limited manner.

There are other external constraints of a "public policy" nature which need to be taken into account in modelling business transactions. These include “individual accessibility”, human rights, etc. In Clause 6.1.6 "*Business transaction model: Classes of constraints*" from ISO/IEC 15944-1, these form part of the category of *"External Constraints: Public Administration*" (as identified in Figure 8 in ISO/IEC 15944-1).

Now we focus on some of the most basic categories of public policy as external constraints that need to be taken into account when modelling (electronic) business transactions which involve "individuals" as "buyers". Those already identified include:

- privacy protection
- consumer protection;
- individual accessibility; and,
- human rights.

This is illustrated in Figure 6 below.

[59] Note: A natural person, a human being, acting in the role of “seller” is deemed to be an “organization” (as per ISO/IEC 6523 definition and common (legal) practices.

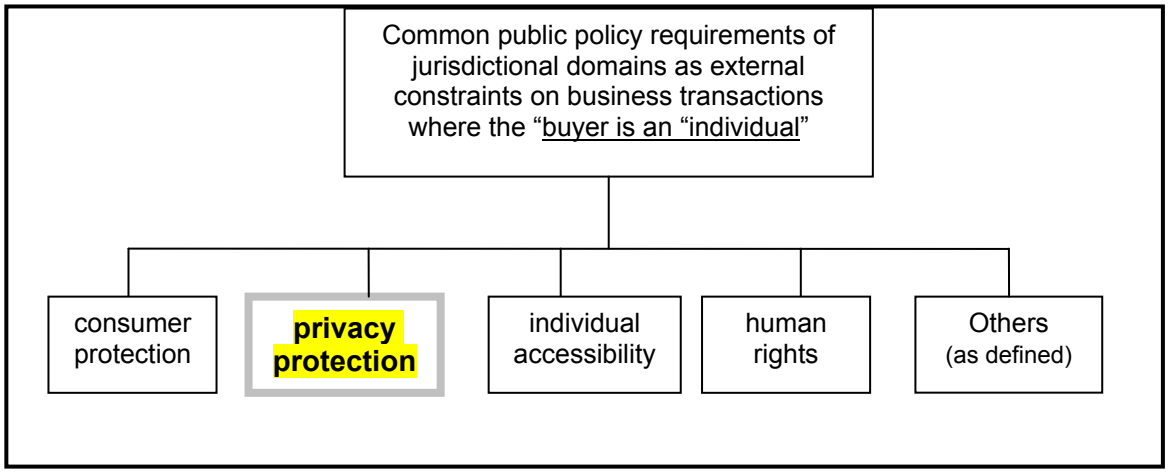


Figure 6 — Common public policy requirements, i.e., external constraints, applying to a business transaction where the "buyer" is an "individual"

The following four sub-clauses summarize the minimal external constraints of this nature in a very simple form. It is outside the scope of this part of ISO/IEC 15944 to address and specify external constraints on a business transaction of the nature of "consumer protection", "accessibility", etc., in specific detail. The purpose of this clause is to ensure that when ISO/IEC 15944-8 is used to model business transactions (or parts of business transactions as reusable business objects in the form of scenarios and scenario components), one is able to identify in the template provided in Clause 12 under "external constraints requirements of a "public policy" nature.

7.2.1 Privacy protection

When modelling (electronic) business transactions, a common minimum external constraint that needs to be taken into account is that commonly referred to as "privacy" requirements (or in some jurisdictional domains as "data protection"). Here the term "privacy protection" is used to identify the public policy requirements addressing both of these topics. Privacy protection requirements apply to any business transaction in which an individual is a "buyer".

Rule 038:

A common set of external constraints of a jurisdictional domain on a business transaction, where the buyer is an individual, are those of a privacy protection nature.

Rule 039:

Where the buyer in a business transaction is an individual, external constraints of a privacy protection nature of jurisdictional domains apply and shall be supported in applicable business scenarios and scenario components.

The principles governing privacy protection and associated rules are in Clause 5 above.

The focus of this sub-Clause is to specify key rules which are applied to any Person in the role of a seller, i.e., as an organization and public administration, who offers or provides a good, service, and/or right to prospective buyers.

It is noted that from a supplier perspective, privacy protection requirements can be summarized as maintaining recorded information about an identifiable individual which is as timely, accurate, and relevant as possible, is used only for its original purpose and not for any other purpose (unless consented to by the individual concerned), and that any such recorded information which does not meet these requirements is

expunged, unless there are other external constraints of a jurisdictional domain nature which override such privacy protection requirements, (e.g., law enforcement, national security, etc.). The privacy protection principles which apply here are stated above in Clause 5.

The application and implementation of this rule has as a logical consequence that any Person offering a good, service and/or right as a seller in a business transaction shall explicitly state that the good, services and/or right, as a goal in a business transaction, is, or is not offered to a buyer as an individual.

Rule 040:

Any Person offering a good, service, and/or right as a seller shall explicitly state whether or not the same is available for purchase by any Person in its role as an "individual".

For example, certain goods, services and/or rights may be proscribed from being offered for sale, and therefore are not sold to an individual.

Rule 041:

Where the buyer in a business transaction is an individual, external constraint of a privacy protection nature of jurisdictional domains apply and shall be supported in applicable business scenarios and scenario components.

Rule 042:

A seller shall ascertain, at the identification phase in the process leading to a business transaction, whether or not the buyer is an individual (not someone as organization Person buying on behalf of an organization or public administration)[60].

Guideline 042G1:

Where a jurisdictional domain differentiates in criteria for privacy protection with respect to a natural person in its role as an "individual" or an "organization Person," this needs to be specified.

Guideline 042G2:

Where a jurisdictional domain has privacy protection requirements as a set of external constraints which are applicable to a specific sector (public versus private, per industry sector, etc.), or type of business transaction, this shall to be specified.

---

60 See further in ISO/IEC 15944-1 Clauses 6.2 "*Rules governing Person*"; Clause 6.3 "*Rules governing the process component*"; and, Clause 6.4 "*Rules governing the data component*". Here the development work on the "process" component is specifically structured to support privacy protection requirements in its five fundamental activities which are:

- planning;
- identification;
- negotiation;
- actualization; and,
- post-actualization.

Examples in the text or in the footnotes for this Clause 6.3 are based on privacy protection requirements. Annex F (Informative) titled "*Business transaction model: process component*" in ISO/IEC 15944-1 takes a similar approach.

7.2.2 Person and external constraints: Consumer protection[61]

In modelling (electronic) business transactions, an external constraint that needs to be taken into account is that commonly known as "consumer protection".[62]

Rule 043:

A common set of external constraints of a jurisdictional domain on a business transaction, where the buyer is an individual, are those of a consumer protection nature[63]. As such, any business transaction involving an "individual" in the role of buyer shall be structured to be able to support applicable "consumer protection" requirements.

"Consumer" and "vendor" have already been defined in ISO/IEC 15944-1:2010 and "consumer protection" in ISO/IEC 15944-5:2008. {See further above Clauses 3.27, 3.115, and 3.28 respectively for the text of the definitions of these three concepts}.

Rule 044:

Where the buyer is an individual, the seller shall ascertain that the individual has the age qualification required by the jurisdictional domain to be able to be involved in and make commitments pertaining to the good, service and/or right being offered in the proposed business transaction

Guideline 044G:

A seller shall take the required precautions to ensure that it does not communicate inappropriate information, engage in monetary transactions, or in the making of any commitments with those who do not have the capacity to engage in them such as minors, (without the verifiable consent of their parents or guardians), or those without legal capacity, as may be required by the jurisdictional domain of the buyer.

This rule and guideline captures common consumer protection requirements pertaining to sales in general as well as to particular goods or services to children and minors who may not have the legal capacity to engage in such actions in the jurisdictional domain of the buyer (and/or seller).

Rule 045:

A seller shall ensure that where it intends to sell a good, service and/or right to a buyer as an individual that consumer protection requirements of the applicable jurisdictional domain of the buyer are supported.

These consumer protection requirements include the provision of "complete" information, the use of language of the individual, terms of contract formation and fulfillment, privacy of the on-line information, security of the personal information and payment, procedures for redress, stop to unsolicited e-mail, etc. Note that the place of delivery may affect the ability of the buyer and seller to act.

---

61 Clause 6.3.2 builds on and uses Clause 6.2.8 *"Person and external constraints: Consumer and vendor"* of ISO/IEC 15944-1.

62 It is noted that:

- *many of the external constraints pertaining to personal information of an individual for privacy protection in a business transaction are similar in nature to consumer protection requirements; the 1st edition of his Part of ISO/IEC 15944 focuses on most primitive aspects only; and,*
- *linkages and similarities between privacy protection and consumer protection requirements will be addressed in the 2nd edition of ISO/IEC 15944-8 or in a separate new part of ISO/IEC 15944.*

63 This is a restatement of "Rule 38" in ISO/IEC 15944-1.

7.2.3 Individual accessibility

This is an external constraint of a public policy nature that shall to be taken into account in modelling (electronic) business transactions through re-useable business objects, including those which are categorized as individual accessibility[64] requirements. These take the form of either (1) rights of individuals in their use of information technologies at the human interface; and/or (2) those providing goods or services in general or in particular ensure that the provisioning of the same does not discriminate against or prevent participation by "non-typical" users, i.e., those persons with an impairment or disability of some kind, who require some form of adaptive semantics and technologies to participate in a business transaction, viz. "individual accessibility". Here "individual accessibility" pertains to ensuring that goods or services being provided in (electronic) business transactions can be used by people with impairments or disabilities.

Jurisdictional domains often specify human accessibility requirements as being: (1) of a generic nature and applicable irrespective of the goals of a business transaction and the commitments being entered into among participating parties, (e.g., as part of basic human rights, as part of its constitution, etc.); and/or (2) as applicable to a particular sector, (e.g., e-government, education, etc.). Particular human accessibility requirements may also exist at the UN member state's sub-division level, (e.g., a state, province, länder, etc.), at the regional level, (e.g., the European Union)[65].

Here disabilities can be of either a functional or cognitive nature.

It is noted that language and cognitive disabilities are very difficult to specify and thus model as human interface requirements[66], but often it is possible to do so. They include mental retardation, lack of short term memory, dyslexia, dyscalculia, dysgraphia, auditory and perceptual disabilities, cognitive disorganization, and visual perceptual disabilities.[67]

Unless a human disability(ies) of an individual is of the nature where the jurisdictional domain considers or declares the individual to be "incompetent", i.e., not able to make a commitment as a party to a business transaction, from an external constraints perspective, there is a need to be able to support human accessibility requirements. This includes the provision of "alternate formats", i.e. the provision of the semantics of the recorded information is in a representation form, which the individual as (prospective) buyer is able to understand in an unambiguous manner in order to be able to decide whether or not to make the commitment(s) associated with the actualization of a business transaction. This also applies to the protection of their personal data.

---

64 The concept of "Individual accessibility" has already been defined in ISO/IEC 15944-5 and is reproduced in Clause 3.56 above.

65 The United Nations has published an "*Overview of International Frameworks for Disability Legislation"* available at <<http://www.un.org/esa/socdev/enable/disother.htm>>.

66 Annex A in ISO/IEC 5218 "*Codes representing the human sexes"* titled "*Annex A (Informative) — Codes for the representation of the human sexes supporting (linguistic) cultural adaptability/Annexe A (Informative) — Codes de représentation des sexes humains supportant l'adaptabilité culturelle (linguistique)*" provides an example of this.

67 See further the US National Institute of Neurological Disorders and Stroh resources on dyslexia at <http://www.ninds.nih.gov/disorders/dyslexia/dyslexia.htm>, and the "*IMS Guidelines for Developing Accessible Learning Applications*", Version 1.0 White Paper, 2002-06-22, as well as other IMS documents containing IT systems specifications for individual accessibility requirements from an "e-learning" perspective. {http://imsglobal.org/accessibility}. This IMS work is being progressed as a multipart international standard through JTC1/SC36 as ISO/IEC 24751 *Individualized Adaptability and Accessibility in E-learning, Education and Training*:

Part 1: Framework and Reference Model

Part 2: "AccessForAll" Personal Needs and Preferences for Digital Delivery"

Part 3 : "AccessForAll" Digital Resource Description"

The ISO/IEC JTC1/SC36 multipart ISO/IEC 20016 standard *ITLET — Language Accessibility and Human Interface Equivalencies (HIEs) in e-Learning applications: Principles, Rules, and Attributes* is also relevant.

Rule 046:

In the development of human interface equivalents (HIEs) for an ID code[68] or a semantic identifier, these must also include those HIEs of a nature to ensure individual accessibility[69].

7.2.4 Human rights

The three public policy requirements identified above apply to Persons in their role as an individual engaged as a "buyer" (or "consumer") in a business transaction. There are other public policy requirements which may need to be supported of a "human rights" nature in modelling a business transaction. Here, in the context of "cultural adaptability" as the third strategic direction of ISO/IEC JTC1 for its standards development[70], other public policy requirements which may need to be incorporated into the specification and re-use of business objects include:

- the UN "Universal Declaration of Human Rights" (1948);
- the UN "Universal Declaration of Rights of Persons belonging to National or Ethnic, Religious and Linguistic Minorities";
- the UN "Universal Declaration of Cultural Diversity" (Paris, November, 2001); and,
- International Covenant on Economic, Social and Cultural Rights 1966, United Nations (UN).
- UN Convention on the Rights of Disabled Persons (2006).

7.2.5 Privacy as a right of an "individual" and not the right of an organization or public administration[71]

Rule 047:

Privacy protection requirements apply only to a natural person, i.e., human being, acting in the role of an individual.

Organizations or public administration do not normally have any common law or statute law right" to privacy protection because public policy does not consider them to require statutory protection. They by definition are "legal persons" and not "natural persons". {See further Figure 16 Clause 6.2.7 and Figure E.19 Annex E in ISO/IEC 15944-1 as well as associated rules and text}

An organization or public administration may introduce and maintain requirements of a "confidentiality" or "secrecy" nature with respect to an identified set(s) of recorded information (included as semantic components or information bundles among participating parties to a business transaction). However, requirements of a "confidentiality" and "secrecy" nature would need to be identified, negotiated and agreed to as part of contract formation pertaining to a business transaction, and are not in the scope of this part of ISO/IEC 15944, although similar methods may be used in modelling confidentiality or secrecy as those for privacy.

---

68 The development of "Coded domains" of ISO/IEC 15944-10 incorporates the ability to support individual accessibility requirements.

69 Table 1 in Annex A of ISO/IEC 5218:2004 provides an example of an IT-enabled approach to supporting individual accessibility. It has been reproduced in Annex D. ISO/IEC 15944-7 is structured to be able to support individual accessibility requirements through the development of additional normative Annexes.

70 The other two strategic directions of ISO/IEC JTC1 for standards development are "portability" and "interoperability".

71 In the preparation of this part of ISO/IEC 15944 no applicable law or regulation has been identified in jurisdictional domains which state that an organization has an explicit right to "privacy protection" as an organization.

This is part of the broader field referred to as of information security labelling in ISO/IEC 27002.[72] Information is labelled according to the overall protection constraints that are to be applied to it. Information that is confidential is generally labelled so that supporting FSV mechanisms can be provided that determine if the information is being accessed by an entity that is properly authorized. Privacy protection labels (as shown in Section 5) are used to indicate what subsequent use (if any) the authorized entity may make of the information that is labelled. So, at a simple level, the recipient of information that is confidential is not limited in the subsequent use that they make of that information, whilst the recipient of information that has privacy is explicitly constrained as to the subsequent use. As such, privacy protection labelling is separate and independent from confidentiality labelling, although both make use of similar supporting mechanisms (FSV).

72 See further ISO/IEC 27002:2005 *Information technology — Security techniques — Code of practice for information security management.* In addition, the ITU-T has standards development activities pertaining to privacy protection and use of ICT, i.e., from a FSV perspective. Similar, ISO/IEC JTC1 has several standard development committees addressing privacy protection issues from both a BOV and FSV perspective, (e.g., JTC1/SC31 and SC37) or from an FSV perspective, (e.g., ISO/IEC JTC1/SC27)

THIS PAGE INTENTIONALLY LEFT BLANK

8 Principles and rules governing the establishment, management and use of identities of an individual[73]

8.1 Introduction

The concept of "identity management" is not clearly defined with reference to international standards, although there is relevant work in ISO/IEC JTC1/SC27/WG5 *"Identity management and privacy technologies"*. Published work seems to focus on the Functional Services View (FSV) aspects: the "How to," without first defining the business operational view (BOV) requirements, the "WHATs". In addition to addressing the establishment, management, and use of identities of an individual based on external constraints, this section focuses on supporting external constraints of a privacy protection nature.

The concept of "identity management", or more accurately "management of identity(ies)" of an entity since it is viewed differently from various perspectives. Its widest perspective is that at the entity, i.e., pertaining to any person, object, event, idea, process, etc. {See further Clause 3.44 definition of entity} Within an Open-edi and eBusiness context, a differentiation is made between "Person" and "non-Person". {See further Annex C *"Unambiguous identification of entities in (electronic) business transaction*" in ISO/IEC 15944-1[74]} The focus of this part of ISO/IEC 15944 with respect to "management of identities" is not on Persons in general but that of an individual and as a sub-type of Person in particular.[75]

The need for unambiguous identification of entities in (electronic) business transaction is identified in Annex C of ISO/IEC 15944-1 titled *"(informative) Unambiguous identification of entities in (electronic) business transactions*. In Annex C of ISO/IEC 15944-1, (1) the ISO/IEC JTC1 definition for the concept "entity" provides as examples "person, object, event, ideas, process"; and (2) that the focus of the multipart ISO/IEC 15944 standard Is only the unambiguous identification in a business transaction of Persons[76], and thus not objects[77], events, processes, etc. Objects, events, processes when defined or referenced in the modeling of Open-edi scenarios and scenario components, are registered as business objects. {See further ISO/IEC 15944-2}

Users of this part of ISO/IEC 15944 should be aware that many of the issues pertaining to "identity management" with respect to a Person (natural or legal) are also identified and addressed in ISO/IEC 15944-1 as well as ISO/IEC 15944-2. ISO/IEC 15944-4, and ISO/IEC 15944-5.

This Part of ISO/IEC 15944 sets out the principles and rules governing the establishment, management, and use of identities of an individual which are to:

1) to be based on those which already apply to a Person in a generic manner, as already found in the following normative Clauses of ISO/IEC 15944-1,

   Clause 6.1.4 – *Business transaction: unambiguous identification of entities*

---

73 See further Annex E below titled *(Normative) Key existing concepts and definitions applicable to the establishment, management, and use of identities of a single individual*

74 A guiding principle in the development of the multipart ISO/IEC 15944 standard is that it is structured to be able to support the need to differentiate among the three sub-types of "Person" namely "individual", "organization" and "public administration".

75 This part of ISO/IEC 15944 maximizes the use of other ISO and IEC standards as well as Referenced Specifications relevant to the privacy protection requirements in a BOV (and not FSV) context.

76 In support of this approach ISO/IEC 15944-1 also contains an Annex D titled "*Existing standards for the unambiguous identification of Persons in business transactions (organizations and individuals) and common policy and implementation considerations"*.

77 ISO, IEC and ITU standards for the unambiguous identification of objects (including tokens) are many. Standards here developed and maintained by ISO/IEC JTC1/SC17 "Identification cards" and those by JTC1/SC31 "Automatic identification and data capture techniques" and the resulting ubiquitous use of bar codes are the most commonly known. In addition, various industry sectors also served by one or more international standard of registration and identification schemas and assignment of unique identifiers for each unique objects, (which in turn usually has many clones with the same ID as result of mass manufacturing, publishing, etc.).

Clause 6.2.2 – *Person, personae identification, and Person signature*; and,

Clause 6.2.3 – *Person, identity and authentication*;

2) apply the Clause 5 Privacy Protection principles to an "individual" as a defined sub-type of "Person"; and,

3) modify the relevant figures found Clause 6.2.2 and 6.2.3 to focus on "individual" only, i.e., identification of organizations and/or public administrations is not included.

Key concepts and definitions applicable to the establishment, management and use of identities of a (single) individual along with associated rules are already defined and stated in ISO/IEC 15944-1, ISO/IEC 15944-2, ISO/IEC 15944-4, and ISO/IEC 15944-5.

Annex E below contains the key concepts and definitions applicable to the establishment, management and use of identities of an individual in a business operational view (BOV) context[78].

8.2 Rules governing the establishment of personae, identifiers and signatures of an individual

This sub-clause and its rules:

1) applies the existing rules as well as associated concepts and their definitions in ISO/IEC 15944-1 pertaining to Person, and adapts them based on the privacy protection principles set out in Clause 5 above, doing so from a collaboration space perspective as stated in Clause 6 above;

2) includes added rules which apply where an individual is a buyer in a business transaction; and,

3) do so in an integrated approach.

4) supports this integrated approach and support the real world conditions noted above;

5) supports the fact that it is up to a Registration Authority to decide, and therefore accept due liability (which must be made clear to the parties) for the correctness of their assertion, based on applicable criteria in the jurisdictional domain of that Registration Authority, i.e., applicable set(s) of internal constraints; whether or not to register an individual as a member, of a coded domain, and if so assign an ID code, to that individual together with any qualifications as to the liability taken by the Registration Authority as to the provenance they grant individuals.

(It is noted that a Registration Authority, i.e. an organization or public administration, may be responsible for the management of more than one registration schema (RS). Consequently, the "same" real world individual may or may not be eligible to become a member of the different RSs being managed by a single RA.)

From an external constraints perspective, a single organization may be a Person, as an incorporated (legal) entity with the associated accepted legal name(s)[79] as part of the incorporation, and also may use other names in conducting its business transactions including trademarks.

Here, a Registration Authority is an organization or public administration that is responsible for the management of one or more registration schema (RS). Consequently, the "same" real world individual may or may not be eligible to become a member of the different RSs being managed by a single RA.

---

78 It is noted that various ISO/IEC, ISO, IEC and ITU communities are working on developing standards in support of management of identities of entities (including individuals). This is especially true from a Functional Services View, i.e., FSV technical support services view perspective.

79 Where a jurisdictional domain has more than one official language, a "legal" person may well have more than one official name, i.e. in each of those official languages. This is most often the case with public administrations.

Rule 048:

The primary set of generic principles and rules, as well as associated concepts and their definitions governing the creation, recognition, use, management of identities of a Person as stated in Clauses 6.1.4, and 6.2.2 of ISO/IEC 15944-1, apply here.

A Person has one or more personae (and associated identifier(s) with each resulting in one or more Person identities (Pi) depending on the status and role qualification requirements of the Person to able to be registered for and obtain the resulting assignment of a unique identifier. This also applies to an individual obtaining a unique identifier from a RA.

The interworking with the rules in Clause 6.2.2, ISO/IEC 15944-1, results in a variety of combinations of linkages currently existing among personae, identifications and Person signatures for the same single real world individual. This is illustrated in Figure "7" below, which integrates and is a composite of Figures 9, 10 and 11 found in Clause 6.2.2. of ISO/IEC 15944-1). Figure 7 uses different fonts and representations for "Person signature" to recognize the wide variety of forms and information technologies utilized to capture "Person signatures[80]."

[80] One should note that the definition of signature created in Clause 6.2.2 in ISO/IEC 15994-1 allows for the use of different forms and each may be created by different processes, ranging from physical to advanced biometrics

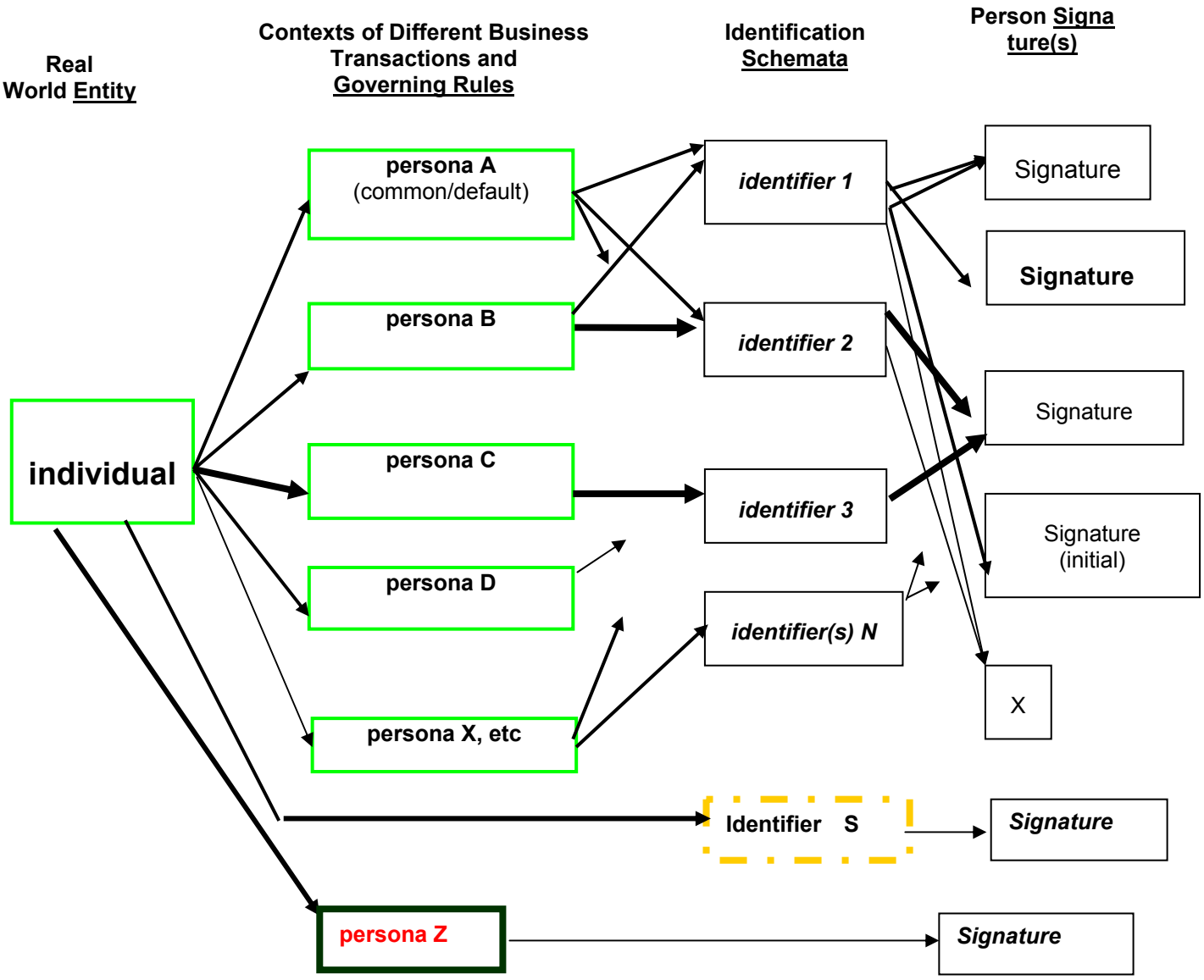


Figure 7 — Illustration of relationships of links of a (real world) individual to (its) persona (e) to identification schemas and resulting identifiers to associated Person signatures — in the context of different business transactions and governing rules

Clause 6.2.2 in ISO/IEC 15944-1 has therefore been adapted to focus on "individual" as a sub-type of Person as is illustrated in Figure 7 above. This includes and supports the following real world conditions[81]:

1) in addition to identifiers, an individual, during its lifetime, may have many multiple different personae, i.e. names, depending on the roles that it has or qualifies for.

81 Throughout this part of ISO/IEC 15944 the use of the phrase "real world conditions" means supporting identified existing internal and external constraints. It is outside the scope of this part of ISO/IEC 15944 to identify data management and interchange conditions of an external constraints nature which would result in more efficient and cost-effective data management and interchange among parties to a business transaction involving personal information. This should reduce significantly existing common "administrative" costs and inefficiencies in Open-edi among parties to a business transaction (as well as in the internal behaviour of their data management).

In addition, identifier "S" is used to represent an identifier being assigned to an individual without a persona, (an anonymous ID, usually associated in its use with techniques such as the introduction of a password or code or similar which may be used instead of a persona).

For some personae, the individual may assign or adopt for itself, while other personae used may be qualified as to whether or not they may be used as a persona in the identification schema of a Registration Authority (based on the rules governing the formation, representation and use of names of registrants of that Registration Authority) or otherwise. For instance, people at the time of marriage may create personae that were not previously in existence, as well as retain previous personae. (At the time of marriage an individual may acquire and use a new (legal) persona.)

Similarly, based on the rules and criteria of the applicable Registration Authority, the persona of an individual as written on its birth certificate, may not be the same as stated on an immigration record, a passport, a driver's licence, a social insurance or health insurance card, and so on. Consequently, any individual may well have multiple legally recognized names (LRNs), recognized individual names (RINs), recognized individual identities (riis), all at the same time (and so used in various business transactions).

2) unless proscribed by a specific external constraint, an individual is free to use any "persona" to represent itself[82]

3) an individual, during its lifetime, may have and use multiple different identifiers, i.e. individual identities depending on the roles that it has, qualifies for, or is assigned by nature of its status or actions[83];

   It is likely that an individual identity (ii) established by an individual in the context of a specific Registration Authority (RA) may have limited use as decided by the individual and/or Registration Authority (see further Clause 6.4 below)

   Examples include a persona which an individual assign to itself and is one which also serves as an identifier such as an e-mail address (an anonymous hotmail or gmail account), Facebook, Twitter as an "avatar", etc.

4) an individual, during its lifetime, often has and does use different forms or representation of its Person signature.

   Common examples here include the use by an individual of a "short name signature, the use of an initial, the use of a first name and surname only, the use of a initial and surname only and other signature forms whether physical or electronic in nature, (e.g. personal seals, symbols, document embossings, stampings, etc.).

5) only a specific persona of an individual may be eligible for use in an identification schema of a Registration authority before an associated identifier can be assigned by the RA.

   This is illustrated with "persona C", i.e., an individual shall use the persona as stated in its birth certificate, landed immigrant, or residence permit document (or its accepted Latin-1 alphabet equivalent where the IT systems of identification schema of the Registration Authority supports only the Latin-1 character subset of ISO/IEC 10646);

6) An individual, in qualifying for a new role and becoming a member of a registration schema of a Registration Authority, may be assigned a "new persona" in addition to their associated identifier.

---

82 The misuse of an existing persona by an individual for fraudulent purposes, a.k.a. "personation" is a criminal offence in (most) jurisdictional domains.

83 For example, at the time of marriage an individual may acquire and use a new (legal) persona. similarly, based on rules and criteria of the applicable Registration Authority) the persona of an individual as written on its birth certificate may not be the same as stated in an immigration record, a passport, a drivers' licence, a social insurance or health insurance card, etc. Consequently, an individual may and will have multiple legally recognized names (LRNs), recognized individual names (LRNs), recognized individual identities (riis) at the same time (as so used in various business transactions.

The fact that an individual is assigned a "new" persona is a not infrequent occurrence (for instance where the movement of an individual from one jurisdictional domain to another results in the individual obtaining a new or different civil status in that jurisdictional domain for no more reason than the written form of the persona of the individual who moves to another jurisdictional domain as immigrant, resident, refugee, etc., may well be in a language and or writing system which is different from or not supported in the new jurisdictional domain). This is evidenced in documents issued as proof of civil status.

7) the Person signature form used by the individual at the time the persona was registered and the identifier assigned shall be same in all transactions (and interactions) of that individual when using the identifier assigned by that Registration Authority.

   Common examples here include requirements in the financial services and banking sector, where the signature form of the individual when first registered with a bank or financial service recorded manually on a signature card maintained by the issuer or on the back of the card issued) or electronically by that registration authority, must match and continue to match the signature form used by the individual when using that specific identifier for a particular purpose.

8) a persona used by an individual need not be linked to any registered identification schema and thus any identifier, i.e., ID code in a registration schema of an RA providing that is fit for the purpose of the transaction.

   This is illustrated by the box representing "persona Z".

9) an individual may be registered in a registration schema (RS) of a Registration Authority (RA) by its resulting identifier without a specific persona being maintained.

   This is illustrated by the box representing "identifier S". An example here is an individual having a numbered account with a bank which does not require the individual's persona for its use but other (non-) personal information which is deemed by the RA to be sufficient to absolutely identify the persona for the purposes of effecting transactions for money or money's worth.

10) the identifier assigned by the Source Authority is of the nature of a composite identifier based on a set of rules, and the identifier assigned is therefore parse-able.

    For example, the identifier on one's credit/debit card or any other card issued based on the use of the ISO/IEC 7812, is a composite identifier[84], as is any organization identifier based on ISO/IEC 6523[85].

With respect to the identification schema and the creation of identifiers[86], in that identification schema, it is noted that

1) it is the Registration Authority (RA) which assigns the identifier when the individual meets the stated criteria and is registered as a member of that coded domain(s) of the RA;

84 For information on how this composite identifier is composed and related summary information, see ISO/IEC 15944-1, Clause D.4.2.3 *"(Global) unambiguous identification of "buyers" and "sellers" – ISO/IEC 7812"*

85 For information on how this composite identifier is composed and related summary information, see ISO/IEC 15944-1 Clause D.4.2.2 *(Global) unambiguous identification of "organizations" – ISO/IEC 6523".* Here the IANA is registered under ISO/IEC 6523 with its international code designation (IDC) being "0090" for the Internet IP addressing, i.e., internet IP addresses, like international telephone numbers are composite identifiers and thus parse-able which facilitates their use in IT systems.

86 Note that these can include the use of identifiers in coded domains. {See further ISO/IEC 159440-10}.

2) the status, eligibility and/or qualifications of the individual may result in:

a) "mandatory[87]" registration with a particular RA, i.e. often due to specified external constraints of a jurisdictional domain; or,

b) "voluntary" registration by the individual with an RA which can be based on a requirement of an internal constraints nature by the seller; i.e. that based on internal constraints of the seller[88]; or those based on external constraints of a regulator.[89]

Rule 049:

An individual may have and often does have multiple different personae, i.e., names in the lifetime of that individual. More than one persona may be valid in one or more jurisdictional domains at the same time.

During the course of the life of an individual multiple personae may be required to be used. In addition, the individual may also use a variety of different personae. Significant factors here include:

- mobility and migration of individuals from one jurisdictional domain to another including the fact that this involves the use of different official languages. The most common example here is that the jurisdictional domain in which the individual is born has a language and/or writing system which is different from the jurisdictional domain into which the individual has immigrated to (or becomes a legal resident or citizen of);
- through marriage (or similar change in civil status), the individual (legally) obtains or uses a persona different from its "birth certificate persona";
- the individual decides to use a variant (or new) persona which is different than that stated on its birth certificate, and uses this new persona as a default "persona" which in turn may become a RIN.;
- the fact that an individual as a child (or minor) may be subject to a divorce of its parents and thus obtain, a changed family name;
- the fact that an individual may request and receive a legal change of name in the applicable jurisdictional domain;
- an individual in using ICT and in particular the Internet may well represent itself with a persona which is quite different from any of its personae used in the "physical" or jurisdictional world.

Rule 050:

An individual may have, and often has, one or more recognized individual names (RINs), including two or more simultaneously existing RINs, and thus more than one recognized individual identity (rii).

A recognized individual name is any persona associated with a role of an individual which is recognized as having legal status, so any legally recognized name (LRN) recognized in a jurisdictional domain as accepted or assigned in compliance with the rules applicable of the registration schema of that jurisdictional domain as governing the coded domain of which the RIN is a member can be valid. Associated with a registered

87 Primary examples here are the mandatory requirement of registration of an individual at birth, registration of marriage i., or pursuant to the issue of a passport or similar travel document for crossing international boundaries, etc. Here the individual is not issued an "identifier" as such but the document attesting the existence and status of an individual is assigned an unique and unambiguous identifier. Often identities are linked to permitted methods of payment (e.g. use by the buyer of a credit or debit card only for payment in a business transaction.

88 Often these are linked to permitted methods of payment (e.g. use by the buyer of a credit or debit card only for payment in a business transaction.

89 Examples here include an individual qualifying for a license of some kind (driver's license, professional license for a doctor, engineer, architect, etc.)

individual name is (usually) a registration number of the document attesting to the RIN and its legal status of some kind.

Common examples of RINs with directly associated riis include:

- a birth certificate name and birth registration number as issued by the jurisdictional domain in which the birth of the individual was registered;

- a marriage certificate name and marriage registration number as issued by the jurisdictional domain in which the marriage of the individual was registered. Note: an individual may have more than one married name but (normally) only one is valid at any one time.

- a passport name and passport registration number as issued by the jurisdictional domain which issued the passport based on the applicable eligibility rules for that coded domain. Note: An individual may have more than one type of passport (depending on its role) as well as more than one passport issued by different jurisdictional domains (depending on the rules of those jurisdictional domains). Some individuals may hold multiple passports both in their own apparent names and also different apparent names;

- a medical or health name and card registration number as issued by the jurisdictional domain which issues the card based on applicable eligibility rules;

- a driver's license and registration number as issued by a jurisdictional domain based on the individual qualifying for such a license.

It is noted that, on the whole, the establishment of a RIN and its associated rii for an individual by a jurisdictional domain may be based on, either or a combination of:

1) recognition of the status of an individual

   This relates to the civil status of an individual in a jurisdictional domain of a geo-political nature, (e.g., such as birth, marriage, death, citizenship, landed immigrant, resident, etc.), and the rights and obligations which are "automatically" conferred relating to the status of an individual.

2) the individual qualifying is based on meeting a set of pre-defined criteria, and passing the associated test.

   Qualifications of the individual may include:

   a) those of an age nature, i.e. an individual must have attained the age of "n" years to be able to play a particular role, (e.g., get married, authority to buy cigarettes, alcohol, a firearm, vote in local, regional or national elections, etc.);

   b) those of a criteria and /or test nature, in addition to likely having to meet "1)" and "2.a" aspects as well. Examples here include a driver's license, a professional qualification (as an individual qualified and so registered in a recognized "official" profession such as medical doctor or lawyer, in a jurisdictional domain), etc.

8.3 Rules governing the assignment of unique identifiers to an individual by Registration Authorities (RAs)

Rule 051:

Any Person acting in the capacity of a Registration Authority (RA) shall, for each of its Registration Schemas (RS) involving the registration of an individual, be identified as observing the rules governing and ensuring the assignment of a unique identifier for each individual as a member of that registration schema.

The rules governing the eligibility of an entity to become a member of a registration schema (RS), administered by its Registration Authority are for the Registration Authority to determine. This includes determining whether the entity, i.e., as a Person and then as "individual" has the qualification to be an eligible candidate in order (to submit a request) to become a member of that Registration Schema, including the assignment of a unique identifier.

Rule 052:

A Registration Authority shall assign a unique identifier to each of its registered members including, where relevant, where the member is acting as an individual.

This unique identifier has the properties and behaviours of an ID code in the coded domain used to support management and maintenance of the Registration Authority Schema[90].

Rule 053:

Where the Registration Schema (RS) of a Registration Authority allows for the registration of Persons and differentiates among sub-types of Persons, i.e., individuals, organizations and/or public administrations, the Registration Authority shall ensure that:

1) **any registration involving an individual is so identified; and,**

2) **that privacy protection requirements which apply to resulting or associated personal information are identified and supported.**

This is important because where different sub-types of Persons may be members of the same coded domain, resulting from the application of a Registration Schema of a Registration Authority, privacy protection requirements apply only to those members of the coded domain who are individuals. This is because recorded information about a member of a coded domain who is an individual is personal information and thus subject to privacy protection requirements.

Rule 054:

Where a Registration Authority (RA) administers more than one Registration Schema which involves individuals (and their associated personal information), the RA shall not use personal information provided by the individual under one Registration Schema (RS) in another RS of the RA without the explicit consent of the individual concerned unless required by applicable law.

This rule supports the privacy protection requirements stated in Clause 5.3.4 above.

8.4 Rules governing individual identity, authentication, recognition, and use

Business transactions differ in their nature and goals. The rules governing a business transaction, may (a) allow a Person to use one of several Person identities, (e.g., one of several different credit cards or passports); or, (b) require a Person to have/utilize a pre-specified Person identity (e.g. a Blue Cross card, a national health insurance card, etc.)

Rule 055:

The individual identity, i.e., the persona and the associated identifier, used by an individual in a business transaction, shall be capable of being prescribed depending on the context and goal of the business transaction.

90 The rules and best practices governing the development, management and interchange of coded domain are the focus of ISO/IEC 15944-10 on "*Coded Domains".*

Based on the rules in Clause 8.3 and 8.4 above, and drawing on elements in Figure 7 above, Figure 8 below Illustrates the range of one-to-one bindings that can occur between the personae and identifiers of an individual as individual identities (ii) defined as:

individual identity (ii)

Person identity *of an* ***individual****, consisting of the combination of the* ***persona*** *information and* ***identifier*** *used by an* ***individual*** *in a* ***business transaction****, i.e. the making of any kind of* ***commitment***

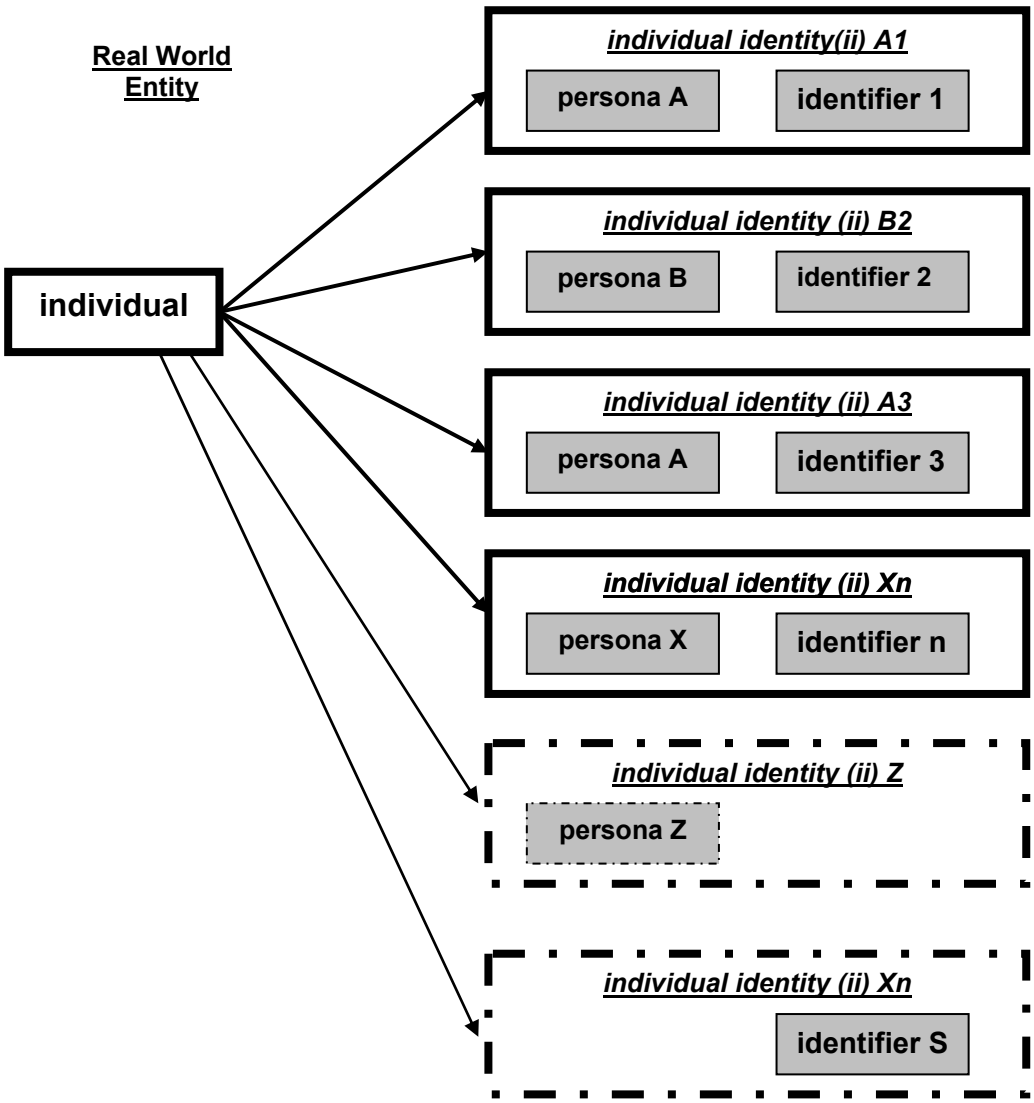


Figure 8 — Illustration of range of links between personae and identifiers of an individual identity(ies) of an individual

Rule 056:

A specific individual identity (ii) established by a Registration Authority, (organization or public administration), should not be used for any purpose other than that for which it was created, without the express and explicit consent of the individual.

Guideline 056G1:

A recognized individual identity (rii) based on a Registration Schema(RS) of Registration Authority (RA) has the added attribute of being re-useable and thus is the preferred approach for Open-edi.

An individual identity which is recognized for use in a business transaction is know as a "recognized individual identity" and is defined based on the existing ISO/IEC 15944-1 definition of for the concept of "recognized person identity" (rPi)" adapted as follows:

recognized individual identity (rii)

*identity of an **individual,** established to the extent necessary for the specific purpose of a business transaction*

As stated in Clause 6.2.3 in ISO/IEC 15944-1:

"*When a Person identity is presented for use in a business transaction, it has to be "recognized" by the other parties to the business transaction. Each party to the transaction may have its own rules governing the requirements for establishing a "recognized Person identity (rPi)"*[91]

Applying the existing ISO/IEC 15944-1 rules governing identification and authentication of Person to an individual based on applicable common external constraints, i.e., those stated in Clause 5 above is illustrated in Figure 9 below, which is an adaptation of Figure 12 in Clause 6.2.3 in ISO/IEC 15944-1.

Since a persona Registration Schema (RS), of a Registration Authority (RA),

1) may or may not, include the registration of individuals; and,

2) if the RS, does allow for the registration of individuals as members,

then external constraints of a privacy protection requirements nature apply, and it is necessary that one distinguishes between a pRS which does not contain individuals as members and those which does, in whole or in part, i.e., as individual persona Registration Schema (ipRS).

Rule 057:

For any persona Registration Schema which includes, in whole or in part, individuals as members, external constraints of a privacy protection nature apply and all its registrants which are individuals shall be managed as members of an individual persona Registration Schema (ipRS) in accordance with applicable privacy protection requirements.

Expanding the ISO/IEC 15944-1 definition for the concept of "persona Registration Schema (pRS), an "individual persona Registration Schema (ipRS)" is defined as follows:

individual persona Registration Schema (ipRS)

persona Registration Schema (pRS) *where the **persona** is, or includes, that of an **individual** being registered*

NOTE 1 Where an persona Registration Schema includes persona of subtypes of Persons, i.e. individuals, organizations, and/or, public administrations, those which pertain to individuals shall be identified as such because public policy as external constraints apply including those of a privacy protection requirements nature.

91 "Depending on the rules governing a business transaction, a Person identity for interchange purposes can be comprised of a finite set of data elements such as those required for identification systems for Persons based on international standards such as found in ISO/IEC 7501 or ISO/IEC 7812 (See further Annex D in ISO/IEC 15944-1). Or the set of data element required may be more extensive, but it must still be finite and prescribed. These and similar specifications are expected to be registered as "re-useable" in accordance with ISO/IEC 15944-2"

NOTE 2 In an individual persona Registration Schema, one shall state whether or not a truncated name, i.e. registered persona, of the individual, is allowed or mandatory, and if so the ipRS shall explicitly state the rules governing the formation of the same.[92]

The selection of an individual identity in a business transaction between the seller and the buyer, where the buyer is an individual, i.e., one which is recognized for use between the buyer and the seller in a business transaction (as well as any other parties to that business transaction) is established in one of two ways:

1) the individual identity to be recognized (and accepted) for use in a business transaction is the one that is established and mutually agreed to between the buyer and the individual. It is thus a "mutually defined - recognized individual identity (md-rii)".

Use of such a "md-rii" is found in business transaction involving internal constraints only. Such identities may be of a one time nature only and not "re-useable". Although the use of a "md-rii" could be modelled in an Open-edi scenario as a scenario component, information bundle, and/or semantic component, it does not have the generally property of re-usability and thus is not a preferred approach in Open-edi.

2) the individual identity to be recognized (and accepted) for use in a business transaction where the buyer is an individual is one based on that established through a Registration Schema (RS) of a Registration Authority. It is thus a "Registration Schema (based) – recognized individual identity" (RS-rii").

These two basic approaches to recognized individual identities are defined as follows:

mutually defined - recognized individual identity (md-rii)

recognized individual identity (rii) *which is mutually defined and agreed to for use between the* ***seller*** *and the i****ndividual****, as* ***buyer****, in a* ***business transaction***

NOTE 1 The establishment of a mutually agreed to and recognized individual between a seller and individual, as buyer, does not extinguish the applicable privacy protection rights of that individual.

NOTE 2 A mutually defined recognized individual identity (md-rii) shall be established between the seller and the individual no later than the end of the negotiation phase.

NOTE 3 Use of a mutually defined recognized individual identity (md-rii) may not be permitted where external constraints apply.

and,

Registration Schema (based) –recognized individual identity (RS-rii)

recognized individual identity (rii) *for use in a* ***business transaction****, by the buyer as an* ***individual****, which is one based on the use by an* ***individual*** *as a member of a specified* ***Registration Schema (RS****) of a particular* ***Registration Authority (RA)***

92 Note the ISO/IEC 7501 multipart standard re Machine Readable Travel documents (e.g. passports, already does this. Similarly the ISO/IEC multipart 7812 Identification cards standard also does this.

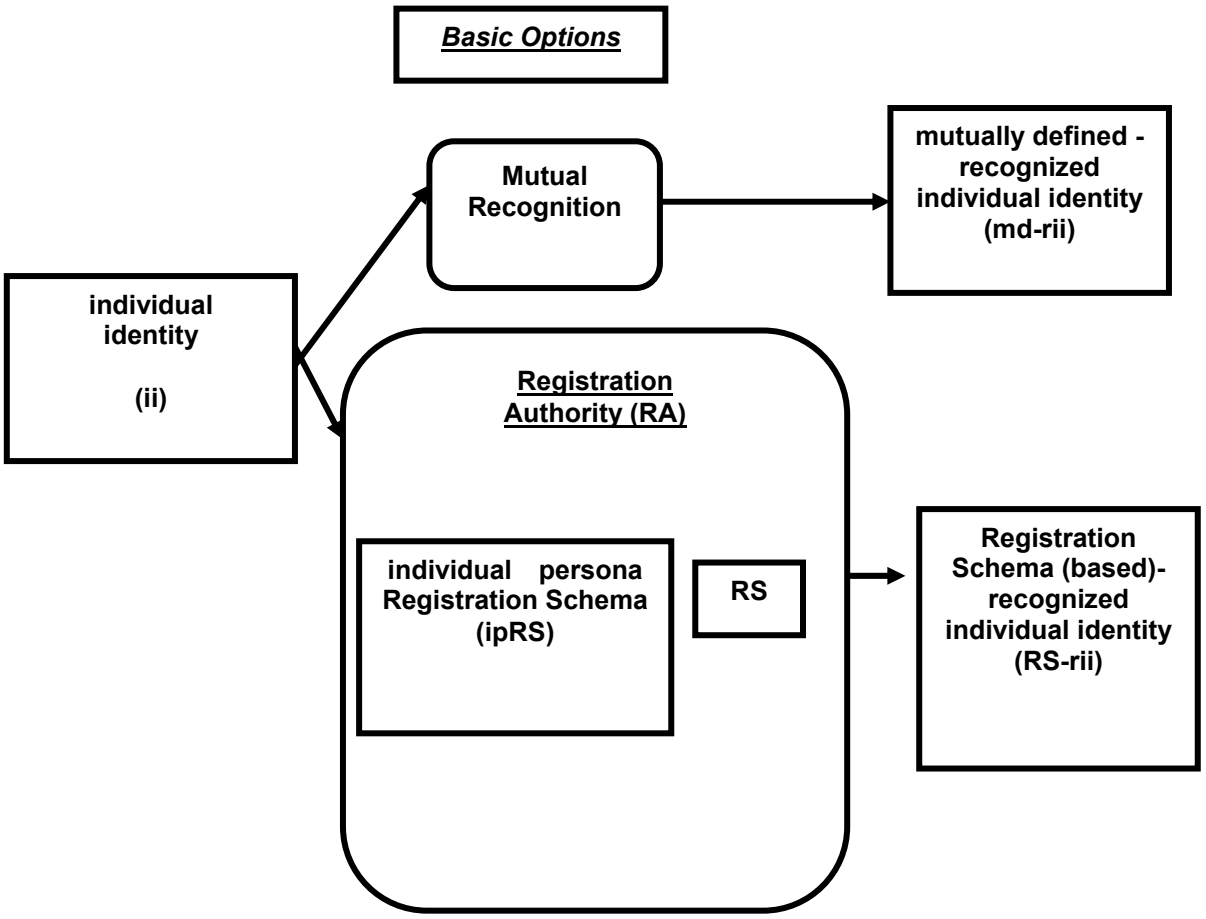


Figure 9 — Illustration of two basic options for establishment of a recognized individual identity (rii)

Rule 058:

A Registration Authority (RA) for individuals shall have explicitly stated rules for transforming an individual identity into a recognized individual identity to meet a stated business requirement.

Rule 059:

The rules governing a business transaction shall either require the use of a specified recognized individual identity (rii) or allow for several of a similar nature.

For example, if payment by credit or debit card is allowed in a business transaction, several different brands of cards may be allowed, but not necessarily all. It can also happen that for specific business transactions, an individual may be required to present a "legally" recognized individual identity such as a birth certificate, passport, a driver's license, a landed immigrant card, etc.

The establishment or verification of a recognized individual identity will require the capability for authentication, i.e., individual authentication, especially in electronic business transaction. As such individual authentication is defined as:

individual authentication

provision of the assurance of a ***recognized individual identity (rii)*** *sufficient for the purpose of the* ***business transaction***

For individual authentication to be successful, the following actions must have taken place:

- the individual identity must have been established; and,
- the individual identity must be recognized, i.e. a recognized individual identity (rii), must exist.

Rule 060:

In a business transaction, individual authentication is established by either:

1) mutual definition and acceptance: or,

2) **referring to predefined individual persona registration schema (ipRS) and process of a particular RA**

8.5 Legally recognized individual identifies (LRIIs)

A buyer may remain "anonymous" in a business transaction or use a "pseudonym"[93]. However, the nature of the good, service and/or right being provided by the seller (or a regulator as seller) may require a high level of unambiguity as to the identity of the individual. Where this is the case it is most often related to a role qualification the individual needs to have, i.e., as a legally recognized individual identity (LRII) which in turn is issued by a legally (recognized) individual persona Registration Schema (LipRS).

The definitions for these two concepts are as follows:

legally (recognized) individual persona Registration Schema (LipRS)

individual persona Registration Schema (ipRS) *which has legal status and is so recognized in recognized in a* ***jurisdictional domain*** *as being able to register a* ***recognized individual name (RIN)*** *and unique* ***identifie****r associated with such a registration.*

and,

legally recognized individual identity (LRII)

recognized individual identity (rii) *which includes the use of a* ***recognized individual name (RIN)*** *and the associated* ***identifier****, i.e.,* ***ID code,*** *assigned as part of the* ***personal information*** *for that* ***individual*** *in the* ***individual persona Registration Schema (ipRS)***

Here with respect to a LipRS, it is noted that:

a) it must have the status and recognition in the jurisdiction domain in which they are based;

b) the majority of LipRS are the responsibility of a public administration in a jurisdictional domain;

c) where a LipRS is not a public administration, its operations and "legally recognized" status is covered through applicable laws and regulations, (e.g., the issuance of credit and debit cards is prescribed by rules of the financial services sector).

Further, with respect to LDII, it is recognized that the use of a LRII is directly related to role qualification(s) which apply to a business transaction. These include those which are:

a) related to the age of the individual concerned to be able to make commitments with respect to certain types of business transactions such as marriage, purchase property, issuance of a passport, etc., or purchase of alcohol, tobacco, etc. These are related to applicable "age of majority" requirements in a jurisdictional domain;

93 This requirement was already recognized in Clause D.5.2 "*Anonymity*", in ISO/IEC 15944-1.

and,

b) related to the age of an individual and associate role qualification, (e.g., a driver's licence, professional qualifications, (e.g., doctors, accountants, lawyers, nurses, etc.).

In addition, a legally recognized individual identity (LRII) may:

a) be of general applicability such as those pertaining the existence and status of an individual (including birth, marriage, or death certificates);

b) have a predefined purpose and use such as a passport, a licence or certificate, a security classification;

c) be used for both individual identity and civil status purposes in a business transaction; and/or,

d) be independent of any particular use even though its use is strictly controlled and regulated by privacy requirements, such as any biometric based data used to identify an individual.[94].

94 The standards developed by ISO/IEC JTC1/SC37 *Information technology – biometrics* are relevant here.

THIS PAGE INTENTIONALLY LEFT BLANK

9 Person component – individual sub-type

9.1 Introduction

Many aspects of the individual as a sub-type of Person and the resulting link to privacy protection requirements have already been addressed in Clauses 5, 7, and 8 above. This clause sets out additional requirements on the Person component.

9.2 Role qualification of a Person as an individual

The test as to whether a Person is qualified to play a role as a party to a business transaction is a key aspect in modelling business transactions addressed in ISO/IEC 15944-1. Clause 8.4 *"Rules for the specification of Open-edi roles and role attributes"* as stated in ISO/IEC 15944-1 is mandatory when the business transaction involves an individual as a buyer. (See further Clauses 1.2.2 and 1.2.3 above) In addition, it is very important to ascertain as early as possible whether or not the party to a business transaction, in the role of a buyer, is an individual (or not). Because if buyer is an "individual", then public policy requirements of a public policy nature apply, including privacy protection, consumer protection, individual accessibility, etc. {See further Clause 6.3 *Jurisdictional domains and public policy requirements* (as well as associated rules) as stated in ISO/IEC 15944-5}.

Rule 061:

The Clause 8.4 "Rules for the specification of Open-edi roles and role attributes", as stated in ISO/IEC 15944-1 are mandatory where the business transaction involves an individual as a buyer.

Rule 062:

Prior to the start of the actualization phase of a business transaction, a seller shall ascertain whether or not the Person acting as a buyer is doing so in its capacity or status as an individual (rather than as an organization Person or other roles of a Person).

Guideline 062G1:

A seller should ascertain at the identification phase in a business transaction whether or not the Person acting as a buyer is doing so in its capacity or status as an individual and not in one of the other valid capacities of a Person.

Rule 063:

Where the buyer in a business transaction is an individual, the buyer shall:

1) **ensure that privacy protection requirements as stated in this part of ISO/IEC 15944 are applied; and,**

2) **ascertain whether or not other external constraints apply with respect the individual meeting specified criteria of the applicable jurisdictional domain(s) in qualifying for the role of buyer with respect to the good, service, and/or right which is the goal of the business transaction.**

If the buyer does not wish to permit the transaction if either the seller offered scenario does not support appropriate privacy constraints, or the seller's jurisdictional domain does not offer appropriate safeguards then the buyer should have the option to refuse the scenario.

Rule 064:

When the identification and negation phase of a business transaction does not result in its actualization and the prospective buyer is an individual, the seller (or regulator) shall delete all personal information on that individual gathered at that time.

Guideline 064G1:

The deletion, i.e. expungement, of such recorded information should be part of the organization's "Open-edi disposition" process and be part of the operational policy of an organization or public administration.

The rules stated below in Clauses 11.3 and 11.4 regarding state changes and records retention are applicable here.

Guideline 064G2:

Where Rule 064 applies, it is best practice that the seller or regulator informs the individual that all his/her personal information has been destroyed, [unless the individual requests that his/her personal information be retained, i.e., "left on file"].

9.3 Persona and legally recognized names (LRNs) of an individual

A Person may use any persona in a business transaction as is mutually accepted among all the parties to a business transaction. This is qualified where external constraints especially those imposed by jurisdictional domains are applicable.

However, one result of the application of external constraints is that a Person is not always free to choose and negotiate the nature of the Person identify (Pi) to be used in a business transaction, including the persona forming part of the Pi. Based on the external constraints applicable to the business transaction, a Person may be required to use a persona which is legally recognized, i.e., has the properties and behaviour of a "legally recognized name (LRN)". This requirement is addressed in Clause 6.6.2.3 "Personae as legally recognized names (LRNs)" in ISO/IEC 15944-5. The rules stated in Clause 6.6.2.3 ISO/IEC 15944-5 from a generic Person perspective also apply here.

Rule 065:

The rules in Clause 6.6.2.3 "*Personae as legally recognized names (LRNs)"*, as stated in ISO/IEC 15944-5 apply.

Rule 066:

Where the buyer in a business transaction is an individual, the seller shall inform itself as to whether external constraints apply which require the individual to use a legally recognized name (LRN) as its persona, as well as the nature of the Source Authority for such a LRN.

For example, the persona presented by the individual for use in a business transaction must be one which has the status of being legally recognized for use in a jurisdictional domain, (e.g., the persona as stated on a government issued birth certificate, a passport, a driver's licence, health insurance card, etc.

9.4 Truncation of legally recognized names of individuals

Even though in many, if not most jurisdictional domains, there is no legal limit on the length, (number of characters and/or number of discrete character strings) of the persona of an individual, including it being qualified as a LRN. However, standards such as ISO/IEC 7812 for identification cards (including credit/debit cards) and ISO/IEC 7501 for machine-readable travel documents, (e.g., passports), limit the persona which has a maximum number of characters. The persona of a Person may therefore be truncated, i.e., is a "truncated name" and that "truncated name" is legally recognized and known as a "truncated recognized name (TRN)".

Where a persona of the individual (including birth name) exceeds the maximum number of characters, it needs to be truncated. Therefore, users of this document shall reference ISO 7501 and ISO 7812 these standards shall be used for the technical details and rules for truncation.

Rule 067:

The rules governing the truncation of a persona, as stated in ISO 7501 and ISO 7812 ISO/IEC 15944-1, apply to this Part of ISO/IEC 15944.

Rule 068:

Where external constraints on a business transaction require an individual as a (potential) buyer using a legally recognized name (LRN) as the persona for that individual, the seller shall specify the types of LRNs permitted to be used by the individual.

Rule 069:

Where external constraints on a business transaction require that the personae of the individual be provided using a specified language or character set which is different from the language which the individual uses for his/her persona (or is his/her birth name), then the transliteration rules of ISO 7501 shall apply[95].

Quite often the persona of an individual (including its birth name) is in a language other than that to be used in a business transaction. In addition, external constraints of jurisdictional domains, often prescribe the use of official languages (only).

9.5 Rules governing anonymization of individuals in a business transaction[96]

Commonly in business transactions, particularly electronic business transactions, terms such as clients, consumers, customers, etc., are used rather than “individuals" or "organizations". Significant development has been undertaken by the private and public sector alike to re-use business-to-business transactions in business-to-consumer transactions.

From an eBusiness perspective, it is not always necessary to find out if the entity which is party to a business transaction is a "natural person" or "legal person", or an "individual" or "organization", etc. Credit worthiness, ability to pay, secure payment, etc., of a "Person", as a buyer, is often a more important criterion for doing business by the Person in the role of seller based applications, business (including e-commerce, e-government, e-health, etc.). This is particularly so when modelling Open-edi scenarios and scenario components from an internal constraints perspective only.

In much of consumer trade, a buyer can remain anonymous vis-à-vis a seller by presenting a money token[97] in which a seller has 100% trust, (e.g., cash). Similarly in electronic business transactions where the value token when presented by the buyer to the seller has 100% trust of the seller, the buyer can also remain anonymous (provided the "E-cash" really has the nature of cash, and does not identify the bearer or holder of the token). Similarly, if a Person (undifferentiated as to organization or individual) with an e-mail address of "diamondsR4ever@google.com" presents an acceptable value token which does not link the value token to the buyer, then buyer can remain anonymous to the seller.

---

95 These are stated in Appendix 9 to Section IV of ISO/IEC 7501:2008. The source text for which in turn is ICAO document 9303. This Appendix 9 has the following sub-divisions.

A. Transliteration of multinational characters

B. Transliteration of Cyrillic characters.

Depending on the source text for the persona of individual “A” or “B” apply.

96 The text for this sub-Clause is based on Clause D.5.2 of ISO/IEC 15944-1 and other relevant parts of ISO/IEC 15944 in a privacy protection context.

97 The term “value token” is a generic term used to cover all such tokens including cash, money orders, bearer bonds, pre-paid value tokens, etc.

Thus in electronic business transactions, unambiguous identification does not necessarily require one to distinguish the nature, i.e., sub-type, of the Person in a business transaction, i.e., whether the Person is an individual or organization (or an organization Person).[98]

Rule 070:

Identification of a Person as buyer in a business transaction is not always necessary in (electronic) business transaction involving the seller knowing whether or not the buyer is an individual.

The Process Component of the Business Transaction Model has five basic sets of activities: Planning, Identification, Negotiation, Actualization and Post-Actualization[99]. In the Planning set of activities (the first phase in a business transaction), prospective buyers and sellers can and do often remain anonymous to each other. The fundamental characteristic of the Identification Phase is that of establishing one-to-one bindings among the parties (potentially) involved in a business transaction.

Privacy protection requirements have made "anonymity" an external constraint that needs to be supported, creating the concept of "individual anonymity:"

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

From a process perspective, "anonymization is defined as follows:

> **anonymization**
>
> **process** whereby the association between a **set of recorded information (SRI)** and an identifiable **individual** is removed, even where such an association previously existed
>
> NOTE Adapted from ISO 25237:2008.

Rule 071:

Unless explicitly proscribed, (not allowed) by external constraints of the relevant jurisdictional domain applicable to the specified goal of the business transaction to be entered into, an individual as buyer many decide to remain anonymous in that business transaction, and no personal information on the individual is maintained by the seller or other parties.

One common external constraint of a jurisdictional domain is that of stating a role qualification for an individual as a buyer in a transaction. For example, an individual must be able to provide "proof of age" in the purchase of products which are "age" dependent, (e.g., cigarettes, alcohol, etc.). However, the provision of "proof of age" by an individual (or external constraints of a similar nature) does not necessarily require the capture of any personal information (including any "individual identity") by the seller on the individual as the buyer in that transaction. That is, unless explicitly required by a regulator, the individual identity (and associated personal information) provided by the individual as its "proof of age" is simply "proven" and the actual age not recorded. Only the business transaction identifier generated (on the sales receipt) by the seller for an instantiated business transaction needs to be retained by the parties to the business transaction. {See further Clause 11.2 below}

---

98 Privacy concerns of individuals, who are worried about who knows what you see and spend online on the Internet with whom, for what, etc., have given rise to a demand for "anonymization services". Disabling "cookies" on one's browser's preferences may prevent prospective buyers from exploring websites of sellers. Such services allow one: (1) to browse the Web and go anywhere "cookie free"; (2) to send e-mail through a middle man "remailer"; (3) an anonymous website to allow anyone (individual or organization) to have a homepage without identifying themselves; (4) to support the use of synonyms, etc. {See further, Time, February 8, 1999, p. 62, or visit Internet anonymous based services such as <www.anonymize.com>}, www.anonymize.net, www.anonymize.ws, etc.

99 See Clause 6.1.5 and Clause 6.3 "*Rules Governing the Process Component*".

9.6 Rules governing pseudonymization of personal information in a business transaction[100]

At times it is desired that an individual can establish a long-term relationship (including a reputation, trust relationship, etc.), with some other Person, without the individual's actual identity being disclosed. For convenience, it may be useful for the individual, or the other party concerned, to establish a unique (new) persona, identifier, token, etc., known as "pseudonym" with the other Person. Pseudonymization is recognized as an important method for privacy protection of personal information. Pseudonymization techniques, mechanisms and services may be used within an organization or public administration, within a jurisdictional domain as a whole or across jurisdictional domains for transborder data flows.

Application areas for pseudonymization include, but are not limited to:

- secondary use of personal information, (e.g., research);
- use of pseudonym in publishing; and,
- use on the internet and other computer networks.

In the context of this part of ISO/IEC 15944, a "pseudonym" is defined as follows:

pseudonym

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

NOTE Adapted from ISO/TS 25237.

And in the same context "pseudonymization" is defined as:

pseudonymization

particular type of anonymization that removes the associate with an **individual** and adds an associate between a particular set of **characteristics** relating to the **individual** and one more **pseudonym**

NOTE Adapted from ISO/TR 25237

[100] This Clause 9.6 and its rules make extensive use in summary form of ISO/TS 25237:2008(E) titled *"Health Informatics — Pseudonymization"*

THIS PAGE INTENTIONALLY LEFT BLANK

10 Process component

10.1 Introduction

The text and rules presented here are consistent with Clause 6.5 *"Rules governing the process component"* of in ISO/IEC 15944-1. In Clause 6.3 in ISO/IEC 15944-1, and in its associated Annex F *"(informative) Business transaction model: process component",* the requirements for privacy protection as support for external constraints, when modelling business transactions were already included.

Thus the following rules (39-42 from Clause 6.3.1 ISO/IEC 15944-1 and re-numbered), are reproduced here.

Rule 072:

Conceptually, a business transaction can be considered to be constructed from a set of fundamental activities: planning, identification, negotiation, actualization and post-actualization.

Rule 073:

These five fundamental activities may take place in any order.

Rule 074:

A Person may terminate a business transaction by any agreed method of conclusion.

Rule 075:

The activities may be completed in a single continuous interactive dialogue or through multiple sets of interactions among buyer and seller.

10.2 Planning

In the planning phase, both the seller and buyer are engaged in a process to decide what actions are taken for seller to offer to sell a product, or the buyer to request a product. As such, there is no direct binding between a particular buyer and an identified seller.

Privacy protection requirements are not applicable in that, where a prospective buyer, as an individual, issues a request for purchase (RFP), any personal information associated with such a request is considered to be of a "publicly available personal information (PAPI)" nature.

However, as part of the planning phase, a seller as an organization should make publicly available its privacy policy for the sale of products for which the buyer can be an individual.

10.3 Identification

The identification phase refers to all those actions or events whereby data is interchanged among potential buyers and sellers in order to establish a one-to-one linkage, i.e., binding, between a possible seller(s) and a potential buyer(s). The identification phase also includes the exchange of information bundles (IBs) required to progress from the planning phase to the negotiation phase as is mutually acceptable.

Rule 076:

During the identification phase, the seller shall ascertain whether or not the buyer is an individual, and if so, inform the individual of the privacy policy of the seller.

10.4 Negotiation

The negotiation phase covers all those actions and events involving the exchange of IBs following the identification, i.e., a potential buyer and seller having (1) identified the nature of the goal of the business transaction; and, (2) identified each other at the level of unambiguity, necessary for this mutual agreement to be formalised.

Rule 077:

Where the buyer is an individual, the end of the negotiation phase shall include the explicit consent of the individual for provision of its personal information, as identified and specified, as well as the specification of the information life cycle management (ILCM) and EDI aspects of such personal information, as stated in Clause 5.3 "Privacy Principles".

10.5 Actualization

The actualization phase includes as activities or events and associated exchanges of IBs necessary for the execution and fulfillment of the results of the negotiation for the actual business transaction.

Rule 078:

Where the buyer is an individual, the seller shall ensure and have in place supporting procedures and mechanisms to support both the generic privacy protection requirements as: (1) found in this part of ISO/IEC 15944 and stated in its rules and guidelines; and, (2) as well as those resulting from the negotiation phase, i.e., as negotiated between the seller and the individual as buyer.

10.6 Post-Actualization

The post-actualization phase includes all the activities, events and associated exchanges of IBs that occur between the buyer and seller after the agreed upon good, service and/or right, or is deemed to have been delivered.

Common post-actualization activities are those of the nature of warranties, (extended) service contracts, etc. Where the individual is the buyer it is not uncommon that the individual "gifts", (e.g., as a present) the product that it bought to another individual. In this case it is the individual who is the recipient of the "gift" who completes the warranty card, and becomes the owner of the extended service contract, etc. Actions of this nature impact the creation, management and use of personal information of both the individual as the buyer and the individual who is the recipient of the purchased product as a gift. The following set of rules summarizes the privacy protection requirements which apply.

Rule 079:

A buyer (and its agent(s)) or third party (or any other party to the business transaction), shall not retain any personal information on the individual as the buyer for any time longer than is consented to by the individual for post-actualization purposes unless external constraints of the applicable jurisdictional domain requires retention of such personal information for a longer period.

Rule 080:

Where the buyer gifts the product to another individual, and the terms of the purchase allow the recipient individual to assume the warranty, extended service contract, etc., the seller shall ensure that such a recipient individual is fully informed of its privacy protection rights, including the record retention requirements.

11 Data component

11.1 Introduction

The text and rules presented here are based on Clause 6.6 "Rules governing the data component" of ISO/IEC 15944-1, as well as Clause 6.6.4 "*Data component"* of ISO/IEC 15944-5. The generic perspectives of ISO/IEC 15944-1, ISO/IEC 15944-2, and ISO/IEC 15944-5 form the basis for this Clause 11 in the context of privacy protection requirements.

11.2 Rules governing the role of Business Transaction Identifier (BTI) in support of privacy protection requirements

This Clause creates the generic aspects of the role and requirements for the business transaction identifier (BTI), which is independent of whether internal or external constraints applying to a generic business transaction or a regulatory business transaction. {See further Clause 6.6.4.4 *Business Transaction Identifier (BTI*) and its associated rules and definitions in ISO/IEC 15944-5[101]}

Rule 081:

Each instantiated business transaction involving an individual as a buyer shall have a business transaction identifier (BTI) assigned by the seller or the regulator.

The assignment of the BTI represents the actualization of a business transaction. When an individual is the buyer privacy protection requirements apply to all personal information pertaining to that business transaction. So the seller or regulator when assigning the BTI also binds itself to the privacy protection requirements of the jurisdictional domain of that individual (as well as applicable consumer protection and individual accessibility requirements).

Guideline 081G1:

The seller (or the regulator) which assigns the BTI to an actualized business transaction involving an individual should use the BTI as the ID for all the personal information pertaining to that individual.

Rule 082:

Where an individual as a buyer in a business transaction decides to be anonymous (as permitted by the external constraints of the applicable jurisdictional domain), the business transaction identifier (BTI) serves as the sole identifier.

Rule 083:

Where the business transaction is of the nature of a regulatory business transaction (RBT) and the rules governing the RBT permit an individual to be a buyer, such rules shall explicitly state and define the associated personal information in conformance with this part of ISO/IEC 15944.

The mandatory use of unique BTI in support of a RBT is necessary to be able to support the rules stated in Clause 5 above. This is so that the SRIs pertaining to an instantiated business transaction (as SCs or IBs) which are of the nature of personal information can be tagged and linked to the applicable BTI, and thus managed accordingly from both a privacy protection and information life cycle management (ILCM requirements perspective.

[101] It is advised that users of this part of ISO/IEC 15944 familiarize themselves with this Clause 6.6.4.4 in ISO/IEC 15944-5.

11.3 Rules governing state of change management of business transactions in support of privacy protection requirements

A key characteristic of Open-edi is that "parties control and maintain the states of the recorded information" pertaining to the business transaction of which they are part. {See Clause 5.4 ISO/IEC 14662} It is important to specify whether or not the content of its Information Bundles (IBs) or its Semantic Components (SCs), once interchanged among parties to a business transaction, is allowed to be changed during any phase of the business transaction. Knowing whether or not state changes are allowed for a specific IB or SC is important for the management of the state description and automated change management of the state machines of the parties involved.

This general approach to state changes also applies here because these are mandatory requirements in support of privacy protection.

Rule 084:

The rules governing state changes of recorded information (Clause 6.6.4.3 "State Changes" in ISO/IEC 15944-5) apply to any business transaction involving an individual as a buyer.

The execution and implementation of these rules requires any organization or public administration which collects or creates personal information to determine whether or not a state change, if any, is allowed once the personal information in relation to a business transaction has been recorded. This pertains to any information bundles (IBs), semantic components (SCs), data elements, etc., forming part of the personal information associated with a business transaction. Annex F below provides a formalized approach to specifying state changes. It incorporates two coded domains taken from ISO/IEC 15944;-5 namely:

Coded Domain ID	Title
ISO/IEC 15944-5:05	Codes for specifying state changes allowed for the values of Information Bundles and Semantic Components
ISO/IEC 15944-5:06	Codes representing store change type for Information Bundles and Semantic Components

11.4 Rules governing records retention of personal information in a business transaction

ISO/IEC 15944-1 states that records retention requirements are to be specified:

- in the scoping of an Open-edi scenario, e.g., as a post-actualization requirement or a data component requirement; and,
- as an attribute of an Information Bundle, e.g., for specifying internal constraints. {See ISO/IEC 15944-1, Clause 8.5.2.8, and Rule 140; and for external constraints see Clause 8.5.2.9 and Rule 141}

A common requirement of external constraints of a public policy nature is that they mandate records retention (and deletion) requirements. These are specified in Clause 6.6.4.2 "Records Retention" of ISO/IEC 15944-5.

The general approach to records retention also applies to this part of ISO/IEC 15944 to meet the requirements of privacy protection.

Rule 085:

The rules governing the specification of records retention requirements are stated in Clause 8.5.2.8 and 8.5.2.9 in ISO/IEC 15944-1 and in Clause 6.6.4.2 of ISO/IEC 15944-5 and are mandatory to any business transaction involving an individual as a buyer, i.e., to all resulting information.

Rule 086:

Where the buyer is an individual, the seller shall inform the buyer of all records retention aspects, whether of internal or external information, with respect to the sets of recorded information (SRIs) pertaining to the personal information forming part of the business transaction, and in particular those pertaining to the post-actualization phase.

The execution and implementation of these rules are stated in Annex F, which also incorporates three coded domains taken from ISO/IEC 15944-5; namely:

Coded Domain ID	Title
ISO/IEC 15944-5:02	Codes representing specification of records retention responsibility
ISO/IEC 15944-5:03	Codes representing disposition of recorded information
ISO/IEC 15944-5:04	Codes representing retention triggers

11.5 Rules governing time/date referencing of personal information in a business transaction

Unambiguous date and time referencing (a.k.a., "temporal referencing") has always been an important aspect in the recording of the establishment of the commitment exchanges among all parties to a business transaction. Unambiguity in the specification of temporal referencing has become even more important in the world of e-business where "time" has become as important as "date". This is especially so in online exchanges, (e.g., stock markets, future markets, derivatives, currency hedging, etc.), in actions, (e.g., eBay) or similar very time sensitive transactions where the level of granularity, i.e., detail or precision, used in temporal referencing is of great importance.

In addition, while based on internal constraints only, the seller and buyer can mutually decide on a common temporal reference schema, or where external constraints apply the use of a specific temporal referencing schema may be proscribed.

Rule 087:

The rules governing temporal referencing as stated in Clause 6.6.4.5 "Date/time referencing" as stated in ISO/IEC 15944-5 apply when the individual is a buyer in a business transaction and thus privacy protection requirements apply.

Rule 088:

Unless otherwise specified and agreed to by the individual as buyer in a business transaction, the common temporal referencing schema of the jurisdictional domain of the individual applies.

Rule 089:

The temporal referencing schema governing the business transaction where the buyer is an individual shall also be used to ensure deletion of sets of personal information as required by privacy protection requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

12 Template for identifying privacy protection requirements on business transactions[102]

12.1 Introduction and basic principles

The approach taken for Clause 12 is the same as that for ISO/IEC 15944-1.

This Clause builds on the structure developed in Clauses 1 through 11. Together with the rules contained in these clauses, it provides the user with the rules for the specification of Open-edi scenarios, Open-edi scenario attributes and attributes of scenario components, e.g., roles, information bundles (IBs) and semantic components (SCs). This template is used to capture these aspects in a systematic, coded form.

Note: From an ISO perspective, Decision Codes (in Column 2) are provided only where they pertain to the implementation of this part of ISO/IEC 15944. In modelling, business transactions through scenarios and scenario components, users/implementers will decide on the Decision Codes to be entered depending on applicable internal and external constraints for the scenario and scenario components for the (common) scenario of the business transaction being modelled.

12.2 Template structure and contents

Open-edi scoping attributes from ISO/IEC 15944-1 sub clause 7.3, *"Template for specifying scope of an Open-edi scenario, and specification attributes"*, from ISO/IEC 15944-1 sub clause 8.2.3*, "Consolidated template of attributes of Open-edi scenarios, roles and Information Bundles"*, are included here to simplify implementation.

Rule 090:

It is important in scoping an Open-edi scenario to specify at the outset whether or not external constraints apply to the business transaction being modelled.

If there are no external constraints, i.e., the only internal constraints are those which the buyer and seller mutually agree to, then such an Open-edi scenario can often serve as a generic re-useable 'Lego' block in support of those Open-edi scenarios which do include external constraints.

Rule 091:

It is equally important in scoping an Open-edi scenario which allows for an individual as buyer in a business transaction to note whether this is an adaptation of an existing "generic" Open-edi scenario or a new Open-edi scenario.

It is understood that (a) most of the Open-edi scenarios will be and are modelled at the Person level; and, (b) that many of these need only minor modifications in their modelling of such scenarios to incorporate privacy protection requirements.

Scenario scoping and specification attributes ensure that all the information required for the **Business Operational View (BOV)** of an Open-edi scenario, its components and all attributes required to be specified, (and registered for re-use) are captured in a systematic and explicit manner. They are captured at the scenario scoping level as "scenario scoping attributes[103]" and at the scenario level itself as "attributes of Open-edi scenarios, roles and Information bundles"[104].

---

102 This Clause is based on and similar in structure to Clauses 7, 8 and 9 in ISO/IEC 15944-1.

103 See further ISO/IEC 15944-1 Clause 7.3 "*Template for specifying scope of an Open-edi Scenario".*

104 See further ISO/IEC 15944-1 Clause 9.2.3 "*Consolidated Template of attributes of Open-edi scenarios, roles and Information Bundles*". (Also included here are attributes of Semantic Components (SCs)).

Development of scoping of scenarios, the development of scenario components, etc., requires the use of these templates and ensuring that for each of the attributes listed in the templates one enters a Decision Code as specific in ISO/IEC 15944-1, Clause 7.3.1 and with its rules summarized here as follows:

1) Decision Code (Col.2) must be specified, i.e., it shall not have a "blank" or "null" value

2) The two valid Decision Codes are ,

   - applies = 1 (Yes)

   - does not apply = 2 (No)

Once the Decision Codes for scenario scoping and specification attributes of ISO/IEC 15944-1 are determined, the scenario specification would then be formally expressed in an OeDT according to OeDT requirements prescribed in ISO/IEC 14662 and elaborated on in (future) ISO/IEC 15944-3 of this multipart standard. The Open-edi Scenario Scoping ID Tags and Open-edi scenario component **ID codes** of ISO/IEC 15944-1 shall be explicitly associated with the OeDT artefacts. This having been done also permits for the registration of scenarios and scenario components as identifiable and re-useable business objects. {See further ISO/IEC 15944-2 titled "*Part 2: registration of scenarios and their components as business objects*"}

The two templates which follow are those taken from ISO/IEC 15944-1:2010 as found in its 7.3.2 and its Clause 9.2.3. **The attributes which have been added are those resulting from the identification of requirements of jurisdictional domains as sources of external constraints, i.e., Clauses 5, 6 and 7 of this document and the rules it contains**. These are in addition, to rules already stated in ISO/IEC 15944-1:2010 which pertain to external constraints. {See further, in this document, Annex B.3 "*Consolidated List of Rules in ISO/IEC 15944-1 pertaining to External Constraints"*}

Attributes which have been added to these two templates resulting from the requirements of this part of ISO/IEC 15944-5 have been indicated with an asterisk (*) and inserted in the existing templates of ISO/IEC 15944-1.

12.3 Template for specifying the scope of an Open-edi scenario

Table 1 — Template for specifying the scope of an Open-edi scenario

Table 1: Template for specifying the scope of an Open-edi scenario					
IT-Interface		**Linguistic Human-Interface Equivalents**			**Spare**
Scope Tag ID Code	**Decision Code**	**Name (English)**	**Name (French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
1000		**BUSINESS GOAL OF BUSINESS TRANSACTION-** **NO EXTERNAL CONSTRAINTS**			
1010		**Business goal of business transaction includes external constraints**			

Table 1: Template for specifying the scope of an Open-edi scenario					
IT-Interface		**Linguistic Human-Interface Equivalents**			**Spare**
Scope Tag ID Code	**Decision Code**	**Name (English)**	**Name (French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
1040	2	Persons (no external constraint)			
1041+	1	Persons: Individual <-> Individual			
1042+	1	Persons: Individual <-> Organization[105]			
1043+	1	Persons: Individual <-> Public Administration			
1044	2	Persons: Organization <-> Organizations[106]			
1045	2	Persons: Organization <-> Public Administration			
1046	2	Persons: Public Administration <-> Public Administration			
1047	1	Business Transaction Identifier (BTI)			
1048	1	Regulatory Transaction Identifier (RTI)			
1060		Bilateral Transaction Model			
1061		Mediated Business Transaction Model			
1065		Defined Market Model			
1066		Undefined Market Model			
1070		Immediate Settlement Model			
1071		Separate Settlement Model			
1080		EXTERNAL CONSTRAINTS AND PUBLIC POLICY			
1081*+	1	External constraints of a (general) public policy nature apply			

105 Often referred to as “B2C”, i.e., as in “business-to-consumer”. Here it is understood that a “consumer” is an “individual” and not an “organization”.

106 Often referred to as “B2B” i.e., as in “business-to-business”.

Table 1: Template for specifying the scope of an Open-edi scenario					
IT-Interface		**Linguistic Human-Interface Equivalents**			**Spare**
Scope Tag ID Code	**Decision Code**	**Name (English)**	**Name (French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
1082*+		External constraints of a consumer protection nature are supported			
1083*+	1	External constraints of a privacy protection nature are supported			
1084*+		External constraints of an "individual accessibility" nature are supported			
1085*+		External constraints of a human rights nature are supported			
1100		AGENTS AND THIRD PARTIES			
1110		**Business Transaction allows for Agents**[107]			
1111		Buyer Agent			
1112+		Seller Agent			
1130		**Business Transaction allows for Third Parties**[108]			
1131	1	By mutual agreement of buyer and seller (as **internal constraints** only)			
1132+	1	Mandated external constraint(s)			
1150*		**External Constraints and agents**			
1151*+	1	External constraints require a buyer to use an agent			
1152*	1	External constraints require a seller to use an agent			

[107] It is assumed that business rules and constraints relevant to the ability of the two primary parties (the seller and buyer), to be able to delegate all or part(s) of their role and associated commitment(s) to agent(s) will be specified as part of "Role Attributes", see further Clause 8.4.2.5 in ISO/IEC 15844-1.

[108] It is assumed that business rules and constraints pertaining to the ability of the two primary parties (the seller and buyer), to agree to delegate all or part(s) of their role(s) and associated commitment(s) to a "third party(ies)" will be specified as part of "Role Attributes", see further Clause 8.4.2.5 in ISO/IEC 15944-1.

Table 1: Template for specifying the scope of an Open-edi scenario					
IT-Interface		**Linguistic Human-Interface Equivalents**			**Spare**
Scope Tag ID Code	**Decision Code**	**Name (English)**	**Name (French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
1160		EXTERNAL CONSTRAINTS AND THIRD PARTY			
1161*	1	External constraints require participation of a qualified third party			
1170		EXTERNAL CONSTRAINTS AND REGULATOR			
1171*	1	External constraints require direct participation of a regulator			
1172*	1	External constraints allow for a third party to act on behalf of a regulator, i.e. interacting with both buyer and seller			
1173*	1	External constraints allow for an agent to act on behalf of the regulator			
1180		DATE/TIME REFERENCING[109]			
1181*+	1	Applicable Calendar Specified			
1182*	1	Applicable Clock (and level of granularity) specified			
1183	1	Specification of date ((time of sale)			
1200		PROCESS COMPONENT: All five sets of distinct activities covered.			
1210		PLANNING			
1215	1	Public information on goods/services provided by a seller			

109 For applicable rules, see above Clause 6.6.4.5.

Table 1: Template for specifying the scope of an Open-edi scenario					
IT-Interface		**Linguistic Human-Interface Equivalents**			**Spare**
Scope Tag ID Code	**Decision Code**	**Name (English)**	**Name (French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
1216	1	Privacy policy of seller publicly available			
1220		Public information on goods/services needed by buyer			
1225	1	Predefined/referenceable Catalogue			
1230	1	Buyer initiated goods/service request			
1235+	1	Seller initiated goods/service offer			
1240		Predefined Market Model			
1250		IDENTIFICATION			
1255	1	Identification for information exchange purposes only (e.g. an address)[110]			
1260		Identification of Person able to make commitment[111]			
1265+	1	Identification of Person as “individual”			
1270+		Identification of Person as “consumer”			
1300		NEGOTIATION			
1305		Monetary Payment Involved			
1310		Immediate Settlement Model			
1315		Separate Settlement Model payment			

110 A typical example here is an e-mail address or a P.O. Box address.

111 This is usually required for the Negotiation step and certainly for Actualization.

Table 1: Template for specifying the scope of an Open-edi scenario					
IT-Interface		**Linguistic Human-Interface Equivalents**			**Spare**
Scope Tag ID Code	**Decision Code**	**Name (English)**	**Name (French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
1350		ACTUALIZATION			
1355		Immediate Settlement			
1360		Separate Settlement			
1400		POST-ACTUALIZATION			
1405+		Includes warranties			
1410+		Includes records retention			
1415+		Includes staying in contact with buyer (e.g., defect and recall notification)			
1500		DATA COMPONENT			
1505	1	Predefined and Structured, i.e., code sets			
1520	1	Data integrity of any IB			
1525+	1	Retention /Latency Of Any IBs			
1530*+	1	SPECIFICATION OF RECORDS RETENTION RESPONSIBILIY[112] (in support of internal and/or external constraints)			
1540*+	1	SPECIFICATION OF DISPOSITION OF RECORDED INFORMATION[113]			
1541*+	1	Specification of disposition of recorded information from an internal constraints perspective			

[112] If applicable, i.e. as applying to the set of recorded information pertaining to the business transaction as a whole, utilize Coded Domain ISO/IEC 15944-5:02 *Codes representing Specification of Records Retention Responsibility*. See also Clause 6.6.4.2 above.

[113] If applicable, i.e. as applying to the set of recorded information pertaining to the business transaction as a whole, utilize Codes Domain "ISO/IEC 15944-5:03 "*Codes Representing Disposition of Recorded Information".* See also Clause 6.6.4.2 above.

Table 1: Template for specifying the scope of an Open-edi scenario					
IT-Interface		**Linguistic Human-Interface Equivalents**			**Spare**
Scope Tag ID Code	**Decision Code**	**Name (English)**	**Name (French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
1542*+	1	Specification of disposition of recorded information from an external constraints (jurisdictional domain requirements) perspective			
1550*+	1	SPECIFICATION OF RETENTION TRIGGERS[114]			
1560*+	1	SPECIFICATION OF STATE CHANGES[115]			
1570+	1	SPECIFICATION OF STORE CHANGE TYPE[116]			
1600		Business requirements on FSV – No external constraints[117]			
1610+	1	Service: Information Bundle Integrity			
1620+	1	Service: Confidentiality of IB contents			
1625+	1	Service: Non-repudiation of receipt			
1630+	1	Service: Proof of Time IB creation[118]			
1635	1	Service: Notarization of IBs			
1640	1	Service: Quality of Service (QoS)			
1700	1	EXTERNAL CONSTRAINTS			

114 If applicable, i.e. as applying to the set of recorded information pertaining to the business transaction as a whole, utilize Coded Domain "ISO/IEC 15944-5:04 *Codes Representing Retention Triggers* ". See also Clause 6.6.4.2 above.

115 If applicable, i.e. as applying to the set of recorded information pertaining to the business transaction as a whole, utilize Coded Domain "ISO/IEC 15944-5:06 *Codes store change type for Information Bundles and semantic components*". See also Clause 6.6.4.3 above.

116 If applicable, i.e. as applying to the set of recorded information pertaining to the business transaction as a whole, use Coded Domain "ISO/IEC 15944-1:05 *Codes for specifying state changes allowed for IBs and SCs".* See also Clause 6.6.4.3 above.

117 See further Clause 6.5.2 in ISO/IEC 15944-1.

118 Often referred to as time-stamping services. See further Clause 6.6.4.5, "*Date/Time Referencing".*

12.4 Consolidated template of attributes of Open-edi scenarios, roles and information bundles[119]

Table 2 — Consolidated template of attributes of Open-edi scenarios, roles and information bundles

Table 2: Consolidated template of attributes of Open-edi scenarios, roles and information bundles					
IT-Interface		**Human-Interface Equivalents**			**Spare**
Open-edi Scenario Component ID Code	**Deci-sion Code**	**Name (ISO English)**	**Name (ISO French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
2000	1	OPEN-EDI SCENARIO ATTRIBUTES			
2010	1	OeS Identifier			
2020+	1	OeS Name(s)			
2030+	1	OeS Purpose			
2040+	1	OeS Set of Roles OeS Business Requirements, Rules and Constraints			
2050+	1	OeS Set of Information Bundles OeS Scenario Inheritance Identifier(s) and Cross-References			
2060	1	OeS Set of Requirements on Open-edi Parties			
2070	1	OeS Set of external constraints on Business Requirements, i.e., Laws and Regulations			
2080	1	OeS Inheritance Identifier(s) and Cross References			
2090	1	OeS Security Service Requirements			
2100	1	OeS Communication - Quality of Service Requirements			
2120	1	OeS Role Requirements and Constraints			
2130	1	OeS Dependency among Roles in a Scenario			
2140	1	OeS Dependency among Information Bundles in a Scenario			
2150	1	OeS Dependency among Semantic Components of different Information Bundles			

119 This template is based that found in Clause 9.2.3 in ISO/IEC 15944-1.

Table 2: Consolidated template of attributes of Open-edi scenarios, roles and information bundles					
IT-Interface		**Human-Interface Equivalents**			**Spare**
Open-edi Scenario Component ID Code	**Deci-sion Code**	**Name (ISO English)**	**Name (ISO French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
2500	1	OeS Demands on Open-edi Parties			
	1				
2600	1	OeS Demands on Open-edi Infrastructure			
3000	1	ROLE ATTRIBUTES			
3005	1	Role Identifier			
3010	1	Role Name(s)			
3015	1	Role Purpose			
3020	1	Role Business Goal(s)			
3025	1	Role Business Rules and Constraints			
3030		Role Inheritance Identifiers and Cross-References			
3035+	1	Role external constraints on Business Requirements, i.e., Laws and Regulations			
3040	1	Role Security Service Requirements			
3045	1	Role Communications and Quality of Service Requirements			
3050	1	ROLE Demands on Open-edi Parties			
3060	1	Interoperability Demands among Roles			
3065+	1	Role States			
3070+	1	Role Transitions			
3075+	1	Role Events			
3080+	1	Role Actions			
3085	1	Role Internal Function			

Table 2: Consolidated template of attributes of Open-edi scenarios, roles and information bundles					
IT-Interface		**Human-Interface Equivalents**			**Spare**
Open-edi Scenario Component ID Code	**Deci-sion Code**	**Name (ISO English)**	**Name (ISO French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
3090+	1	Role Demands on Open-edi Support Infrastructure			
	1				
4000	1	INFORMATION BUNDLE ATTRIBUTES			
4010+	1	IB Identifier			
4020+	1	IB Name(s)			
4030+	1	IB Purpose			
4040+	1	Business Rules Controlling Content of IBs			
4050+	1	IB external constraints on Business Requirements, Governing Content of an IB, i.e., Laws and Regulations			
4060+	1	IB contents			
4070*+	1	IB recorded information retention – business rules and constraints[120]			
4080*+	1	IB recorded information retention – external constraints on business requirements, i.e., laws and regulations[121]			
4081*+	1	IB specification of disposition[122]			
4082*+	1	IB specification of retention triggers[123]			

[120] If applicable, i.e. as applying to an IB in a scenario or related to a role being modelled, utilize Coded Domain "ISO/IEC 15944-5:02 *Codes Representing Specification of Records Retention Responsibility*". {See also Clause 6.6.4.2 above}

[121] Idem.

[122] If applicable, i.e. as applying to an IB in a scenario or related to a role being modeled, utilize Coded Domain "ISO/IEC 15944-5:03 *Codes Representing Disposition of Recorded Information*". {See also Clause 6.6.4.2 above}

[123] If applicable, i.e. as applying to an IB in a scenario or related to a role being modeled, utilize Coded Domain "ISO/IEC 15944-5:04 "*Codes Representing Retention Triggers*". {See also Clause 6.6.4.2 above}

Table 2: Consolidated template of attributes of Open-edi scenarios, roles and information bundles					
IT-Interface		**Human-Interface Equivalents**			**Spare**
Open-edi Scenario Component ID Code	**Deci-sion Code**	**Name (ISO English)**	**Name (ISO French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
4083*+	1	IB specification of state changes[124]			
4084*+	1	IB specification of store change types[125]			
4085+	1	IB time validity characteristics[126]			
4090+	1	Relationship of Semantic Components within an IB			
4100+	1	IB security service requirements			
4200+	1	IB information for interoperability			
4300	1	IB demands on Open-edi Support Infrastructure			
5000	1	SEMANTIC COMPONENT ATTRIBUTES			
5010+	1	SC Identifier			
5020+	1	SC Name(s)			
5030+	1	SC Definition			
5040+	1	SC Security service requirements			
5081*+	1	IB specification of disposition[127]			

124 If applicable, i.e. as applying to an IB in a scenario or related to a role being modeled, utilize Coded Domain "ISO/IEC 15944-5:05 "*Codes representing State Changes Allowed form the Values of Information Bundles and Semantic Components"*. {See also Clause 6.6.4.3 above}

125 If applicable, i.e. as applying to an IB in a scenario or related to a role being modeled, utilize Coded Domain "ISO/IEC 15944-5:06 *Codes Representing Store Change Type*". {See also Clause 6.6.4.2 above}

126 If applicable, apply rules of Clause 6.6.4.5, "*Date/Time Referencing*".

127 If applicable, i.e. as applying to a SC of an IB being modeled, utilize Coded Domain "ISO/IEC 15944-5:03 *Codes Representing Disposition of Recorded Information*". {See also Clause 6.6.4.2 above}

Table 2: Consolidated template of attributes of Open-edi scenarios, roles and information bundles					
IT-Interface		**Human-Interface Equivalents**			**Spare**
Open-edi Scenario Component ID Code	**Deci-sion Code**	**Name (ISO English)**	**Name (ISO French)**	**Name (Other)**	
(1)	(2)	(3)	(4)	(5)	(6)
5082*+	1	IB specification of retention triggers[128]			
5083*+	1	IB specification of state changes[129]			
5084*+	1	IB specification of store change types[130]			

[128] If applicable, i.e. as applying to a SC of an IB being modeled, use Coded Domain "ISO/IEC 15944-5:04 *Codes Representing Retention Triggers"*. {See also Clause 6.6.4.2 above}

[129] If applicable, i.e. as applying to a SC of an IB being modeled, utilize Coded Domain "ISO/IEC 15944-5:05 "*Codes representing State Changes Allowed from the Values of Information Bundles and Semantic Components*". {See also Clause 6.6.4.3 above}

[130] If applicable, i.e. as applying to a SC of an IB being modeled, utilize Coded Domain "ISO/IEC 15944-5:06 *Codes representing Store Change T*ype". {See also Clause 6.6.4.3 above}

THIS PAGE INTENTIONALLY LEFT BLANK

13 Conformance statement

13.1 Introduction

The two types of conformance statements presented in Clause 13 below are at the most primitive level. More detailed conformance statement(s) with associated rules and procedures, including those pertaining to verification are expected to be developed either as Addendum(s) to this 1st edition or as part of the development of a 2nd edition for this part of ISO/IEC 15944.

Clause 13 is modelled on that found in Clause 6 in the 3rd edition for ISO/IEC 14662.

There are two different categories of conformance statements for this part of ISO/IEC 15944; namely:

(a) Category A – ISO/IEC 14662 Open-edi Reference Model; and, ISO/IEC 15944 compliance; and,

(b) Category B – ISO/IEC 15944-8 conformance only.

The reason for these two categories is to permit users and implementers of ISO/IEC 15944-8 to be conformant to its requirements without using the Open-edi modelling constructs as well as registration of Open-edi scenarios and scenario components as re-usable business objects.

13.2 Conformance to the ISO/IEC 14662 Open-edi Reference Model and the multipart ISO/IEC 15944 eBusiness standard

Any user/implementer conformance statement of this nature shall state:

(a) that it is conformant to the BOV class of standards of ISO/IEC 14662;

(b) the list of the basic concepts of the ISO/IEC Open-edi Reference Model and ISO/IEC eBusiness (BOV standards) as stated in the ISO/IEC 15944-7 eBusiness Vocabulary; and,

(c) whether or not it has any Open-edi compliant scenarios and scenario components registered using ISO/IEC 15944-2.

13.3 Conformance to ISO/IEC 15944-8

Any user/implementer conformance statement of this nature shall state:

> "The existence and interchange of personal information by XYZ [insert name of organization or public administration] with any other party is conformant and consistent with the eleven Privacy Protection principles stated in ISO/IEC 15944-8 definitions its concepts, rules and related requirement".

Annex A
(normative)

Consolidated list of terms and definitions with cultural adaptability: ISO English and ISO French language equivalency

A.1 Introduction

This part of ISO/IEC 15944 maximizes the use of existing standards where and whenever possible including relevant and applicable existing terms and definitions. These are presented in Clause 3 above. This Annex A contains only those new concepts and their definitions introduced in this part of ISO/IEC 15944, i.e. as ISO English and ISO French language HIEs.

The ISO/IEC 15944-7 "*eBusiness Vocabulary*" (a "freely available ISO standard") in its normative Annex E already contains the consolidated ISO English and ISO French language equivalents for all the other concepts and definitions found in Clause 3 of this document ISO/IEC 15944-7 also contains ISO Russian and ISO Chinese langue HIEs for all the concepts and their definitions. It is anticipated that the contents of Annex A.5 below will serve as the basis for an Addendum to ISO/IEC 15944-7 and that this Addendum will also contain the ISO Russian and ISO Chinese HIEs for the contents of Annex A.5 below.

A.2 ISO English and ISO French

This part of ISO/IEC 15944 recognizes that the use of English and French as natural languages is not uniform or harmonized globally. (Other examples include use of Arabic, German, Portuguese, Russian, Spanish, etc., as natural languages in various jurisdictional domains).

Consequently, the terms "ISO English" and "ISO French" are used here to indicate the ISO's specialized use of English and French as natural languages in the specific context of international standardization, i.e., as a "special language".

A.3 Cultural adaptability and quality control

ISO/IEC JTC1 has "cultural adaptability" as the third strategic direction which all standards development work should support. The two other existing strategic directions are "portability" and "interoperability". Not all ISO/IEC JTC1 standards are being provided in more than one language, i.e., in addition to "ISO English," in part due to resource constraints.

Terms and definitions are an essential part of a standard. This Annex serves to support the "cultural adaptability" aspects of standards as required by ISO/IEC JTC1. Its purpose is to ensure that if, for whatever reason, an ISO/IEC JTC1 standard is developed in one ISO/IEC "official" language only, at the minimum the terms and definitions are made available in more than one language.[131]

[131] Other ISO/IEC member bodies are encouraged to provide bilingual/multilingual equivalencies of terms/definitions for the language(s) in use in their countries.

A key benefit of translating terms and definitions is that such work in providing bilingual/multilingual equivalency:

- should be considered a "quality control check" in that establishing an equivalency in another language ferrets out "hidden" ambiguities in the source language. Often it is only in the translation that ambiguities in the meaning, i.e., semantics, of the term/definition are discovered. Ensuring bilingual/multilingual equivalency of terms/definition should thus be considered akin to a minimum "ISO 9000-like" quality control check; and,

- is considered a key element in the widespread adoption and use of standards world-wide, especially by users of this part of ISO/IEC 15944 who include those in various industry sectors, within a legal perspective, policy makers and consumer representatives, other standards developers, IT hardware and service providers, etc.

A.4 Organization of Annex A – Consolidated list in matrix form

The terms/definitions are organized in matrix form in alphabetical order (English language). The columns in the matrix are as follows:

Col. No.	Use
	IT-Interface – Identification
1	Clause 3 ID (ID definition as per ISO/IEC 15944-8 Clause 3)
2	Source. International standard referenced or that of ISO/IEC 15944-8 itself.
	Human Interface Equivalent (HIE) Components
3	ISO English Language – Term
4	Gender of ISO English Language Term+
5	ISO English Language – Definition
6	ISO French Language - Term *
7	Gender of the ISO French language Term+
8	ISO French Language - Definition

The primary reason for organizing the columns in this order is to facilitate the addition of equivalent terms/definitions in other languages as added sets of paired columns, (e.g., Spanish, Japanese, German, Russian, Chinese, etc)[132].

+ The codes representing gender of terms in natural languages are those found in Clause 6.2.6 in ISO/IEC 15944-5 "*Gender, and official, de facto, or LRL languages",* and especially its Table 1 – *"ISO/IEC 15944-5:01 "Codes representing gender and official languages"*;

    - ISO English, in Column 4, the gender code = "99" since the English language does not have gender in its grammar; and,

    - ISO French, in Column 7, the gender codes are 01 = masculine, 02 = feminine, and 03 = neuter

* The use of [French language equivalent required] in Colum (8) means that for these terms and definitions, ISO/IEC 20016-1 itself will be providing the ISO French language equivalent before the FDIS stage.

132 See further ISO/IEC 15944-7 "*eBusiness Vocabulary*" of ISO/IEC 15944 for an implementation of this approach.

A.5 Consolidated list of ISO/IEC 15944-8 terms and definitions

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.001	ISO/IEC 15944-2: 2006 (3.1)	address	99	set of **data elements** that specifies a **location** to which a **recorded information** item(s), a **business object**(s), a material **object**(s) and/or a person(s) can be sent or from which it can be received NOTE 1 An address can be specified as either a physical address and/or electronic address. NOTE 2 In the identification, referencing and retrieving of registered business objects, it is necessary to state whether the pertinent recorded information is available in both physical and virtual forms. NOTE 3 In the context of Open-edi, a "recorded information item" is modelled and registered as an Open-edi scenario (OeS), Information Bundle (IB) or Semantic Component (SC).	adresse	02	ensemble **d'éléments de données** servant à préciser l'**emplacement** où on peut envoyer ou recevoir un élément d'**information enregistrée,** un **objet** d'**affaires**, un **objet** matériel et/ou une (ou des) personne(s) NOTE 1 Une adresse peut être spécifiée comme étant physique et/ou électronique. NOTE 2 Dans l'identification, le référencement et l'extraction des objets d'affaires enregistrés, il est nécessaire d'énoncer si l'information enregistrée pertinente est disponible à la fois sous formes physiques et virtuelles. NOTE 3 Dans le contexte de l'EDI-ouvert, un « article d'information enregistrée » est modélisé et enregistré comme scénario d'EDI-ouvert (OeS), Faisceau d'information (IB) ou Composante sémantique (SC).
3.002	ISO/IEC 15944-1: 2011 (3.1)	agent	99	**Person** acting for another **Person** in a clearly specified capacity in the context of a **business transaction** NOTE Excluded here 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)".	mandataire	01	**Personne** agissant au **nom** d'une autre **Personne** à titre précis dans le contexte d'une **transaction d'affaires** NOTE Sont exclus les mandataires tels que les « automates » (ou les robots, bobots, etc.). Dans la norme ISO/CEI 14662, les « automates » sont pris en compte et prévus, mais à titre de Vue de services fonctionnels (FSV), où ils sont définis comme « domaine de traitement de l'information (IPD)».

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.003	ISO/IEC 15944-8 (3.003)	anonymization	99	**process** whereby the association between a **set of recorded information (SRI)** and an identifiable **individual** is removed where such an association may have existed NOTE Adapted from ISO 25237.	anonymisation	02	**processus** selon lequel est supprimée la corrélation entre **un ensemble d'informations enregistrées (EIE)** et un **individu** identifiable, alors même qu'une telle corrélation a pu préalablement exister NOTE Adapté de l'ISO 25237.
3.004	ISO/IEC 11179-3: 2003 (3.1.3)	attribute	99	**characteristic** of an **object** or **entity**	attribut	02	**caractéristique** d'un **objet** ou d'une **entité**
3.005	ISO/IEC 10181-2: 1996 (3.3)	authentication	99	provision of assurance of the claimed identity of an **entity**	authentifi-cation	01	attestation de l'identité revendiquée par une **entité**
3.006	ISO/IEC TR 13335-1: 1996 (3.3)	authenticity	99	**property** that ensures that the identity of a subject or resource is the one claimed NOTE Authenticity applies to entities such as users, processes, systems and information.	authenticité	02	**propriété** assurant que l'identité d'un sujet ou d'une ressource est celle qui est prétendue NOTE L'authenticité s'applique à des entités telles que des utilisateurs, des processus, des systèmes et des informations.
3.007	ISO/IEC 14662: 2010 (3.2)	business	99	series of **processes**, each having a clearly understood purpose, involving more than one **Person**, realized through the exchange of **recorded information** and directed towards some mutually agreed upon goal, extending over a period of time	affaires	02	série de **processus**, ayant chacun une finalité clairement définie, impliquant plus d'une **Personne**, réalisés par échange d'**information enregistrée** et tendant à l'accomplissement d'un objectif accepté par accord mutuel pour une certaine période de temps

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.008	ISO/IEC 15944-4: 2007 (3.5)	business event	99	occurrence in time that **partners** to a **business transaction** wish to monitor or control NOTE 1 Business events are the workflow tasks that business partners need to accomplish to complete a business transaction among themselves. As business events occur, they cause a business transaction to move through its various phases of planning, identification, negotiation, actualization, and post-actualization. NOTE 2 Occurrences in time can either be (1) internal as mutually agreed to among the parties to a business transaction; and/or, (2) reference some common publicly available and recognized date/time referencing schema, (e.g., one based on using the ISO 8601 and/or ISO 19135 standards).	évènement d'affaires	01	circonstance temporelle que des **partenaires** dans une **transaction d'affaires** souhaitent surveiller ou contrôler NOTE 1 Les évènements d'affaires sont les tâches de flux des travaux que les partenaires d'affaires doivent accomplir pour conclure une transaction d'affaires entre eux. Lorsque des évènements d'affaires se produisent, ils obligent une transaction d'affaires à passer par les différentes étapes de planification, d'identification, de négociation, d'actualisation et de post-actualisation. NOTE 2 Les circonstances temporelles peuvent être (1) internes, comme accord mutuel entre les parties d'une transaction d'affaires; et/ou, (2) une référence à un schéma de référencement horodateur communément reconnu et publiquement disponible, (par ex., une basée sur l'utilisation des normes ISO 8601 et/ou ISO 19135).
3.009	ISO/IEC 15944-2: 2006 (3.6)	business object	99	**unambiguously** identified, specified, referenceable, registered and re-useable **Open-edi scenario** or **scenario component** of a **business transaction** NOTE As an "object", a "business object" exists only in the context of a business transaction.	objet d'affaires	01	**scénario d'EDI ouvert** (ou **composante de scénario**) d'une **transaction d'affaires** qui est identifié, spécifié, référençable, enregistré et réutilisable de manière **non-ambigüe** NOTE En tant qu' « objet », un « objet d'affaires » n'existe que dans le contexte d'une transaction d'affaires.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.010	ISO/IEC 14662: 2010 (3.3)	Business Operational View (BOV)	99	perspective of **business transactions** limited to those aspects regarding the making of **business** decisions and **commitments** among **Persons**, which are needed for the description of a **business transaction**	Vue opérationnelle des affaires (BOV)	01	vue perspective sur les **transactions d'affaires**, restreinte à ceux des aspects relatifs à la prise par les **Personnes** de décisions et d'**engagements** concernant leurs **affaires** qui sont nécessaires pour décrire une **transaction d'affaires**
3.011	ISO/IEC 14662: 2010 (3.4)	business transaction	99	predefined set of activities and/or **processes** of **Persons** which is initiated by a **Person** to accomplish an explicitly shared **business** goal and terminated upon recognition of one of the agreed conclusions by all the involved **Persons** although some of the recognition may be implicit	transaction d'affaires	02	ensemble prédéterminé d'activités et/ou de **processus** menées par des **Personnes** et/ou de procédures qu'elles suivent, déclenché par une **Personne** qui vise à atteindre dans les **affaires** un but expressément partagé, terminé lorsqu'est observée une des conclusions convenues par toutes les **Personnes** prenantes, bien que cette observation puisse être partiellement implicite
3.012	ISO/IEC 15944-5: 2008 (3.12)	business transaction identifier (BTI)	99	**identifier** assigned by a **seller** or a **regulator** to an instantiated **business transaction** among the **Persons** involved NOTE 1 The identifier assigned by the seller or regulator shall have the properties and behaviours of an "identifier (in a business transaction)". NOTE 2 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.	identificateur de transaction d'affaires (BTI)	01	**identificateur** attribué par un **vendeur** ou une autorité de réglementation à une **transaction** d'**affaires** instanciée entre les **Personnes** concernées NOTE 1 L'identificateur attribué par le vendeur ou l'autorité de réglementation doit avoir les propriétés et le comportement d'un « identificateur (dans une transaction d'affaires) ». NOTE 2 En tant qu'identificateur (dans une transaction d'affaires), un ITA sert d'identificateur commun unique pour toutes les Personnes concernées quant à l'identification, le référencement, l'extraction d'information enregistrée, etc. , relatifs aux engagements pris et à l'actualisation (et post actualisation) résultante de la transaction d'affaires conclue.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 3 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 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).			NOTE 3 Un identificateur de transaction d'affaires peut être attribué à n'importe quel moment durant les phases de planification, d'identification ou de négociation, mais doit être attribué au moins avant le début ou durant la phase d'actualisation. NOTE 4 Selon les besoins et le lieu du (des) domaine(s) juridictionnel(s) applicable(s), l'information enregistrée rattachée à l'identificateur de transaction d'affaires (ITA) peut obliger le vendeur d'inclure tous les autres identificateurs (par ex. une taxe sur le produit ou service de valeur ajoutée, etc.) attribués par le(s) domaine(s) juridictionnel(s) applicable(s).
3.013	ISO/IEC 15944-1: 2011 (3.8)	buyer	99	**Person** 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	acheteur	01	**Personne** désirant acquérir un bien, service et/ou droit en fournissant une valeur équivalente acceptable, généralement de l'argent, à la **Personne** qui offre ce bien, service et/ou droit
3.014	ISO 1087-1: 2000 (3.2.4)	characteristic	99	abstraction of a **property** of an **object** or of a set of **objects** NOTE Characteristics are used for describing concepts.	caractère	01	**propriété** abstraite d'un **objet** ou d'un ensemble d'**objets** NOTE Les caractères servent à décrire les concepts.
3.015	ISO/IEC 2382-4: 1999 (04.01.02)	character set	99	finite set of different **characters** that is complete for a given purpose EXAMPLE The international reference version of the character set of ISO 646-1.	jeu de caractères	01	ensemble fini de différents **caractères** considéré comme complet à des fins déterminées EXEMPLE La version internationale de référence du jeu de caractères de l'ISO 646-1.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.016	ISO/IEC 15944-5: 2008 (3.17)	classification system	99	systematic **identification** and arrangement of **business** activities and/or **scenario components** into categories according to logically structured conventions, methods and procedural **rules** as specified in a classification schema NOTE 1 The classification code or number often serves as a semantic identifier (SI) for which one or more human interface equivalents exist. NOTE 2 The rules of a classification schema governing the operation of a classification system at times lead to the use of ID codes which have an intelligence built into them, (e.g., in the structure of the ID, the manner in which it can be parsed, etc. Here the use of block-numeric numbering schemas is an often used convention.	système de classification	01	**identification** et arrangement systématiques des activités d'**affaires** et/ou des **composantes de scénario** en catégories selon des conventions, des méthodes et des **règles** de procédure structurées logiquement, tel que spécifié dans un schéma de classification NOTE 1 Le code ou numéro de classification sert souvent d'identificateur sémantique (SI) pour lequel existent un ou plusieurs équivalents d'interface humaine. NOTE 2 Les règles d'un schéma de classification régissant l'exploitation d'un système de classification mènent parfois à l'utilisation de codes ID à intelligence intégrée (par ex. dans la structure de l'ID, la manière dont il peut être parsé, etc.) En ce cas, on utilise souvent des schémas de numérotation numérique par bloc comme convention.
3.017	ISO 639-2: 1998 (3.1)	code	99	**data** representation in different forms according to a pre-established set of **rules** NOTE In this part of ISO/IEC 15944 the "pre-established set of rules" are determined and enacted by a Source Authority and must be explicitly stated.	code	01	représentation de **données** sous différentes formes, selon un jeu de **règles** préétablies NOTE Dans cette norme, l'«ensemble de règles préétablies» est déterminé et mis en vigueur par une Autorité de source et doit être énouncé explicitement.
3.018	ISO/IEC 15944-5: 2008 (3:19)	code (in coded domain)	99	**identifier**, i.e., an ID **code**, assigned to an **entity** as member of a **coded domain** according to the pre-established set of **rules** governing that **coded domain**	code (dans un domaine codé)	01	**identificateur**, c.-à.-d. **code ID**, attribué à une **entité** en tant que membre d'un **domaine codé** conformément au ensemble de **règles** régissant ce **domaine codé**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.019	ISO/IEC 15944-2: 2006 (3.13)	coded domain	99	domain for which (1) the boundaries are defined and explicitly stated as a **rulebase** of a **coded domain Source Authority**; and, (2) each **entity** which qualifies as a member of that domain is identified through the assignment of a unique **ID code** in accordance with the applicable **Registration Schema** of that **Source Authority** NOTE 1 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 of the Source Authority. NOTE 2 Source Authorities which are jurisdictional domains are the primary source of coded domains. NOTE 3 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 Associated with a code in a coded domain can be: - one and/or more equivalent codes; - one and/or more equivalent representations especially those in the form of Human Interface Equivalent (HIE) (linguistic) expressions.	domaine codé	01	domaine pour lequel (1) les limites sont définies et explicitement énoncées comme **base de règles** de l'**Autorité de source d'un domaine codé** ; et, (2) chaque **entité** se qualifiant comme membre de ce domaine est identifiée grâce à l'attribution d'un **code ID** unique conformément au **Schéma d'enregistrement** applicable de cette **Autorité de source** NOTE 1 Les règles régissant l'attribution d'un code aux membres d'un domaine codé résident dans son Autorité de source et font partie du Schéma d'enregistrement du domaine codé de l'Autorité de source. NOTE 2 Les Autorités de source qui sont des domaines juridictionnels sont la source primaire des domaines codés. NOTE 3 Un domaine codé est un ensemble de données pour lequel le contenu des valeurs des éléments de données est prédéterminé et défini conformément à la base de règles de son Autorité de source et, à ce titre, à une sémantique prédéfinie. NOTE 4 Peuvent être associés à un code dans un domaine codé : un ou plusieurs codes équivalents a) un et/ou plusieurs codes équivalentes; et/ou, b) une ou plusieurs représentations équivalentes, surtout celles qui sont sous forme d'expressions d'Équivalents d'interface humaine (EIH) (linguistique).

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 5 In a coded domain the rules for assignment and structuring of the ID codes must be specified. NOTE 6 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 must be specified as the pivot ID code. NOTE 7 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 A coded domain may contain ID code which pertain 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 Common examples include: (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 In object methodology, entities which are members of a coded domain are referred to as instances of a class. EXAMPLE In UML modelling notation, an ID code is viewed as an instance of an object class.			NOTE 5 Dans un domaine codé, les règles d’attribution et de structuration des codes d’identité doivent être spécifiées. NOTE 6 Lorsqu’on permet à une identité à titre de membre d’un domaine codé d’avoir, c.-à-d. de se voir attribué, plus d’un code d’identité, c.-à-d. des codes d’identité équivalents (pouvant inclure des noms), l’un de ces codes doit être spécifié à titre de code d’identité pivot. NOTE 7 Un domaine codé peut à son tour se composer de plusieurs domaines codés grâce à l’application du principe d’héritage des classes d’objet. NOTE 8 Un domaine codé peut contenir un code d’identité relatif à des conditions prédéfinies autres que la qualification d’appartenance des entités du domaine codé. De plus, les règles régissant un domaine codé peuvent ou non contenir des extensions utilisateur. EXEMPLE Exemples courants : (1) l’utilisation du code d’identité « 0 » (ou « 00 », etc.) pour « Autres », (2) l’utilisation du code d’identité « 9 » (ou « 99 », etc.) pour « Sans objet »; (3) l’utilisation du code d’identité « 8 » (ou « 98 ») pour « Inconnu »; et/ou, si nécessaire, (4) la pré-réservation d’une série de codes d’identité pour l’utilisation d’extensions utilisateur ». NOTE 9 Dans la méthodologie objet, les entités membres d’un domaine codé s’appellent « instances d’une classe ». EXEMPLE Dans la notation modélisée UML, un code d’identité est considéré comme une instance de classe d’objet.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.020	ISO/IEC 15944-5: 2008 (3.21)	coded Domain Registration Schema (cdRS)	99	formal **definition** of both (1) the **data** fields contained in the **identification** and specification of an **entity** forming part of the members a **coded domain** including the allowable contents of those fields; and, (2) the **rules** for the assignment of **identifiers**	Schéma d'enregis-trement du domaine codé (cdRS)	01	**définition** formelle à la fois des (1) champs de **données** contenus dans l'**identification** et la spécification d'une **entité** faisant partie des membres d'un **domaine codé** (y compris les contenus permis de ces champs) ; et (2) **règles** d'attribution des **identificateurs**
3.021	ISO/IEC 15944-2: 2006 (3.14)	coded domain Source Authority (cdSA)	99	**Person**, usually an **organization**, as a **Source Authority** which sets the **rules** governing a **coded domain** NOTE 1 Source Authority is a role of a Person and for widely used coded domains the coded domain Source Authority is often a jurisdictional domain. NOTE 2 Specific sectors, (e.g., banking, transport, geomatics, agriculture, etc.), may have particular coded domain Source Authority(ies) whose coded domains are used in many other sectors. NOTE 3 A coded domain Source Authority usually also functions as a Registration Authority but can use an agent, i.e., another Person, to execute the registration function on its behalf.	Autorité de source du domaine codé (cdSA)	02	**Personne**, habituellement une **organisation**, qui établit les **règles** régissant un **domaine codé** en tant qu'**Autorité de source** NOTE 1 L'Autorité de source est un rôle d'une Personne et, pour les domaines codés largement utilisés, l'Autorité de source du domaine codé est souvent un domaine juridictionnel. NOTE 2 Des secteurs spécifiques (par ex. le domaine bancaire, les transports, la géomatique, l'agriculture, etc.) peuvent avoir une (des) Autorité(s) de source du domaine codé dont les domaines codés sont utilisés dans d'autres secteurs. NOTE 3 Une Autorité de source du domaine codé fonctionne aussi habituellement comme Autorité d'enregistrement, mais peut utiliser un agent, c.-à.-d. une autre Personne, pour exécuter la fonction d'enregistrement à sa place.
3.022	ISO/IEC 15944-4: 2007 (3.12)	collaboration space	99	**business** activity space where an **economic exchange** of valued resources is viewed independently and not from the perspective of any **business partner**	espace de collaboration	01	espace d'activité d'**affaires** dans lequel un **échange économique** de ressources valorisées est considéré indépendamment et non du point de vue de tout **partenaire** d'**affaires**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE In collaboration space, an individual partner's view of economic phenomena is de-emphasized. Thus, the common use business and accounting terms like purchase, sale, cash receipt, cash disbursement, raw materials, and finished goods is not allowed because they view resource flows from a participant's perspective.			NOTE Dans l'espace de collaboration, la perspective qu'un partenaire individuel a d'un phénomène économique est désaccentuée. Ainsi, les termes d'affaires et de comptabilité communément utilisés tels que achat, vente, reçu de caisse, décaissement, matières premières, produits finis, etc. ne sont pas autorisés à être utilisés car ils considèrent les flux de ressources du point de vue d'un participant.
3.023	ISO/IEC 14662: 2010 (3.5)	commitment	99	making or accepting of a right, obligation, liability or **responsibility** by a **Person** that is capable of enforcement in the **jurisdictional domain** in which the **commitment** is made	engagement	01	création ou acceptation d'un droit, d'une obligation, d'une dette ou d'une responsabilité par une **Personne** qui est apte à appliquer le **domain juridictionnel** conformément à laquelle l'**engagement** est pris
3.024	ISO/IEC 15944-2: 2006 (3.16)	composite identifier	99	**identifier** (in a **business transaction**) functioning as a single unique **identifier** consisting of one or more other **identifiers**, and/or one or more other **data elements**, whose interworkings are **rule**-based NOTE 1 Identifiers (in business transactions) are for the most part composite identifiers. NOTE 2 The rules governing the structure and working of a composite identifier should be specified. NOTE 3 Most widely used composite identifiers consist of the combinations of: (1) the ID of the overall identification/numbering schema, (e.g., ISO/IEC 6532, ISO/IEC 7812, ISO/IEC 7506, UPC/EAN, ITU-T E.164, etc.), which is often assumed;	identificateur composite	01	**identificateur** (dans une **transaction d'affaires**) fonctionnant comme **identificateur** simple et unique comprenant un ou plusieurs **identificateurs** et/ou un ou plusieurs **éléments de données**, dont les interconnexions sont basées sur des **règles** NOTE 1 Les identificateurs (dans les transactions d'affaires) sont pour la plupart des identificateurs composites. NOTE 2 Les règles régissant la structure et le fonctionnement d'un identificateur composite doivent être spécifiées. NOTE 3 Les identificateurs composites les plus communément utilisés se composent de combinaisons:

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				(2) the ID of the issuing organization (often based on a block numeric numbering schema); and, (3) the ID of the entities forming part of members of the coded domain of each issuing organization.			(1) de l'identité du schéma d'identification/numérotation global, (par ex. ISO/IEC 6532, ISO/CIE 7812, ISO/CIE 7506, UPC/EAN, ITU-T E.164, etc.), qui est souvent assumé; (2) de l'identité de l'organisation émettrice (souvent basé sur un schéma de numérotation numérique par blocs); et, (3) l'identité des entités faisant partie de membres du domaine codé de chaque organisation émettrice.
3.025	ISO/IEC 15944-2: 2006 (3.18)	computational integrity	99	expression of a **standard** in a form that ensures precise description of behaviour and semantics in a manner that allows for automated processing to occur, and the managed evolution of such **standards** in a way that enables dynamic introduction by the next generation of information systems NOTE Open-edi standards have been designed to be able to support computational integrity requirements especially from a registration and re-use of business objects perspectives.	intégrité informatique	02	expression d'un **norme** sous une forme qui assure la description précise du comportement et de la sémantique d'une façon qui permet un traitement automatique, ainsi que l'évolution gérée de ces **normes** d'une manière qui permet une introduction dynamique par la génération suivante de systèmes informatiques NOTE Les normes de l'EDI-ouvert ont été conçues pour pouvoir appuyer les exigences en matière d'intégrité computationnelle, particulièrement dans des perspectives d'enregistrement et de réutilisation des objets d'affaires.
3.026	ISO/IEC 15944-1: 2011 (3.11)	constraint	99	**rule**, explicitly stated, that prescribes, limits, governs or specifies any aspect of a **business transaction** NOTE 1 Constraints are specified as rules forming part of components of Open-edi scenarios, i.e., as scenario attributes, roles, and/or information bundles.	contrainte	01	**règle**, énoncée explicitement, qui prescrit, limite, régit ou spécifie tout aspect d'une **transaction d'affaires** NOTE 1 Les contraintes sont spécifiées comme des règles faisant partie de composantes de scénarios d'EDI-ouvert, c.-à-d. d'attributs de scénarios, de rôles, et/ou de faisceaux d'information.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 2 For constraints to be registered for implementation in Open-edi, they must have unique and unambiguous identifiers. NOTE 3 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".			NOTE 2 Les contraintes doivent avoir des identificateurs uniques et non-ambigus afin d'être enregistrées pour application dans l'EDI-ouvert. NOTE 3 Une contrainte peut faire l'objet d'un accord entre des parties (clause du contrat), et est par conséquent considérée comme « contrainte interne ». Ou une contrainte peut être imposée à des parties, (par ex. des lois, des règlements, etc.), et est par conséquent considérée comme une « contrainte externe ».
3.027	ISO/IEC 15944-1: 2011 (3.12)	consumer	99	**buyer** who is an **individual** to whom **consumer protection** requirements are applied as a set of **external constraints** on a **business transaction** NOTE 1 Consumer protection is a set of explicitly defined rights and obligations applicable as external constraints on a business transaction. NOTE 2 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 It is recognized that external constraints on a buyer of the nature of consumer protection may be peculiar to a specified jurisdictional domain.	consom-mateur	01	**acheteur**, en tant qu'**individu**, auquel s'appliquent des exigences de **protection des consommateurs** comme ensemble de **contraintes externes** sur une **transaction d'affaires** NOTE 1 La protection des consommateurs est un ensemble de droits et d'obligations définis explicitement et qui s'appliquent à titre de contraintes externes à une transaction d'affaires. NOTE 2 Le postulat est que la protection des consommateurs s'applique uniquement lorsqu'un acheteur dans une transaction d'affaires est un individu. Si ce n'est pas le cas dans une juridiction particulière, il faut spécifier ces contraintes externes comme faisant partie de composantes de scénarios selon le cas. NOTE 3 On reconnaît que les contraintes externes de protection des consommateurs exercées sur un acheteur peuvent relever d'une juridiction particulière.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.028	ISO/IEC 15944-5: 2008 (3.33)	consumer protection	99	set of **external constraints** of a **jurisdictional domain** as rights of a **consumer** and thus as obligations (and possible liabilities) of a **vendor** in a **business transaction** which apply to the good, service and/or right forming the **object** of the **business transaction** (including associated information management and interchange requirements including applicable (sets of) **recorded information**) NOTE 1 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 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 (13th) birthday). NOTE 3 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.	protection du consom-mateur	01	ensemble de **contraintes externes** d’un **domaine juridictionnel** comme droits d’un **consommateur** et ainsi comme obligations (et responsabilités éventuelles) d’un **fournisseur** dans une **transaction d’affaires** qui s’applique au bien, au service et/ou droit faisant l’**objet** de la **transaction d’affaires** (y compris les exigences en matière de gestion et l’échange de l’information qui s’y rattachent, dont l’(ou l’ensemble des) **information enregistrée** applicable NOTE 1 Des domaines juridictionnels peuvent restreindre l’application de leurs exigences en matière de protection du consommateur comme applicables uniquement aux individus participant à une transaction d’affaires de nature commerciale entreprise à des fins personnelles, familiales ou domestiques, c.-à.-d. qu’ils ne s’appliquent pas aux personnes physiques dans leur rôle d’ « organisation » ou de « Personne d’organisation ». NOTE 2 Des domaines juridictionnels peuvent avoir des exigences particulières en matière de protection du consommateur qui s’appliquent spécifiquement à un individu considérés comme un « enfant » ou un « mineur » (par ex. les individus n’ayant pas encore atteint leur treizième anniversaire de naissance). NOTE 3 Certains domaines juridictionnels peuvent avoir des exigences en matière de protection du consommateur propres à la nature du bien, du service, et/ou du droit faisant l’objet d’une transaction d’affaires.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.029	ISO/IEC 15944-5: 2008 (3.34)	controlled vocabulary (CV)	99	**vocabulary** for which the entries, i.e., **definition/term** pairs, are controlled by a **Source Authority** based on a **rulebase** and **process** for addition/deletion of entries NOTE 1 In a controlled vocabulary, there is a one-to-one relationship of definition and term. EXAMPLE The contents of "Clause 3 Definitions" in ISO/IEC standards are examples of controlled vocabularies with the entities being identified and referenced through their ID code, i.e., via their clause numbers. NOTE 2 In a multilingual controlled vocabulary, the definition/term pairs in the languages used are deemed to be equivalent, i.e., with respect to their semantics. NOTE 3 The rule base governing a controlled vocabulary may include a predefined concept system.	vocabulaire contrôlé (CV)	01	**vocabulaire** dont les entrées, c.-à.-d. les paires de **termes** et **définitions**, sont contrôlées par une **Autorité de source** fondée sur une **base de règles** et un **processus** pour ajouter et supprimer des entrées NOTE 1 Dans un vocabulaire contrôlé, une correspondance bi-univoque existe entre le terme et sa définition. EXEMPLE Le contenu des « Définitions de la Clause 3 » des normes ISO/CEI sont des exemples de vocabulaires contrôlés dont les entités sont identifiées et référencées grâce à leur code ID, c.-à.-d. leur numéro de clause. NOTE 2 Dans un vocabulaire contrôlé multilingue, les paires de termes/définitions des langues utilisées sont jugées sémantiquement équivalentes. NOTE 3 La base de règles régissant un vocabulaire contrôlé peut inclure un système de concepts prédéfini.
3.030	ISO/IEC 15944-1: 2011 (3.14)	data (in a business transaction)	99	representations of **recorded information** that are being prepared or have been prepared in a form suitable for use in a **computer system**	donnée (dans une transaction d'affaires)	01	représentations d'**informations enregistrées** qui sont préparées ou l'ont été de façon à pouvoir être traitée par un **ordinateur**
3.031	ISO/IEC 11179-1:2004 (3.3.8)	data element	99	unit of **data** for which the **definition**, **identification**, representation and permissible values are specified by means of a set of **attributes**	élément de données	01	unité de **données** dont la **définition**, l'**identification**, la représentation et les valeurs autorisées sont spécifiées au moyen d'un ensemble d'**attributs**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.032	ISO/IEC 2382-4: 1999 (04.07.01)	data element (in organization of data)	99	unit of **data** that is considered in context to be indivisible EXAMPLE The data element "age of a person" with values consisting of all combinations of 3 decimal digits. NOTE Differs from the entry 17.06.02 in ISO/IEC 2382-17.	élément de données (en organisation de données)	01	**donnée** considérée comme indivisible dans un certain contexte EXEMPLE L'élément de données «âge d'une personne» avec des valeurs comprenant toutes les combinaisons de trois chiffres décimaux. NOTE Cette notion est différente de celle de l'article 17.06.02 dans la norme ISO/CEI 2382-17.
3.033	ISO 19115: 2003 (4.2)	dataset	99	identifiable collection of **data** NOTE A dataset may be a smaller grouping of data which, though limited by some constraint such as spatial extent or feature type, is located physically within a larger dataset. Theoretically, a dataset may be as small as a single feature or feature attribute contained within a larger dataset. A hardcopy map or chart may be considered a dataset.	ensemble de données	01	collecte de **données** identifiables NOTE Un ensemble de données peut être un groupement plus petit données qui, bien que limité par certaines contraintes telles que l'étendue spatiale ou le type de caractéristique, est situé physiquement dans un ensemble de données plus étendu. En théorie, un ensemble de données peut être aussi petit qu'une caractéristique unique ou un attribut de caractéristique contenu dans un ensemble de données plus étendu.
3.034	ISO 19115: 2003 (4.3)	dataset series	99	collection of **datasets** sharing the same product specification	série de données	02	collecte de **ensemble de données** partageant la même spécification de produit
3.035	ISO/IEC 15944-8 (3.035)	data synchroniz-ation (in business transaction)	99	**process** of continuous harmonization of a **set(s)** of **recorded information** among all the parties to a **business transaction** to ensure that the current state of such a **set(s)** of **recorded information** is the same in the **IT systems** of all the participating parties	synchronisa-tion des données (dans les transactions d'affaires)	02	**processus** d'harmonisation continue d'un (ou des) **ensemble(s) d'informations enregistrées** entre les partenaires d'une **transaction d'affaires**, dans le but de s'assurer que l'état actuel de ces éléments **d'information enregistrée** est le même dans les **systèmes de technologie de l'information** de toutes les parties participantes

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE Adapted from GS1 Global Traceability Standard (GDSN) Glossary.			NOTE Adapté de GS1 Global Traceability Standard.
3.036	ISO/IEC 14662: 2010 (3.6)	Decision Making Application (DMA)	99	**model** of that part of an **Open-edi system** that makes decisions corresponding to the **role**(s) that the **Open-edi Party** plays as well as the originating, receiving and managing **data** values contained in the instantiated information bundles which is not required to be visible to the other **Open-edi Party(ies)**	Application à pouvoir de décision (DMA)	02	**modèle** de la partie d'un **système d'EDI-ouvert** qui prend les décisions correspondant au **rôle** ou aux **rôles** que joue le **partenaire** d'**EDI-ouvert**; elle est aussi source, récepteur et gestionnaire des valeurs des **données** contenues dans les instances de faisceaux d'informations; elle n'a pas à être rendue visible au(x) autre(s) **partenaire(s)** d'**EDI-ouvert**
3.037	ISO/IEC 15944-5: 2008 (3.42)	de facto language	99	**natural language** used in a **jurisdictional domain** which has the properties and behaviours of an **official language** in that **jurisdictional domain** without having formally been declared as such by that **jurisdictional domain** NOTE 1 A de facto language of a jurisdictional domain is often established through long term use and custom. NOTE 2 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.	langue de facto	01	**langage naturel** utilise dans un **domaine juridictionnel** qui a les propriétés et comportement d'une **langue officielle** dans ce **domaine juridictionnel** sans avoir été formellement déclaré comme telle par ce **domaine juridictionnel** NOTE 1 Une langue de facto d'un domaine juridictionnel est souvent établie à travers un usage et des coutumes à long terme. NOTE 2 Sauf énoncé explicite contraire et aux fins de modélisation d'une transaction d'affaires à travers un (ou des) scénario(s), attribut(s) de scénario et/ou composantes de scénario, une langue de facto d'un domaine juridictionnel est suppose avoir les mêmes propriétés et comportements qu'une langue officielle.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.038	ISO 1087-1: 2000 (3.3.1)	definition	99	representation of a **concept** by a descriptive statement which serves to differentiate it from related **concepts**	définition	02	représentation d'une **concept** au moyen d'un énoncé descriptif qui sert à la différencier d'autres **concept**
3.039	ISO 1087-1: 2000 (3.4.1)	designation	99	representation of a **concept** by a sign which denotes it NOTE In terminology work three types of designations are distinguished: symbols, appellations, (a.k.a. names), and terms.	designation	02	représentation d'un **concept** par un signe qui le dénomme NOTE Dans le travail terminologique, on distingue trois types de désignation les symboles, les appellations (c-à-d des noms) et les termes.
3.040	ISO/IEC 10181-2: 1996 (3.11)	distinguishing identifier	99	**data** that unambiguously distinguishes an **entity** in the **authentication process**	identificateur distinctif	01	**données** qui différencient sans ambiguïté une **entité** dans le **processus d'authentification**
3.041	ISO/IEC 15944-7: 2009 (3.06)	eBusiness	99	**business transaction**, involving the making of **commitments**, in a defined **collaboration space**, among **Persons** using their **IT systems**, according to **Open-edi standards** NOTE 1 eBusiness can be conducted on both a for-profit and not-for-profit basis. NOTE 2 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).	eAffaires	02	**transaction d'affaires**, impliquant la prise des **engagements**, dans une **espace de collaboration**, entre **Personnes** utilisant leurs **systèmes TI**, par application des **normes d'EDI-ouvert** NOTE 1 On peut entreprendre des eAffaires dans un but lucratif on non. NOTE 2 Une caractéristique clé des eAffaires est l'implication d'engagement(s) de toute(s) sorte(s) entre les Personnes qui poursuivent un but convenu mutuellement et impliquant leurs systèmes TI, et ce faisant, grâce au recours à l'EDI (en utilisant une variété de réseaux de communication dont l'Internet).

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 3 eBusiness includes various application areas such as “e-commerce”, “e-administration”, “e-logistics”, “e-government”, “e-medicine”, “e-learning”, etc. NOTE 4 The equivalent French language term for “eBusiness” is always presented in its plural form.			NOTE 3 Les eAffaires incluent divers secteurs d’applications tels que le « e-commerce »commerce électronique, « e-administration », « e-logistique » , « e-gouvernement », « e-médicine », e-apprentissage », etc. NOTE 4 Le terme français « eAffaires » s’emploie toujours au pluriel.
3.042	ISO/IEC 15944-2: 2006 (3.32)	electronic address	99	**address** used in a recognized electronic addressing scheme, (e.g., telephone, telex, IP, etc.), to which **recorded information** item(s) and/or **business object**(s) can be sent to or received from a **Contact**	adresse électronique	02	**adresse** utilisée dans un système d’adressage électronique reconnu (par ex. le téléphone, le télex, l’IP, etc.) à laquelle un **Contact** peut envoyer ou recevoir un (ou des) article(s) d’**information enregistrée** et/ou un (ou des) **objet(s) d’affaires**
3.043	ISO/IEC 14662: 2010 (3.8)	Electronic Data Interchange (EDI)	99	automated exchange of any predefined and structured **data** for **business** purposes among information systems of two or more **Persons** NOTE This definition includes all categories of electronic business transactions.	Echange de Données Informatisé (EDI)	01	échange automatisé de **données** structurées et prédéfinies pour traiter des **affaires** entre les systèmes d'information de deux ou plusieurs **Personnes**. NOTE Cette définition inclut toutes les catégories de transactions d’affaires électroniques.
3.044	ISO/IEC 2382-17: 1999 (17.02.05)	entity	99	any concrete or abstract thing that exists, did exist, or might exist, including associations among these things EXAMPLE A person, object, event, idea, process, etc. NOTE An entity exists whether data about it are available or not.	entité	01	tout objet ou association d'objets, concret ou abstrait, existant, ayant existé ou pouvant exister EXEMPLE Personne, événement, idée, processus, etc. NOTE Une entité existe que l'on dispose de données à son sujet ou non.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.045	ISO/IEC 9788-1: 1997 (3.3.1)	entity authentication	99	the corroboration that the **entity** is the one claimed	authentifi-cation de l'entité	99	corroboration que l'**entité** est bien celle qui est revendiquée
3.046	ISO/IEC 15944-5: 2008 (3.49)	exchange code set	99	a set of **ID codes** identified in a **coded domain** as being suitable for information exchange as shareable **data** EXAMPLE The 3-numeric, 2-alpha and 3-alpha code sets in ISO 3166-1.	ensemble de codes d'échange	01	ensemble de **codes ID** identifié dans un **domaine codé** comme convenant à l'échange d'information en tant que **données** partageables EXEMPLE L'ensemble des 3 codes numériques, alphabétiques à 2 lettres et alphabétiques à 3 lettres, dans l'ISO 3166-1.
3.047	ISO/IEC 15944-1: 2011 (3.23)	external constraint	99	**constraint** which takes precedence over **internal constraints** in a **business transaction**, i.e., is external to those agreed upon by the parties to a **business transaction** NOTE 1 Normally external constraints are created by law, regulation, orders, treaties, conventions or similar instruments. NOTE 2 Other sources of external constraints are those of a sectorial nature, those which pertain to a particular jurisdictional domain or a mutually agreed to common business conventions, (e.g., INCOTERMS, exchanges, etc.). NOTE 3 External constraints can apply to the nature of the good, service and/or right provided in a business transaction.	contrainte externe	01	**contrainte** qui l'emporte sur les **contraintes internes** dans une **transaction d'affaires**, c.-à-d. qui est externe à celles convenues entre les parties dans une **transaction d'affaires** NOTE 1 Normalement, les contraintes externes découlent des lois, règlements, décrets, traités, conventions, ou autres instruments semblables. NOTE 2 D'autres sources de contraintes externes sont de nature sectorielle, qui relèvent d'une juridiction particulière, ou de conventions d'affaires convenues mutuellement, (par ex. INCOTERMS, les échanges, etc.). NOTE 3 Des contraintes externes peuvent s'exercer sur la nature des biens, des services, et/ou au droit accordé dans une transaction d'affaires.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 4 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 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 must be recorded. EXAMPLE 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 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".			NOTE 4 Des contraintes externes peuvent exiger qu'une partie dans une transaction d'affaires réponde aux exigences spécifiques d'un rôle. EXEMPLE 1 Seul un médecin diplômé peut prescrire une ordonnance pour un médicament contrôlé. EXEMPLE 2 Seul un courtier en actions accrédité peut effectuer des transactions à la bourse de New York. EXEMPLE 3 Seule une entreprise attitrée peut transporter des déchets dangereux. NOTE 5 Lorsque les faisceaux d'information, y compris leurs composantes sémantiques, d'une transaction d'affaires constituent l'ensemble d'une transaction d'affaires (par ex. à des fins juridiques ou comptables), toutes les contraintes doivent être enregistrées. EXEMPLE Il peut exister une exigence juridique ou comptable de conserver la totalité des documents enregistrés relatifs à une transaction d'affaires, c.-à-d. les faisceaux d'information échangés, comme un «enregistrement». NOTE 6 Une contrainte externe minimum applicable à une transaction d'affaires exige souvent de distinguer si une Personne, c.-à-d. une partie dans une transaction d'affaires, est un «individu», une «organisation» ou une «administration publique». Par ex., les droits de protection de la vie privée ne s'appliquent qu'à une Personne en tant qu' «individu».

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.048	ISO/IEC 14662: 2010 (3.9)	Formal Description Technique (FDT)	99	specification method based on a description **language** using rigorous and **unambiguous rules** both with respect to developing expressions in the language (formal syntax) and interpreting the meaning of these expressions (formal semantics)	Technique de description formelle (FDT)	02	méthode de spécification fondée sur un **langage** de spécification faisant appel à des **règles** rigoureuses et **non ambiguës** tant pour le développement d'expressions dans le langage (syntaxe formelle) que pour l'interprétation de la signification de ces expressions (sémantique formelle)
3.049	ISO/IEC 14662: 2010 (3.10)	Functional Service View (FSV)	99	perspective of **business transactions** limited to those information technology interoperability aspects of **IT Systems** needed to support the execution of **Open-edi transactions**	Vue fonctionnel-le des services (FSV)	02	vue perspective sur les **transactions d'affaires**, restreinte à ceux des aspects relatifs au fonctionnement informatique coopératif entre **systèmes d'information** qui sont nécessaires à l'exécution des **transactions d'EDI-ouvert**
3.050	ISO/IEC 15944-2: 2006 (3.35)	Human Interface Equivalent (HIE)	99	representation of the **unambiguous** and IT-enabled semantics of an **IT interface equivalent** (in a **business transaction**), often the **ID code** of a **coded domain** (or a **composite identifier**), in a formalized manner suitable for communication to and understanding by humans NOTE 1 Human interface equivalents can be linguistic or non-linguistic in nature but their semantics remains the same although their representations may vary. NOTE 2 In most cases there will be multiple Human Interface Equivalent representations as required to meet localization requirements, i.e. those of a linguistic nature, jurisdictional nature, and/or sectoral nature.	Équivalent d'interface humaine (ÉIH)	01	représentation de la sémantique **non-ambigüe** et habilitée TI d'un **équivalent interface TI** (dans une **transaction d'affaires**), souvent le **code ID** d'un **domaine codé** (ou d'un **identificateur composite**), d'une manière formalisée qui convient à la communication et qui est compréhensible par les humains NOTE 1 Les Équivalents d'interface humaine peuvent être de nature linguistique on non, mais leur sémantique reste la même bien que leurs représentations puissent varier. NOTE 2 Dans la plupart des cas, il y aura des représentations d' Équivalents d'interface humaine multiples selon les besoins pour répondre aux exigences en matière de localisation, c.-à.d. ceux de nature linguistique, juridictionnelle et/ou sectorielle.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 3 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.).			NOTE 3 Les Équivalents d'interface humaine comprennent les représentations sous formes et formats différents (par ex. en plus du texte écrit, l'audio, les symboles, les icônes, les glyphes, les images, etc.).
3.051	ISO/IEC 15944-2: 2006 (3.36)	IB Identifier	99	unique, linguistically neutral, **unambiguous** referenceable **identifier** for an **Information Bundle**	identificateur IB	01	**identificateur** d'un **Faisceau d'informations** unique, linguistiquement neutre et référençable de façon **non-ambigüe**
3.052	ISO/IEC 15944-2: 2006 (3.37)	ID Code	99	**identifier** assigned by the **coded domain Source Authority** (**cdSA**) to a member of a **coded domain ID** NOTE 1 ID codes must be unique within the Registration Schema of that coded domain. NOTE 2 Associated with an ID code in a coded domain can be: - one or more equivalent codes; - one or more equivalent representations, especially those in the form of human equivalent (linguistic) expressions. NOTE 3 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 must be specified as the pivot ID code. NOTE 4 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	code ID	01	**identificateur** attribué par l'**Autorité de source du domaine codé (cdSA**) à un membre d'une **ID de domaine codé** NOTE 1 Les codes ID doivent être uniques dans le Schéma d'enregistrement de ce domaine codé. NOTE 2 On peut rattacher à un code ID dans un domaine codé: a) un ou plusieurs codes équivalents, b) une ou plusieurs représentations équivalentes; en particulier ceux et celles qui sont sous forme d'expressions (linguistiques) équivalentes humaines. NOTE 3 Lorsque l'on permet à une entité en tant que membre d'un domaine codé d'avoir plus d'un code ID, c.-à.-d. comme codes équivalents, l'un de ces codes doit être spécifié comme code ID pivot. NOTE 4 Un domaine codé peut contenir des codes ID relatifs aux entités qui ne sont pas membres à titre d'entités paires, c.-à.-d. ont les mêmes propriétés et comportements, tels que les codes ID relatifs à des conditions prédéfinies autres que celles des entités

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				this is the case, the rules governing such exceptions must be predefined and explicitly stated. EXAMPLE Common examples include: (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 In UML modeling notation, an ID code is viewed as an instance of an object class.			membres. Dans ce cas, les règles régissant de telles exceptions doivent être prédéfinies et énoncées explicitement. EXEMPLE Comme exemples communs, on trouve: (1) l’utilisation d’un code ID « 0 » (ou « 00 », etc.) pour « Autres »; l’utilisation d’un code ID « 9 » (ou « 99 ») pour « Sans objet »; l’utilisation du « 8 » (ou « 88 ») pour « non connu »; et/ou, si nécessaire, (4) la pré réservation d’une série ou d’ensemble de codes ID pour usage dans les « extensions utilisateur ». NOTE 5 Dans la notation de modélisation UML, un code ID est considéré comme instance de classe d’objet.
3.053	ISO/IEC 15944-1: 2011 (3.26)	identification	99	**rule**-based **process**, explicitly stated, involving the use of one or more **attributes**, i.e., **data elements**, whose value (or combination of values) are used to identify uniquely the occurrence or existence of a specified **entity**	identification	02	**processus** basé sur des **règles**, énoncées explicitement, impliquant l'utilisation d'un ou plusieurs **attributs**, c-à-d. des **éléments de données**, dont la valeur (ou une combinaison de valeurs) sert à identifier de façon unique l'occurrence ou l'existence d'une **entité** spécifiée
3.054	ISO/IEC 15944-1: 2011 (3.27)	identifier (in business transaction)	99	**unambiguous**, unique and a linguistically neutral value, resulting from the application of a **rule**-based **identification process** NOTE 1 Identifiers must be unique within the identification scheme of the issuing authority. NOTE 2 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)}	identificateur (transacttion d'affaires)	01	valeur **non-ambiguë** et linguistiquement neutre, résultant de l'application d'un **processus** d'**identification** à base de **règles** NOTE 1 Les identificateurs doivent être uniques dans le système d'identification de l'autorité émettrice. NOTE 2 Un identificateur est une séquence de caractères linguistiquement indépendante capable d’identifier de façon unique et permanente ce à quoi il est associé. {voir ISO 19135:2005 (4.1.5)}

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.055	ISO/IEC 15944-1: 2011 (3.28)	individual	99	**Person** who is a human being, i.e., a natural person, who acts as a distinct indivisible **entity** or is considered as such	individu	01	**Personne** qui est un être humain, c-à-d. une personne physique, qui agit à titre d'**entité** indivisible distincte ou qui est considérée comme telle
3.056	ISO/IEC 15944-5: 2008 (3.60)	individual accessibility	99	set of **external constraints** of a **jurisdictional domain** as rights of an **individual** with disabilities to be able to use IT systems at the human, i.e., user, interface and the concomitant obligation of a **seller** to provide such adaptive technologies NOTE Although "accessibility" typically addresses users who have a disability, the concept is not limited to disability issues. EXAMPLE Examples of disabilities in the form of functional and cognitive limitations include: - people who are blind; - people with low vision; - people with colour blindness; - people who are hard of hearing or deaf, i.e., are hearing impaired; - people with physical disabilities; - people with language or cognitive disabilities.	accessibilité individuelle	01	ensemble de **contraintes externes** d'un **domaine juridictionnel** comme droits d'un **individu** atteint de déficience d'être capable d'utiliser des systèmes TI au niveau de l'interface humaine, c.-à.-d. utilisateur, et l'obligation concomitante d'un **vendeur** d'offrir ce type de technologies adaptatives NOTE Bien que l'« accessibilité » s'adresse typiquement aux utilisateurs qui ont une déficience, le concept ne se limite pas aux questions de déficience. EXEMPLE Comme exemples de déficiences sous formes de limitations fonctionnelles et cognitives, on trouve: - les personnes aveugles; - les personnes à basse vision; - les personnes atteintes d'achromatopsie; - les personnes sourdes ou ayant une déficience auditive; - les personnes atteintes de déficience physique; - les personnes atteintes de déficience linguistique ou cognitive.
3.057	ISO/IEC 15944-8 (3.057)	individual anonymity	99	state of not knowing the identity or not having any recording of **personal information** on or about an **individual** as a **buyer** by the **seller** or **regulator**, (or any other party) to a **business transaction**	anonymité individuelle	02	état d'indisponibilité de l'identité ou de l'enregistrement de **l'information personnelle** sur (ou au sujet d') un **individu** constatée chez un **acheteur** ou un **régulateur** (ou tout autre tiers) partie prenante d'une **transaction d'affaires**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.058	ISO/IEC 15944-8 (3.058)	individual authentication	99	provision of the assurance of a **recognized individual identity (rii)** sufficient for the purpose of the **business transaction**	authentication individuelle	02	présentation d'une garantie concernant une **identité individuelle reconnue (rii)** et suffisante pour la réalisation d'une **transaction d'affaires**
3.059	ISO/IEC 15944-8 (3.059)	individual identity (ii)	99	**Person identity** of an **individual**, i.e., an individual identity, consisting of the combination of the **persona** information and **identifier** used by an **individual** in a **business transaction**, i.e., the making of any kind of **commitment**	identité individuelle (ii)	02	**identité de Personne** d'un **individu,** c.-à.-d., identité individuelle consistant en la combinaison d'information sur la **persona** et l'**identifiant** utilisée par un individu dans une **transaction d'affaires**, c.-à.-d. la prise de toute forme d'**engagement**
3.060	ISO/IEC 15944-8 (3.060)	individual persona Registration Schema (ipRS)	99	**persona Registration Schema (pRS)** where the **persona** is, or includes, that of an **individual** being registered NOTE 1 Where an persona Registration Schema includes persona of sub-types of Persons, i.e., individuals, organizations, and/or, public administrations, those which pertain to individuals shall be identified as such because public policy as external constraints apply including those of a privacy protection requirements nature. NOTE 2 In a individual persona Registration Schema (ipRS), one shall state whether or not a truncated name, i.e. registered persona, of the individual, is allowed or mandatory, and if so the ipRS shall explicitly state the rules governing the formation of the same.	Schéma d'enregistre-ment d'une personne individuelle (ipRS)	01	**Schéma d'enregistrement d'une persona (pRS)** selon lequel la **persona** est, ou inclut, celle d'un **individu** en cours d'enregistrement NOTE1 Lorsque le Schéma d'enregistrement d'une persona inclut des persona de sous-catégories de personnes, c.-à.-d. des individus, des organisations, et/ou des administrations publiques, les éléments précités qui se réfèrent à des individus doivent être identifiés comme tels, car les politiques publiques en tant que contraintes externes s'appliquent alors, y compris celles de nature des exigences de protection de la vie privée. NOTE 2 Dans un schéma d'enregistrement d'une persona individuelle (ipRS), on est tenu de préciser si un nom complet ou abrégé (c.-à.-d. la persona enregistrée) est autorisé et obligatoire, et en ce cas, l'ipRS doit définir clairement les règles applicables à sa formation.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.061	ISO/IEC 14662: 2010 (3.11)	Information Bundle (IB)	99	formal description of the semantics of the **recorded information** to be exchanged by **Open-edi Parties** playing **roles** in an **Open-edi scenario**	Faisceau d'informations (IB)	01	description formelle de la valeur sémantique des **informations enregistrées** échangées entre **partenaires** d'**EDI-ouvert** jouant un **rôle** dans un **scénario d'EDI-ouvert**
3.062	ISO/IEC 15944-8 (3.062)	information law	99	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**, 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**	loi sur l'information	02	toute loi, règlement, politique ou code (ou partie de ceux-ci) qui exige la création, la réception, la collecte, la description ou le listage, la production, l'extraction, la soumission, la rétention, le stockage la préservation ou la destruction **d'information enregistrée** et /ou qui impose des conditions à l'accès et à l'utilisation, à la confidentialité, à la protection de la vie privée, à l'intégrité, aux responsabilités, à la continuité et la disponibilité du traitement, de la reproduction, de la distribution, de la transmission, de la vente, du partage ou de tout autre manipulation de **l'information enregistrée**
3.063	ISO/IEC 14662: 2010 (3.12)	Information Processing Domain (IPD)	99	**Information Technology System** which includes at least either a **Decision Making Application** and/or one of the components of an **Open-edi Support Infrastructure** (or both), and acts/executes on behalf of an **Open-edi Party** (either directly or under a delegated authority)	Domaine de traitement de l'information (IPD)	01	**système d'information** comprenant au moins une **Application à pouvoir (DMA) de décision** ou un des composants de l'**infrastructure de support d'EDI-ouvert** (ou les deux), agissant ou fonctionnant au nom d'un **partenaire** d'**EDI-ouvert** (directement ou par délégation d'autorité)
3.064	ISO/IEC 14662: 2010 (3.13)	Information Technology System (IT System)	99	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	système d'information (IT System)	01	ensemble constitué d'un ou de plusieurs **ordinateurs**, avec leurs logiciels associés, de périphériques, de terminaux, d'opérateurs humains, de **processus** physiques et de moyens de transfert d'information, formant un tout autonome capable de traiter l'information et/ou de la transmettre

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.065	ISO/IEC 15944-1: 2011 (3.33)	internal constraint	99	**constraint** which forms part of the **commitment**(s) mutually agreed to among the parties to a **business transaction** NOTE 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.	contrainte interne	01	**contrainte** qui fait partie de l'**engagement** convenu mutuellement entre les parties d'une **transaction d'affaires** NOTE Les contraintes internes sont volontaires. Elles présentent une vue simplifiée de modélisation et de réutilisation des composantes de scénario d'une transaction d'affaires sans contraintes ou restrictions externes quant à la conduite d'une transaction d'affaires autres que celles convenues mutuellement entre l'acheteur et le vendeur.
3.066	ISO/IEC 15944-5: 2008 (3.65)	IT-enablement	99	transformation of a current **standard** used in **business transactions**, (e.g., **coded domains**), from a manual to computational perspective so as to be able to support **commitment** exchange and **computational integrity**	habilitation TI	01	transformation des **normes** actuelles utilisées dans le **transaction d'affaires** (par exemple, les **domaines codés**) de mode manuel en mode informatique, afin de pouvoir assurer un échange d'**engagements** et une **intégrité informatique**
3.067	ISO/IEC 15944-2: 2006 (3.48)	IT interface equivalent	99	computer processable **identification** of the **unambiguous** semantics of a scenario, **scenario attribute** and/or **scenario component**(s) pertaining to a **commitment** exchange in a **business transaction** which supports **computational integrity** NOTE 1 IT interface equivalents have the properties of identifiers (in business transaction) and are used to support semantic interoperability in commitment exchange. NOTE 2 The value of an IT interface equivalent at times is a composite identifier.	équivalent d'interface TI	01	**identification** informatisable des sémantiques **non-ambigües** d'un scénario, d'un **attribut de scénario** et/ou de **composante(s) de scénario** concernant un échange d'**engagements** dans une **transaction d'affaires** qui soutient l'**intégrité computationnelle** NOTE 1 Les équivalents d'interface IT ont les propriétés d'identificateurs (dans une transaction d'affaires) et sont utilisés pour soutenir l'interopérabilité sémantique dans l'échange d'engagements. NOTE 2 La valeur d'un équivalent d'interface IT est parfois un identificateur composite.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 3 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 An IT interface equivalent is at times used as a semantic identifier. NOTE 5 An IT interface equivalent may have associated with it one or more Human Interface Equivalents (HIEs). NOTE 6 The value of an IT Interface is independent of its encoding in programming languages or APIs.			NOTE 3 Un équivalent d'interface IT en tant qu'identificateur composite peut se composer de l'identificateur d'un domaine codé plus un code ID de ce domaine codé. NOTE 4 Un équivalent d'interface IT est parfois utilisé comme identificateur sémantique. NOTE 5 Un équivalent d'interface IT peut être rattaché à un ou plusieurs Équivalents d'interface humaine (HIE). NOTE 6 La valeur d'un équivalent d'interface IT est indépendante de son codage dans les langages de programmation ou des API.
3.068	ISO/IEC 15944-5: 2008 (3.67)	jurisdictional domain	99	jurisdiction, recognized in law as a distinct legal and/or regulatory framework, which is a source of **external constraints** on **Persons**, their behaviour and the making of **commitments** among **Persons** including any aspect of a **business transaction** NOTE 1 The pivot 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 Jurisdictional domains can combine to form new jurisdictional domains, (e.g., through bilateral, multilateral and/or international treaties).	domaine jurisdictionnel	01	juridiction, reconnue par la loi comme cadre juridique distinct et/ou de réglementation, qui est une source de **contraintes externes** pour les **Personnes**, leur comportement et la prise d'**engagements** entre les **Personnes**, y compris tout aspect d'une **transaction** d'**affaires** NOTE 1 Le domaine juridictionnel pivot est un état membre reconnu par les Nations unies (ONU). Dans une perspective juridique et de souveraineté, tous les états sont considérés comme des entités « paires ». Chaque état membre de l'ONU (alias pays) peut avoir des subdivisions administratives comme domaines juridictionnels reconnus (par ex. provinces, territoires, cantons, länder, etc.), tel que décidé par cet état membre de l'ONU. NOTE 2 Des domaines juridictionnels peuvent être combinés pour former de nouveaux domaines juridictionnels (par ex., grâce à des traités bilatéraux, multilatéraux et/ou internationaux).

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				EXAMPLE Included here, for example, are the European Union (EU), NAFTA, WTO, WCO, ICAO, WHO, Red Cross, the ISO, the IEC, the ITU, etc. NOTE 3 Several levels and categories of jurisdictional domains may exist within a jurisdictional domain. NOTE 4 A jurisdictional domain may impact aspects of the commitment(s) made as part of a business transaction including those pertaining to the making, selling, transfer of goods, services and/or rights (and resulting liabilities) and associated information. This is independent of whether such interchange of commitments are conducted on a for-profit or not-for-profit basis and/or include monetary values. NOTE 5 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.			EXEMPLES l'Union européenne (UE), l'ALENA, l'OMC, l'OMD, l'OACI, l'OMS, la Croix-Rouge, l'ISO, la CEI, l'UIT, etc. NOTE 3 Plusieurs niveaux et catégories de domaines juridictionnels peuvent exister à l'intérieur d'un domaine juridictionnel. NOTE 4 Un domaine juridictionnel peut avoir des répercussions sur des aspects des engagements pris dans le cadre de transactions d'affaires, y compris celles qui ont trait à la fabrication, la dispensation, la vente et le transfert de biens, de services et/ou de droits (et des responsabilités qui en résultent), et l'information connexe. Ceci indépendamment du fait que de tels échanges d'engagements peuvent s'effectuer dans un (ou sans) but lucratif et/ou inclure des valeurs monétaires. NOTE 5 Les lois, règlements, directives, etc., promulgués par un domaine juridictionnel sont considérés comme faisant partie de ce domaine juridictionnel et sont les sources principales de contraintes externes exercées sur les transactions d'affaires.
3.069	ISO/IEC 15944-2: 2006 (3.47)	jurisdictional domain identifier	99	**ID code** of a **jurisdictional domain** as recognized for use by peer **jurisdictional domains** within a system of mutual recognition	identificateur de domaine juridictionnel	01	**code ID** d'un **domaine juridictionnel** reconnu pour utilisation par des d**omaines juridictionnels** pairs dans un système de reconnaissance mutuelle
3.070	ISO 5127003A 2001 (1.1.2.01)	language	99	system of signs for communication, usually consisting of a **vocabulary** and **rules**	langue	01	système de signes de communication compose habituellement d'un **vocabulaire** et de **règles**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE In this part of ISO/IEC 15944, language refers to natural languages or special languages, but not "programming languages" or "artificial languages".			NOTE Dans la présente norme, la langue se réfère aux langues naturelles ou aux langues de spécialité, mais pas aux « langages de programmation » ou « langages artificiels ».
3.071	ISO 639-2: 1998 (3.2)	language code	99	combination of **characters** used to represent a **language** or **languages** NOTE In ISO/IEC 15944, the ISO 639-2/T (terminology) three alpha-code, shall be used.	codet de langue	01	combinaison de **caractères** utilisées pour représenter une **langue** ou des **langues** NOTE Dans la présente norme multiparties ISO/IEC 15944, le code alpha trois de l'ISO 639-2/T (terminologie) doit être utilisé.
3.072	ISO/IEC 15944-5: 2008 (3.71)	legally recognized language (LRL)	99	**natural language** which has status (other than an **official language** or **de facto language**) in a **jurisdictional domain** 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 The LRL can be specified through either: - the identification of a language by the name used; or, - the identification of a people and thus their language(s). EXAMPLE In addition to acts and regulations, legal instruments include self-government agreements, land claim settlements, court decisions, jurisprudence, etc.	langue reconnue légalement (LRL)	01	**langage naturel** ayant le statut (autre que celui de **langue officielle** ou de **langue de facto**) dans un **domaine juridictionnel** tel qu'énoncé dans une loi, un règlement ou tout autre instrument légal, qui accorde à une communauté de personnes (ou à ses **individus**) le droit d'utiliser ce **langage naturel** dans le contexte stipulé par l'(ou les) instrument(s) léga(ux) NOTE La langue reconnue légalement peut être spécifiée - soit par l'identification d'une langue par son nom utilisé; ou, - soit par l'identification d'un peuple et ainsi de sa (ou ses) langue(s). EXEMPLE En plus des lois et règlements, les instruments légaux comprennent les ententes d'autonomie gouvernementale, les règlements en matière de revendication territoriale, les décisions de tribunal, la jurisprudence, etc.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.073	ISO/IEC 15944-5: 2008 (3.72)	legally recognized name (LRN)	99	**persona** associated with a **role** of a **Person** recognized as having legal status and so recognized in a **jurisdictional domain** as accepted or assigned in compliance with the **rules** applicable of that **jurisdictional domain**, i.e. as governing the **coded domain** of which the **LRN** is a member NOTE 1 A LRN may be of a general nature and thus be available for general use in commitment exchange or may arise from the application of a particular law, regulation, program or service of a jurisdictional domain and thus will have a specified use in commitment exchange. NOTE 2 The process of establishment of a LRN is usually accompanied by the assignment of a unique identifier. NOTE 3 A LRN is usually a registry entry in a register established by the jurisdictional domain (usually by a specified public administration within that jurisdictional domain) for the purpose of applying the applicable rules and registering and recording LRNs (and possible accompanying unique identifiers accordingly). NOTE 4 A Person may have more than one LRN (and associated LRN identifier).	nom légalement reconnu (NLR)	01	**persona** associée au **rôle** d'une **Personne** reconnue comme ayant un statut légal et ainsi reconnue dans un **domaine juridictionnel** comme acceptée ou attribuée conformément aux **règles** applicables de ce **domaine juridictionnel**, c.-à.-d. celles régissant le **domaine codé** dont le **NLR** est membre NOTE 1 Un NLR peut être de nature générale et ainsi être disponible pour usage général dans l'échange d'engagements ou peut découler de l'application d'une loi, d'un règlement, d'un programme ou d'un service particulier d'un domaine juridictionnel et ainsi avoir un usage spécifié dans l'échange d'engagements. NOTE 2 Ce processus d'établissement d'un NLR s'accompagne habituellement de l'attribution d'un identificateur unique. NOTE 3 Un NLR est habituellement une entrée de registre dans un registre établi par le domaine juridique (habituellement par une administration publique spécifiée dans ce domaine juridictionnel) aux fins d'application des règles applicables et de l'enregistrement et de l'inscription des NLR (et par conséquent de leurs identificateurs uniques possibles les accompagnant). NOTE 4 Une Personne peut avoir plus d'un NLR (et identificateur NLR connexe).
3.074	ISO/IEC 2382-4: 1999 (04.08.01)	list	99	ordered **set** of **data elements**	liste	01	**ensemble** d'**éléments de donnée** dont l'ordre est défini

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.075	ISO/IEC 15944-5: 2008 (3.75)	localization	99	pertaining to or concerned with anything that is not global and is bound through specified sets of **constraints** of: (a) a linguistic nature including **natural** and **special languages** and associated multilingual requirements; (b) jurisdictional nature, i.e., legal, regulatory, geopolitical, etc.; (c) a sectorial nature, i.e., industry sector, scientific, professional, etc.; (d) a human rights nature, i.e., privacy, disabled/handicapped persons, etc.; (e) **consumer** behaviour requirements; and/or (f) safety or health requirements. Within and among "locales", interoperability and harmonization objectives also apply	localisation	01	se rapportant à ou concernant tout ce qui n'est pas mondial et est lié par une série de **contraints** particuliers: (a) une nature linguistique comprenant les **langues naturelles** et **spéciales** ainsi que les exigences multilingues connexes; (b) une nature juridique, par exemple légale, de réglementation, géopolitique, etc.; (c) une nature sectorielle, par exemple, par exemple le secteur industriel, scientifique, professionnel, etc.; (d) une nature des droits de la personne, par exemple le respect de la vie privée, les handicapés, etc.; (e) les exigences en matière de comportement des **consommateurs**; et/ou; (f) les exigences en matière de sécurité et de santé. Des objectifs d'interopérabilité et d'harmonisation s'appliquent également à la localisation
3.076	ISO/IEC 15944-2: 2006 (3.50)	location	99	place, either physical or electronic, that can be defined as an **address**	emplacement	01	lieu, physique ou électronique, pouvant être défini par une **adresse**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.077	ISO/IEC 15944-1: 2011 (3.34)	medium	99	physical material which serves as a functional unit, in or on which information or **data** 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 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 The inclusion of the "non-volatile in nature" attribute is to cover latency and records retention requirements. NOTE 3 This definition of "medium" is independent of: i)form or format of recorded information; ii)physical dimension and/or size; and, iii)any container or housing that is physically separate from material being housed and without which the medium can remain a functional unit. NOTE 4 This definition of "medium" also captures and integrates the following key properties: i)the property of medium as a material in or on which information or data can be recorded and retrieved; ii)the property of storage; iii)the property of physical carrier; iv)the property of physical manifestation, i.e., material; v) the property of a functional unit; and, vi)the property of (some degree of) stability of the	support	01	matériel physique qui sert d'unité fonctionnelle, et dans lequel ou sur lequel l'information ou les **données** sont normalement stockées, dans lequel de l'information ou des **données** peuvent être retenues et transportées, à partir duquel de l'information ou des **données** peuvent être extraites, et qui est non-volatile par nature NOTE 1 Cette définition est indépendante de la nature matérielle sur laquelle l'information est enregistrée et/ou de la technologie utilisée pour enregistrer l'information (par exemple du papier, des supports photographiques (chimiques), magnétiques, optiques, des circuits imprimés, ainsi que d'autres catégories qui ne sont plus utilisées de façon courante telles que le vélin, le parchemin (et autres peaux animales), les plastiques (par exemple la bakélite ou le vinyl), les textiles (par exemple le lin et la toile), les métaux, etc. NOTE 2 L'inclusion de l'attribut «nature non-volatile» couvre les exigences en matière de latence et de rétention des dossiers. NOTE 3 La définition de «support» est indépendante des éléments suivants: i)la forme ou le format de l'information enregistrée; ii)la dimension physique et/ou la taille; et, iii)tout conteneur ou boîtier qui est séparé physiquement du matériel logé et sans lequel le support peut demeurer une unité fonctionnelle. NOTE 4 La définition de «support» reflète et intègre aussi les propriétés clés suivantes: i)propriété du support comme matériel dans ou sur lequel de l'information ou des données peuvent être stockées et extraites; ii)la propriété du stockage; iii)la propriété du

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				material in or on which the information or data is recorded.			porteur physique; iv)la propriété de la manifestation physique, par exemple le matériel; v)la propriété d'une unité fonctionnelle; et, vi)la propriété (jusqu'à un certain degré) de la stabilité du matériel dans ou sur lequel l'information ou les données sont stockées.
3.078	ISO 19115: 2003 (4.9)	model	99	abstraction of some aspect of reality	modèle	01	abstraction de certains aspects de la réalité
3.079	ISO/IEC 15944-5: 2008 (3.82)	multilingual-ism	99	ability to support not only **character sets** specific to a (natural) **language** (or family of **languages**) and associated **rules** but also **localization** requirements, i.e., use of a **language** from **jurisdictional domain**, sectoral and/or **consumer** marketplace perspectives	multilin-guisme	01	capacité de supporter non seulement les **jeux de caractères** particuliers à une **langue** naturelle (ou une famille de **langues** ainsi que les **règles** connexes, mais aussi les exigences en matière de **localisation**, par ex. l'utilisation d'une **langue** dans une perspective de **domaine juridictionnel**, sectorielle et/ou de marché du **consommateur**
3.080	ISO/IEC 15944-8 (3.080)	mutually-defined recognized individual identity (md-rii)	99	**recognized individual identity (rii)** which is mutually defined and agreed to for use between the **seller** and the i**ndividual**, as **buyer**, in a **business transaction** NOTE 1 The establishment of a mutually agreed to and recognized individual between a seller and individual, as buyer, does not extinguish the applicable privacy protection rights of that individual. NOTE 2 A mutually defined recognized individual identity (md-rii) shall be established between the seller and the individual no later than the end of the negotiation phase.	identité individuelle mutuellement définie reconnue (md-rii)	02	**identité individuelle reconnue (rii)** mutuellement définie et d'un commun accord pour usage entre **l'acheteur et l'individu** comme **acheteur,** dans une **transaction d'affaires** NOTE1 La mise en place d'un cadre reconnu d'un commun accord entre un vendeur et un individu n'exclut pas les règles applicables à la protection de la vie privée de l'individu concerné. NOTE 2 Une identité individuelle mutuellement définie-reconnue (md-rii) doit être établie entre l'acheteur et l'individu avant le terme de la période de négociation.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 3 Use of a mutually defined recognized individual identity (md-rii) may not be permitted where external constraints apply.			NOTE 3 L'utilisation d'une identité individuelle mutuellement définie-reconnue (md-rii) peut ne pas être permise lorsque s'appliquent des contraintes externes.
3.081	ISO 5127: 20001 (1.1.2.13)	name	99	**designation** of an **object** by a linguistic expression NOTE Adapted from ISO 1087-1:2000	nom	01	**désignation** d'un **objet** par une unité linguistique NOTE Adapté de l'ISO 1087-1:2000
3.082	ISO 5127: 20001 (1.1.2.02)	natural language	99	**language** which is or was in active use in a community of people, and the **rules** of which are mainly deduced from the usage	langage naturel	01	**langage** qui est ou était pratiqué dans une communauté de personnes et **règles** qui sont essentiellement déduites de son usage
3.083	ISO 1087-1: 2000 (3.1.1)	object	99	anything perceivable or conceivable NOTE 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).	objet	01	tout ce qui peut être perçu ou conçu NOTE Les objets peuvent être matériels (par exemple un moteur, une feuille de papier, un diamant), immatériels (par exemple un rapport de conversion, un plan de projet) ou imaginaires (par exemple une licorne).
3.084	ISO/IEC 11179-1: 2004 (3.3.22)	object class	99	set of ideas, abstractions, or things in the real world that can be identified with explicit boundaries and meaning and whose properties and behavior follow the same **rules**	classe d'objets	02	ensemble d'idées, d'abstractions ou de choses du monde réel qui peuvent être identifiées avec des limites et une signification explicites et dont les propriétés et le comportement suivent les mêmes **règles**
3.085	ISO/IEC 15944-5: 2008 (3.87)	official language	99	**external constraint** in the form of a **natural language** specified by a **jurisdictional domain** for official use by **Persons** forming part of and/or subject to that **jurisdictional domain** for use in communication(s) either	langue officielle	02	**contrainte externe** sous forme de **langage naturel** spécifié par un **domaine juridictionnel** pour usage officiel par des **Personnes** faisant partie ou sujettes de ce **domaine juridictionnel** dans la (ou les) communication(s) soit

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				(1) within that **jurisdictional domain**; and/or, (2) among such **Persons**, where such communications are **recorded information** involving **commitment**(s) NOTE 1 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 A jurisdictional domain decides whether or not it has an official language. If not, it will have a de facto language. NOTE 3 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 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 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 must be specified. NOTE 6 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.			(1) à l'intérieur de ce **domaine juridictionnel**, soit (2) entre ces **Personnes**, lorsque ces communications sont une **information enregistrée** impliquant un (ou des) **engagement**(s) NOTE 1 Sauf exigence contraire concernant une langue officielle, les Personnes sont libres de choisir leur langage naturel mutuellement acceptable et/ou leur langue de spécialité dans les communications et l'échange d'engagements. NOTE 2 Un domaine juridictionnel décide s'il dispose d'une langue officielle. Dans le cas contraire, il disposera d'une langue de facto. NOTE 3 Une (ou des) langue(s) officielle(s) peut (ou peuvent) être exigée(s) dans les communications officielles et la disposition de biens et de services aux Personnes sujettes de ce domaine juridictionnel et dans le(s) système(s) juridique(s) et autre(s) système(s) de résolution de conflit de ce domaine juridictionnel, etc. NOTE 4 S'il y a lieu, l'utilisation d'une langue officielle peut être exigée dans l'exercice de droits et d'obligations des individus de ce domaine juridictionnel. NOTE 5 Lorsqu'une langue officielle d'un domaine juridictionnel dispose d'un vocabulaire contrôlé de la nature d'une terminologie, elle peut très bien avoir les caractéristiques d'une langue de spécialité. Dans de tels cas, la terminologie à utiliser doit être spécifiée.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				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 Another example is that of Norway which has two official writing systems, both Latin-1 based, namely, Bokmål (Dano-Norwegian) and Nynorsk (New Norwegian). NOTE 7 A jurisdictional domain may have more than one official language but these may or may not have equal status. EXAMPLE Canada has two official languages, Switzerland has three, while the Union of South Africa has eleven official languages. NOTE 8 The BOV requirement of the use of a specified language will place that requirement on any FSV supporting service. EXAMPLE 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.			NOTE 6 En ce qui concerne une langue officielle, le(s) système(s) d'écriture à utiliser doit(doivent) être spécifié(s) lorsque l'usage parlé d'un langage naturel a plus d'un système d'écriture. EXEMPLE 1 La langue parlée d'une langue officielle peut parfois avoir plus d'un système d'écriture. L'Inuktitut, par ex., a trois systèmes d'écriture. Le Canada utilise deux de ces systèmes d'écriture, notamment l'alphabet latin-1 (romain) et l'alphabet syllabique. Le troisième est utilisé en Russie et est basé sur des caractères cyrilliques. EXEMPLE 2 Un autre exemple est celui de la Norvège qui a deux systèmes d'écriture officiels, tous les deux basés sur l'alphabet latin-1 : le Bokmål (Dano-Norvégien) et le Nynorsk (Nouveau Norvégien). NOTE 7 Un domaine juridictionnel peut avoir plusieurs langues officielles. EXEMPLE le Canada a deux langues officielles, la Suisse trois et l'Afrique du Sud onze. NOTE 8 L'exigence BOV concernant l'usage d'une langue spécifique s'applique également à tout service de soutien FSV. EXEMPLE Une exigence BOV pour l'arabe, le chinois, le russe, le japonais, le coréen, etc. comme langue officielle exige que le service de soutien FSV soit capable de soutenir les jeux de caractères associés.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.086	ISO/IEC 14662: 2010 (3.14)	Open-edi	99	**electronic data interchange** among multiple autonomous **Persons** to accomplish an explicitly shared **business** goal according to **Open-edi standards**	EDI-ouvert	01	**échange de données informatisé** par application des **normes d'EDI-ouvert** entre plusieurs **Personnes** autonomes visant un objectif d'**affaires** explicitement partagé
3.087	ISO/IEC 14662: 2010 (3.16)	Open-edi Description Technique (OeDT)	99	specification method such as a **Formal Description Technique**, another methodology having the **characteristics** of a **Formal Description Technique**, or a combination of such techniques as needed to formally specify **BOV** concepts, in a computer processable form	Technique de description d'EDI-ouvert (OeDT)	02	méthode de spécification, **technique de description formelle**, ou toute autre technique ayant les **caractéristiques** d'une **technique de description formelle**, ou combinaison de ces techniques, permettant de spécifier formellement les concepts de la **BOV** sous forme calculable par un ordinateur
3.088	ISO/IEC 15944-5: 2008 (3.90)	Open-edi disposition	99	**process** governing the implementation of formally approved records retention, destruction (or expungement) or transfer of **recorded information** under the control of a **Person** which are documented in disposition authorities or similar instruments NOTE Adapted from ISO 15489-1.	disposition d'EDI-ouvert	01	**processus** gouvernant l'application d'une rétention d'enregistrement formellement approuvée, la destruction (ou radiation) ou le transfert d'**information enregistrée** sous le contrôle d'une **Personne** qui sont documentés dans des autorités de disposition ou instruments semblables NOTE Adapté de l'ISO 15489-1.
3.089	ISO/IEC 14662: 2010 (3.17)	Open-edi Party (OeP)	99	**Person** that participates in **Open-edi** NOTE Often referred to generically in this, and other eBusiness standards, (e.g., parts of the 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.	Partenaire d'EDI-ouvert (OeP)	01	**Personne** participant à l'**EDI-ouvert** NOTE Souvent mentionnée de façon générique dans la présente norme, et dans d'autres normes d'eAffaires (par ex. dans certaines parties de la norme multiparties d'«eAffaires» ISO/CE 15944), comme «partie» ou «parties» pour toute entité modélisée comme une Personne jouant un rôle dans les scénarios d'EDI-ouvert.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.090	ISO/IEC 15944-5: 2008 (3.92)	Open-edi Record Retention (OeRR)	99	specification of a period of time that a **set of recorded information** must be kept by a **Person** in order to meet operational, legal, regulatory, fiscal or other requirements as specified in the **external constraints** (or **internal constraints**) applicable to a **Person** who is a party to a **business transaction**	Rétention d'enregistre-ment d'EDI-ouvert (OeRR)	01	spécification d'une période de temps pendant laquelle un **ensemble d'informations enregistrées** doit être conserve par une **Personne** afin de répondre à des exigences opérationnelles, légales, de réglementation, fiscales ou autres, tel que spécifié dans les **contraintes externes** (ou les **contraintes internes**) applicables à une **Personne** faisant partie d'une **transaction d'affaires**
3.091	ISO/IEC 14662: 2010 (3.22)	Open-edi system	99	**information technology system (IT system)** which enables an **Open-edi Party** to participate in **Open-edi transactions**	Système d'EDI-ouvert	01	**système d'information (IT system)** permettant à un **partenaire** d'**EDI-ouvert** de prendre part à des **transactions** d'**EDI-ouvert**
3.092	ISO/IEC 6523-1: 1998 (3.1)	organization	99	unique framework of authority within which a person or persons act, or are designated to act, towards some purpose NOTE 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 and/or services including: 1) partnerships; 2) social or other non-profit organizations or similar bodies in which ownership or control is vested in a group of individuals; 3) sole proprietorships	organisation	02	cadre unique d'autorité dans lequel une ou plusieurs personnes agissent ou sont désignées pour agir afin d'atteindre un certain but NOTE Les types d'organisations couverts par la présente partie de l'ISO/CEI 6523 comprennent par exemple les éléments suivants: EXEMPLE 1 Organisations constituées suivant des formes juridiques prévues par la loi. EXEMPLE 2 Autres organisations ou activités fournissant des biens et/ou des services, tels que: 1) sociétés en participation; 2) organismes sociaux ou autres à but non lucratif dans lesquels le droit de propriété ou le contrôle est dévolu à un groupe de personnes;

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				4) governmental bodies. EXAMPLE 3 Groupings of the above types of organizations where there is a need to identify these in information interchange.			3) entreprises individuelles; 4) administrations et organismes de l'état. EXEMPLE 3 Regroupements des organisations des types ci-dessus, lorsqu'il est nécessaire de les identifier pour l'échange d'informations.
3.093	ISO/IEC 6523-1: 1998 (3.2)	organization part	99	any department, service or other **entity** within an **organization**, which needs to be identified for information interchange	partie d'organisation	02	n'importe quel département, service ou autre **entité** au sein d'une **organisation**, qu'il est nécessaire d'identifier pour l'échange d'informations
3.094	ISO/IEC 15944-1: 2011 (3.46)	organization Person	99	**organization part** which has the properties of a **Person** and thus is able to make **commitments** on behalf of that **organization** NOTE 1 An organization can have one or more organization Persons. NOTE 2 An organization Person is deemed to represent and act on behalf of the organization and to do so in a specified capacity. NOTE 3 An organization Person can be a "natural person" such as an employee or officer of the organization. NOTE 4 An organization Person can be a legal person, i.e., another organization.	Personne d'organisation	02	**partie d'une organisation** qui a les propriétés d'une **Personne** et est ainsi capable de prendre des **engagements** au nom de cette **organisation** NOTE 1 Une organisation peut avoir une ou plusieurs Personnes d'organisation. NOTE 2 Une Personne d'organisation est considérée représenter une organisation et agir en son nom, et ce à titre de capacité spécifiée. NOTE 3 Une Personne d'organisation peut être une «personne physique» telle qu'un employé ou un agent de l'organisation. NOTE 4 Une Personne d'organisation peut être une personne morale, c.à-d. une autre organisation.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.095	ISO/IEC 14662: 2010 (3.24)	Person	99	**entity**, i.e., a natural or legal person, recognized by law as having legal rights and duties, able to make **commitment**(s), assume and fulfil resulting obligation(s), and able of being held accountable for its action(s) NOTE 1 Synonyms for "legal person" include "artificial person", "body corporate", etc., depending on the terminology used in competent jurisdictions. NOTE 2 "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 Minimum and common external constraints applicable to a business transaction often require one to differentiate among three common subtypes of Person, namely "individual", "organization", and "public administration".	Personne	02	**entité**, c-à-d. une personne physique ou morale, reconnue par la loi comme ayant des droits et des devoirs, capable de faire des **engagements**, d'assumer et de remplir les obligations résultantes, et capable d'être tenue responsable de ses actions NOTE 1 Parmi les synonymes de «personne morale», on trouve «personne juridique», «personne fictive», «corporation», etc., selon la terminologie utilisée par les juridictions compétentes. NOTE 2 «Personne» prend la majuscule pour indiquer que ce terme est utilisé tel que défini officiellement dans les normes et pur le différencier de son usage ordinaire. NOTE 3 Les exigences minima et communes applicables aux transactions d'affaires obligent souvent à faire une différence entre les trois sous-catégories communes de «Personne», notamment «individu», «organisation», «administration publique».
3.096	ISO/IEC 15944-1: 2011 (3.48)	Person authentication	99	provision of the assurance of a **recognized Person identity** (**rPi**) (sufficient for the purpose of the **business transaction**) by corroboration	Authentifi-cation d'une Personne	02	don de l'assurance de l'**identité d'une Personne reconnue (rPi)** (suffisante aux fins de la **transaction d'affaires**) par corroboration
3.097	ISO/IEC 15944-1: 2011 (3.51)	persona	99	set of **data elements** and their values by which a **Person** wishes to be known and thus identified in a **business transaction**	persona	01	série d'**éléments de données** et leurs valeurs selon lesquelles une **Personne** désire être connue et ainsi identifiée dans une **transaction d'affaires**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.098	ISO/IEC 15944-1: 2011 (3.52)	persona Registration Schema (pRS)	99	formal **definition** of the **data** fields contained in the specification of a **persona** of a **Person** and the allowable contents of those fields, including the **rules** for the assignment of **identifiers**. (This may also be referred to as a **persona** profile of a **Person**)	schéma d'enregis-trement d'une persona (pRS)	02	**définition** officielle des champs de **données** contenus dans la description d'une **persona** d'une **Personne**, et du contenu autorisé de ces champs, y-compris les **règles** d'attribution des **identifiants**. (Cette notion peut également être désignée comme le profil **persona** d'une **Personne**)
3.099	ISO/IEC 15944-5: 2008 (3.103)	personal information	99	any information about an identifiable **individual** that is recorded in any form, including electronically or on paper NOTE Some examples would be recorde information about a person's religion, age, financial transactions, medical history, address, or blood type.	renseigne-ments personnels	01	tout renseignement au sujet d'un **individu** identifiable, qui est enregistré sous une forme quelconque, y compris électroniquement ou sur papier NOTE Cela comprend, par exemple, les information enregistrée à propos de la religion, de l'âge, des opérations financières, du passé médical, de l'adresse ou du groupe sanguin de quelqu'un.
3.100	ISO/IEC 15944-1: 2011 (3.49)	Person identity (Pi)	99	combination of **persona information** and **identifier** used by a **Person** in a **business transaction**	identité d'une Personne (Pi)	01	combinaison de l'**information** d'une **persona** et de l'**identificateur** utilisé par une **Personne** dans une **transaction d'affaires**
3.101	ISO/IEC 15944-1: 2011 (3.50)	Person signature	99	signature, i.e., a **name** representation, distinguishing mark or usual mark, which is created by and pertains to a **Person**	signature d'une Personne	01	signature, c.-à-d.la représentation d'un **nom**, marque de distinction ou marque habituelle, qui est créée par une **Personne** et se rapporte à celle-ci
3.102	ISO/IEC 15944-8 (3.102)	personal information filing system	99	any structured set of personal information which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis	système de classement des informations personnelles	01	tout ensemble structuré d'**informations personnelles** accessible en fonction de critères spécifiques, que l'accès soit centralisé, décentralisé ou dispersé, sur une base fonctionnelle ou géographique

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.103	ISO/IEC 15944-2: 2006 (3.80)	physical address	99	**address** that is used/recognized by a postal authority and/or courier service to deliver information item(s), material **object**(s), or **business object**(s) to a **Contact** at either an actual **address** or a pick-up point **address**, (e.g., P.O. Box, rural route, etc.)	adresse physique	02	**adresse** qui est utilisée/reconnue par une autorité postale et/ou un service de messagerie pour livraison d'article(s) d'information, d'**objet**(s) matériel(s), ou d'**objet**(s) **d'affaires** à un **Contact**, soit à une **adresse** réelle, soit à une **adresse** de point de ramassage, (par ex. une boîte postale, une route rurale, etc.)
3.104	ISO/IEC 15944-5: 2008 (3.104)	pivot code set	99	set of **ID codes** in a **coded domain** which is made publicly known and available, the most stable, representing the defined semantics. (Most often it is the same as the **ID code**) NOTE 1 The use of the pivot code set as distinguished from the ID code supports the requirement of a Source Authority to maintain internally and on a confidential basis the ID code of its members. NOTE 2 At times a coded domain has more than one valid code set, (e.g., ISO 639, ISO 3166, etc.). EXAMPLE In ISO 3166-1 the 3-digit numeric code is the pivot. The 2-alpha and 3-alpha code sets can change when the name of the entity referenced is changed by that entity.	ensemble de codes pivots	01	ensemble de **codes ID** dans un **domaine codé** qui est rendu public et disponible, le plus stable représentant la sémantique définie. (Le plus souvent, c'est le même que le **code ID**) NOTE 1 L'utilisation de l'ensemble de codes pivots différent du code ID appuie les exigences d'une Autorité de source pour conserver à l'interne et confidentiellement le code ID de ses membres. NOTE 2 Parfois, un domaine codé a plus d'un ensemble de codes valides (par ex. l'ISO 639, l'ISO 3166, etc.). EXEMPLE Dans l'ISO 3166-1, le code numérique à 3 chiffres est le code pivot. L'ensemble des codes alphabétique à 2 lettres et alphabétique à 3 lettres peut changer lorsque le nom de l'entité référencée est changé par cette entité.
3.105	ISO/IEC 15944-5: 2008 (3.105)	pivot ID code	99	most stable **ID code** assigned to identify a member of a **coded domain** where more than one **ID code** may be assigned and/or associated with a member of that **coded domain**	code ID pivot	01	**code ID** le plus stable attribué pour identifier un membre d'un **domaine codé** lorsque plusieurs **code**s ID peuvent être attribués et/ou rattachés à un membre de ce **domaine codé**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				EXAMPLE ISO 3166-1:2006 (E/F) "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes/Codes pour la représentation des noms de pays et de leur subdivisions - Partie 1: Codes pays" contains three code sets: - a three digit numeric code; - a two alpha code - a three alpha code. Here, the three digit numeric code serves as the pivot code. It is the most stable, remains the same even though the two alpha and/or three alpha codes may and do change.			EXEMPLE L'ISO 3166-1:2006 (E/F) «Codes for the representation of names of countries and their subdivisions - Part 1: Country codes/Codes pour la représentations des noms de pays et de leur subdivisions - Partie 1: Codes pays» contient trois ensembles de codes: - un code numérique à trois chiffres; - un code alphabétique à deux lettres; et, - un code alphabétique à trois lettres. Dans ce cas, le code numérique à trois chiffres sert de code pivot. C'est le plus stable, il reste le même, même si les codes alphabétiques à deux et trois lettres peuvent changer (comme cela se produit).
3.106	ISO/IEC 15944-2: 2006 (3.81)	principle	99	fundamental, primary assumption and quality which constitutes a source of action determining particular objectives or results NOTE 1 A principle is usually enforced by rules that affect its boundaries. NOTE 2 A principle is usually supported through one or more rules. NOTE 3 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.	principe	01	hypothèse fondamentale et primaire, et qualité qui constitue une source d'action pour déterminer des objectifs ou des résultats particuliers NOTE 1 Un principe est habituellement mis en vigueur par des règles qui touchent ses limites. NOTE 2 Un principe est habituellement soutenu par une ou plusieurs règles. NOTE 3 Un principe fait habituellement partie d'un ensemble de principes qui ensemble forment un tout unifié. EXEMPLE Dans un domaine juridique, une charte, une constitution, etc., sont des exemples d'un ensemble de principes.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.107	ISO/IEC 15944-8 (3.107)	privacy collaboration space (PCS)	99	modelling or inclusion of an **Open-edi scenario** of a **collaboration space** involving an **individual** as the **buyer** in a potential or actualized **business transaction** where the **buyer** is an **individual** and therefore privacy protection requirements apply to personal information of that individual provided in that **business transaction**	espace de collaboration sur la vie privée	02	modélisation ou inclusion d'un **scénario d'edi-ouvert** d'un **espace de collaboration** concernant un **individu** comme **acheteur** dans une **transaction d'affaires** potentielle ou actualisée dans laquelle l'**acheteur** est un **individu,** et où par conséquent des exigences de protection de la vie privée s'appliquent à l'information personnelle sur cet individu fournie dans cette **transaction d'affaires**
3.108	ISO/IEC 15944-5: 2008 (3.109)	privacy protection	99	set of **external constraints** of a **jurisdictional domain** pertaining to **recorded information** on or about an identifiable **individual**, i.e., **personal information**, 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 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 Privacy requirements include the right of an individual to be able to view the recorded information about him/her and to request corrections to the same in order to ensure that such recorded information is accurate and up-to-date.	protection de la vie privée	01	ensemble de **contraintes externes** exercées sur un **domaine juridictionnel** relatives à l'**information enregistrée** ou à propos d'un **individu** identifiable, c.-à.-d. de l'**information personnelle**, en ce qui concerne la création, la collecte, la gestion, la rétention, l'accès et l'utilisation et/ou la distribution d'une telle **information enregistrée** relative à cet **individu**, y compris son exactitude, son opportunité et sa pertinence NOTE 1 L'information enregistrée recueillie ou créée dans un but spécifique concernant un individu identifiable (c.-à.-d. le but partagé et explicite de la transaction d'affaires concernant un individu) ne peut être utilisée dans un autre but sans le consentement explicite et informé de l'individu auquel l'information enregistrée se rapporte.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 3 Where jurisdictional domains have legal requirements which override privacy protection requirements these must be specified, (e.g., national security, investigations by law enforcement agencies, etc.).			NOTE 2 Les exigences en matière de vie privée incluent le droit d'un individu de pouvoir examiner l'information enregistrée le (ou la) concernant, et de demander d'y apporter des corrections afin de s'assurer que l'information enregistrée est exacte et à jour. NOTE 3 Lorsque des domaines juridictionnels ont des exigences légales qui ont préséance sur les exigences en matière de protection de la vie privée (par ex. la sécurité nationale, les enquêtes policières, etc.), ils doivent être spécifiés.
3.109	ISO/IEC 15944-8 (3.109)	privacy protection officer (PPO)	99	**organization Person** authorized by the **organization** to act on behalf of that **organization** and entrusted by the **organization** as the officer responsible for the overall governance and implementation of the privacy protection requirements for information life cycle management not only within that **organization** but also with respect to any **electronic data interchange** of **personal information** on the **individual** concerned with parties to the **business transaction**, including a **regulator** where required, as well as any **agents**, **third parties** involved in that **business transaction**	officier responsable de la protection des données personnelles	02	**Personne d'organisation** autorisée par l'**organisation** à agir au nom de cette **organisation** et mandatée par l'**organisation** comme officier responsable de la gouvernance et de l'application des exigences de protection de la vie privée pour la gestion du cycle de vie de l'information à l'intérieur de l'**organisation** et dans les opérations **d'échanges de données informatisés** contenant des **informations personnelles** sur un **individu** concerné par les tiers d'une **transaction d'affaires** incluant un **régulateur** selon le besoin, ainsi que tous **agents** ou **tiers** impliqués dans une **transaction d'affaires**
3.110	ISO/IEC 15944-1: 2011 (3.53)	process	99	series of actions or events taking place in a defined manner leading to the accomplishment of an expected result	processus	01	série d'actions ou d'événements qui se produisent d'une manière définie et qui aboutissent à un résultat attendu

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.111	ISO/IEC 15944-8 (3.111)	processing of personal information	99	any operation or set of operations which is performed upon personal data, 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 or destruction	traitement d'informations personnelles	01	toute opération (ou ensemble d'opérations) réalisée sur des données personnelles, par des moyens automatiques ou non, tels que la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou l'altération, l'extraction, la consultation, l'usage, la divulgation par transmission, la dissémination, ou tout autre pratique rendant disponibles, alignant ou combinant, bloquant ou détruisant ces informations personnelles
3.112	ISO/IEC 11179-1: 2004 (3.3.29)	property	99	peculiarity common to all members of an **object class**	propriété	01	particularité commune à tous les membres d'une **classe d'objets**
3.113	ISO/IEC 15944-8 (3.114)	pseudonym	99	use of a **persona** or other **identifier** by an **individual** which is different from that used by the **individual** with the intention that it be not linkable to that **individual** NOTE Adapted from ISO TS 25237.	pseudonyme	01	utilisation d'une **persona** ou d'un autre **identificateur** par un **individu** qui est différent de celle qui est utilisée par l'**individu** dans l'intention de ne pas pouvoir établir de lien avec cet individu NOTE Adapté de l'ISO TS 25237.
3.114	ISO/IEC 15944-8 (3.115)	pseudonymm-ization	99	particular type of anonymization that removes the associate with an **individual** and adds an associate between a particular set of **characteristics** relating to the **individual** and one more **pseudonym** NOTE Adapted from ISO TR 25237.	pseudonym-misation	02	type particulier d'anonymisation qui supprime le correspondant avec un **individu** et ajoute un correspondant entre un ensemble particulier de **caractéristiques** se rapportant à cet individu et un autre **pseudonyme** NOTE Adapté de l'ISO TS 25237.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.115	ISO/IEC 15944-1: 2011 (3.54)	public administration	99	**entity**, i.e., a **Person**, which is an **organization** and has the added **attribute** of being authorized to act on behalf of a **regulator**	administration publique	01	**entité**, c.-à-d. une **Personne**, qui est une **organisation** et a l'**attribut** supplémentaire d'être autorisé à agir au nom d'une **autorité de réglementation**
3.116	ISO/IEC 15944-5: 2008 (3.113)	public policy	99	category of **external constraints** of a **jurisdictional domain** specified in the form of a right of an **individual** or a requirement of an **organization** and/or **public administration** with respect to an **individual** pertaining to any exchange of **commitments** among the parties concerned involving a good, service and/or right including information management and interchange requirements NOTE 1 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 15944-1:2002} NOTE 2 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 (13) 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.	politique publique	01	catégorie de **contraintes externes** d'un **domaine juridictionnel** spécifié sous la forme d'un droit d'un **individu** ou d'une exigence exercée sur une **organisation** et/ou une **administration publique** en ce qui concerne un **individu** relatif à tout échange d'**engagements** entre les parties concernées à propos d'un bien, d'un service et/ou d'un droit, y compris les exigences en matière de gestion de l'information et d'échange NOTE 1 Des exigences en matière de politique publique peuvent s'appliquer à l'une ou à toutes les combinaisons des activités fondamentales touchant une transaction d'affaires, c.-à.-d. la planification, l'identification, la négociation, l'actualisation et la post-actualisation. {Voir plus loin la Clause 6.3 «Règles régissant la composante de processus» dans l'ISO/IEC 15944-1:2002} NOTE 2 Il appartient à chaque domaine juridictionnel de déterminer si l'âge d'un individu qualifie une exigence en matière de politique publique (par ex. celles qui s'appliquent spécifiquement à un individu de moins de treize (13) ans en tant qu'«enfant», celles qui exigent qu'un individu ait atteint l'âge adulte, (par ex. 18 ou 21 ans), pour qu'un individu soit en mesure de prendre un engagement d'une certaine nature.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 3 Jurisdictional domains may have consumer protection or privacy requirements which apply specifically to individuals who are considered to be "children", "minors", etc. (e.g. those who have not reached their 18th or 21st birthday according to the rules of the applicable jurisdictional domain).			NOTE 3 Des domaines juridictionnels peuvent avoir des exigences en matière de protection du consommateur ou de la vie privée qui s'appliquent spécifiquement à des individus qui sont considérés comme des «enfants» ou des «mineurs», etc. (c.-à.-d. ceux qui n'ont pas encore atteint leur 18e ou 21e anniversaire de naissance conformément aux règles du domaine juridictionnel applicable).
3.117	ISO/IEC 15944-8 (3.117)	publicly available personal information	99	**personal information** about an **individual** that the **individual** knowingly makes or permits to be made available to the public, or is legally obtained and accessed from: (a) government records that are available to the public; or, (b) information required by law to be made available to the public EXAMPE 1 Examples of 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, etc. EXAMPLE 2 Examples of 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	information personnelle d'accès public (IPPI)	01	**information personnelle** sur un i**ndividu** que celui-ci produit délibérément ou autorise de rendre accessible, ou qui est obtenue légalement par accès: (a) aux documents gouvernementaux accessibles au public; ou, (b) à l'information que la loi prévoit de rendre publique EXEMPLE 1 L' information personnelle qu'un inidividu fournit ou dont il autorise délibérément la diffusion inclut ainsi les annuaires téléphoniques publics, les publicités dans la presse, les documents publiés, les articles sur internet de cette nature, etc. EXEMPLE 2 Les documents gouvernementaux publiquement accessibles tels que les listes électorales, les transactions sur les propriétés, ou toute autre information personnelle qu'un domaine juridictionnel exige pour être rendue publique.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.118	ISO/IEC 15944-8 (3.118)	recognized individual identity	99	identity of an **individual,** i.e., **individual identity**, established to the extent necessary for the specific purpose of a business transaction	identité individuelle reconnue (RII)	02	Identité d'un **individu**, c.-à.-d. **identité individuelle** établie avec la portée nécessaire au besoin spécifique d'une **transaction d'affaires**
3.119	ISO/IEC 15944-5: 2008 (3.114)	recognized individual name (RIN)	99	**persona** of an **individual** having the properties of a **legally recognized name** (**LRN**) NOTE 1 On the whole, a persona presented by an individual should have a basis in law (or recognized jurisdictional domain) in order to be considered as the basis for a recognized individual name (RIN). NOTE 2 An individual may have more than one RIN and more than one RIN at the same time. NOTE 3 The establishment of a RIN is usually accompanied by the assignment of a unique identifier, i.e. by the jurisdictional domain (or public administration) which recognizes the persona as a RIN.	nom reconnu d'individu (NRI)	01	**persona** d'un **individu** ayant les propriétés d'un **nom reconnu légalement (LRN)** NOTE 1 En définitive, une persona présentée par un individu doit avoir une base légale (ou un domaine juridictionnel reconnu) pour être considérée comme base d'un nom reconnu d'individu (NRI). NOTE 2 Un individu peut avoir plus d'un NRI ou plus d'un nom reconnu d'individu en même temps. NOTE 3 L'établissement d'un nom individuel reconnu s'accompagne généralement de l'attribution d'un identificateur unique par le domaine juridictionnel (ou l'administration publique) qui reconnaît la persona comme nom reconnu d'individu (NRI).
3.120	ISO/IEC 15944-1: 2011 (3.55)	recognized Person identity (rPi)	99	identity of a **Person**, i.e., **Person identity**, established to the extent necessary for a specific purpose in a **business transaction**	identité d'une Personne reconnue (rPi)	01	identité d'une **Personne**, c-à-d l'**identité d'une Personne**, établie selon les besoins nécessaires d'une **transaction d'affaires** dans un but spécifique
3.121	ISO/IEC 15944-1: 2011 (3.56)	recorded information	99	any **information** that is recorded on or in a **medium** irrespective of form, recording **medium** or technology used, and in a manner allowing for storage and retrieval	information enregistrée	02	toute **information** enregistrée sur ou dans un **support** quelle que soit sa forme, le **support** de stockage ou la technologie utilisés, et de façon à permettre son stockage et son extraction

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 1 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 Through the use of the term "information," all attributes of this term are inherited in this definition. NOTE 3 This definition covers: (i) any form of recorded information, means of recording, and any medium on which information can be recorded; and, (ii) all types of recorded information including all data types, instructions or software, databases, etc.			NOTE 1 Cette définition est générique et indépendante de toute ontologie, (par exemple le point de vue des «faits» par rapport aux «données», à «l'information», aux «renseignements», à la «connaissance», etc.). NOTE 2 Dans l'utilisation du terme «information», tous les attributs de ce terme sont hérités dans cette définition. NOTE 3 Cette définition couvre les élément suivants: i) toute forme d'information enregistrée, tout moyen d'enregistrement, et tout support sur lequel l'information peut être enregistrée; et, (ii) tous types d'information enregistrée, y compris tous les types de données, instructions ou logiciels, bases de données, etc.
3.122	ISO 19135: 2005 (4.1.9)	register	99	set of files containing **identifiers** assigned to items with descriptions of the associated items	registre	01	ensemble de fichiers contenant des **identificateurs** attribués à des articles avec une description des articles qui s'y rattachent
3.123	ISO/IEC 15944-2: 2006 (3.95)	registration	99	**rule**-based **process**, explicitly stated, involving the use of one or more **data elements**, whose value (or combination of values) are used to identify uniquely the results of assigning an **OeRI**	enregis-trement	01	**processus** à base de **règles**, énoncé explicitement, impliquant l'utilisation d'un ou de plusieurs **éléments de données**, dont la valeur (ou la combinaison de valeurs) sert à identifier uniquement les résultats de l'attribution d'un **OeRI**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.124	ISO/IEC 15944-1: 2011 (3.57)	Registration Authority (RA)	99	**Person** 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**)	organisme d'enregistre-ment (RA)	02	**Personne** responsable du maintien d'un ou de plusieurs **schémas d'enregistrement (RS),** y compris l'attribution d'un **identificateur** unique pour chaque **entité** reconnue d'un **schéma d'enregistrement** (**RS**)
3.125	ISO/IEC 11179-1: 2004 (3.3.32)	Registration Authority Identifier (RAI)	99	**identifier** assigned to a **Registration Authority** (**RA**)	Idendificateur d'Autorité d'enregis-trement (RAI)	01	**identificateur** attribué à une autorité d'**enregistrement** (**RA**)
3.126	ISO/IEC 15944-1: 2011 (3.58)	Registration Schema (RS)	99	formal **definition** of a set of **rules** governing the **data** fields for the description of an **entity** and the allowable contents of those fields, including the **rules** for the assignment of **identifiers**	schéma d'enregis-trement (RS)	01	**définition** officielle d'un ensemble de **règles** régissant les champs de **données** pour la description d'une **entité** ainsi que le contenu autorisé de ces champs, y-compris les **règles** d'attribution des **identifiants**
3.127	ISO/IEC 15944-8 (3.127)	Registration Schema (based)-recognized individual identity (RS-rii)	99	**Registration Schema (based) –recognized individual identity (RS-rii)** **recognized individual identity (rii)** for use in a **business transaction**, by the buyer as an **individual**, which is one based on the use by an **individual** as a member of a specified **Registration Schema (RS**) of a particular **Registration Authority (RA)**	identité individuelle reconnue basée sur un schéma d'enregis-trement (RS-rii)	02	**identité individuelle reconnue (rii)** à utiliser dans une **transaction d'affaires** par un acheteur à titre d'**individu**, qui est basée sur l'utilisation par un **individu** en tant que membre d'un **schéma d'enregistrement (RS)** spécifié d'une **autorité d'enregistrement (RA)** particulière
3.128	ISO/IEC 15944-2: 2006 (3.99)	registry	99	information system on which a **register** is maintained	registre	01	système d'information sur lequel est maintenu un **registre**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.129	ISO/IEC 15944-1: 2011 (3.59)	regulator	99	**Person** who has authority to prescribe **external constraints** which serve as **principles**, policies or **rules** governing or prescribing the behaviour of **Persons** involved in a **business transaction** as well as the provisioning of goods, services, and/or rights interchanged	autorité de réglemen-tation	02	**Personne** autorisée à prescrire des **contraintes externes** qui servent de **principes**, de politiques ou de **règles** régissant ou prescrivant le comportement des **Personnes** concernées par une **transaction d'affaire**, ainsi que la fourniture des biens, services et/ou droits échangés
3.130	ISO/IEC 15944-5: 2008 (3.124)	regulatory business transaction (RBT)	99	class of **business transactions** for which the explicitly shared goal has been established and specified by a **jurisdictional domain**, as a **Person** in the **role** of a **regulator** NOTE 1 A regulatory business transaction (RBT) can itself be modelled as a stand-alone business transaction and associated scenario(s). For example, the filing of a tax return, the making of a customs declaration, the request for and issuance of a license, the provision of a specified service of a public administration, a mandatory filing of any kind with a regulator, etc. NOTE 2 A regulatory business transaction (modelled as a scenario) can form part of another business transaction. NOTE 3 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 A RBT may require or prohibit the use of an agent or third party.	transaction d'affaires réglementaire (RBT)	01	classe de **transaction d'affaires** pour laquelle l'objectif partagé explicitement a été établi et spécifié par un **domaine juridictionnel** , à titre de **Personne** dans le **rôle** d'une **autorité de réglementation** NOTE 1 Une transaction d'affaires réglementaire (RBT) peut elle-même être modélisée comme transaction d'affaires autonome, et comme scénarios connexes. Par exemple, une déclaration de revenu, une déclaration de douane, une demande de délivrance de permis, une disposition d'un service spécifique d'une administration publique, une déclaration obligatoire de toute nature auprès d'une autorité de réglementation, etc. NOTE 2 Une transaction d'affaires réglementaire (modélisée comme scénario) peut faire partie d'une autre transaction d'affaires. NOTE 3 Une transaction d'affaires réglementaire peut ne s'appliquer qu'à un vendeur, un acheteur, ou au deux, ainsi qu'à n'importe quelle combinaison de parties dans une transaction d'affaires. NOTE 4 Une transaction d'affaires réglementaire peut exiger ou prohiber l'utilisation d'un agent ou d'un tiers de confiance.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 5 A regulatory business transaction (RBT) may be specific to the nature of the good, services and/or right forming part of a business transaction.			NOTE 5 Une transaction d'affaires réglementaire (RBT) peut être spécifique à la nature du bien, des services et/ou du droit faisant partie d'une transaction d'arffaires.
3.131	ISO/IEC 2382-12: 1988 (12.04.01)	retention period	99	length of time for which **data** on a **data medium** is to be preserved	période de rétention	01	durée pendant laquelle des **données** enregistrées sur un **support de données** doivent être conservées
3.132	ISO/IEC 14662: 2010 (3.25)	role	99	specification which models an external intended behaviour (as allowed within a **scenario**) of an **Open-edi Party**	rôle	01	spécification qui modélise le comportement externe attendu d'un **partenaire** d'**EDI-ouvert** dans le cadre permis par un **scénario**
3.133	ISO/IEC 15944-2: 2006 (3.101)	rule	99	statement governing conduct, procedure, conditions and relations NOTE 1 Rules specify conditions that must be complied with. These may include relations among objects and their attributes. NOTE 2 Rules are of a mandatory or conditional nature. NOTE 3 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: - content of the information flows in the form of precise and computer-processable meaning, i.e. the semantics of data; and, - the order and behaviour of the information flows themselves.	règle	02	énoncé régissant une conduite, une procédure, des conditions ou des rapports NOTE 1 Les règles spécifient les rapports entre les objets et leurs attributs. NOTE 2 Les règles sont de nature obligatoire ou conditionnelle. NOTE 3 Les règles spécifient formellement les engagements et le(s) rôle(s) des parties concernées, et le(s) comportement(s) prévu(s) des parties concernées tels que perçus par d'autres parties concernées par des transactions (électroniques) d'affaires. Ces règles s'appliquent aux éléments suivants: - contenu des flux d'information sous forme de signification précise et traitable par ordinateur, c-à-d. la sémantique des données; et, - l'ordre et le comportement des flux d'information eux-mêmes.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 4 Rules must be clear and explicit enough to be understood by all parties to a business transaction. Rules also must 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)". NOTE 5 Specification of rules in an Open-edi business transaction should be compliant with the requirements of ISO/IEC 15944-3 "Open-edi Description Techniques (OeDT)".			NOTE 4 Les règles doivent être suffisamment claires et explicites pour être comprises par toutes les parties d'une transaction d'affaires. En même temps, les règles doivent pouvoir être spécifiées en utilisant une ou des technique(s) de description formelle(s) (FDT). EXEMPLE L'une des techniques de description formelles actuellement et couramment utilisées est l'UML (Langage de modélisation unifié ou Unified Modelling Language). NOTE 5 Les spécficiations des règles dans une transaction d'affaires EDI-ouvert doivent être conformes aux exigences de l'ISO/IEC 15944-3 «Techniques de description de l'EDI-ouvert (OeDT)».
3.134	ISO/IEC 15944-2: 2006 (3.102)	rulebase	99	pre-established set of **rules** which interwork and which together form an autonomous whole NOTE One considers a rulebase to be to rules as database is to data.	base de règles	02	ensemble préétabli de **règles** qui s'appliquent en concordance et qui ensemble forment un tout autonome NOTE On considère qu'une base de règles est aux règles ce qu'une base de données est aux données.
3.135	ISO/IEC 15944-2: 2006 (3.107)	SC identifier	99	unique, linguistically neutral, **unambiguous**, referencable **identifier** of a **Semantic Component**	identificateur de composante sémantique	01	**identificateur** unique, linguistiquement neutre, **non ambiguë** et référencable d'une **composant sémantique**
3.136	ISO/IEC 14662: 2010 (3.26)	scenario attribute	99	formal specification of information, relevant to an **Open-edi scenario** as a whole, which is neither specific to **roles** nor to **Information Bundles**	attribut de scénario	01	spécification formelle d'une information d'intérêt pour la globalité d'un **scénario d'EDI-ouvert**, qui ne ressortit spécifiquement ni aux **rôles** ni aux **faisceaux d'informations**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.137	ISO/IEC 15944-2: 2006 (3.104)	scenario component	99	one of the three fundamental elements of a scenario, namely **role**, **information bundle**, and **semantic component**	composante de scénario	02	l'un des trois éléments fondamentaux d'un scénario, nommément le **rôle**, le **faisceau d'informations**, et la **composante sémantique**
3.138	ISO/IEC 15944-2: 2006 (3.105)	scenario content	99	**set of recorded information** containing **registry** entry **identifiers**, labels and their associated **definitions** and related **recorded information** posted (or reposted) in any **registry** for **business objects**	contenu de scénario	01	**ensemble d'information enregistrée** contenant les **identificateurs** d'entrée de **registre**, les labels, leurs **définitions** connexes, et l'**information enregistrée** connexe publiée (ou republiée) dans tout **registre d'objets** d'**affaires**
3.139	ISO/IEC 15944-2: 2006 (3.106)	scenario specification attribute	99	any **attribute** of a scenario, **role**, **information** bundle, and/or **semantic component**	attribut de specification de scénario	01	tout **attribut** d'un scénario, d'un rôle, d'un **faisceau d'informations**, et/ou d'une **composante sémantique**
3.140	ISO/IEC 15944-1: 2011 (3.62)	seller	99	**Person** 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	vendeur	01	**Personne** qui vise à fournir, volontairement ou suite à une demande, un bien, un service et/ou un droit à une autre **Personne**, et qui reçoit en retour une valeur équivalente acceptable, habituellement en argent
3.141	ISO/IEC 14662: 2010 (3.27)	Semantic Component (SC)	99	unit of **recorded information** unambiguously defined in the context of the **business** goal of the **business transaction** NOTE A SC may be atomic or composed of other SCs.	composante sémantique (SC)	02	unité d'**information enregistrée** définie de manière non ambigué dans le contexte de l'objectif d'**affaires** d'une **transaction d'affaires** NOTE Un SC peut être atomique ou composé d'autres SC.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.142	ISO/IEC 15944-5: 2008 (3.136)	semantic identifier (SI)	99	IT-interface **identifier** for a **semantic component** or other semantic for which (1) the associated context, applicable **rules** and/or possible uses as a semantic are predefined and structured and the **Source Authority** for the applicable **rulebase** is identified (as per Part 5); and (2) for which more than one or more **Human Interface Equivalents**(**HIEs**) exist NOTE 1 The identifier for a Semantic Component (SC), an Information Bundle (IB) and/or an ID Code for which one or more Human Interface Equivalents (HIEs) exist are considered to have the properties or behaviours of semantic identifiers.	identificateur sémantique (SI)	01	**identificateur** d'interface TI d'une **composante sémantique** ou d'une autre sémantique pour lequel (1) le contexte qui s'y rattache, les **règles** applicables et/ou les utilisations possibles comme sémantique sont prédéfinies et structurées, et l'**Autorité de source** de la **base de règles** applicable est identifiée, et (2) existe un ou plusieurs **Équivalents d'interface humaine (HIEs)** NOTE 1 L'identificateur d'une Composante sémantique (SC), d'un Faisceau d'informations (IB) et/ou d'un Code ID pour lequel un ou plusieurs Équivalents d'interface humaine (HIEs) sont considérés comme ayant les propriétés ou les comportements d'identificateurs sémantiques.
3.143	ISO/IEC 15944-5: 2008 (3.137)	set of recorded information (SRI)	99	**recorded information** of an **organization** or **public administration**, which is under the control of the same and which is treated as a unit in its information life cycle NOTE 1 A 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 A 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.	ensemble d'information enregistrée (EIE)	01	**informations enregistrées** relatives à une **organisation** ou à une **administration publique** qui en assure le contrôle et qui sont traitées comme une unité pour ce qui a trait au cycle de vie NOTE 1 Un EIE peut être un enregistrement ou un document physique ou numérique, un dossier, un fichier, etc., qui peut être lu, perçu ou entendu par une personne, un système informatique ou un dispositif semblable. NOTE 2 Un EIE est une unité d'information enregistrée qui est définie sans ambiguïté dans le contexte des objectifs d'affaires de l'organisation, c.-à.-d. une composante sémantique.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 3 A 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.			NOTE 3 Un EIE peut être une unité autonome (atomique). Il peut s'agir de deux EIE ou plus regroupés dans un «nouvel» EIE. Les deux types d'EIE peuvent exister simultanément dans les systèmes de gestion de l'information d'une organisation.
3.144	ISO/IEC 15944-2: 2006 (3.109)	Source Authority (SA)	99	**Person** recognized by other **Persons** as the authoritative source for a set of **constraints** NOTE 1 A Person as a Source Authority for internal constraints may be an individual, organization, or public administration. NOTE 2 A Person as Source Authority for external constraints may be an organization or public administration. EXAMPLE n 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 A Person as an individual shall not be a Source Authority for external constraints. NOTE 4 Source Authorities are often the issuing authority for identifiers (or composite identifiers) for use in business transactions. NOTE 5 A Source Authority can undertake the role of Registration Authority or have this role undertaken on its behalf by another Person. NOTE 6 Where the sets of constraints of a Source Authority control a coded domain, the SA has the role of a coded domain Source Authority.	Autorité de source (AS)	02	**Personne** reconnue par d'autres **Personnes** comme source faisant autorité pour un ensemble de **contraintes** NOTE 1 Une personne comme Autorité de source pour des contraintes internes peut être un individu, une organisation ou une administration publique. NOTE 2 Une personne comme Autorité de source pour des contraintes externes peut être une organisation ou une administration publique. EXEMPLE Dans le domaine du transport aérien, l'IATA, comme Autorité de source, est une « organisation », tandis que l'OACI en tant qu'Autorité de source est une « administration publique ». NOTE 3 Une Personne en tant qu'individu ne peut être une Autorité de source pour des contraintes externes. NOTE 4 Les Autorités de source sont souvent les autorités émettrices des identificateurs (ou des identificateurs composites) à utiliser dans les transactions d'affaires. NOTE 5 Une Autorité de source peut jouer le rôle d'un organisme d'enregistrement ou faire jouer ce rôle à sa place par une autre Personne. NOTE 6 Lorsque l'ensemble de contraintes d'une Autorité de source contrôle un domaine codé, l'AS joue le rôle d'Autorité de source d'un domaine codé.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.145	ISO 1087-1: 2000 (3.1.3)	special language	99	**language** for special purposes (LSP), **language** used in a subject field and characterized by the use of specific linguistic means of expression NOTE The specific linguistic means of expression always include subject-specific terminology and phraseology and also may cover stylistic or syntactic features.	langue de spécialité	02	**langue** spécialisée utilisée dans un domaine et caractérisée par l'utilisation de moyens d'expression linguistique spécifiés NOTE Les moyens d'expression linguistique spécifies incluent toujours une terminologie et une phraséologie propres au domaine et peuvent également couvrir des tournures stylistiques ou syntaxiques.
3.146	ISO/IEC 15944-1: 2011 (3.64)	standard	99	documented agreement containing technical specifications or 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 NOTE 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)}	norme	02	accord documenté contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que **règles**, lignes directrices ou **définitions** de **caractéristiques** pour assurer que des matériaux, produits, **processus** et services sont aptes à leur emploi NOTE Cette définition est la définition «normalisée» par l'ISO et la CEI (et qui se trouve dèsomais dans la Directives de l'ISO/CEI JTC1, Partie 1, Section 2.5:1998). {voir aussi le Guide 2:1996 (1.7) de l'ISO/CEI}
3.147	ISO 1087-1: 2000 (3.4.3)	term	99	**designation** of a defined **concept** in a **special language** by a linguistic expression NOTE A term may consist of one or more words i.e. simple term, or complex term or even contain symbols.	terme	01	**désignation** au moyen d'une unité linguistique d'une **notion** définie dans une **langue de spécialité** NOTE Un terme peut être constitué d'un ou de plusieurs mots (terme simple ou terme complexe) et même de symboles.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.148	ISO/IEC 2382-23: 1994 (23.01.01)	text	99	**data** in the form of **characters**, 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.	texte	01	**données** sous forme de **caractères**, de symboles, de mots, d'expressions, de paragraphes, de phrases, de tableaux ou d'autre arrangements de caractères, ayant une signification particulière, dont l'interprétation dépend essentiellement de la connaissance de la part du lecteur d'un **langage naturel** ou d'un **langage artificiel** EXEMPLE Une lettre commerciale imprimée sur papier ou affichée à l'écran.
3.149	ISO/IEC 15944-1: 2011 (3.65)	third party	99	**Person** besides the two primarily concerned in a **business transaction** who is **agent** of neither and who fulfils a specified **role** or function as mutually agreed to by the two primary **Persons** or as a result of **external constraints** NOTE It is understood that more than two Persons can at times be primary parties in a business transaction.	tierce partie	01	**Personne**, autre que les deux **Personnes** concernées en premier lieu par une **transaction d'affaires** et qui n'est le **mandataire** d'aucune d'elles, et qui joue un **rôle** ou remplit une fonction spécifiés, selon l'accord mutuel des deux **Personnes** concernées en premier lieu, ou le résultat de **contraintes externes** NOTE Il est entendu que plus de deux Personnes peuvent parfois être les parties de première part dans une transaction d'affaires.
3.150	ISO/IEC 15944-5: 2008 (3.144)	treaty	99	international agreement concluded between **jurisdictional domains** in written form and governed by international law NOTE 1 On the whole a treaty is concluded among UN member states.	traité	01	accord international conclu par écrit entre des **domaines juridictionnels** et régi par le droit international NOTE 1 Virtuellement, tous les traités sont conclus entre des états membres de l'ONU.

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
				NOTE 2 Treaties among UN member states when coming into force are required to be transmitted to the Secretariat of the United Nations for registration or filing or recording as the case may be and for publication. {See further Article 80 or the Charter of the UN} NOTE 3 Treaties can also be entered into by jurisdictional domains other than UN member states, i.e., non-members such as international organizations and the rare sub-national units of federations which are constitutionally empowered to do so. NOTE 4 A treaty can be embodied in a single instrument or in two or more related instruments and whatever it particular designations. However, each treaty is a single entity. NOTE 5 Jurisdictional domains can make agreements which they do not mean to be legally binding for reasons of administrative convenience or expressions of political intent only, (e.g., as a Memorandum of Understanding (MOU)). [adapted from the Vienna Convention on the Law of Treaties, 1(a)]			NOTE 2 Les traités entre les états membres de l'ONU, lorsqu'ils entrent en vigueur, doivent être transmis au Secrétariat des nations unies pour être enregistrés et classés ou déposés selon le cas, et publiés. {Voir plus loin l'Article 80 ou la Charte de l'ONU} NOTE 3 Les traits peuvent également être conclus entre des domaines juridictionnels autres que les états membres de l'ONU, c.à.d., des organisations internationales et les rares organismes fédérés infranationaux qui en ont constitutionnellement le pouvoir. NOTE 4 Un traité peut être concrétisé en un seul instrument ou en plusieurs instruments lies et quelles que soient ses appellations particulières. Chaque traité, cependant, est une entité unique. NOTE 5 Des domaines juridictionnels peuvent conclure des accords qu'ils n'ont pas l'intention de rendre légalement obligatoires pour des raisons de commodité administrative ou pour exprimer une intention politique uniquement, (par ex. comme dans le cas d'un protocole d'entente). [adapté de la Convention de Vienne sur le droit des traités, 1(a)]
3.151	ISO/IEC 15944-5: 2008 (3.145)	truncated name	99	short form of a **name** or **persona** of a **Person** resulting from the application of a **rule**-based **truncation process**	nom tronqué	01	forme abrégée du **nom** ou **persona** d'un **Personne** résultant de l'application d'un **processus de troncation** à base de **règle**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.152	ISO/IEC 15944-5: 2008 (3.146)	truncated recognized name (TRN)	99	**truncated name**, i.e., **persona**, of a **Person** which has the properties of a **legally recognized name** (**LRN**) NOTE 1 Truncated recognized name(s) may be required for use in machine-readable travel documents, (e.g., passports or visas), identity tokens, drivers' licenses, medicare cards, etc.). NOTE 2 The source of a truncated recognized name may be a legally recognized name.	nom reconnu tronqué (NRT)	01	**nom** tronqué, c.-à.-d., **persona** d'une **Personne** qui a les propriétés d'un **nom légalement reconnu** (**NLR**) NOTE 1 Un (ou des) nom(s) reconnu(s) tronqué(s) peut(peuvent) être exigé(s) dans l'utilisation des documents de voyage lisibles optiquement (par ex. passeports ou visas, jetons d'identité, permis de conduire, cartes d'assurance-maladie, etc.). NOTE 2 La source d'un nom reconnu tronqué peut être un nom légalement reconnu.
3.153	ISO/IEC 15944-5: 2008 (3.147)	truncation	99	**rule**-base **process**, explicitly stated, for shortening an existing **name** of an **entity** to fit within a predefined maximum length (of **characters**) NOTE Truncation may be required for the use of names in IT systems, electronic data interchange (EDI), the use of labels in packaging, in the formation of a Person identity (Pi), etc.	troncation	01	**processus** à base de **règle**, énoncé explicitement, pour raccourcir le **nom** existant d'une **entité** de façon à ne pas dépasser une longueur de **caractères** maximum prédéfinie NOTE Une troncation peut s'avérer nécessaire pour l'utilisation de noms dans les systèmes TI, l'échange de données informatisées (EDI), les étiquettes d'emballage, la formation de l'identité d'une personne (Pi), l'identité d'une personne reconnue (iPr), etc.
3.154	ISO/IEC 15944-1: 2011 (3.66	unambiguous	99	level of certainty and explicitness required in the completeness of the semantics of the **recorded information** interchanged appropriate to the goal of a **business transaction**	non-ambigu	03	niveau de certitude et d'explicité exigé dans la complétude de la sémantique d'une **information enregistrée** et échangée dans le but d'une **transaction d'affaires**

IT-Interface		Human Interface Equivalent (HIE) Components					
Identification		ISO English (eng)			ISO French (fra)		
Clause 3 ID	Source Ref. ID	Term	G	Definition	Term	G	Definition
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
3.155	ISO/IEC 15944-1: 2011 (3.67)	vendor	99	**seller** on whom **consumer protection** requirements are applied as a set of **external constraints** on a **business transaction** NOTE 1 Consumer protection is a set of explicitly defined rights and obligations applicable as external constraints on a business transaction. NOTE 2 It is recognized that external constraints on a seller of the nature of consumer protection may be peculiar to a specified jurisdictional domain.	fournisseur	01	**vendeur** auquel s'appliquent des exigences de **protection des consommateurs** comme ensemble de **contraintes externes** sur une **transaction d'affaires** NOTE 1 La protection des consommateurs est un ensemble de droits et d'obligations explicitement définis, et qui s'appliquent comme contraintes externes à une transaction d'affaires. NOTE 2 On reconnaît que les contraintes externes, telles que la protection des consommateurs, exercées sur un fournisseur, peuvent relever d'une juridiction particulière.
3.156	ISO 1087-1: 2000 (13.7.2)	vocabulary	99	terminological **dictionary** which contains **designations** and **definitions** for one or more specific subject fields NOTE The vocabulary may be monolingual, bilingual or multilingual.	vocabulaire	01	**dictionnaire** terminologique contenant des **désignations** et des **définitions** tirées d'un ou plusieurs domaines particuliers NOTE Un vocabulaire peut être unilingue, bilingue ou multilingue.

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

B.1 Introduction

This part of ISO/IEC 15944 already makes extensive use of relevant rules and guidelines as found in referenced Clauses in ISO/IEC 15944-1 and adapts them in a privacy protection requirements context. Similarly relevant rules and guidelines found in ISO/IEC 15944-2, ISO/IEC 15944-4, and ISO/IEC 15944-5 have been adapted or serve as the basis for rules of this nature required to support privacy protection requirements.

The purpose of Annex B is to provide a consolidated presentation of all the rules in the existing parts of ISO/IEC 15944 for the scoping and specification of Open-edi scenarios and their components which pertain to external constraints relevant to privacy protection requirements. Jurisdictional domains are the primary source of external constraints. The existing parts of ISO/IEC 15944 address, in an integrated manner, the already many of the requirements arising pertaining to specifying common external constraints of jurisdictional domains which are relevant to privacy protection requirements either in a generic or specific manner.

Only the Rules themselves are presented here. For related text, as well as associated Guidelines, where applicable, see the relevant Clauses in the current editions of Parts of ISO/IEC 15944 identified in the matrixes below.

Also there are parts of ISO/IEC 15944 which do not contain any rules (or guidelines) of relevance to privacy protection requirements. These are:

1) ISO/IEC 15944-4

The primary reason for this is that ISO/IEC 15944-4 focuses on “accounting and economic ontology” at the Person level as parties to a business transaction, i.e., in their roles as buyers, sellers, and/or regulators.

2) ISO/IEC 15944-6

ISO/IEC 15944-6 is of the nature of an ISO/IEC “technical report (TR)” providing a “Technical Introduction to e-Business Modelling. As such, it contains no rules.

B.2 Organization of Annex B: Consolidated list in matrix form

The rules and associated references are presented in matrix form. The rules are presented in the numeric order in which they are presented in ISO/IEC 15944-1. The columns in the matrix are as follows:

Col. No	Use
1	Number of Rule as per ISO/IEC 15944-1.
2	Clause ID in ISO/IEC 15944-1 of which the Rule is part
3	Rule Statement as per ISO/IEC 15944-1 Note: Only text of the Rule itself is presented. For associated guidelines, requirements and text see the relevant clauses in that part of ISO/IEC 15944. All Parts of ISO/IEC 15944 are ISO "freely available standards".

B.3 Consolidated list of rules in ISO/IEC 15944-1 pertaining to external constraints relevant to supporting privacy protection requirements

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
3	6.1.3	In (electronic) business transactions, all commitments shall be stated explicitly and unambiguously and be understood by all Persons involved in a business transaction.
13	6.2.2	The level of unambiguity, i.e., certainty/reliability of a persona and resulting identification of the Person identity used by a Person shall be appropriate to the goal of the business transaction.
15	6.2.2	Business transactions having different goals may allow a Person to use the same persona and its associated identification schema (including resulting identifiers), while others may prohibit this.
27	6.2.4	Unless bound by external constraints, "buyers" and "sellers" as Persons are free to undertake any business transaction involving any good, service, and/or right they mutually agree to.
28	6.2.4	External constraints governing rules and practices of "buyers" and "sellers" in business transactions apply either to Persons (undifferentiated) or distinguish among "individuals", "organizations", and "public administrations".
29	6.2.5	Rights or obligations arising from commitments in a business transaction shall be fulfilled either directly by the Person as the end entity or by an agent acting on its behalf.
30	6.2.5	The ability to delegate a role to an agent shall be explicitly stated. If constraints must be satisfied before such delegation can take place they shall be explicitly stated.
31	6.2.5	Where delegation of a role cannot take place this shall be explicitly stated.
32	6.2.5	A business transaction takes place between two Persons. Other Persons, i.e., third parties, may fulfil specified role(s) or functions(s) on mutual agreement or as a result of external constraints.

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
33	6.2.6	External constraints exist on the provisioning of goods and services and the behaviour of Persons as players in business transactions including those provided via electronic commerce.
34	6.2.7	From a minimal external constraints perspective, the three basic sub-types of Persons as role players in any business scenario are: A. individual, B. organization, and C. public administration.
35	6.2.7	A legal (or artificial) Person consists of one or more natural persons and/or one or more other legal persons. A unifying term and common concept used internationally is the standard term "organization" as the collective common term for all the different ways legal (or artificial) persons can be composed and be recognized in various jurisdictions.
38	6.2.8	From a minimal external constraints perspective, a common set of constraints on a business transaction where the buyer is an individual are those of a consumer protection nature.
39	6.3.1	Conceptually a business transaction can be considered to be constructed from a set of fundamental activities. They are planning, identification, negotiation, actualization and post-actualization.
40	6.3.1	The five fundamental activities may take place in any order.
44	6.4.1	Electronic business transactions require "recorded information".
47	6.4.2	The definition of "data", and related information technology terms and definitions found in this part of ISO/IEC 15944 shall able to be mapped into legal frameworks.
48	6.4.2	Standards development work in support of electronic business transactions shall incorporate and support data granularity requirements. The level of granularity reflects the degree of detail appropriate to the level of certainty required in the data being interchanged among the parties participating in a business transaction.
49	6.5.1	Open-edi scenarios and Information Bundles shall therefore be capable of reflecting constraints to be applied which may be as a result of: - commitments among parties, i.e., as internal constraints; - external constraints.
50	7.2	The requirement for an Open-edi scenario to incorporate external constraints on a business transaction shall be stated at the outset.
51	7.2	It is necessary to state whether the Open-edi Parties in the business transaction being modelled are (a) Persons in general, i.e., undifferentiated; or (b) differentiated among categories of Persons, i.e., subtypes, as individuals, organizations and public administration.

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
57	7.2	If the business transaction being modelled through an Open-edi scenario incorporates external constraints which impact FSV demands on Open-edi Support Infrastructure (OeSI), these shall be specified.
66	8.3.2.4	The set of Roles applicable to the scenario shall be specified and referenced through their Role Identifiers.
67	8.3.2.4	One shall state which roles are mandatory, conditional, or mandatory subject to a conditional.
68	8.3.2.4	Where applicable, constraints on the same Open-edi Party playing more than one of the roles in the set of roles applicable to the OeS shall be specified
70	8.3.2.5	If applicable, one should state which IBs are mandatory, conditional, or mandatory subject to a conditional.
71	8.3.2.5	Where applicable, constraints on IBs pertaining to roles in the OeS shall be specified.
72	8.3.2.6	The business requirements, rules and practices applicable at the scenario level shall be specified. This specification shall be stated at a level of detail to ensure that there is no ambiguity in the commitments among Open-edi Parties at the scenario level.
73	8.3.2.6	Business constraints, if any at the scenario level, pertaining to Open-edi Parties and scenario components shall be specified. All of these shall be accounted for in scenario components, i.e., roles and/or Information Bundles.
74	8.3.2.7	Requirements or constraints arising from applicable laws or regulations at the scenario level shall be explicitly stated including the source jurisdictions.
75	8.3.2.7	Where multiple laws and regulations apply at the scenario level, the constraints applicable shall be integrated.
101	8.4.2.5	Constraints, if any, on an Open-edi Party being able to play a role shall be specified.
103	8.4.2.7	Any external constraints arising from laws or regulations to any aspect of the role and its attributes shall be identified and stated including the reference/source of the applicable law or regulation, i.e., qualifications for a role, prescribed behaviour, restrictions on the delegation of a role, etc.
135	8.5.2.4	Any business rules controlling content of an IB shall be identified and the nature and functioning of these rules explicitly stated. The source of such business rules shall also be referenced.
136	8.5.2.5	Any external constraints arising from laws and regulations governing the content of an IB shall be identified, the requirements explicitly stated and the source referenced.
137	8.5.2.5	Any IB created to meet a requirement of external constraints of the nature of laws and regulations should be so identified, the contents of the IB explicitly defined, at the level of granularity required, and the source law/regulation referenced.

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
140	8.5.2.8	Requirements for retention of recorded information for an IB, if any, shall be specified as well as which OePs involved in the associated role(s) have the primary responsibility for retaining this recorded information
141	8.5.2.9	Requirements arising from laws or regulations for the retention of recorded information applicable to the IB, if any, shall be explicitly stated and the source(s) referenced.
146	8.5.5.1	A Semantic Component can be a single (simple) data element, a composite data element, or a data structure, (e.g., a set of data elements which interwork in order to ensure semantic completeness and ensure the required unambiguousness).
147	8.5.5.1	A Semantic Component shall be a component of at least one Information Bundle when exchanged among Open-edi Parties.
153	8.5.5.2.2	A SC name is the designation of the SC ID by a linguistic expression. More than one SC name as equivalent linguistic expressions may be associated with an SC ID, (e.g., as "aliases").

B.4 Consolidated list of rules in ISO/IEC 15944-2 pertaining to external constraints of relevance to supporting privacy protection requirements

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
2	5.3	The registration of any scenario or scenario component shall be capable of supporting multilingual semantic equivalents at the human interface.
3	5.3	On the while, and from an internal constraints only based perspective, parties to a business transaction are free to choose the language(s) to be used.
9	6.5	Only valid, superseded, and retired OeRIs shall be exposed when the contents of a register are made available to the public.

B.5 Consolidated list of rules in ISO/IEC 15944-5 pertaining to external constraints of relevance to supporting privacy protection requirements

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
002	5.2.1	Unless a particular external constraint governing the commitment made requires that it be made in a specific jurisdictional domain, Persons are free to choose the jurisdictional domain in which the business transaction is (deemed) to take place
003	5.2.3	Depending on the nature of the goods, services or rights being provided (as the goal of the business transaction being modelled), applicable external constraints may specify and require the transaction to be enacted in a specified jurisdictional domain
004	5.2.3	Within a particular jurisdictional domain, it may be required to reference a specific act or regulation as well as require the participation (in some form) of a regulator.
005	5.2.3	For any business transaction (or part thereof) which involves external constraint(s), the role of regulator(s) shall be included and modelled as part of the scenario and scenario components.
006	5.3	The primary source of a regulator having the authority to prescribe external constraints is that of the nature of a jurisdictional domain.
008	5.4	When modelling a business transaction, where one includes external constraints, it is necessary to differentiate among the three common sub-types of Person, namely "individual", "organization" and "public administration". A jurisdictional domain shall be modelled as a "public administration".
016	5.7	An external constraint may specify the "explicitly shared goal" of a business transaction as a whole.
017	6.2.1	It is vital that all parties to a business transaction have a complete and unambiguous understanding, i.e., level of certainty and explicitness required, to ensure that the commitments being entered into are fully and completely understood and agreed upon by all the parties involved.
018	6.2.1	Persons, whether as “individuals” or as “organization Persons” acting on behalf of their organization or public administration (on whose behalf they are qualified and authorized as role players to make commitments), must agree to the language(s) to be utilized in a business transaction, i.e., by all the parties involved, in order to ensure that the semantics of the commitments being entered into are completely understood by all parties involved.
019	6.2.1	Choice of use of language(s) is governed by three primary factors: (1) seller, i.e., supplier choice; (2) buyer, i.e., user, demands; and/or; (3) regulator, i.e., requirements of a jurisdictional domain.
020	6.2.1	In business transactions which are modelled and registered as scenarios and scenario components which involve internal constraints only, the parties involved are free to choose and decide among themselves the natural language(s) to be used for the recorded information in a business transaction.

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
021	6.2.1	In modelling a business transaction which involves internal constraints only, it is advisable that parties concerned use the 3-alpha language code(s) as stated in ISO 639-2/T code set for the identification of the language(s) to be used and/or supported.
022	6.2.2	In business transactions which are modelled (and registered) as scenarios and scenario components, i.e., as business objects, which involve external constraints, one shall specify the official language(s) to be supported based on the requirements of the jurisdictional domain(s) which is the source(s) for these external constraints.
023	6.2.2	In modelling a business transaction (or parts thereof) and registering them as re-useable business objects involving external constraints, these shall be modelled in a manner which supports the language requirements, including a multilingual approach, of the source of such external constraint(s), (e.g., jurisdictional domain(s)).
024	6.2.2	A jurisdictional domain has either an official language(s) or a de facto language.
025	6.2.2	It is for a jurisdictional domain to decide whether or not it has an official language. If not, it will have a de facto language.
026	6.2.2	A law or regulation of a jurisdictional domain may require the use of or the ability to support a specific language within a particular context, i.e., as a “legally recognized language (LRN)”.
027	6.2.3	Where a jurisdictional domain has more than one official language, Persons as suppliers shall be capable of communicating with buyers (particularly as individuals) in any one of the official languages of that jurisdictional domain.
028	6.2.4	A jurisdictional domain may have either one or more official languages and, if not, may have only one “de facto language”.
029	6.2.6	In order to be able to specify the gender of a noun or term used as may be required based on the official (or de facto) language utilized, the set of "Codes Representing Gender in Natural Languages" shall be used in the modelling of a business transaction and registration of any related business object.
030	6.2.6	Where the official language (or de facto language) of a jurisdictional domain has no gender this shall be stated.
031	6.2.7	Where a jurisdictional domain has more than one official language, human interface equivalents (HIEs) are required in each official language in order to ensure unambiguity in the semantics of the commitments made.
032	6.2.7	It is up to a jurisdictional domain to establish HIEs in its official language(s) where these are part of the specification and implementation of external constraints.
033	6.2.8	In order to ensure unambiguity in the use of a natural language in business transactions it is necessary to specify the jurisdictional domain for the varied forms of that natural language to be utilized using common standard default conventions for the unambiguous identification, interworkings and referencing of combinations of codes representing countries, language and currencies.

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
034	6.2.8	In modelling a business transaction through scenarios and scenario components which involve external constraints and for which the Source Authority is a UN member state (or an administrative sub-division of the same), it is advisable that all parties concerned use the 3-digit numeric country code plus the 3-alpha language code, and in this order.
035	6.2.9	The official language of a treaty-based international organization recognized as having primary competence in a specific sector can override the official language requirements of the jurisdictional domains of UN member states.
036	6.2.9	In modelling a business transaction (or parts thereof) as scenarios and scenario components, and registering them as re-useable business objects involving internal constraints, these should be modelled in a manner which supports the language(s) of the source authorities referenced and utilized in such referenced specifications.
037	6.3.2	A common set of external constraints of a jurisdictional domain on a business transaction, where the buyer is an individual, are those of a consumer protection nature.
038	6.3.2	Where the buyer is an individual, the seller shall ascertain that the individual has the age qualification required by the jurisdictional domain to be able to be involved in and make commitments pertaining to the good, service and/or right being offered in the proposed business transaction.
039	6.3.2	A seller shall ensure that where its intends to sell a good, service and/or right to a buyer as an individual that consumer protection requirements of the applicable jurisdictional domain of the buyer are supported.
040		A common set of external constraints of a jurisdictional domain on a business transaction, where the buyer is an individual, are those of a privacy protection nature.
041	6.4	When an external constraint of a jurisdictional domain requires use of a specific identification system with respect to a recognized Person identity (rPi) and/or with respect to a good, service and/or right, pertaining to the business transaction being modelled as scenarios and scenario components as re-useable business objects, such modelling shall be done in a manner which supports the requirement of the identification system referenced.
042	6.5	Where an external constraint of a jurisdictional domain requires the use of a specific classification system and the same forms part of the business transaction being modelled, or as an identifiable and registered scenario component, i.e., as a re-useable business object, this shall be done in a manner which supports the requirements of the classification system being referenced.
043	6.5	Where a classification system uses identifiers for each distinct entry, (with the associated semantics in that classification system), such identifiers (or "composite identifiers") shall be utilized as well as their structure in modelling a scenario or scenario component.
044	6.6.2.2	Any external constraint of a jurisdictional domain which governs, limits or qualifies a Person, a Person sub-type, any role qualification, etc., with respect to a business transaction of a particular nature shall be specified unambiguously and in a

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
		manner so as to be able to be modelled using an OeDT.
045	6.6.2.3	A LRN may have both a long, i.e., complete, persona, or a short, i.e., truncated, persona.
046	6.6.2.3	The formation of a LRN of an incorporated organization, i.e., a legal person, is governed by the rules of the jurisdictional domain in which it is incorporated, registered and recognized as such.
047	6.6.2.3	The establishment and representation of name(s) of a public administration, i.e., its personae, is determined by the jurisdictional domain of which it is part.
048	6.6.2.3	The personae of an individual shall include at least one LRN in order to confirm the existence of that individual as a "natural person", i.e., the birth certificate name (or a similar name).
049	6.6.2.3	The establishment and representation of an individual, i.e., its personae, is determined by the role and context of that individual within a jurisdictional domain, i.e., as controlled by a regulator and the associated public administration.
050	6.6.3	Conceptually a business transaction can be considered to be constructed from a set of fundamental activities. They are planning, identification, negotiation, actualization and post-actualization.
051	6.6.3	The five fundamental activities may take place in any order.
052	6.6.3	A Person may terminate a business transaction by any agreed method of conclusion.
053	6.6.3	The five fundamental sets of activities may be completed in a single continuous interactive dialogue or through multiple sets of interactions among buyer and seller and possibly involve agents or third parties as well.
054	6.6.4.3	An instantiated business transaction shall have one or more IB or SC for which no state changes are permitted. One of these is to serve as the transaction ID number, i.e., a business transaction identifier (BTI), for the instantiated business transaction.
055	6.6.4.5	In the modelling of a business transaction, through a scenario and scenario components, and/or registering them as referenceable and reusable business objects, one shall specify the temporal schema, i.e., date/time referencing system, if one is utilized as well as the level of granularity supported.
056	6.6.4.5	Any calendar, date/time referenced, etc., identified and referenced shall be one based on (or linkable to) an ISO 8601 or ISO 19108 and conformant to the requirements of either one of these two standards.
057	66.4.	Where the Gregorian calendar is utilized, the ISO 8601 compliant representation of 1) a date in a YYYY-MM-DD format ; and, 2) a time of day in an hh:mm:ss format , shall be used.

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
058	6.6.4.5	Where from an IT-system perspective and/or financial system needs perspective, a "GPS calendar clock" or an "atomic clock" is to be used, this shall be specified.
059	7.1	The basic rules for the formation and identification of jurisdictional domains are governed by the Charter of the United Nations and more specifically by the Vienna Convention on the Law of Treaties.
060	7.2	UN member states as peer jurisdictional domains are to be referenced by their 3-digit numeric code as stated by the UN statistical system.
061	7.2	Where the 3-digit numeric code of a UN member state is to be utilized in conjunction with, i.e. required to interwork with (1) a code representing an official (or de facto) language of that jurisdictional domain; (2) a code representing a currency recognized for use in that jurisdictional domain; and/or, (3) both (1) and (2), one shall use the standard default conventions for the identification, interworking and referencing of combinations of codes representing countries, languages and currencies as provided in Annex D.
063	7.3.2	Two jurisdictional domains, of whatever category, can bind themselves in a bilateral treaty, to form a new common jurisdictional domain, either generally or as pertaining to a specified set of goods, services and/or rights
064	7.3.3	Three or more jurisdictional domains, of whatever category, can bind themselves via a plurilateral treaty to form a new jurisdictional domain, either generally or as pertaining to a specified set of goods, services and/or rights.
065	7.3.4	Three or more jurisdictional domains can bind themselves via a multilateral treaty to form a new jurisdictional domain either generally or as pertaining to a specified set of goods, services an/or rights.
066	7.8.2	In order to ensure unambiguous identification in referencing UN member states, the 3-digit numeric codes of the UN Statistical Division representing the UN member state shall be utilized as its primary identifier.
070	8.2	It is important in scoping an Open-edi Scenario to specify at the outset whether or not external constraints apply to the business transaction being modelled.

B.6 Consolidated list of rules in ISO/IEC 15944-7 pertaining to external constraints of relevance to supporting privacy protection requirements

ISO/IEC 15944-7 titled "…*eBusiness Vocabulary"* provides the ISO English and ISO French language equivalents, i.e., as HIEs, for all the definitions of concepts (and associated terms) found in the most recent editions of the ISO/IEC 14662 *Open-edi Reference Model* and ISO/IEC 15944-1, ISO/IEC 15944-2, ISO/IEC 15944-4, and ISO/IEC 15944-6 *Business Operational View.*

Although ISO/IEC 15944-7 is of the nature of a consolidated and integrated "controlled vocabulary", it does contain rules which are relevant from a privacy protection requirements perspective. These are rules which are of the nature of supporting and assuring "unambiguity" in definitions of (key) concepts in the recorded information provided in support of a business transaction where the buyer is an individual and thus privacy protection requirements apply. These rules also support (and facilitate) the provision of HIEs in many a languages. Finally, it is a requirement that any organization or public administration (which is subject to privacy protection requirements) shall make publicly available its privacy protection policy. As such, it is

advised that any definitions in an organization‘s privacy protection policy apply and implement these ISO/IEC 15944-7 rules to support and ensure “unambiguity” in any definitions as well as HIE support.

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
001	5.2	The use of a rule-based and flexible object oriented approach for the eBusiness Vocabulary requires rigorous quality and integrity control of the definitions to ensure that there is no tautology, i.e. circularity, in the full set of concepts defined in the international standard.
002	5.2	In order to ensure a harmonized “system of concepts,” a definition for a concept shall be established as early as possible in the development of the standard.
003	5.2	A concept may be totally atomic or may consist, i.e., inherit, one or more other concepts.
004	5.2	A concept may be part of one or more other concepts.
005	5.2	The presentation for a HIE eBusiness Vocabulary shall be in a form and format as already provided in Annex D, E or F in this part of ISO/IEC 15944.
006	5.3	The set of essential elements of each entry (or record) in the eBusiness Vocabulary, for each defined concept, consists of: (a) the definition (of the concept); (b) the term (representing the concept); (c) the abbreviation of the concept (as applicable); (d) the gender code for the term; (e) the composite identifier (for the concept); and, (f) the internal eBusiness vocabulary identifier.
007	5.3.1	The characteristics (and their unique combination) of a (new) concept shall be identified and agreed to prior to the drafting of a definition for that concept.
008	5.3.1	In the identification of the unique combination of characteristics for a concept, one shall maximize use of those already defined in existing international standards, i.e., where and whenever applicable or relevant.
009	5.3.1	Any concept requiring a definition for the clarity of the understanding and use of the ISO/IEC JTC1 international eBusiness standards shall be included in that standard.
010	5.3.1	There must be 1) a business case and rationale for the need to introduce a (new) concept into an international standard with its resulting definition and assigned term; and, 2) such a business case and rationale must maximize re-use and integration of existing international standards, i.e. those of ISO, IEC, ISO/IEC and/or ITU.
011	5.3.1	The descriptive statement comprising a definition must be clear, explicit and unambiguous and stated in the form of a single sentence.
012	5.3.1	Only a concept with a single definition shall be included and both the definition and associated term shall be stated in the singular.

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
013	5.3.1	Any definition of an eBusiness concept must be developed with two or more human interface equivalencies (HIEs) in order to maximize its unambiguity and subsequent use in support of any and all commitments made among parties to a business transaction.
014	5.3.1	As stated in 5.1, a concept can consist of, i.e. inherit, one or more other concepts. Consequently, where this occurs, the definition for a concept of this nature shall explicitly support this requirement.
015	5.3.1	When a concept incorporates one or more other concepts, the terms representing these concepts shall be included **in bold** in the definition for that concept.
016	5.3.2	The issue of “polysemy” shall be avoided in international standards development.
017	5.3.2	The term chosen to designate a concept and its definition shall be unambiguous and not easily confused with terms representing other concepts.
018	5.3.2	The fact that the primary use of the eBusiness Vocabulary is to support the making of commitments, it is important that the term chose to designate a concept and its definition, is unambiguous and not confused with other concepts (meanings).
019	5.3.2	A term assigned to a definition of a concept is deemed to be a “noun” (or the gerundial form of a noun like “identification”).
020	5.3.3	In the development of a definition for a concept, the committee responsible shall decide as to whether or not an abbreviation or acronym needs to be assigned to the definition of a concept in addition to the term.
021	5.3.4	The gender of each term, as a noun, in the eBusiness Vocabulary shall be specified using Coded Domain ISO/IEC 15944-5:01 “Codes Representing Gender in a Natural Language”.
022	5.3.5	The identifier of any eBusiness Vocabulary entry is of the nature of a composite identifier and shall meet the requirements of “identifier (in business transaction)”.
023	5.3.5	The eBusiness Vocabulary composite identifiers are composed of a minimum set of four discrete and mandatory data elements, consisting of: (a) the source international standard reference for the vocabulary entry; (b) the unique identifier assigned by international standards organization for the standards (c) document including part number where applicable; (d) the date of the standard document as applicable (e) the identifier of the Clause number in the standards document referenced.
024	5.3.5	An eBusiness Vocabulary identifier, as a composite identifier is deemed to be linguistically neutral and as such will have one or more Human Interface Equivalents (HIEs) for the definitions and terms they represent.
025	5.3.6	Each eBusiness Vocabulary identifier shall be assigned an internal unique identifier (as its common pivot code) as part of its entry in Annex D of ISO/IEC 15944-7, i.e., in the form of “Dnnn”. See Annex D.

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
026	5.3.6	Any subsequent, i.e., new, entry to the eBusiness Vocabulary shall be assigned the next available sequential “Dnnn” number.
027	5.4	In the development of a controlled vocabulary for an international standard, or a family of international standards (e.g. as here in the field of eBusiness), one shall maximize use (re-use) of applicable concepts already defined in existing international standards.
028	5.4	Where the term assigned to a defined concept, essential to the identification and referencing of a concept is already in use, the term shall be accompanied by the qualification, (e.g., as for “identifier (in a business transaction))”.
029	6.2	The ISO/IEC JTC1/SC32 P-member bodies working with and through their national body standards organization are responsible in their jurisdictional domains for developing the human interface equivalents (HIEs) of the term/definition of a concept into the official language(s) of that jurisdictional domain as an Annex to this part of ISO/IEC 15944.
030	6.2	Any submission by an ISO/IEC, ISO, IEC and/or ITU P-member body of an Annex of HIEs to this part of ISO/IEC 15944 shall use the template of Clause 9 to specify the criteria governing the presentation of the eBusiness Vocabulary in that language.
031	6.3	Any UN member may submit, via its National Standards body, a new Annex to this part of ISO/IEC 15944 of the eBusiness Vocabulary in the official language(s) of its jurisdictional domain.
032	6.4	It is up to each ISO/IEC JTC1 P-member (or UN member state working via its national standards body), to develop and decide on the development of the HIE definition and assignment of the associated term for each ISO concept.
033	6.4	For the definition of a concept, the ISO/IEC JTC1 P-member body (or UN member state) may use (1) a transliteration of the ISO English (or ISO French) term for that concept in one’s language(s); or, (2) one can coin a new term for that concept.
034	6.4	Where a concept also has an abbreviation for the term in ISO English (or ISO French), the ISO/IEC JTC1 P-member (or UN member state), may (1) use an existing ISO English (or ISO French) abbreviation; or (2) develop a new abbreviation in its language(s).
035	7.0	The structure and presentation of any eBusiness Vocabulary to be added in other languages, i.e., as an Annex to this part of ISO/IEC 15944, shall be considered to be a set of HIE equivalent(s) in the official language(s) of the jurisdictional domain submitting such a new Annex to this part of ISO/IEC 15944.
036	7.0	The submission of such a set of eBusiness Vocabulary entries as a new Annex to this part of ISO/IEC 15944 shall be done in conformance with the rules stated in Clause 6.

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
037	7.0	The structure and representation of any additional eBusiness Vocabulary as an HIE Annex to this part of ISO/IEC 15944 shall conform to one or more of the following options (or combinations thereof): 1) be only in the official language(s) of the submitting ISO/IEC JTC1 P-member body (or UN member state); 2) include an ISO official language, i.e., English, French or Russian, as part of its submission for an Annex, the equivalent language(s) of the jurisdictional domain of the ISO/IEC P-member (or UN member state); 3) where there is more than one writing system for the official language(s) of that jurisdictional domain specify the applicable writing systems.
038	7.0	In support of the above rules, any submission of the addition of a HIE version of an eBusiness Vocabulary, i.e., as an Annex to this part of ISO/IEC 15944 shall be in one of the following formats: (1) the format as presented in Annex D of this ISO/IEC 15944-7(with either unilingual, bilingual or multilingual HIEs); or, (2) the format as per Clause 3 in ISO/IEC 15944-7 (with either unilingual, bilingual, or multilingual HIEs).
039	7.0	Where the official language(s) of an ISO/IEC JTC1 P-member (or UN member state), or any jurisdictional domain includes the use of more than one writing system for the official language(s) of that jurisdictional domain, the submitting ISO/IEC JTC1 P-member or submitting jurisdictional domain shall state in its submission, as a new Annex to ISO/IEC 15944-7 whether it: (a) submits such in only one writing system of its official language; or, (b) submits such an Annex in two (or more) writing systems for representation of its language.
040	7.0	Any structure and presentation of a HIE version of the eBusiness Vocabulary shall contain the mandatory essential elements of such a “controlled vocabulary” as stated in 5.3.
041	7.0	In addition, any eBusiness Vocabulary of a HIE nature, submitted as an added Annex, to this part of ISO/IEC 15944 shall include the, 1) its UN member 3 digit ID code for which the UN is the coded domain Source Authority (cdSA). (This 3 digit code is also repeated in ISO 3166-1); 2) the 3 alpha code(s) of its official language(s) used in the HIE version of the eBusiness Vocabulary provided. The 3 alpha code shall be one based on the ISO 639-2/T set of codes; and, 3) the Annex D entry ID number, (e.g., D125) which serves as the pivot ID code).

Rule No.	Clause ID	Rule Statement
(1)	(2)	(3)
042	8.1	The source for any amendments or additions to the entries in the eBusiness Vocabulary as stated in Annex D of this part of ISO/IEC 15944 shall be either: 1) this part of ISO/IEC 15944 itself; 2) amendments or additions to existing eBusiness standards namely ISO/IEC 14662 or current Parts of ISO/IEC 15944 which are already international standards, i.e., ISO/IEC 15944-1, ISO/IEC 159544-2, ISO/IEC 15944-4, ISO/IEC 15944-5, ISO/IEC 15944-6, and ISO/IEC 15944-7; and/or, 3) new parts of ISO/IEC 15944 which are under development, namely: ISO/IEC 15944-3 and ISO/IEC 15944-8.
043	8.2	A repository of the eBusiness Vocabulary, as an integrated and harmonized controlled vocabulary, shall be maintained for ISO eBusiness standards. Currently, these include ISO/IEC 14662, ISO/IEC 15944-1, ISO/IEC 15944-2, ISO/IEC 15944-4, ISO/IEC 15944-5, ISO/IEC 15944-6, and ISO/IEC 15944-7 eBusiness standard (and ISO/IEC 15944-3, and ISO/IEC 15944-8 which are currently under development).
044	8.2	The eBusiness Vocabulary shall also be maintained in the form of an online computer database.
045	8.3	The form and format for referencing an eBusiness Vocabulary entry is that of “ISO/IEC 15944-7::nnn” where the “nnn” is that of the “nnn” in the “Dnnn” entry in Annex D of ISO/IEC 15944-7.
046	8.3	The overall approach to the maintenance of entries in the eBusiness Vocabulary shall be based on and harmonized with the rules governing the maintenance of “business objects” as stated in ISO/IEC 15944-2.
047	8.4	An eBusiness Vocabulary Dnnn once assigned is deemed to be permanent and if retired shall not be re-assigned.
048	8.4	The definition in an eBusiness Vocabulary entry, in a Clause 3, which is part of more than one eBusiness standard, shall not be changed without taking into consideration the other standards in which it is also a sub-clause in Clause 3.

Annex C
(normative)

Business Transaction Model (BTM): Classes of constraints

Business transactions are modelled for registering, reference and re-use as scenarios and scenario components. Business semantic descriptive techniques are used to identify and specify the key components of a business transaction, i.e., as business objects.

The Business Transaction Model (BTM), as stated in Clause 6.1.5 of ISO/IEC 15944-1, has three required components namely "Person", "Process", and "Data. These three fundamental components of the Business Transaction Model are presented graphically in Figure 8[133].

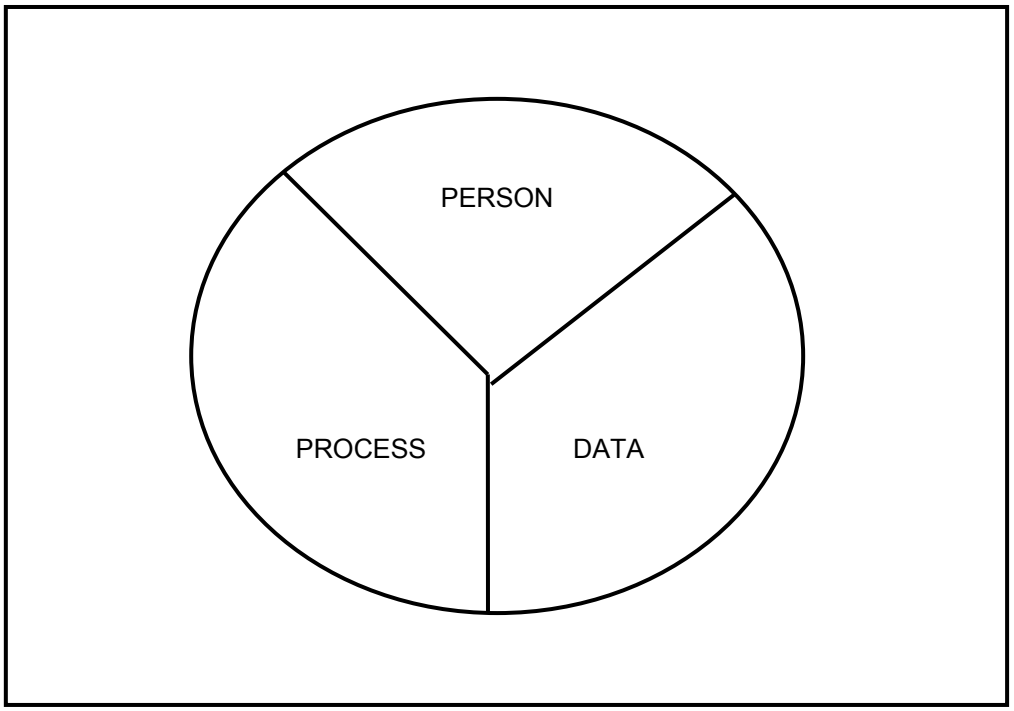


Figure C.1 — Business Transaction Model - Fundamental components (Graphic illustration)

Using UML as a Formal Description Technique yields the following UML-based representation of the Business Transaction Model and is presented as Figure C.2[134].

[133] In ISO/IEC 15944-1 for these three fundamental elements, the essential BOV aspects of the business transaction model, along with associated rules, definitions and terms as well as other attributes are stated in the following clauses:

(1) Clause 6.2 "Rules governing the Person Component" (and further Annex E);

(2) Clause 6.3 "*Rules governing the Process Component"* (and further Annex F); and,

(3) Clause 6.4 *"Rules governing the Data Component"* (and further Annex G).

[134] This UML-based representation incorporates the rules governing the interworking of these three fundamental components as specified in ISO/IEC 15944-1.

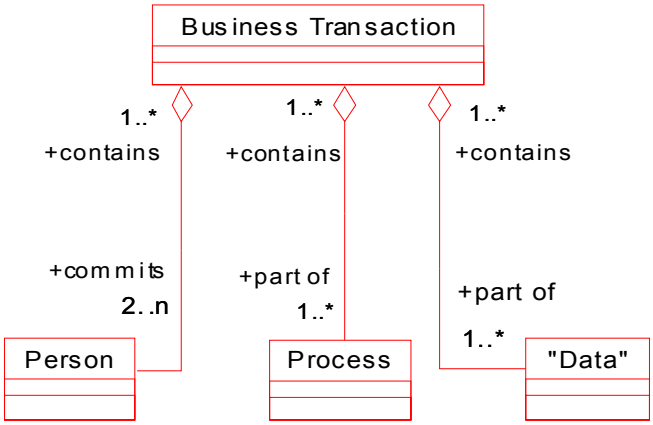


Figure C.2 — UML-based Representation of Figure C.1 — Business Transaction Model

The business transaction model (BTM) focuses on and addresses the essential needs of commitment exchange among autonomous parties, i.e., the ability of Persons as parties to a business transaction being able to make commitments and to do so while maximizing the use of automated methods. This is in addition to existing standards which pertain to various aspects of information exchange only.[135]

As such, what sets Open-edi (or e-business) apart from information exchange in general are six (6) characteristics[136]. They are:

- actions based upon following clear, predefined rules;
- commitments of the parties involved;
- commitments among the parties are automated;
- parties control and maintain their states;
- parties act autonomously; and,
- multiple simultaneous transactions can be supported.

Electronic business transactions therefore require:

(1) a clearly understood purpose, mutually agreed upon goal(s) explicitness and unambiguity;

(2) pre-definable set(s) of activities and/or processes, pre-definable and structured data;

(3) commitments among Persons being established through electronic data interchange;

(4) computational integrity and related characteristics; and,

(5) the above being specifiable through Open-edi Description Technique(s) (OeDTs) (as the use of a Formal Description Technique(s) in support of modelling e-business), and executable through information technology systems for use in real world actualizations.

---

135 It is important that users of this part of ISO/IEC 15944 familiarize themselves with ISO/IEC 15944-1, Clause 6.3.1 titled *"Business transactions commitment exchange added to information exchange*" including the rules and definitions/terms, i.e., "Person", and "commitment" as well as its normative text.

136 See further in ISO/IEC 15944-1 Clause 5 "*Characteristics of Open-edi",* where of these six (6) characteristics is described in more detail.

These and related requirements of electronic business transactions are specified in the form of "constraints".

"Constraint" has already been defined as:

constraint

rule**, explicitly stated, that prescribes, limits, governs or specifies any aspect of a **business transaction

NOTE 1 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 For constraints to be registered for implementation in Open-edi, they must have unique and unambiguous identifiers.

NOTE 3 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". [ISO/IEC 15944-1:2010:3.11]

The Business Transaction Model 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**"; and,

(2) those which are imposed on the parties to a business transaction based on the nature of the good, service and/or rights exchanged, the nature of the commitment made among the parties (including ability to make commitments, the location, etc.), i.e., "**external constraints".**

They are defined as follows:

internal constraint

constraint** which forms part of the **commitment**(s) mutually agreed to among the parties to a **business transaction

NOTE Internal constraints are self-imposed. They provide a simplified view for modeling 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.

external constraint

constraint which takes precedence over internal constraints in a business transaction, i.e., is external to those agreed upon by the parties to a business transaction

NOTE 1 Primary sources of external constraints are created by law, regulation, orders, treaties, conventions or similar instruments.

NOTE 2 Other sources of external constraints include those of a sectoral nature, those which pertain to a particular jurisdiction or a mutually agreed to common business conventions, (e.g., INCOTERMS, exchanges, etc.).

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

NOTE 4 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 Where the Information Bundles (IBs), including their Semantic Components (SCs) of a business transaction form the whole of a business transaction, (e.g., for legal or audit purposes), all constraints must be recorded.

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

NOTE 6 A minimum external constraint that is often applicable to a business transaction requires one to differentiate whether the Person, i.e., that is a party to a business transaction, is an "individual", "organization", or "public administration".

EXAMPLE Privacy rights apply only to a Person as an "individual".

The class of "internal constraints" has been derived to provide a simplified view of business transactions for which there are no external constraints or restrictions to the nature and conduct of the transaction. The only constraints are those mutually agreed to by the buyer and seller for the explicitly stated goal of the business transaction, i.e., they are self-imposed. This allows one to build scenarios and scenario components for referencing, registering and re-use as generic or base scenarios without having to include potential external constraints. The rules governing specification of Open-edi scenarios and their components require that all applicable external constraints must be stated at the time of instantiation but need not exist at the time of registration. {See further, Clause 9 in ISO/IEC 15944-1 and its Annex I}

However, in most business transactions external constraints do apply, i.e., applicable laws and regulations. These range from taxation related regulation; health and safety or packaging and labelling requirements; ensuring that nature of the business transaction and/or the goods or services delivered do not comprise behaviour of a criminal nature. Whilst laws and regulations exist within and among jurisdictions and are the primary source of "external constraints" on Business Transactions, categorization and specification of sub-classes of external constraints is outside the scope of this part of ISO/IEC 15944.

External constraints exist which are horizontal in nature. These are the common and generic rules for business transactions, (e.g., privacy/data protection, consumer policy, uniform commercial codes, etc.).

The imposition of these horizontal external constraints on business transactions is exemplified by the introduction of a third type of role in a business transaction, namely that of “regulator” as a third sub-type of Person as a player in a business transaction representing "public administration".

External constraints of a horizontal and common nature are constraints imposed by regulators (and enacted through public administrations) which apply regardless of the type of business or sector within which the business occurs. This categorization allows one to build scenarios and scenario components for referencing, registering and reuse of specific common sets of external constraints. These can then be combined with scenarios which focus on internal constraints for building application use scenarios.

There are also external constraints that are of a sectoral nature. In addition, some external constraints can be common to two or more sectors and supported through common standards. Sectoral constraints are found in telecommunications, transportation and delivery, financial/banking, import/export restrictions specific to a good or service, inter-or intra-state trade, and so on. Where a sector imposes specific ways of conducting business transactions within itself and with other sectors, such sector specific constraints and conditions must be identified and specified where applicable, as part of specification of scenarios and scenario components.[137)] This allows one to build scenarios and scenario components for referencing, registering and reuse of sets of

137 A useful characteristic of external constraints is that at the sectoral level, national and international focal points, recognized authorities often already exist. The rules and common business practices in many sectorial areas are already known. Use of this part of ISO/IEC 15944 (and related standards) will facilitate the transformation of these external constraints (business rules) into specified, registered and re-useable scenarios and scenario components.

sectoral external constraints such as “customs clearance”, “transport of dangerous goods”[138], etc. These two basic classes of constraints on business transactions are illustrated below in Figure 8: Business Transaction Model: Classes of Constraints.

These two basic classes of constraints on business transactions are illustrated here in Figure C.3.

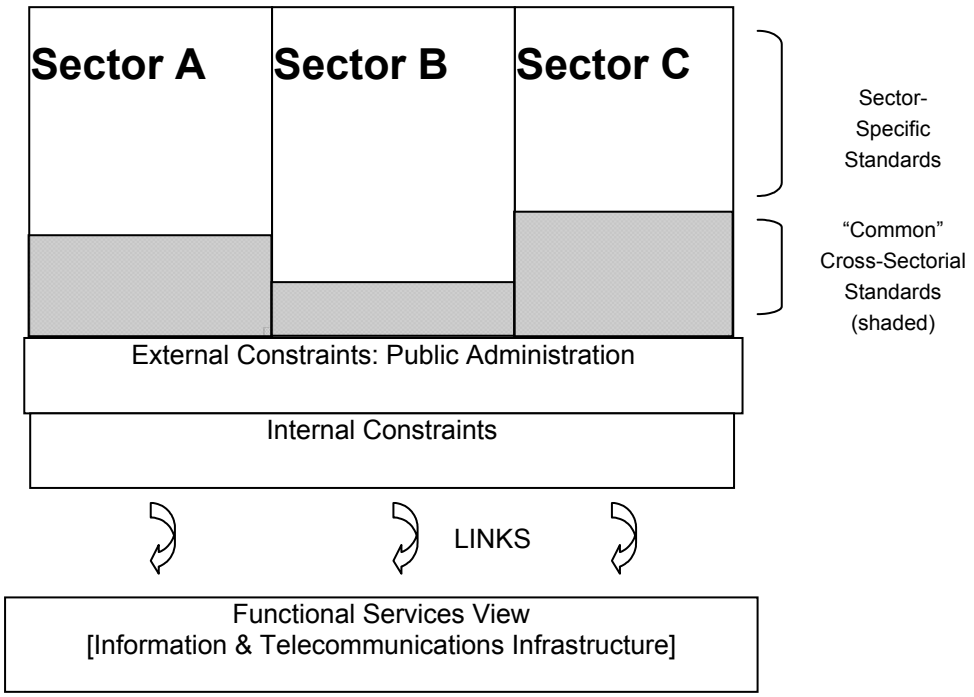


Figure C.3 — Business Transaction Model: Classes of constraints

138 Note: There are also requirements for establishing common rules for interchanges between as well as among sectors. These rules are normally imposed by a particular sector on the others. For example, the banking sector may impose certain rules for the exchange of financial information between itself and other sectors. Sometimes the rules are established to enhance or facilitate services of a particular sector with others. The transportation sector is a good example. It establishes business rules in conjunction with other sectors for the transport and handling of specialty goods, (e.g., radioactive materials, live animals, etc.).

Annex D
(normative)

Integrated set of information life cycle management (ILCM) principles in support of information law compliance

D.1 Introduction

From a business transaction perspective, one deals only with recorded information. Privacy/data protection is part of a set of public policy requirements which include consumer protection, individual accessibility, human rights, etc.

Further, there are also legal requirements which pertain to any set of recorded information interchanged among parties to a business transaction. These include record retention requirements, those of an evidentiary nature, archiving, contingency/disaster planning, etc., a.k.a., "information law" requirements, governing information management and data interchange of an organization.

The purpose of this Annex D is to consolidate these Business Operational View (BOV) requirements (including those of an external constraints nature) into a single set of high level or "primitive" principles. Having such a short Annex in this part of ISO/IEC 15944 (including the concept and definition of "information law") will facilitate the use of this development of this part of ISO/IEC 15944. This is because it provides a generic context and reference for information management and data interchange requirements.

D.2 Purpose

The procedures, documentation and related activities pertaining to business transactions and resulting sets of recorded information (consisting of one or more IBs or SCs) require that the highest standards of integrity and trustworthiness are maintained. A primary factor here is that business transactions represent the most common form of making and executing commitments among the parties to the business transactions.

These pertain not only to the flows of information and the contents of the recorded information but also there exists many other laws, regulations, etc., impacting information management and interchange and supporting documentation. Examples of such laws impacting business transactions include those pertaining to records keeping, access and use, disposition, archiving, etc. These are stated in the form of laws, pursuant regulations, statutory instruments, policies, codes, etc. They are of a generic "information law" nature. Information law is defined as:

> ***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****, 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****.*

It is (totally) outside the scope of this multipart standard to identify all the information law requirements applicable to the recorded information of any kind under the control of an organization (or public administration).

The purpose of this Annex D is to bring forward a **high level set of generic information life cycle management (ILCM) principles** which integrate and consolidate the essential elements of any law, regulation, etc., which have an information law component(s). These principles are generic in nature. On the

whole they apply to both internal constraints and external constraints. These ILCM principles therefore also provide an overall context for the privacy protection principles presented in Clause 5.3 above.

D.3 Approach

From a high level perspective, and taking into account federal and provincial/territorial, generic and sector specific information law requirements of jurisdictional domains (as well as those pertaining to access, privacy, confidentiality, security, etc.), one can group these ILCM requirements into a number of discrete categories.

Discrete categories of "information law" already identified include those that:

- require one to keep or retain certain recorded information;
- require one to have the ability to produce or retrieve certain types of recorded information;
- require one to submit or file recorded information to a government or regulatory agency;
- require one to create and/or make available recorded information if one undertakes a particular activity, i.e., pertaining to a product, service and/or right;
- require one retain recorded information “indefinitely” or for a specified period of time;
- require one to destroy recorded information;
- place conditions on access, use and/or confidentiality of recorded information;
- place conditions on the manner in which one handles recorded information;
- place conditions on the reproduction, distribution or sale of recorded information;
- place conditions on the sharing, linking or flows of recorded information (within or among jurisdictions); and,
- require “public” release/disclosure of certain recorded information (*a priori* or on request).

With respect to these categories:

(1) one or more of these categories of information law can apply to a "set of recorded information (SRI); and,

(2) an "information law" can include more than one category of requirements.

D.4 Integrated set of information life cycle management (ILCM) principles

Given the definition of "information law" and the examples of categories of information law already identified, any user or implementer of this part of ISO/IEC 15944 can quickly identify ten (10) or more different laws and regulations of an "information law" nature which apply to the recorded information forming part of a business transaction.

Two basic approaches are possible. The first, which is the current, traditional approach, is that of addressing each information law requirement on its own, i.e., as a "vertical silo". Here different operational areas within an organization comply with information law requirements on their own, integrate them into their applications, and deal with issues as they are identified, a crisis occurs, an audit discovers gaps, lack of compliance results in court actions, liability suits, etc. Convergence in and information communication technologies (ICT), increased the need for trustworthiness and integrity, accountability, etc., has made this "traditional" approach increasingly less viable.

It is vital that such an integrated approach to information life cycle management of the recorded information of an organization be senior management approved and driven. It is also very important that such ILCM principles focus on the WHATs not the HOWs and be stated in simple, non-technical language.

The eight (8) key Information Life Cycle Management (ILCM) Principles presented here incorporate a wide variety of information law requirements common to most jurisdictional domains as well as widely accepted best management practices of an "organization". They are:

1) **Any "recorded information" which exists at an organization must be directly relatable to, and be in support of, an authorized mandate, program, delivery of product and/or service, (research) project, administrative mandate, or other specified and approved activity of the organization.**

2) **An organization (for-profit or not-for-profit basis) (or public administration) must have: (a) an accurate and up-to-date list of all information law requirements which apply to the organization, i.e., both of a generic horizontal nature and those specific to the mix of goods and/or services it provides; and, (b) must be in full compliance with such information law requirements.**

3) **All recorded information must be timely, accurate and relevant, and under "control", i.e., it must be identifiable, retrievable and accountabilities must be assigned.**

4) **Information management policies and practices, as well as those for supporting information handling systems, must ensure the level of trustworthiness, (data) integrity, quality and dependability is consistent with and supports the organization's objectives and information law requirements.**

5) **Where warranted, recorded information should be protected from premature and/or non-authorized disclosure. Adequate safeguards must be enacted to ensure the required levels of confidentialities.**

   It is important to note that the corollary of this policy principle, i.e., mandated disclosure, is supported equally. That is, recorded information, to which the public in general and/or specified Persons have a right of access to, must not be withheld from disclosure.

6) **Recorded information which has long-term value and/or forms part of the corporate memory should be identified and conserved. This includes recorded information required for contingency planning, back-up, emergency response and related requirements.**

7) **Recorded information which may have historical value should be identified and conserved (as part of the organization's and/or electronic cultural heritage/«patrimoine informatisée»).**

8) **Any recorded information which is no longer relevant to an organization's operations and which does not meet the above criteria should be disposed of immediately.**

THIS PAGE INTENTIONALLY LEFT BLANK

Annex E
(normative)

Key existing concepts and definitions applicable to the establishment, management, and use of identities of a single individual

The ISO/IEC 14662 "Open-edi Reference Model" and various Parts of the multipart "Business Operational View" ISO/IEC 15944 standard contain existing concepts and their definitions which are applicable to the establishment, management and use of identities of a single individual. These concepts and their definitions apply to this part of ISO/IEC 15944. Key concepts of this nature are identified below via their assigned label (or "term"). They are presented and organized in matrix form as follows:

Column	Title	Description
(1)	eBus Vocab. ID	i.e., eBusiness Vocabulary ID. The ID as taken from the eBusiness vocabulary entry in ISO/IEC 15944-7 (Annex D).
(2)	eBus Vocabulary Term (ISO English)	i.e.., eBusiness Vocabulary Term (English). The English language term for the eBusiness vocabulary as taken from Annex D of ISO/IEC 15944-7.
(3)	Explanatory Notes (from an ISO/IEC 15944-8 perspective)	Explanatory notes on how this eBusiness concept applies to this part of ISO/IEC 15944.

It is noted that the ISO/IEC 15944-7 "…*e-Business Vocabulary*…" is a "freely available standard" and provides Human Interface Equivalents for both the definitions and associated terms in ISO English, French, Russian and Chinese.

eBus. Vocab. ID	eBusiness Vocabulary Term (ISO English)	Explanatory Notes (from ISO/IEC 15944-8 Perspective)
(1)	(2)	(3)
D025	business transaction identifier (BTI)	any instantiated business transaction has a BTI including those where the buyer is an individual
D034	Coded domain Registration Schema (cdRS)	Most, if not all, identities of an individual have an identifier based on a cdRS
D035	coded domain Source Authority (cdSA)	Any identifier used as part of an individual's identifier has a cdSA
D073	distinguishing identifier	Any identifier used in a business transaction including those involving an individual will have one or more distinguishing identifiers (directly associated with the same).
D094	entity authentication	The use of a recognized individual identity in a business transaction may need to be corroborated.
D188	persona	An individual may have, and usually has, more than one persona (and often in different languages and their writing systems)
D207	recognized individual name (RIN)	An individual may have, and usually has, more than one RIN.
D208	recognized Person identity (rPi)	A Person may have and usually has more, than one (rPi).
D222	Registration Authority	Any identifier used to establish the identifier must have a Registration Authority for referencing and/or using of that identifier in a business transaction;
D223	Registration Authority Identifier (RAI)	Each RA has its own unique RAI. These are either (1) explicitly included in a "rii" or "rPi"; or, (2) automatically invoked in an authentication process pertaining to that individual in an instantiated business transaction. This includes rules governing the use of personal information obtained/retained by a RAI as part of the registration process.
D224	Registration Schema (RS)	The rules governing the registration schema (RS) of a Registration Authority, which include the registration of individuals as members, shall be made available to any individual who is registered in that RS.
D262	truncated name	An individual often has one or more truncated names which he/she uses as personae.
D263	truncated recognized name (TRN)	An individual often has a TRN where the source persona, i.e., full text of the individual's name is "too long" to be incorporated into a RIN.

Annex F
(normative)

Coded domains for specifying state change and record retention management in support of privacy protection requirements

F.1 Introduction

Generic aspects of external constraints of jurisdictional domains as rules governing business transactions are found in ISO/IEC 15944-5.

Note: Users of this document are advised to familiarize themselves with the rules, definitions and associated text of Clause 6.6.4 "*Data component*", as found in ISO/IEC 15944-5 (a "freely available standard").

Within a data management and interchange context, it is important that parties to a business transaction control the states of their IT systems. This is a fundamental characteristic of Open-edi. Under internal constraints it is a best practice of organizations and public administrations to maintain control of the sets of recorded information in their IT systems (as especially those in their DMAs). This includes both state changes and records retention requirements. This pertains to basic information life cycle management (ILCM) principles in support of information law compliance. {See further above Annex D}

The need for information law compliance is even more so and mandatory when the set(s) of recorded information pertain to a business transaction, i.e., a "commitment exchange", where the buyer is an individual.

These generic Open-edi aspects and rules pertaining to a business transaction are mandatory in any business transaction context which involves an individual as a buyer. This is because where this is the case privacy protection requirements apply.

The purpose of this Annex F is therefore to bring these generic Open-edi requirements of ISO/IEC 15944-5 forward in the particular context of this part of ISO/IEC 15944 which focuses on privacy protection requirements; namely:

1) those pertaining to state changes in the sets of recorded information (at whatever level of granularity);

and;

2) those pertaining to records retention requirements (including assured destruction of personal information.

The purpose of Annex F is to bring forward normative text, rules and associated coded domains from ISO/IEC 15944-5, Clause 6.6.4.2 and 6.6.4.3 and present them in an amended form, as and where required, in the context of privacy protection requirements. (This approach is similar to that taken for Clause 8 in this document which also applies normative text from others parts of ISO/IEC 15944 and applies it in a privacy protection requirements context.)

A common requirement of external constraints of a public policy nature is that they mandate records retention (and deletion) requirements, (e.g., consumer protection, privacy protection, etc.). In order to bridge legal, operational, public policy and IT perspectives, records retention is defined as in an Open-edi context [139] as:

[139] Multiple definitions exist for "records retention" within a single jurisdictional domain as well as among jurisdictional domains, professional organizations, etc. In order to differentiate the concept of "records retention" within the context of e-business, e-government, etc., a unique label or term has been invented/coined, i.e. that of "Open-edi records retention (OeRR).

Open-edi records retention (OeRR)

*specification of a period of time that a **set of recorded information** must be kept by a **Person** in order to meet operational, legal, regulatory, fiscal or other requirements as specified in the **external constraints** (or **internal constraints**) applicable to a **Person** who is a party to a **business transaction***

As stated in ISO/IEC 15944-1 records retention requirements need to be specified:

- in the scoping of an Open-edi scenario, (e.g., as a Post-actualization requirement, or a Data Component requirement);
- as an attribute of an Information Bundle, (e.g., for specifying internal constraints). {See ISO/IEC 15944-1 Clause 8.5.2.8 and Rule 140; and, for external constraints, see ISO/IEC 15944-1, Clause 8.5.2.9 and Rule 141}.

It is important to be able to specify which of the parties to a business transaction is responsible for retention of IBs or the complete set of recorded information

Many, if not most, of the privacy protection requirements are of an information management nature. A key reason here is the privacy protection requirements are a type of information law. Consequently, the integrated set of information life cycle management (ILCM) principles apply. {See further Annex D above}

Rule F-001:

Management and control of state change, retention and destruction of personal information shall be based on the application of the integrated set of information life cycle management (ICLM) principles.

The following two clauses in Annex F focus on the:

a) state changes and state change management of personal information; and,

b) management of record retention[140] requirements of personal information; and,

c) as part of privacy protection requirements.

F.2 State changes

F.2.1 Introduction

A fundamental aspect of data management and interchange among autonomous Persons (or even within an organization or public administration) is that of ensuring the accuracy, timeliness and relevancy of its (sets of) recorded information. A second fundamental aspect here is that any Person (or whatever nature) shall do so in compliance with applicable external constraints of the relevant jurisdictional domain.

A key characteristic of Open-edi is that "**parties control and maintain their states**". {See Clause 5.4, ISO/IEC 15944-1}. As such, it is important to know whether or not the value of an Information Bundle (IB) (or one of its Semantic Components (SCs) interchanged among parties to a business transaction is allowed to be changed during any stage in the process component. **Knowing whether or not state changes are allowed for a specific IB or SC is important for the management of state description and automated change management of the state machines of the parties involved in an electronic business transaction.**

This is a requirement which also exists in modelling business transactions involving internal constraints only. However, those which exist here are likely to be a sub-set of those which arise from external constraints.

[140] Another common requirement is that of security services. Here many ISO/IEC and ITU standards already exist of a FSV nature which facilitates the specification and implementation of the same based on BOV requirements.

A related issue is that of "What happens to recorded information which existed prior to a state change being made"? It is important for parties to a business transaction to know this. In summary, two attributes are required to specify state change of data. They are:

- number of state changes allowed, if any; and,
- store change type.

The inter-working of these two attributes, i.e., as codes in two coded domains, covers the various combinations of state changes in the data value for each IB and SC as well as what actions are required with respect to both "new" and "old" data including those required for information life cycle management (ILCM) within an organization, audit trains, evidentiary requirements and any external constraints of this nature of jurisdictional domains.

The coded domains presented below address the most primitive, i.e., essential, requirements of specifying and managing state changes (at whatever level of granularity) of SRIs in an IT system.

F.2.2 Specification of state changes allowed to personal information

Rule F-002:

Where an individual is a party to a business transaction, i.e., as a buyer, the seller (as an organization or public administration) shall have in place rules governing state changes, if any, for personal information (at whatever level of granularity required) in support of data management and interchange required to comply with privacy protection requirements.

Table F.1 — ISO/IEC 15944-5:05 Codes for specifying state changes allowed for the values of Information Bundles and Semantic Components[141]

ISO/IEC 15944-5:05 Codes for Specifying State Changes Allowed for the Values of Information Bundles and Semantic Components				
IT Interface			Human Interface Equivalents(HIEs): Linguistic – Written Form	
Source Authority ID	Coded Domain ID	ID Code	ISO English	ISO French
15944-5	05	00	no state change allowed (default)	
15944-5	05	01	one state change allowed	
15944-5	05	02	two state changes allowed	
15944-5	05	03	three state changes allowed	
15944-5	05	04	four state changes allowed	
15944-5	05	05	five state changes allowed	
15944-5	05	06	six state changes allowed	
15944-5	05	07	seven state changes allowed	
15944-5	05	08	eight state changes allowed	
15944-5	05	09	no limit on the number of state changes allowed	

141 NOTE: Should there be a requirement for additional conditions for the specification of records retention responsibilities these can be added via a Technical Corrigenda to this part of ISO/IEC 5944 or in the next edition of this part of ISO/IEC 15944.

An example of use of Code "0" would be the transaction record ID number as the business transaction identifier (BTI), {See further Clause 11.2 above} i.e., the unique ID number assigned by the seller to an instantiated business transaction. Codes "1", "2", "3", etc., are used to deal with IBs and SCs pertaining to location information, (e.g., physical or electronic addresses), price and terms negotiations, the buyer changing its decision on a choice of options, etc.

An example of an IB (or SC) having a Code "09" with respect to state changes would be in item tracking in a logistics system, (e.g., the seller provides to a buyer a facility to access the seller or logistic provider system to track the movement of an item to be delivered to the buyer).

Rule F-002:

An instantiated business transaction shall have one or more IB or SC for which no state changes are permitted. One of these is to serve as the transaction ID number, i.e., a business transaction identifier (BTI), for the instantiated business transaction.

Guideline F002G1:

It is advised that in modelling scenarios, scenario attributes roles, information bundles and scenario components that one set the state change code to "00" wherever applicable.

This Guideline serves to ensure that all parties to a business transaction agree to and have knowledge of permitted state change to the value of an IB or SC.

Rule F-003:

If a state change is required, the seller (and/or regulator) shall specify the number of state changes permitted.

Guideline F003G1:

In support of rules F-002 and F-003, the seller as well as other parties to the business transaction as applicable, (e.g., the regulator, an agent, or third party) should use the ISO/IEC 15944-5 Coded domain 05 to specify the applicable state change ID codes.

F.2.3 Store change type

If a state change is permitted to the original data value of the IB (or its associated SCs), i.e., (1) any entered in the DMA(s) of the IT system(s) of the organization or public administration which acting in the role of a seller or a regulatory in a business transaction involving an individual and/or as, (2) interchanged among the Persons involved, it is necessary to specify in the business object being modelled the store change type permitted.

The most common, i.e., primitive, store change types are stated in the coded domain for "*Codes Representing Store Change Type".*

Guideline F-003G2:

In support of rule F-003, the seller as well as other parties to the business transaction as applicable. (e.g., the regulator, an agent or a third party) should use the ISO/IEC 15944-5 Coded Domain 06 to specify store change type.

Table F.2 — ISO/IEC 15944-5:06 Codes representing store change type for Information Bundles and Semantic Components[142]

ISO/IEC 15944-5:06 Codes Representing Store Change Type for Information Bundles and Semantic Components				
IT Interface			Human Interface Equivalents(HIEs): Linguistic – Written Form	
Source Authority	Coded Domain ID	ID Code	ISO English	ISO French
15944-5	06	00	others	autre
15944-5	06	01	store new data value and expunge previous data value	
15944-5	06	02	store new data value, expunge previous value with date/time stamp when state change occurred	
15944-5	06	11	store new data value and previous data value only	
15944-5	06	12	store new data value and previous data value only and add a date/time stamp	
15944-5	06	21	store new data value and “nn” previous values maintaining a sequence number of all state changes. here “nn” must be specified	
15944-5	06	22	store new data value and “nn” previous values maintaining a date/time stamp for each state change. here “nn” must be specified	
15944-5	06	31	store new data value and all changes maintaining a sequence number of all state changes	
15944-5	06	32	store new data value and all changes, maintain a date/time stamp for each state change	
15944-5	06	99	not applicable, i.e., no state change allowed	

One notes that a code “99” here works in tandem with a Code “00” in the previous Coded Domain. Use of a Code “01” or “02” means that having the previous value only is sufficient. This is often the case for change in location, (e.g., for physical or electronic address information). The use of the other codes links to ensuring record of decision, audit trails, evidentiary requirements and other external constraints which may apply due to the nature of the business transaction.

[142] NOTE: Should there be a requirement for additional conditions for the specification of records retention responsibilities these can be added via a Technical Corrigenda to this part of ISO/IEC 15944 or in the next edition of this part of ISO/IEC 15944.

F.3 Records retention

Rule F-004:

Where an individual is a buyer to a business transaction, the seller shall specify who is responsible for the retention of any (combination of) set(s) of recorded information during the negotiation phase and no later than at the actualization phase in accordance with privacy protection requirements.

Rule F-005:

Where an individual is a buyer in a business transaction the seller shall ensure that all other parties to the instantiated business transaction, as applicable, (e.g., a regulator, an agent, and/or third party) are informed of records retention (and destruction requirements).

Guideline F-005G1:

In support of Rules F-004 and F-005 the seller, as well as any other parties to the business transaction, (e.g., a regulator, an agent, and/or third party) should use ISO/IEC 15944-5 Coded domain 02 Codes Representing Specification of Records Retention Requirements. This coded domain is presented below as Table F.3.

Within the context of collaboration space of a business transaction, a number of basic common options exist for specifying responsibility for Open-edi records retention (OeRR) among the parties to a business transaction. They have already been identified in the following coded domain of SO/IEC 15944-5. They are presented below in a privacy protection requirements context.

External constraints of a public policy nature such as privacy protection (and consumer protection as well) require, i.e., make mandatory, both (1) the retention of personal information pertaining to a business transaction where the individual is the buyer; and, (2) the assured destruction of personal information based on both legal requirements and contractual obligations. {See further above Annex D *(Normative) Integrated set of information life cycle management (ILCM) principles in support of information law compliance*}.

Table F.3 — ISO/IEC 15944-5:02 Codes Representing Specification of Records Retention Responsibility[143]

ISO/IEC 15944-5:02 Codes Representing Specification of Records Retention Responsibility				
IT Interface			**Human Interface Equivalents (HIEs):** **Linguistic – Written Form**	
Source Authority ID	**Coded Domain ID**	**ID Code**	**ISO English**	**ISO French**
15944-5	02	00	other	autre
15944-5	02	01	seller is responsible	
15944-5	02	02	buyer is responsible	
15944-5	02	03	seller and buyer are both responsible	
15944-5	02	04	buyer shall specify to seller what IB to retain, (e.g., order number, transaction number, etc.)	

[143] NOTE: Should there be a requirement for additional conditions for the specification of records retention responsibilities these can be added via a Technical Corrigenda to this part of ISO/IEC 15944 or in the next edition of this part of ISO/IEC 15944.

ISO/IEC 15944-5:02 Codes Representing Specification of Records Retention Responsibility				
IT Interface			Human Interface Equivalents (HIEs): Linguistic – Written Form	
Source Authority ID	Coded Domain ID	ID Code	ISO English	ISO French
15944-5	02	05	seller and buyer shall use a common third party, (e.g., a notary)	
15944-5	02	06	regulator is responsible	
15944-5	02	07	regulator and seller are responsible	
15944-5	02	08	regulator and buyer are responsible	
15944-5	02	09	regulator, buyer and seller are all responsible	
15944-5	02	10	regulator mandates the involvement of a (role) qualified or designated third party, i.e., on behalf of seller, buyer and regulator.	
15944-5	02	98	not known	inconnu
15944-5	02	99	not applicable	sans objet

On the whole, the greater and more specific the external constraint governing the nature of the good, service or right being transacted the more extensive and specific the records retention requirements, (e.g., a business transaction involving radioactive isotopes (for medical purposes) requires records retention of a much more detailed nature than that for aspirin).

It is common external constraints of jurisdictional domains that a Person is required to retain sets of recorded information for a specified period of time. This is even more so where the recorded information pertains to a business transaction (and particularly where the buyer is an individual).

External constraints of a records retention nature have requirements which specify (1) when a retention requirement is to start, i.e., via a limited number of triggers; and, (2) then a specified (minimum) retention period. On the whole, records retention requirements are triggered by an action or event. The basic conditions here from an external constraints perspective for "retention triggers" are limited. The most common ones are presented in the following Coded Domain 04 of ISO/IEC 15944-5.

Rule F-006:

Where an individual is a buyer to a business transaction, the seller shall specify the "retention trigger" activating records retention requirements in accordance with privacy protection requirements of the applicable jurisdictional domain(s).

Guideline F-006G1:

In support of Rule F-006, the seller as well as any other parties to the business transaction, (e.g., a regulator, an agent, and/or third party) should use the ISO/IEC 15944-5 Coded Domain 04 "Codes representing retention triggers".

It is reproduced here below as Table F.4.

Table F.4 — ISO/IEC 15944-5:04 Codes representing retention triggers[144]

ISO/IEC 15944-5:04 Codes Representing Retention Triggers				
IT Interface			Human Interface Equivalents(HIEs): Linguistic – Written Form	
Source Authority ID	Coded Domain ID	ID Code	ISO English	ISO French
15944-5	04	00	other	autre
15944-5	04	01	start required retention period at date/time recorded information was received, created or collected	
15944-5	04	02	start required retention period from date of last action or use	
15944-5	04	03	start retention period at end of calendar year	
15944-5	04	04	start retention period at end of fiscal year	
15944-5	04	98	not known	inconnu
15944-5	04	99	not applicable [145]	sans objet

F.4 Records destruction

A key privacy protection requirement is that of the mandatory destruction, i.e. as the reverse of records retention. Within an information/records management and archiving context this is known as "disposition". Disposition is an authorized action to remove, i.e., alienate, a set of recorded information, from under the control of a Person and thereby extinguishing ownership and accountability[146]. In the context of this part of ISO/IEC 15944, "Open-edi disposition" is defined as:

Open-edi disposition

process

governing the implementation of formally approved records retention, destruction (or expungement) or transfer of ***recorded information*** *under the control of a* ***Person*** *which are documented in disposition authorities or similar instruments*

NOTE Adapted from ISO 15489-1:2001

There are basically a limited number of disposal actions. These are identified in the following coded domain 03 found in this part of of ISO/IEC15944.

144 NOTE: Should there be a requirement for additional conditions for the specification of records retention responsibilities these can be added via a Technical Corrigenda to this part of ISO/IEC 15944 or in the next edition of this part of ISO/IEC 15944.

145 This would apply to recorded information deemed to be ephemeral or transitory in nature and thus would (likely) also have an ID code of 99 under Coded Domain 15944-5:03.

146 This is more than "erasing" or "deleting" an SRI in an IT system. From an "evidentiary" requirements perspective, the requirement here is that of "expungement" (= eliminate completely, wipe out, destroy or obliterate an electronic record).

Rule F-007:

Where an individual is a buyer to a business transaction, the seller shall specify the disposition action to be taken at the end of the expiry of the record retention period in accordance with privacy protection requirements of the applicable jurisdictional domain.

Guideline F-007G1:

In support of Rule F-007, the seller as well as any other parties to the business transaction, (e.g., a regulator, an agent, and/or third party) should use the ISO/IEC 15944-5 Coded Domain 03 "Codes representing disposition of recorded information".

It is reproduced here below as Table F.5.

Table F.5 — ISO/IEC 15944-5:03 Codes representing disposition of recorded information[147]

ISO/IEC 15944-5:03 Codes Representing Disposition of Recorded Information				
IT Interface			**Human Interface Equivalents(HIEs): Linguistic – Written Form**	
Source Authority ID	**Coded Domain ID**	**ID Code**	**ISO English**	**ISO French**
15944-5	03	00	other	autre
15944-5	03	01	destruction or expungement	
15944-5	03	02	transfer to another organization	
15944-5	03	03	transfer to an archive (for historical and research purposes)	
15944-5	03	04	do not destroy, maintain and conserve as a permanent SRI	
15944-5	03	98	not known	inconnu
15944-5	03	99	not applicable [148]	sans objet

147 NOTE; Should there be a requirement for additional conditions for the specification of records retention responsibilities these can be added via a Technical Corrigenda to this part of ISO/IEC 15944 or in the next edition of this part of ISO/IEC 15944.

148 This would apply to recorded information deemed to be transitory or ephemeral which can be discarded anytime.

Bibliography

The bibliography is organized in two parts. The first identifies sources that are ISO and ISO/IEC international standards. The second cites other cited sources which are useful to the understanding of this part of ISO/IEC 15944.

1. ISO and ISO/IEC international standards

ISO/IEC 9798-1:1997(E), *Information technology — Security techniques — Entity authentication — Part 1: General*

ISO/IEC 10181-2:1996(E), *Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework*

ISO/IEC 11179-1:2004(E), *Information technology — Metadata Registries (MDR) — Part 1: Framework*

ISO/IEC 11179-3:2003(E), *Information technology — Metadata Registries (MDR) — Part 3: Registry metamodel and basic attributes*

ISO/IEC TR 13335-1:1996(E), *Information technology — Guidelines for the management of IT Security — Part 1: Concepts and models for IT Security*

ISO/IEC TR 15285:1998(E), *Information technology — An operational model for characters and glyphs*

ISO 15489-1:2001(E/F), *Information and documentation — Records management — Part 1: General/ Information et documentation — «Records management» — Partie 1: Principes directeurs*

ISO/IEC 15944-6:2009(E), *Information technology — Business Operational View — Part 6: Technical introduction to eBusiness modelling*

ISO 19115:2003(E), *Geographic information — Metadata*

ISO 19135:2005(E), *Geographic information — Procedures for item registration*

ISO/TS 25237:2008(E), *Health informatics — Pseudonymization*

ISO/IEC 27002:2005(E), *Information technology — Security techniques — Code of practice for information security management*

2. Other

GS1Global Traceability Standard (GDSN). Issue 1.2.2. (March, 2010). Available from: http://www.gs1.org/docs/gsmp/traceability/Global_Traceability_Standard.pdf (Accessed 2011-10-04)

GS1 Global Data Dictionary: http://gdd.gs1.org/GDD/public/searchableglossary.asp (Accessed 2011-10-04)

Quittner, Joshua. (Monday, 8 February, 1999). Going private. Time 153(5):62 (8 February, 1999). Available from: http://www.time.com/time/magazine/article/0,9171,990168,00.html (Accessed 2011-10-04)

UN. *International Covenant on Economic, Social and Cultural Rights.* (1966), Available from: http://www2.ohchr.org/english/law/cescr.htm. (Accessed 2011-10-04)

UN *Universal Declaration of Human Rights* (1948) Available from http://www.un.org/en/documents/udhr/ (Accessed 2011-10-04)

UN. *Universal Declaration of Rights of Persons belonging to National or Ethnic, Religious and Linguistic Minorities*. Available from: http://www2.ohchr.org/english/law/minorities.htm (Accessed 2011-10-04)

UNESCO *Universal Declaration of Cultural Diversity* (Paris, November, 2001). Available from http://unesdoc.unesco.org/images/0012/001271/127160m.pdf (Accessed 2011-10-04)

ICS 35.240.60

Price based on 221 pages