BS ISO/IEC 15944-12:2020

BSI Standards Publication

Information technology — Business operational view

Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 15944-12:2020

National foreword

This British Standard is the UK implementation of ISO/IEC 15944-12:2020.

The UK participation in its preparation was entrusted to Technical Committee IST/40, Data management and interchange.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 04919 0

ICS 35.240.63

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2020.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 15944-12:2020

INTERNATIONAL STANDARD

ISO/IEC 15944-12

First edition
2020-05

Information technology — Business operational view —

Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)

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

Partie 12: Exigences en matière de protection de la vie privée (PPR) relatives à la gestion du cycle de vie de l'information (ILCM) et de l'EDI des renseignements personnels (PI)

Reference number
ISO/IEC 15944-12:2020(E)

Documents
Document Sharing Hub
© ISO/IEC 2020

Full document details: BS ISO/IEC 15944-12:2020

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

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

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 15944-12:2020

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **2**

4 Abbreviated terms **30**

5 Fundamental privacy protection principles **31**
5.1 Overview 31
5.2 Primary sources of privacy protection principles 31
5.3 Key eleven (11) privacy protection principles 32
5.4 Link to "consumer protection" and "individual accessibility" requirements (see ISO/IEC 15944-8:2012, 6.3) 33
5.5 Privacy protection principles in the context of ILCM requirements 34
5.6 Requirement for tagging (or labelling) sets of personal information (SPIs) in support of privacy protection requirements (PPR) in accordance with ISO/IEC 15944-8:2012, 5.4 34
5.7 Requirements for making all personal information (PI) available to the buyer where the buyer is an individual 34
5.8 Rules governing ILCM aspects of personal information profiles (PIPs) 35

6 Integrated set of information life cycle management (ILCM) principles in support of information law and privacy protection requirements (PPR) **36**
6.1 Primary purpose of Clause 6 36
6.2 Information life cycle management (ILCM) principles that support privacy protection requirements (PPR) 38
6.2.1 Compliance with privacy protection requirements (PPR) and associated information law requirements 38
6.2.2 Direct relevance, informed consent and openness 38
6.2.3 Ensuring that personal information is "under the control of" the organization throughout its ILCM 40
6.2.4 Limiting use, disclosure and retention 41
6.2.5 Timely, accurate, relevant 43
6.2.6 Data integrity and quality 45
6.2.7 Safeguards for non-authorized disclosure requirements 45
6.2.8 Back-up, retention and archiving 46
6.2.9 Disposition and expungement 47
6.2.10 Organizational archiving 47
6.2.11 Historical, statistical and/or research value 47
6.3 Requirement for tagging (or labelling) data elements in support of privacy protection requirements (PPR) 49

7 Rules governing ensuring accountability for and control of personal information (PI) **49**
7.1 Purpose 49
7.2 Key aspects of Open-edi requirements 49
7.3 Key aspects of "under the control of" 50
7.4 "under the control of" in support of PPR and in an ILCM context 50
7.5 Implementing "under the control of" and accountability 51

8 Rules governing the specification of ILCM aspects of personal information **56**
8.1 Overview 56
8.2 Rules governing establishing ILCM responsibilities for personal information (PI) 57
8.3 Rules governing establishing specifications for retention of personal information (PI) — applicable "SRI retention triggers" 59

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 15944-12:2020

8.4 Rules governing identification and specification of state changes of personal information (PI) 62
8.4.1 General requirements 62
8.4.2 Specification of state changes allowed to personal information (PI) 63
8.4.3 Specification of store change type 65
8.4.4 Rules governing specification of source of state changes 67
8.5 Rules governing disposition of personal information (PI) 68
8.6 Rules governing the establishment and maintenance of record retention and disposal schedules (RRDS) for sets of personal information (SPIs) 71

9 Data conversion, data migration and data synchronization 73
9.1 Purpose 73
9.2 Rules governing data conversion of set(s) of personal information (SPI) 74
9.3 Rules governing requirements for data synchronization of sets of personal information (SPI) 74

10 Rules governing EDI of personal information (PI) between primary ILCM Person, i.e., the seller, and its "agent", "third party" and/or "regulator" 76
10.1 General requirements 76
10.2 ILCM rules pertaining to use of an "agent" 77
10.3 ILCM rules pertaining to use of a "third party" 78
10.4 ILCM rules pertaining to involvement of a "regulator" 78

11 Conformance statement 79
11.1 Overview 79
11.2 Conformance to the ISO/IEC 14662 Open-edi reference model and the ISO/IEC 15944 series 79
11.3 Conformance to ISO/IEC 15944-12 80
11.4 Conformance by agents and third parties to ISO/IEC 15944-12 80

Annex A (normative) **Consolidated list of terms and definitions with cultural adaptability: ISO English and ISO French language equivalency 81**

Annex B (normative) **Consolidated set of rules in the ISO/IEC 15944 series of particular relevance to privacy protection requirements (PPR) as external constraints on business transactions which apply to personal information (PI) in an ILCM requirements context 96**

Annex C (informative) **Business transaction model (BTM): Classes of constraints 112**

Annex D (informative) **Linking ILCM to process phases of a business transaction 116**

Annex E (informative) **Generic approach to ILCM decisions in a PPR context — ILCM compliance decision tree 118**

Annex F (informative) **Generic approach to identification of properties and behaviours of personal information (PI) as transitory records and their disposition/expungement 121**

Annex G (informative) **Notes on referential integrity and privacy protection transactional integrity (PPTI) in Open-edi among IT systems 123**

Annex H (informative) **Exclusions to the scope of ISO/IEC 15944-12 125**

Annex I (informative) **Aspects not currently addressed in this document 127**

Annex J (informative) **List of parts of the ISO/IEC 15944 series 130**

Annex K (informative) **Abstract of ISO/IEC 15944-12: ISO English, ISO French and ISO Chinese 131**

Bibliography 134

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

Foreword

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

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

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

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

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

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

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 15944-12:2020

Introduction

NOTE This document is intended to be used in conjunction with ISO/IEC 14662, ISO/IEC 15944-1, ISO/IEC 15944-5 and ISO/IEC 15944-8.

0.1 Purpose and overview

Modelling business transactions using scenarios and scenario components includes specifying the applicable constraints on the data content using explicitly stated rules. ISO/IEC 14662 identifies two basic classes of constraints, "internal constraints" and "external constraints". External constraints apply to most business transactions. External constraints have governance over any processing of personal information including that exchanged among parties to a business transaction and doing so from an information life cycle management (ILCM) requirements perspective.

Jurisdictional domains are the primary source of external constraints on business transactions (see Annex C). 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 document, unless they are implicitly needed to apply privacy protection requirements to data).

The focus of this document is on any kind of recorded information concerning identifiable living individuals as buyers in a business transaction or whose personal information is used in a business transaction or any type of commitment exchange.

This document describes the added business semantic descriptive techniques needed to support information life cycle management (ILCM) aspects as part of privacy protection requirements when modelling business transactions using the external constraints of jurisdictional domains. ILCM aspects are central to the ability to ensure that privacy protection requirements (PPR) are passed on and supported among all the parties to a business transaction using EDI.

This document applies to any organization which receives, creates, process, maintains, communicates, etc. personal information (PI) and, in particular, to those who receive, create, capture, maintain, use, store or dispose of sets of recorded information (SRIs) electronically. This document applies to private and public sector activities of Persons irrespective of whether such activities are undertaken on a for-profit or not-for-profit basis.

This document is intended for use by those organizations to which privacy protection requirements apply and who therefore need to ensure that the recorded information (electronic records and transactions) in their IT Systems is trustworthy, reliable and recognized as authentic. Typical users of this document include

a) managers of private and public sector organizations;

b) IT systems and records/information management system professionals;

c) privacy protection officers (PPOs) and other personnel in organizations, including those responsible for risk management; and

d) legal professionals and others within an organization responsible for information law compliance by the organization.

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

0.2 Use of ISO/IEC 14662 and ISO/IEC 15944

0.2.1 ISO/IEC 14662: Open-edi reference model[1)]

ISO/IEC 14662[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, taken from ISO/IEC 14662:2010, Figure 1, illustrates the Open-edi environment. (For definitions of the terms used, see Clause 3.)

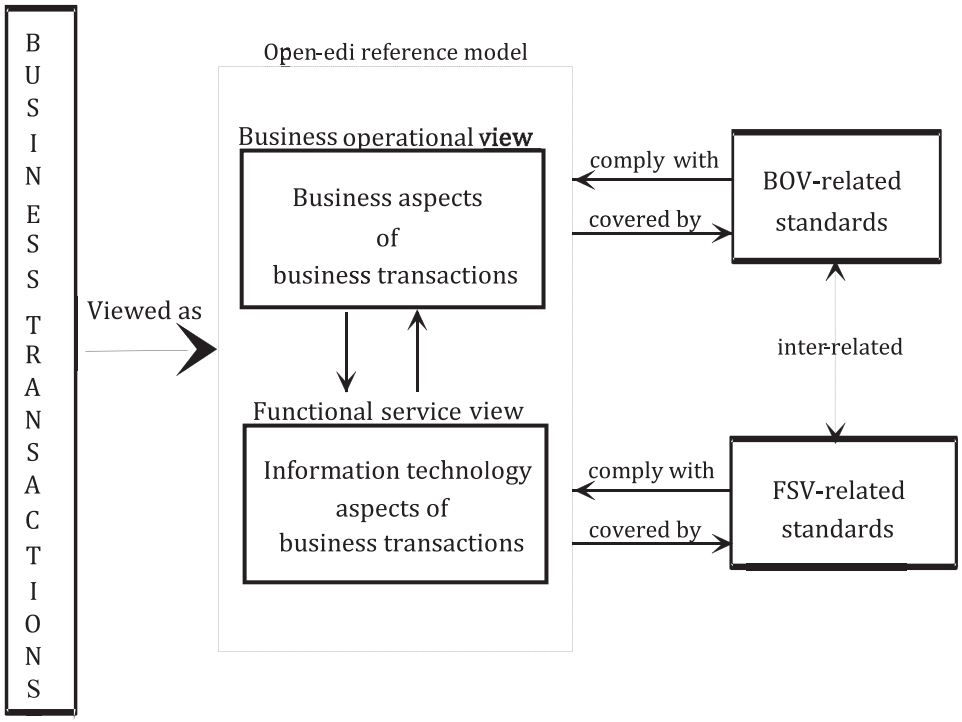

Figure 1 — Open-edi reference model environment

ISO/IEC 15944 is a multipart eBusiness standard which is based on and focuses on the BOV perspective of the ISO/IEC 14662 Open-edi reference model. This document focuses on addressing commonly definable aspects of external constraints that relate to information life cycle management (ILCM) in a privacy and data protection[3)] context 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 document (and related standards) addresses the transformation of these external constraints (business rules) into specified, registered, and re-useable scenarios and scenario components.

1) The Memorandum of Understanding between ISO, IEC, ITU and UN/ECE (2000) concerning standardization in the field of electronic business is based on this *Model*. See https://www.unece.org/fileadmin/DAM/oes/MOU/2000/24March2000_IEC_ISO_ITU.pdf.

2) ISO/IEC 14662 is freely-available at https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

3) "Privacy protection" is the common set of worldwide requirements. In the European Union, "data protection" is the equivalent concept (used mainly due to historical reasons). In many other non-European countries,(Australia, Canada, New Zealand, USA, etc., "privacy" is the legal term used in applicable legislation and pursuant regulations. This is because "privacy" applies to not just "data" but any form of recorded information containing "personal information". Thus from an international standards perspective "privacy protection" integrates "privacy" and "data protection" requirements. In many other countries, "privacy" is the legal term used in applicable legislation and pursuant regulations.

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

This document is based on ISO/IEC 14662 as well as existing parts of the ISO/IEC 15944 series, which serve as its key normative references and overall boundaries for the scope of this document. ISO/IEC 15944-5 and ISO/IEC 15944-8, in particular, serve as the basis for this document as they both focus on external constraints.

0.2.2 ISO/IEC 15944-1: Business operational view (BOV) – operational aspects of Open-edi for implementation

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

— Commercial frameworks and associated requirements.

— Legal frameworks and associated requirements.

— Public policy requirements particularly which apply to individuals, i.e., are rights of individuals, which are of a generic nature such as consumer protection, privacy protection, and accessibility (see ISO/IEC 15944-5:2008, 6.3).

— Requirements arising from the need to support cultural adaptability. This includes meeting localization and multilingual requirements, (e.g., as can 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 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, based on ISO/IEC 15944-1:2011, Figure 3, shows an integrated view of these business operational requirements. Since the focus of this document is that of external constraints for which jurisdictional domains are the primary source, these primary sources have been shaded in Figure 2.

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

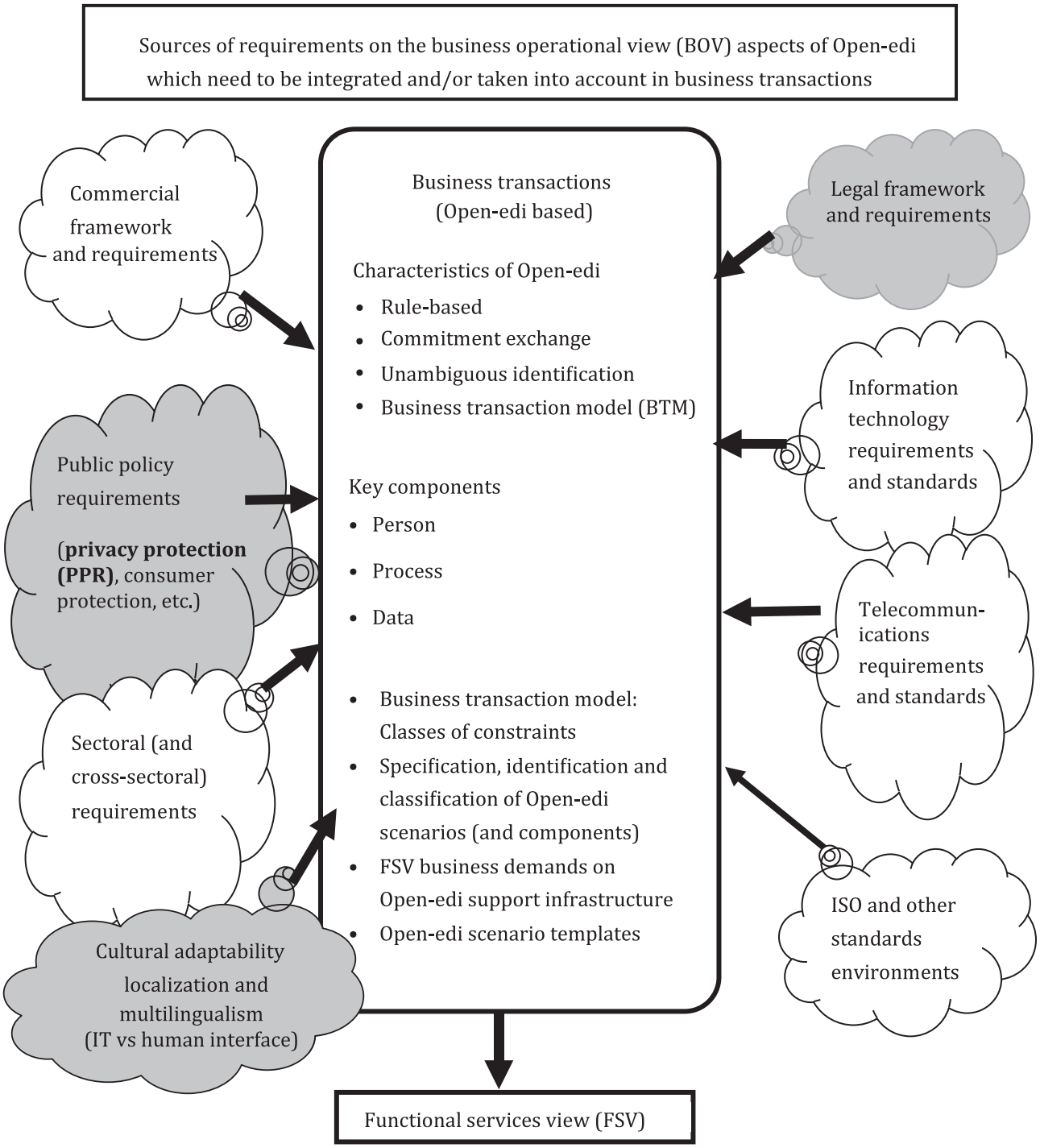

Figure 2 — Integrated view of business operational requirements with an external constraints focus

In electronic business transactions, whether undertaken on a for profit or not-for-profit basis, the key element is commitment exchange among Persons made through their decision-making applications (DMAs) of their information technology systems (IT Systems, see ISO/IEC 14662:2010, 5.2) acting on behalf of "Persons". "Persons" are the only entities able to make commitments.

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

The **business operational view (BOV)** was defined as:

*"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**".*

[SOURCE: ISO/IEC 14662:2010, 3.3]

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"[4]. 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".

0.2.3 Link to ISO/IEC 15944-5 and ISO/IEC 15944-8

ISO/IEC 15944-5 focuses on external constraints the primary source of which is jurisdictional domains, at various levels. It also identified a common class of external constraints known as "public policy", which apply where and when the "buyer" in a business transaction is an "individual". It identified three key sub-types, along with applicable rules; of public policy constraints, namely: "consumer protection", "privacy protection" and "individual accessibility" (see ISO/IEC 15944-5:2008, 6.3). In addition, ISO/IEC 15944-5 specifies how and where (common) external constraints of jurisdictional domains impact the "Person", "process", and "data "components of the business transaction model (BTM), as introduced in ISO/IEC 15944-1.

ISO/IEC 15944-8, which is based on ISO/IEC 15944-5, focuses on providing a more detailed identification and specification of the common privacy protection requirements as they apply to any business transaction where the buyer is an individual.

This document:

— is based on both ISO/IEC 15944-5 and ISO/IEC 15944-8;

— integrates applicable concepts and definitions, principles, rules, etc., found in both ISO/IEC 15944-5 and ISO/IEC 15944-8 (as well as applicable elements of the Open-edi reference model and other parts of the ISO/IEC 15944 series); and

— focuses on information life cycle management (ILCM) aspects at a more granular level, i.e., that required to be able to support implementation of the same.

0.3 Link to Privacy-by-Design (PbD) [48] approach

The overall purpose of the Privacy by Design (PbD) approach is to ensure that privacy protection requirements (as stated in applicable legal and/or regulatory requirements) are identified and specified in a systematic and rule-based manner for those developing any IT systems within their organization.

It is noted that although this is the first part in the ISO/IEC 15944 series in which Privacy by Design is formally mentioned, the PbD approach has always been supported and "imbedded" in the development of the ISO/IEC 15944 series. The need to comply with and support privacy protection requirements was already incorporated in ISO/IEC 15944-1:2002, D.1.1.

The development of the ISO/IEC 15944 series fully supports the seven "foundation principles" of the PbD approach[5]. In particular it provides the detailed rules, definitions and related guidelines necessary

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

5) 1. Proactive and not reactive; preventative and not reactive; 2. Privacy as the default setting; 3. Privacy embedded in design; 4. Full functionality – positive-sum, not zero-sum; 5. End to end security – full lifecycle protection; 6. Visibility and transparency – keep it open; 7. Respect for user privacy – keep it user-centric. [48]

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

to ensure that privacy protection requirements are identified and implemented not only throughout the entire life cycle of the recorded information involved, i.e., “cradle-to-grave”, information life cycle management (ILCM) but especially that for any personal information interchanged via EDI among parities to a particular business transaction.

0.4 Importance and role of terms and definitions

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

This subclause is included in each part of the ISO/IEC 15944 series to emphasize that harmonized concepts and definitions (and assigned terms) are essential to the continuity of the overall series.

In order to minimize ambiguity in the definitions and their associated terms, each definition and its associated term has been made available in at least one language other than English in the document in which it is introduced. In this context, it is noted that ISO/IEC 15944-7 already also contains human interface equivalents (HIEs) in ISO Chinese, ISO French, and ISO Russian[6)].

0.5 Based on rules and guidelines

This document is intended to be used by diverse sets of users having different perspectives and needs (see Figure 2).

The ISO/IEC 15944 series 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.

These rules also serve as a common understanding bridging the varied perspectives of the commercial framework, the legal framework, the information technology framework, standardisers, consumers, etc.[7)]

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

Throughout this document:

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

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

— the use of the words “person(s)” and “party (ies)” without a capital “P” indicates their use in a generic context independent of “Person”, as a defined concept in ISO/IEC 14662 and the ISO/IEC 15944 series.

NOTE A "party" to a business transaction has the properties and behaviours of a "Person”.

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

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

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

0.7 Use of “identifier” (in a business transaction) and roles of an individual

ISO/IEC 15944-1:2011, 6.1.4 focuses on the requirement for the unambiguous identification of entities in business transactions (see also ISO/IEC 15944-1:2011, Annex C). "Unambiguous" is a key issue in business transactions because states of ambiguity and uncertainty are an anathema from commercial, legal, consumer and information technology perspectives. Issues of unambiguousness apply to all aspects of a business transaction and even more so to those which are EDI-based. Open-edi transactions anticipate that all entities are fully and clearly identified prior to the instantiation of a business transaction.

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

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

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

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

0.9 Use of “privacy protection” in the context of business transaction, EDI and any type of commitment exchange

Jurisdictional domains, such as UN member states (and/or their administrative sub-divisions), have enacted various “privacy” laws, “data protection” laws, “protection of personal information” laws, etc. (as well as pursuant regulations). Some of these sources of legal requirements focus on the protection of personal information in IT systems only (e.g., “data protection”), while others focus on the protection of personal information irrespective of the medium (see ISO/IEC 15944-1:2011, 6.4.1) used for the recording of personal information and/or its communication to other Persons.

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

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

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

The concepts of “record”, “document”, “data”, “message”, etc., are defined and used in ISO standards and in different levels of jurisdictional domains. However, multiple differing definitions exist for each of these terms. To address this polysemy issue, the unifying concept and definition of “set of recorded information” was introduced and defined in ISO/IEC 15944-5.

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

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

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

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

— ***set of personal information (SPI)***;

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

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

0.11 Aspects currently not addressed

This first edition of this document focuses on the essential and basic ILCM aspects of privacy protection requirements.

Many other aspects identified in the development of this document remain to be addressed. For detailed information on these see Annex I.

0.12 IT-systems environment neutrality

This document, like all the other parts 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 document maximizes an IT-enabled approach to its implementation and maximizes semantic interoperability.

0.13 Organization and description of this document

This document identifies basic common requirements of information life cycle management (LCM) requirements in a privacy protection context, 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 a common approach and similar content in the ISO/IEC 15944 series, Clause 5 summarizes the 11 "Fundamental privacy protection principles" introduced and defined in detail in ISO/IEC 15944-8:2012, Clause 5 along with its associated rules and guidelines. Clause 5 also provides a link to related "consumer protection" and "individual accessibility" requirements. A key purpose of Clause 5 is to place privacy protection principles in the content of ILCM requirements. A related purpose is to bring forward the requirement that any and all sets of personal information (SPIs) are identified, i.e., tagged or labelled, as such in support of privacy protection requirements.

Clause 6 identifies an integrated (minimum) set of ILCM principles along with associated rules and guidelines required to support both general information law requirements and in particular those required to be implemented in support of privacy protection requirements.

Clause 7 focuses on the need to ensure accountability for and control of personal information by any organization (or public administration). Clause 8 expands on this by providing the rules governing specification of ILCM aspects of personal information, i.e., from an implementation perspective.

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

The fact that in their "normal" operations organizations need to undertake data conversions and data migration in the decision-making applications (DMAs) of their IT systems is recognized in Clause 9. However, it is also important that applicable privacy protection requirements remain being supported, i.e., within and among, organizations including data synchronization among their IT systems.

Clause 10 summarizes key rules and requirements found in ISO/IEC 15944-1, ISO/IEC 15944-5 and ISO/IEC 15944-8 which govern EDI of personal information between the primary ILCM Person, i.e., seller, and its use of agents and/or third parties. The clause concludes with a conformance statement.

Finally, annexes are provided for elaboration of points raised in the main body. Of these Annexes A and B are normative, and the remaining annexes are informative.

Annex A is a consolidated list of the definitions and their associated terms introduced in this document in ISO English and ISO French. (For the complete set of ISO French (and ISO Russian and ISO Chinese) equivalents of the entries in Clause 3, see ISO/IEC 15944-7.) As stated in the main body of this document, 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 document.

Annex C is common to ISO/IEC 15944-2, ISO/IEC 15944-4, ISO/IEC 15944-5 and ISO/IEC 15944-8. It summarizes the business transaction model (BTM).

The focus of Annex D is to link the ILCM process to the process phases of a business transaction. Annex E provides a generic approach to ILCM decisions in a privacy protection requirements context along with an ILCM compliance decision tree template.

The purpose of Annex F is to provide a generic approach to the identification of properties and behaviours of PI as SRI transitory records and their disposition/expungement. In Annex G some notes on referential integrity in Open-edi are presented.

Annex H provides details on a number of exclusions to the scope of this document while Annex I identifies aspects of the scope of this document which have not yet been addressed in this current edition.

Annex J provides the list of all parts in the ISO/IEC 15944 series. Annex K contains abstracts in ISO English, French and Chinese.

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

Information technology — Business operational view —

Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)

1 Scope

This document:

— 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;

— integrates existing normative elements in support of privacy and data protection requirements as are already identified in ISO/IEC 14662 and ISO/IEC 15944-1, ISO/IEC 15944-2, ISO/IEC 15944-4, ISO/IEC 15944-5, ISO/IEC 15944-8, ISO/IEC 15944-9, and ISO/IEC 15944-10;

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

— focuses on the life cycle management of personal information i.e., the contents of SPIs (and their SRIs) related to the business transaction interchanged via EDI as information bundles and their associated semantic components among the parties to a business transaction.

NOTE Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information as stated in this document serve as a minimum set of ILCM policy and operational requirements for all recorded information pertaining to a business transaction in particular, as well as ILCM implementation in any organization in general.

This document does not specify the technical mechanisms, i.e., functional support services (FSV) which are required to support BOV-identified requirements. Detailed exclusions to the scope of this document are provided in Annex H.

2 Normative references

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

ISO/IEC 14662:2010, *Information technology — Open-edi reference model*

ISO/IEC 15944-1:—,[8] *Information technology — Business operational view — Part 1: Operational aspects of Open-edi for implementation*

ISO/IEC 15944-5:2008, *Information technology — Business operational view — Part 5: Identification and referencing of requirements of jurisdictional domains as sources external constraints*

8) Third edition under preparation. Stage at time of publication: ISO/IEC DIS 15944-1.

© ISO/IEC 2020 – All rights reserved

Documents Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

ISO/IEC 15944-8:2012, *Information technology — Business operational view — Part 8: Identification of privacy protection requirements as external constraints on business transactions*

3 Terms and definitions

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

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

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

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

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

3.1
address
set of *data elements* (3.32) that specifies a *location* (3.67) to which a *recorded information* (3.110) item(s), a *business object(s)* (3.8), a material *object(s)* (3.73) and/or a person(s) can be sent or from which it can be received

Note 1 to entry: An address can be specified as either a physical address and/or electronic address.

Note 2 to entry: 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 to entry: 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).

[SOURCE: ISO/IEC 15944-2:2015, 3.1]

3.2
agent
Person (3.89) acting for another *Person* in a clearly specified capacity in the context of a *business transaction* (3.10)

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

[SOURCE: ISO/IEC 15944-1:—, 3.1]

3.3
anonymization
process (3.100) whereby the association between a *set of recorded information (SRI)* (3.128) and an identifiable *individual* (3.52) is removed where such an association may have existed

[SOURCE: ISO/IEC 15944-8:2012, 3.3.]

3.4
attribute
characteristic (3.14) of an *object* (3.73) or *entity* (3.43)

[SOURCE: ISO/IEC 15944-5:2008, 3.4]

3.5
authentication
provision of assurance of the claimed identity of an *entity* (3.43)

[SOURCE: ISO/IEC 10181-2:1996, 3.3]

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.6
back-up copy of data
copy that is any of the following: (a) additional resource or duplicate copy of *data* (3.28) on different a storage *medium* (3.68) stored off-line for emergency purposes; (b) disk, tape or other machine-readable copy of a data or program file; (c) data or program file recorded and stored off-line for emergency or archival purposes; and, (d) record that preserves the evidence and information it contains if the original is not available

3.7
business
series of *processes* (3.100), each having a clearly understood purpose, involving more than one *Person* (3.89), realized through the exchange of *recorded information* (3.110) and directed towards some mutually agreed upon goal, extending over a period of time

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

3.8
business object
unambiguously (3.141) identified, specified, referenceable, registered and re-useable *Open-edi scenario* (3.81) or *scenario component* (3.124) of a *business transaction* (3.10)

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

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

3.9
business operational view
BOV
perspective of *business transactions* (3.10) limited to those aspects regarding the making of *business* (3.7) decisions and *commitments* (3.20) among *Persons* (3.89), which are needed for the description of a business transaction

[SOURCE: ISO/IEC 14662:2010, 3.3]

3.10
business transaction
predefined set of activities and/or *processes* (3.100) of *Persons* (3.89) which is initiated by a *Person* to accomplish an explicitly shared *business* (3.7) goal and terminated upon recognition of one of the agreed conclusions by all the involved *Persons* although some of the recognition may be implicit

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

3.11
business transaction audit trail
chronological record of *IT system* (3.59) activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event pertaining to *sets of recorded information (SRIs)* (3.128) in a *business transaction* (3.10) through all its *processes* (3.100), i.e., from planning to the end of post-actualization

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

3.12
business transaction identifier
BTI
identifier assigned by a *seller* (3.125) or a *regulator* (3.116) to an instantiated *business transaction* (3.10) among the *Persons* (3.89) involved

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

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

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

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

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

[SOURCE: ISO/IEC 15944-5:2008, 3.12]

3.13
buyer
Person (3.89) who aims to get possession of a good, service and/or right through providing an acceptable equivalent value, usually in money, to the *Person* providing such a good, service and/or right

[SOURCE: ISO/IEC 15944-1:—, 3.8]

3.14
characteristic
abstraction of a *property* (3.102) of an *object* (3.73) or of a set of *objects*

Note 1 to entry: Characteristics are used for describing concepts.

[SOURCE: 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/IEC 10646.

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

3.16
code
<coded domain> identifier, i.e., an *ID code* (3.49), assigned to an *entity* (3.43) as member of a *coded domain* (3.17) according to the pre-established set of *rules* (3.120) governing that coded domain

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

3.17
coded domain
domain for which (1) the boundaries are defined and explicitly stated as a *rulebase* (3.121) of a *coded domain source authority (cdSA)* (3.18); and, (2) each *entity* (3.43) 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 (RS)* (3.114) of that *source authority (SA)* (3.129)

Note 1 to entry: The rules governing the assignment of an ID code to members of a coded domain reside with its source authority and form part of the coded domain registration schema (cdRS) of the source authority.

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

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

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

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

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

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

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

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

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

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

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

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

3.18
coded domain source authority
cdSA
Person (3.89), usually an *organization* (3.86), as a *source authority* (3.129) which sets the *rules* (3.120) governing a *coded domain* (3.17)

Note 1 to entry: 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 to entry: Specific sectors, (banking, transport, geomatics, agriculture, etc.), may have particular coded domain source authority(ies) whose coded domains are used in many other sectors.

Note 3 to entry: 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.

[SOURCE: ISO/IEC 15944-2:2015, 3.14]

3.19
collaboration space
business (3.7) activity space where an economic exchange of valued resources is viewed independently and not from the perspective of any *business* partner

Note 1 to entry: 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, etc. is not allowed because they view resource flows from a participant’s perspective.

[SOURCE: ISO/IEC 15944-4:2015, 3.12]

3.20
commitment
making or accepting of a right, obligation, liability or responsibility by a *Person* (3.89) that is capable of enforcement in the *jurisdictional domain* (3.62) in which the *commitment* (3.20) is made

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

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.21
composite identifier
identifier (in business transaction) (3.51) functioning as a single unique identifier consisting of one or more other identifiers, and/or one or more other *data elements* (3.32), whose interworkings are rule-based

Note 1 to entry: Identifiers (in business transactions) are for the most part composite identifiers.

Note 2 to entry: The rules governing the structure and working of a composite identifier should be specified.

Note 3 to entry: Most widely used composite identifiers consist of the combinations of: (a) the ID of the overall identification/numbering schema (the ISO/IEC 6523 series, ISO/IEC 7812, the ISO/IEC 7501 series, UPC/EAN, ITU-T E.164, etc.), which is often assumed; (b) the ID of the issuing organization (often based on a block numeric numbering schema); and, (c) the ID of the entities forming part of members of the coded domain of each issuing organization.

[SOURCE: ISO/IEC 15944-2:2015, 3.16]

3.22
computational integrity
expression of a *standard* (3.137) 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 1 to entry: 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.

[SOURCE: ISO/IEC 15944-2:2015, 3.18]

3.23
constraint
rule (3.120), explicitly stated, that prescribes, limits, governs or specifies any aspect of a *business transaction* (3.10)

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

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

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

[SOURCE: ISO/IEC 15944-1:—, 3.11]

3.24
consumer
buyer (3.13) who is an *individual* (3.52) to whom *consumer protection* (3.26) requirements are applied as a set of *external constraints* (3.45) on a *business transaction* (3.10)

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

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

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

[SOURCE: ISO/IEC 15944-1:—, 3.12]

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.25
consumer information profile
CIP
any one or more, *personal information profiles (PIPs)* (3.92) and any related *personal information* (3.90) on or about an identifiable *individual* (3.52) to which *consumer protection* (3.26) requirements apply, i.e., in addition to applicable *privacy protection* (3.97) requirements

3.26
consumer protection
set of *external constraints* (3.45) of a *jurisdictional domain* (3.62) as rights of a *consumer* (3.24) and thus as obligations (and possible liabilities) of a *vendor* (3.143) in a *business transaction* (3.10) which apply to the good, service and/or right forming the *object* (3.73) of the *business transaction* including associated information management and interchange requirements including applicable *set(s) of recorded information (SRIs)* (3.128)

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

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

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

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

3.27
controlled vocabulary
CV
vocabulary (3.144) whose entries, i.e., *definition* (3.37)/*term* (3.138) pairs, are controlled by a *source authority* (3.129) based on a *rulebase* (3.121) and *process* (3.100) for addition/deletion of entries

Note 1 to entry: In a controlled vocabulary (CV), there is a one-to-one relationship of definition and term.

EXAMPLE The contents of Clause 3 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 to entry: In a multilingual CV, the definition/term pairs in the languages used are deemed to be equivalent, i.e., with respect to their semantics.

Note 3 to entry: The rulebase governing a CV may include a predefined concept system.

[SOURCE: ISO/IEC 15944-5:2008, 3.34]

3.28
data
reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing

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

[SOURCE: ISO/IEC 2382:2015, 2122101]

3.29
data
<business transaction> representations of *recorded information* (3.110) that are being prepared or have been prepared in a form suitable for use in a computer system

[SOURCE: ISO/IEC 15944-1:—, 3.14]

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.30
data back-up
process (3.100) of duplicating and archiving *data* (3.28), often on a different storage *medium* (3.68), so that it may be restored to its original state after a data loss event

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

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

3.31
data conversion
process (3.100) of changing *data* (3.28), i.e., as *set(s) of recorded information (SRI(s))* (3.128), from one format or representation to another while maintaining the *characteristics* (3.14) of the *SRIs* including the authenticity, integrity, reliability and usability of the *sets of recorded information (SRI(s))* as well as relevant *information life cycle management (ILCM)* (3.58) requirements, and especially those of an *external constraints* (3.45) nature including *privacy protection* (3.97) requirements where the *data* involves *personal information* (3.90)

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

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

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

[SOURCE: Adapted from CAN/CGSB-72.34-2005, 3.16 and ISO 13008:2012, 3.5]

3.32
data element
unit of *data* (3.28) for which the *definition* (3.37), *identification* (3.50), representation and permissible values are specified by means of a set of *attributes* (3.4)

[SOURCE: ISO/IEC 15944-1:—, 3.15]

3.33
data migration
process (3.100) of moving *data* (3.28), i.e., as *sets of recorded information (SRIs)* (3.128) including their existing *characteristics* (3.14) from one *IT System* (3.59), (e.g., hardware or software configuration) to another, as required by changes in an *IT System* configuration or as requested by the user, while assuring that the *SRI(s)* will remain addressable and that data authenticity, integrity, reliability and usability of the *SRI(s)* will be maintained in the new environment

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

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

3.34
data synchronization
<business transaction> *process* (3.100) of continuous harmonization of a *set(s) of recorded information (SRI(s))* (3.128) among all the parties to a *business transaction* (3.10) to ensure that the current state of the content value(s) of such a *set(s) of recorded information (SRI(s))* is the same in the *IT systems* (3.59) of all the participating parties

[SOURCE: ISO/IEC 15944-8:2012, 3.35. Adapted from GS1 Global Traceability Standard (GDSN) Glossary.]

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.35
decision-making application
DMA
model (3.69) of that part of an *Open-edi system* (3.84) that makes decisions corresponding to the *role(s)* (3.119) that the *Open-edi Party* (3.78) plays as well as the originating, receiving and managing *data* (3.28) values contained in the instantiated *information bundles* (3.56) which is not required to be visible to the other *Open-edi Parties (OeP)*

[SOURCE: ISO/IEC 14662:2010, 3.7]

3.36
de facto language
natural language (3.72) used in a *jurisdictional domain* (3.62) 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 to entry: A de facto language of a jurisdictional domain is often established through long term use and custom.

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

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

3.37
definition
representation of a concept by a descriptive statement which serves to differentiate it from related concepts

[SOURCE: ISO 1087-1:2000, 3.3.1]

3.38
designation
representation of a concept by a sign which denotes it

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

[SOURCE: ISO/IEC 15944-2:2015, 3.79.]

3.39
eBusiness
business transaction (3.10), involving the making of *commitments* (3.20), in a defined *collaboration space* (3.19), among *Persons* (3.89) using their *IT systems* (3.59), according to *Open-edi standards* (3.82)

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

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

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

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

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

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.40
electronic address
address (3.1) used in a recognized electronic addressing scheme (telephone, telex, IP, etc.), to which *recorded information* (3.110) item(s) and/or *business object(s)* (3.8) can be sent to or received from a contact

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

3.41
electronic data interchange
EDI
automated exchange of any predefined and structured *data* (3.28) for *business* (3.7) purposes among information systems of two or more *Persons* (3.89)

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

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

3.42
electronic signature
signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with a particular digital/electronic *set of recorded information (SRI)* (3.128)

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

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

3.43
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 1 to entry: An entity exists whether data about it are available or not.

[SOURCE: ISO/IEC 2382:2015, 2121433]

3.44
expungement
process (3.100) of ensuring complete elimination, wiping out, destroying, or obliteration of any *recorded information* (3.110) [or *sets of recorded information (SRIs)*] (3.128), often including the *medium* (3.68) on which it is recorded, so that there can be no reconstruction of any its contents in whole or in part

3.45
external constraint
constraint (3.23) which takes precedence over *internal constraints* (3.60) in a *business transaction* (3.10), i.e., is external to those agreed upon by the parties to a business transaction

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

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

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

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

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

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

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

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

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

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

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

[SOURCE: ISO/IEC 15944-1:—, 3.23]

3.46
formal description technique
FDT
specification method based on a description *language* (3.63) using rigorous and *unambiguous* (3.141) *rules* (3.120) both with respect to developing expressions in the *language* (formal syntax) and interpreting the meaning of these expressions (formal semantics)

[SOURCE: ISO/IEC 14662:2010, 3.9]

3.47
functional service view
FSV
perspective of *business transactions* (3.10) limited to those information technology interoperability aspects of *IT Systems* (3.59) needed to support the execution of *Open-edi transactions* (3.85)

[SOURCE: ISO/IEC 14662:2010, 3.10]

3.48
human interface equivalent
HIE
representation of the *unambiguous* (3.141) and IT-enabled semantics of an IT interface equivalent (in a *business transaction* (3.10)), often the *ID code* (3.49) of a *coded domain* (3.17) (or a *composite identifier* (3.21)), in a formalized manner suitable for communication to and understanding by humans

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

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

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

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

3.49
ID code
identifier assigned by the *coded domain source Authority (cdSA)* (3.18) to a member of a *coded domain* (3.17) ID

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

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

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

© ISO/IEC 2020 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

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

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

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

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

3.50
identification
rule-based *process* (3.100), explicitly stated, involving the use of one or more *attributes* (3.4), i.e., *data element(s)* (3.32), whose value (or combination of values) are used to identify uniquely the occurrence or existence of a specified *entity* (3.43)

[SOURCE: ISO/IEC 15944-1:—, 3.26]

3.51
identifier
<business transaction> *unambiguous* (3.141), unique and a linguistically neutral value, resulting from the application of a rule-based *identification* (3.50) *process* (3.100)

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

Note 2 to entry: An identifier is a linguistically independent sequence of characters capable of uniquely and permanently identifying that with which it is associated [see ISO 19135:2015 (4.1.5)].

[SOURCE: ISO/IEC 15944-1:—, 3.27]

3.52
individual
Person (3.89) who is a human being, i.e., a natural person, who acts as a distinct indivisible *entity* (3.43) or is considered as such

[SOURCE: ISO/IEC 15944-1:—, 3.28]

3.53
individual accessibility
set of *external constraints* (3.45) of a *jurisdictional domain* (3.62) as rights of an *individual* (3.52) with disabilities to be able to use *IT Systems* (3.59) at the human, i.e., user, interface and the concomitant obligation of a *seller* (3.125) to provide such adaptive technologies

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

EXAMPLE Disabilities in the form of functional and cognitive limitations include: (a) people who are blind; (b) people with low vision; (c) people with colour blindness; (d) people who are hard of hearing or deaf, i.e., are hearing impaired; (e) people with physical disabilities; and, (f) people with language or cognitive disabilities.

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

3.54
individual anonymity
state of not knowing the identity or not having any recording of *personal information* (3.90) on or about an *individual* (3.52) as a *buyer* (3.13) by the *seller* (3.125) or *regulator* (3.116), (or any other party) to a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-8:2012, 3.57]

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.55
individual identity
ii
Person identity (Pi) (3.93) of an *individual* (3.52) consisting of the combination of the *persona* (3.95) information and *identifier* used by an individual in a *business transaction* (3.10), i.e., in the making of any kind of *commitment* (3.20)

[SOURCE: ISO/IEC 15944-8:2017, 3.59]

3.56
information bundle
IB
formal description of the semantics of the *recorded information* (3.110) to be exchanged by *Open-edi parties* (3.78) playing *roles* (3.119) in an *Open-edi scenario* (3.81)

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

3.57
information law
any law, regulation, policy, or code (or any part thereof) that requires the creation, receipt, collection, description or listing, production, retrieval, submission, retention, storage, preservation or destruction of *recorded information* (3.110), and/or that places conditions on the access and use, confidentiality, privacy, integrity, accountabilities, continuity and availability of the processing, reproduction, distribution, transmission, sale, sharing or other handling of *recorded information*

[SOURCE: ISO/IEC 15944-8:2012, 3.62]

3.58
information life cycle management
ILCM
series of actions and *rules* (3.120) governing the management and its *electronic data interchange (EDI)* (3.41) of *set(s) of recorded information (SRIs)* (3.128) *under the control of* (3.142) a *Person* (3.89) from its creation to final disposition, including *expungement* (3.44), in compliance with applicable *information law* (3.57) requirements

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

3.59
information technology system
IT System
set of one or more computers, associated software, peripherals, terminals, human operations, physical *processes* (3.100), information transfer means, that form an autonomous whole, capable of performing information processing and/or information transfer

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

3.60
internal constraint
constraint (3.23) which forms part of the *commitment(s)* (3.20) mutually agreed to among the parties to a *business transaction* (3.10)

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

[SOURCE: ISO/IEC 15944-1:—, 3.33]

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.61
IT-enablement
transformation of a current *standard* (3.137) used in *business transactions* (3.10), (e.g., *coded domains* (3.17)), from a manual to computational perspective so as to be able to support *commitment* (3.20) exchange and *computational integrity* (3.22)

[SOURCE: ISO/IEC 15944-5:2008, 3.65]

3.62
jurisdictional domain
jurisdiction, recognized in law as a distinct legal and/or regulatory framework, which is a source of *external constraints* (3.45) on *Persons* (3.89), their behaviour and the making of *commitments* (3.20) among *Persons* including any aspect of a *business transaction* (3.10)

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

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

EXAMPLE European Union (EU), NAFTA, WTO, WCO, ICAO, WHO, Red Cross, ISO, IEC, ITU-T.

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

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

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

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

3.63
language
system of signs for communication, usually consisting of a *vocabulary* (3.144) and *rules* (3.120)

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

[SOURCE: ISO 5127:2017, 1.1.2.01]

3.64
legally recognized name
LRN
persona associated with a *role* (3.119) of a *Person* (3.89) recognized as having legal status and so recognized in a *jurisdictional domain* (3.62) as accepted or assigned in compliance with the *rules* (3.120) applicable of that *jurisdictional domain*, i.e., as governing the *coded domain* (3.17) of which the *legally recognized name (LRN)* (3.64) is a member

Note 1 to entry: 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 to entry: The process of the establishment of a LRN is usually accompanied by the assignment of a unique identifier.

Note 3 to entry: 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).

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

Note 4 to entry: A Person may have more than one LRN (and associated LRN identifier).

[SOURCE: ISO/IEC 15944-5:2008, 3.72]

3.65
list
ordered set of *data elements* (3.32)

[SOURCE: ISO/IEC 15944-5:2008, 3.73]

3.66
localization
pertaining to or concerned with anything that is not global and is bound through specified sets of *constraints* (3.23) of: (a) a linguistic nature including *natural language* (3.72) and *special languages* (3.130) and associated multilingual requirements; (b) jurisdictional nature, i.e., legal, regulatory, geopolitical, etc.; (c) a sectoral nature, i.e., industry sector, scientific, professional, etc.; (d) a human rights nature, i.e., privacy, disabled/handicapped persons, etc.; (e) *consumer* (3.24) behaviour requirements; and/or, (f) safety or health requirements

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

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

3.67
location
place, either physical or electronic, that can be defined as an *address* (3.1)

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

3.68
medium
physical material which serves as a functional unit, in or on which information or *data* (3.28) is normally recorded, in which information or data can be retained and carried, from which information or data can be retrieved, and which is non-volatile in nature

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

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

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

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

[SOURCE: ISO/IEC 15944-1:—, 3.34]

3.69
model
abstraction of some aspect of reality

[SOURCE: ISO 19115:2014, 4.9]

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.70
multilingualism
ability to support not only *character sets* (3.15) specific to a (*natural*) *language* (or family of *languages* (3.63)) and associated *rules* (3.120) but also *localization* (3.66) requirements, i.e., use of a language from *jurisdictional domain* (3.62), sectoral and/or *consumer* (3.24) marketplace perspectives

[SOURCE: ISO/IEC 15944-5:2008, 3.82]

3.71
name
designation (3.38) of an *object* (3.73) by a linguistic expression

[SOURCE: ISO/IEC 15944-1:—, 3.35.]

3.72
natural language
language (3.63) which is or was in active use in a community of people, and the *rules* (3.120) of which are mainly deduced from the usage

[SOURCE: ISO 5127:2017, 3.1.5.2]

3.73
object
anything perceivable or conceivable

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

[SOURCE: ISO 1087-1:2000, 3.1.1]

3.74
object class
set of ideas, abstractions, or things in the real world that can be identified with explicit boundaries and meaning and whose *properties* (3.102) and behaviour follow the same *rules* (3.120)

[SOURCE: ISO/IEC 11179-1:2015, 3.3.18]

3.75
official language
external constraint (3.45) in the form of a *natural language* (3.72) specified by a *jurisdictional domain* (3.62) for official use by *Persons* (3.89) forming part of and/or subject to that jurisdictional domain for use in communication(s) either: (a) within that *jurisdictional domain*; and/or, (b) among such *Persons*, where such communications are *recorded information* (3.110) involving *commitment(s)* (3.20)

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

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

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

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

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

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

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

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

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

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

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

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

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

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

3.76
Open-edi
electronic data interchange (3.41) *(EDI)* among multiple autonomous *Persons* (3.89) to accomplish an explicit shared *business* (3.7) goal according to *Open-edi standards* (3.82)

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

3.77
Open-edi disposition
process (3.100) governing the implementation of formally approved records retention, destruction (or *expungement* (3.44)) or transfer of *recorded information* (3.110) *under the control of* (3.142) a *Person* (3.89) which are documented in a records scheduling and disposition authority(ies) or similar instrument of the *organization* (3.86)

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

[SOURCE: ISO/IEC 15944-5:2008, 3.90]

3.78
Open-edi party
OeP
Person (3.89) that participates in *Open-edi* (3.76)

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

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

3.79
Open-edi record retention
OeRR
specification of a period of time that a *set of recorded information (SRI)* (3.128) is required to be kept by a *Person* (3.89) in order to meet operational, legal, regulatory, fiscal or other requirements as specified in the *external constraints* (3.45) (or *internal constraints* (3.60)) applicable to a *Person* who is a party to a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-5:2008, 3.92]

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.80
Open-edi registry item
OeRI
recorded information (3.110) within a *registry* (3.115) relating to a specific *Open-edi scenario* (3.81) or *scenario components* (3.124) of a *scenario* (3.122) including linkage information to a *scenario* content

[SOURCE: ISO/IEC 15944-2:2015, 3.70]

3.81
Open-edi scenario
OeS
formal specification of a class of *business transactions* (3.10) having the same *business* (3.7) goal

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

3.82
Open-edi standard
standard (3.137) that complies with the *Open-edi* (3.76) reference model

[SOURCE: ISO/IEC 14662:2010, 3.19]

3.83
Open-edi support infrastructure
OeSI
model (3.69) of the set of functional capabilities for *Open-edi systems* (3.84) which, when taken together with the *decision-making applications* (3.35), allows *Open-edi* (3.76) parties to participate in *Open-edi transactions* (3.85)

[SOURCE: ISO/IEC 14662:2010, 3.20]

3.84
Open-edi system
information technology system (IT system) (3.59) which enables an *Open-edi party* (3.78) to participate in *Open-edi transactions* (3.85)

[SOURCE: ISO/IEC 14662:2010, 3.22]

3.85
Open-edi transaction
business transaction (3.10) that is in compliance with an *Open-edi scenario* (3.81)

[SOURCE: ISO/IEC 14662:2010, 3.23]

3.86
organization
unique framework of authority within which a person or persons act, or are designated to act, towards some purpose

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

EXAMPLE 1 An organization incorporated under law.

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

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

[SOURCE: ISO/IEC 15944-1:—, 3.44.]

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.87
organization part
any department, service or other *entity* (3.43) within an *organization* (3.86), which needs to be identified for information interchange

[SOURCE: ISO/IEC 6523-1:1998, 3.2]

3.88
organization Person
organization part (3.87) which has the *properties* (3.102) of a *Person* (3.89) and thus is able to make *commitments* (3.20) on behalf of that *organization* (3.86)

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

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

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

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

[SOURCE: ISO/IEC 15944-1:—, 3.46]

3.89
Person
entity (3.43), i.e., a natural or legal person, recognized by law as having legal rights and duties, able to make *commitment(s)* (3.20), assume and fulfil resulting obligation(s), and able of being held accountable for its action(s)

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

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

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

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

3.90
personal information
PI
any information on or about an identifiable *individual* (3.52) that is recorded in any form, including electronically or on paper

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

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

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.91
personal information controller
PIC
organization Person (3.88) authorized and so formally designated by the *organization* (3.86) to ensure that *personal information* (3.90) remains (fully) *under the control of* (3.142) the *organization* and ensures its *privacy protection transactional integrity (PPTI)* (3.99) in compliance with applicable *privacy protection* (3.97) requirements including in any use by the *organization* of *agents* (3.2) and/or *third parties* (3.139) in support of a *business transaction(s)* (3.10)

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

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

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

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

3.92
personal information profile
PIP
any collection of *personal information (PI)* (3.90) or aggregation of *sets of personal information (SPIs)* (3.127) including associated identifiers, linkages and/or associations, on or about an identifiable *individual* (3.52) being collected, retained, managed, used, etc., by any other *Person* (3.89) and in particular an *organization* (3.86) *or public administration* (3.105) and as such to which *privacy protection* (3.97) requirements apply including those of a *ILCM* (3.58) nature

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

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

3.93
Person identity
Pi
combination of *persona* (3.95) information and *identifier* (3.51) used by a *Person* (3.89) in a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-1:—, 3.49]

3.94
Person signature
signature, i.e., a *name* (3.71) representation, distinguishing mark or usual mark, which is created by and pertains to a *Person* (3.89)

[SOURCE: ISO/IEC 15944-1:—, 3.50]

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.95
persona
set of *data elements* (3.32) and their values by which a *Person* (3.89) wishes to be known and thus identified in a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-1:—, 3.51]

3.96
principle
fundamental, primary assumption and quality which constitutes a source of action determining particular objectives or results

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

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

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

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

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

3.97
privacy protection
set of *external constraints* (3.45) of a *jurisdictional domain* (3.62) pertaining to *recorded information* (3.110) on or about an identifiable *individual* (3.52), i.e., *personal information* (3.90), with respect to the creation, collection, management, retention, access and use and/or distribution of such *recorded information* about that *individual* including its accuracy, timeliness, and relevancy

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

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

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

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

3.98
privacy protection officer
PPO
organization Person (3.88) authorized by the *organization* (3.86) 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* (3.97) requirements for *information life cycle management* (3.58) not only within that *organization* but also with respect to any *electronic data interchange* (3.41) of *personal information* (3.90) on the *individual* (3.52) concerned with parties to the *business transaction* (3.10), including a *regulator* (3.116) where required, as well as any *agents* (3.2), *third parties* (3.139) involved in that *business transaction*

[SOURCE: ISO/IEC 15944-8:2012, 3.115]

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.99
privacy protection transactional integrity
PPTI
process (3.100) of ensuring that the *seller* (3.125) ensures that *data synchronization (in business transaction)* (3.34) requirements among the *IT systems* (3.59) of all parties to a *business transaction* (3.10) conform to, and are compliant with, applicable *privacy protection* (3.97) requirements (PPR) of (all) the *jurisdictional domain(s)* (3.62) applicable to that instantiated *business transaction* where and whenever such a business transaction involves a *buyer* (3.13) as an *individual* (3.52), i.e., whenever any part of the *recorded information* (3.110) of that *business transaction* involves *personal information (PI)* (3.90)

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

3.100
process
series of actions or events taking place in a defined manner leading to the accomplishment of an expected result

[SOURCE: ISO/IEC 15944-1:—, 3.53]

3.101
processing of personal information
any operation or set of operations which is performed upon *personal information* (3.90), whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, destruction, or expungement of such *personal information*

[SOURCE: ISO/IEC 15944-8:2012, 117]

3.102
property
peculiarity common to all members of an *object class* (3.74)

[SOURCE: ISO/IEC 15944-5:2008, 3.111]

3.103
pseudonym
use of a *persona* or other identifier by an *individual* (3.52) which is different from that used by the *individual* (3.52) with the intention that it be not linkable to that *individual* (3.52)

[SOURCE: ISO/IEC 15944-8:2012, 3.119]

3.104
pseudonymization
particular type of *anonymization* (3.3) that removes the association with an *individual* (3.52) and adds an association between a particular set of *characteristics* (3.14) relating to the *individual* and one more *pseudonym* (3.103)

[SOURCE: ISO/IEC 15944-8:2012, 3.120.]

3.105
public administration
entity (3.43), i.e., a *Person* (3.89), which is an *organization* (3.86) and has the added *attribute* (3.4) of being authorized to act on behalf of a *regulator* (3.116)

[SOURCE: ISO/IEC 15944-1:—, 3.54]

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.106
public policy
category of *external constraints* (3.45) of a *jurisdictional domain* (3.62) specified in the form of a right of an *individual* (3.52) or a requirement of an *organization* (3.86) and/or *public administration* (3.105) with respect to an *individual* pertaining to any exchange of *commitments* (3.20) among the parties concerned involving a good, service and/or right including information management and interchange requirements

Note 1 to entry: Public policy requirements may apply to any one, all or combinations of the fundamental activities comprising a business transaction, i.e., planning, identification, negotiation, actualization and post-actualization (see further ISO/IEC 15944-1:—, 6.3).

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

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

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

3.107
publicly available personal information
PAPI
personal information (3.90) about an *individual* (3.52) that the *individual* knowingly makes or permits to be made available to the public, or is legally obtained and accessed from: (1) government records that are available to the public; or, (2) information required by law to be made available to the public

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

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

[SOURCE: ISO/IEC 15944-8:2012, 3.123]

3.108
recognized individual identity
rii
individual identity (ii) (3.55) established to the extent necessary for the specific purpose of a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-8:2012, 3.124]

3.109
recognized Person identity
rPi
Person identity (Pi) (3.93), established to the extent necessary for a specific purpose in a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-1:—, 3.56]

3.110
recorded information
information that is recorded on or in a *medium* (3.68) irrespective of form, recording *medium* or technology used, and in a manner allowing for storage and retrieval

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

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

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

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

[SOURCE: ISO/IEC 15944-1:—, 3.56]

3.111
register
set of files containing identifiers assigned to items with descriptions of the associated items

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

3.112
registration
rule-based *process* (3.100), explicitly stated, involving the use of one or more *data elements* (3.32), whose value (or combination of values) is used to identify uniquely the results of assigning an *Open-edi registry item (OeRI)* (3.80)

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

3.113
registration authority
RA
Person (3.89) responsible for the maintenance of one or more *registration schemas (RS)* (3.114) including the assignment of a unique identifier for each recognized *entity* (3.43) in a *registration schema (RS)*

[SOURCE: ISO/IEC 15944-1:—, 3.57]

3.114
registration schema
RS
formal *definition* (3.37) of a set of *rules* (3.120) governing the *data* (3.28) fields for the description of an *entity* (3.43) and the allowable contents of those fields, including the rules for the assignment of *identifiers* (3.51)

[SOURCE: ISO/IEC 15944-1:—, 3.58]

3.115
registry
information system on which a *register* (3.111) is maintained

[SOURCE: ISO/IEC 15944-2:2015, 3.99]

3.116
regulator
Person (3.89) who has authority to prescribe *external constraints* (3.45) which serve as *principles* (3.96), policies or *rules* (3.120) governing or prescribing the behaviour of *Persons* involved in a *business transaction* (3.10) as well as the provisioning of goods, services, and/or rights interchanged

[SOURCE: ISO/IEC 15944-1:—, 3.59]

3.117
regulatory business transaction
RBT
class of *business transactions* (3.10) for which the explicitly shared goal has been established and specified by a *jurisdictional domain* (3.62), as a *Person* (3.89) in the *role* (3.119) of a *regulator* (3.116)

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

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

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

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

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

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

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

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

3.118
retention period
length of time for which *data* (3.28) on a *data medium* (3.68) is to be preserved

[SOURCE: ISO/IEC 15944-5:2008, 3.136]

3.119
role
specification which models an external intended behaviour (as allowed within a scenario) of an *Open-edi party* (3.78)

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

3.120
rule
statement governing conduct, procedure, conditions and relations

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

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

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

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

EXAMPLE A current and widely used FDT is "unified modelling language (UML)".

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

3.121
rulebase
pre-established set of *rules* (3.120) which interwork and which together form an autonomous whole

Note 1 to entry: One considers a rulebase to be to rules as database is to data.

[SOURCE: ISO/IEC 15944-2:2015, 3.102]

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.122
scenario
formal specification of a class of *business* (3.7) activities having the same business goal

[SOURCE: ISO 9735-1:2002, 4.89]

3.123
scenario attribute
formal specification of information, relevant to an *Open-edi scenario* (3.81) as a whole, which is neither specific to *roles* (3.119) nor to *Information Bundles* (3.56)

[SOURCE: ISO/IEC 14662:2010, 3.26]

3.124
scenario component
one of the three fundamental elements of a scenario, namely *role* (3.119), *information bundle* (3.56), and *semantic component* (3.126)

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

3.125
seller
Person (3.89) who aims to hand over voluntarily or in response to a demand, a good, service and/or right to another *Person* and in return receives an acceptable equivalent value, usually in money, for the good, service and/or right provided

[SOURCE: ISO/IEC 15944-1:—, 3.62]

3.126
semantic component
SC
unit of *recorded information* (3.110) *unambiguously* (3.141) defined in the context of the *business* (3.7) goal of the *business transaction* (3.10)

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

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

3.127
set of personal information
SPI
set of *recorded information (SRI)* (3.128) which is of the nature of, or contains, *personal information* (3.90)

3.128
set of recorded information
SRI
recorded information (3.110) of a *Person* (3.89), which is *under the control of* (3.142) the same and which is treated as a unit in its information life cycle

Note 1 to entry: 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 to entry: 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 to entry: 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.

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

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.129
source authority
SA
Person (3.89) recognized by other *Persons* as the authoritative source for a set of *constraints* (3.23)

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

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

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

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

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

Note 5 to entry: A source authority can undertake the role of registration authority or have this role undertaken on its behalf by another Person.

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

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

3.130
special language
language (3.63) for special purposes (LSP), language used in a subject field and characterized by the use of specific linguistic means of expression

Note 1 to entry: The specific linguistic means of expression always include subject-specific terminology and phraseology and also may cover stylistic or syntactic features.

[SOURCE: ISO/IEC 15944-5:2008, 3.139]

3.131
SPI expungement
process (3.100) of ensuring *expungement* (3.44) of a *set of personal information (SPI)* (3.127) in accordance with *privacy protection* (3.97) laws and regulations of the applicable *jurisdictional domain* (3.62)

Note 1 to entry: In a business transaction the seller shall ensure that all parties to the business transaction including agents, and/or third parties with whom such a set(s) of personal information was exchanged are also expunged, i.e., as part of ensuring transactional integrity.

3.132
SRI custody
association between a *Person* (3.89) having physical or virtual possession of a *set(s) of recorded information (SRIs)* (3.128) in the *role* (3.119) of an *agent* (3.2) or a *third party* (3.139) on behalf of the *Person* who is responsible for *under the control of* (3.142) associated legal/regulatory requirements pertaining to the *SRI(s)*, in particular *privacy protection* (3.97) requirements

Note 1 to entry: On the whole, the default is that of the SRI pertaining to any business transaction as being the Person in the role of seller for the instantiation of that business transaction.

3.133
SRI destruction
process (3.100) of eliminating or deleting a *set of recorded information* (3.128), beyond any possible reconstruction

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.134
SRI integrity
reliability and trustworthiness of a *set(s) of recorded information (SRI(s))* (3.128), as well as of any as copies, duplicates or comparable representations of the *SRI(s)*; and reliability and trustworthiness of the *IT system(s)* (3.59) in which the *SRI(s)* were recorded or stored to produce reliable and trustworthy copies and duplicates of *set(s) of recorded information (SRI(s))*

Note 1 to entry: SRI integrity is important in the electronic records provisions of the evidence acts in the phrases "the integrity of the electronic records system" and "the integrity of the electronic record." However, the term integrity is not defined in rules governing forensic data in 'evidence acts'. In the absence of a statutory or judicially created definition, the principles of this document shall serve as an operational definition of the word "integrity" when used in the context of 'evidence acts'.

Note 2 to entry: Certain evidence acts provide that the integrity of the electronic record may be proved by evidence of reliable and adequately implemented encryption.

Note 3 to entry: Organizations which implement the requirements of the rules (and associated guidelines) pertaining to records retention requirements and state changes to the content values of an SRI, as defined in Tables 1–7 are deemed to meet basic SRI integrity requirements.

3.135
SRI life cycle
stages in the life cycle of a *set of recorded information (SRI)* (3.128) which include but are not limited to its planning; creation and organization; the receipt and capture of data; the retrieval, processing, dissemination and distribution of a *set of recorded information (SRI)*; its storage, maintenance and protection; its archival preservation or destruction or *expungement* (3.44)

3.136
SRI retention period
specified period of time that a *set(s) of recorded information (SRI(s))* (3.128) is kept by a *Person* (3.89) in order to meet operational, legal, regulatory, fiscal or other requirements

3.137
standard
documented agreement containing technical specifications or other precise criteria to be used consistently as *rules* (3.120), guidelines, or *definitions* (3.37) of *characteristics* (3.14), to ensure that materials, products, *processes* (3.100) and services are fit for their purpose

Note 1 to entry: This is the definition of standard in ISO and IEC (see also ISO/IEC Guide 2:2004, 1.7).

[SOURCE: ISO/IEC 15944-1:—, 3.64]

3.138
term
designation (3.38) of a defined concept in a *special language* (3.130) by a linguistic expression

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

[SOURCE: ISO 1087-1:2000, 3.4.3]

3.139
third party
Person (3.89) besides the two primarily concerned in a *business transaction* (3.10) who is *agent* (3.2) of neither and who fulfils a specified *role* (3.119) or function as mutually agreed to by the two primary *Persons* or as a result of *external constraints* (3.45)

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

[SOURCE: ISO/IEC 15944-1:—, 3.65]

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

3.140
transitory record
set of recorded information (SRI) (3.128) that is required only for a very limited and specified (retention period) time to ensure the completion of a routine action or the preparation of a subsequent *set of recorded information (SRI)*

Note 1 to entry: A transitory SRI is expunged at the end of a short existence.

3.141
unambiguous
level of certainty and explicitness required in the completeness of the semantics of the *recorded information* (3.110) interchanged appropriate to the goal of a *business transaction* (3.10)

[SOURCE: ISO/IEC 15944-1:—, 3.66]

3.142
under the control of
set of requirements on an *organization* (3.86), especially those of *external constraint* (3.45) nature, i.e., *privacy protection* (3.97) and related *information law* (3.57) requirements, requiring full and complete *information life cycle management (ILCM)* (3.58) of *personal information* (3.90) as *set(s) of recorded information (SRIs)* (3.128) related to the agreed upon goal of the instantiated *business transaction* (3.10), including state changes to the content of the *SRIs* with respect to their creation/collection, recording processing, organization, storage, use, retrieval, disclosure, retrieval, aggregation, dissemination, *disposition* (including *expungement* (3.44)), *electronic data interchange (EDI)* (3.41), etc., and in particular that of any and all state changes in the *decision making application (DMAs)* (3.35) of the *organization* and any of its *agents* (3.2) and/or *third parties* (3.139) (as well as any other parties) to the *business transaction*

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

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

3.143
vendor
seller (3.125) on whom *consumer protection* (3.26) requirements are applied as a set of *external constraints* (3.45) on a *business transaction* (3.10)

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

Note 2 to entry: It is recognized that external constraints on a seller of the nature of consumer protection may be peculiar to a specified jurisdictional domain.

[SOURCE: ISO/IEC 15944-1:—, 3.67]

3.144
vocabulary
terminological dictionary which contains *designations* (3.38) and *definitions* (3.37) for one or more specific subject fields

Note 1 to entry: The vocabulary may be monolingual, bilingual or multilingual.

[SOURCE: ISO 1087-1:2000, 3.7.2]

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

4 Abbreviated terms

ATI	access to information
BTM	business transaction model
cdRS	coded domain registration schema
CGSB	Canadian General Standards Board
CRPD	(UN) Convention on Rights of Persons with Disabilities
FOI	freedom of information
FTC	(USA) Federal Trade Commission
HTML	hypertext mark-up language
HTTP	hypertext transfer protocol
ICT	information communication technologies
IPD	information processing domain
NAFTA	North American Free Trade Agreement
OeDT	Open-edi descriptive techniques
OeR	Open-edi registry
OeRA	Open-edi registration authority
Oe-RRDS	Open-edi records retention and disposal schedule
OVN	open value network
PbD	privacy by design
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
PPR	privacy protection requirement
pRS	persona registration schema
RAI	registration authority identifier
RRDS	records retention and disposal schedule
SI	semantic identifier
UML	unified modelling language (specified in ISO/IEC 19501 [25])

© ISO/IEC 2020 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020

5 Fundamental privacy protection principles

5.1 Overview

This Clause is based on ISO/IEC 15944-8:2012, Clause 5. The rules found in ISO/IEC 15944-8:2012, Clause 5 are specified in Annex B.7. As such, this document shall meet the requirements of ISO/IEC 15944-8.

Rule 001:

The rules stated in Annex B of other parts of the ISO/IEC 15944 series, and in particular those of ISO/IEC 15944-8 (see Annex B.7), are relevant and shall be applied as specified in Annex B.

Rule 002:

"Aspects not currently addressed" as identified in ISO/IEC 15944-8:2012, 1.3 also apply to this document.

"Unambiguous" is an issue in business transactions because states of ambiguity and uncertainty are not desired from commercial, legal, consumer and information technology perspectives. Issues of unambiguousness apply to all aspects of a business transactions and even more so to those which are EDI-based. The need to support unambiguity facilitates requires international semantic interoperability among parties to a business transaction and thus the use of human interface equivalents (HIEs). In support of these eBusiness requirements, Annex A provides the HIEs in ISO English and ISO French language equivalents and does so in a matrix-based approach which facilitates it being extended to other HIEs for other languages (see ISO/IEC 15944-7 which provides the fundamental principles and rules for the development of a definition for a concept and the rules governing development of multilingual equivalents, i.e., as HIEs).

5.2 Primary sources of privacy protection principles

Figure 3 is taken from ISO/IEC 15944-8:2012, Figure 3. It is repeated to provide an overview of the sources of requirements of the privacy protection principles as they also apply to this document.

© ISO/IEC 2020 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-12:2020