BS ISO/IEC 15944-17:2024

BSI Standards Publication

Information technology — Business operational view

Part 17: Fundamental principles and rules governing Privacy-by-Design (PbD) requirements in an EDI and collaboration space context

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 15944-17:2024

National foreword

This British Standard is the UK implementation of ISO/IEC 15944-17:2024.

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 committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 30384 1

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 2024.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 15944-17:2024

International Standard

ISO/IEC 15944-17

First edition
2024-04

Information technology — Business operational view —

Part 17: Fundamental principles and rules governing Privacy-by-Design (PbD) requirements in an EDI and collaboration space context

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

Partie 17: Règles et principes fondamentaux régissant les exigences de protection de la vie privée par conception (PbD) dans un contexte d'EDI et d'espace de collaboration

Reference number
ISO/IEC 15944-17:2024(en)

© ISO/IEC 2024

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 15944-17:2024

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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

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

Published in Switzerland

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 15944-17:2024

Contents

Page

Foreword ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **1**

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

4 Abbreviated terms ... **18**

5 Fundamental privacy protection principles ... **19**
- 5.1 Overview ... 19
- 5.2 Primary sources of privacy protection principles ... 20
- 5.3 Exceptions to the application of the privacy protection principles ... 20
- 5.4 Key eleven (11) privacy protection principles ... 20
- 5.5 Link to "consumer protection" and "individual accessibility" requirements ... 21
- 5.6 Requirements for tagging (or labelling) sets of personal information (SPIs) in support of privacy protection requirements (PPR) ... 22
- 5.7 Requirements for making all personal information (PI) available to the buyer where the buyer is an individual ... 22

6 Fundamental principles and rules governing Privacy by Design (PbD) requirements ... **22**
- 6.1 Overview ... 22
- 6.2 Fundamental principles of Privacy by Design ... 23
  - 6.2.1 Privacy by Design Principle 1: Proactive not reactive; preventative not remedial ... 23
  - 6.2.2 Privacy by Design Principle 2: Privacy as the Default Setting ... 23
  - 6.2.3 Privacy by Design Principle 3: Privacy Embedded into Design ... 24
  - 6.2.4 Privacy by Design Principle 4: Full Functionality — Positive-Sum, not Zero-Sum ... 25
  - 6.2.5 Privacy by Design Principle 5: End-to-End Safeguards — Full Information Management Life Cycle (ILCM) Protection ... 25
  - 6.2.6 Privacy by Design Principle 6: Visibility and Transparency — Keep it Open ... 26
  - 6.2.7 Privacy by Design Principle 7: Respect for User Privacy — Keep it User-Centric ... 26
- 6.3 Exceptions to the application of any of the Privacy by Design principles ... 27
- 6.4 Mapping the eleven (11) Privacy Protection Principles (PPP) to the seven (7) Privacy by Design principles ... 27

7 Collaboration space and privacy protection ... **27**
- 7.1 Overview ... 27
- 7.2 Collaboration space: Role of consumer (as individual), vendor and regulator ... 28

8 Ensuring that personal information is 'under the control of' the organization throughout its ILCM ... **30**
- 8.1 Overview ... 30
- 8.2 Rules governing the specification of ILCM aspects of personal information ... 31
- 8.3 Implementing "under the control of" and accountability ... 31

9 Conformance statement ... **32**
- 9.1 Overview ... 32
- 9.2 Conformance to the ISO/IEC 14662 Open-edi Reference Model and the multipart ISO/IEC 15944 eBusiness standard ... 33
- 9.3 Conformance to ISO/IEC 15944-17 ... 33
- 9.4 Conformance by agents and third parties to ISO/IEC 15944-17 ... 33

Annex A (normative) **Consolidated controlled vocabulary definitions and associated terms, as human interface equivalents (HIEs), with cultural adaptability: English and French language equivalency in an IT standardization context** ... **34**

Annex B (normative) **Consolidated set of rules in existing Parts of ISO/IEC 15944 of particular relevance to PbD as external constraints on business transactions which apply to personal information (PI) in an EDI and collaboration space context** ... **37**

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

Annex C (informative) **Mapping ISO/IEC 15944-8 Privacy Protection Principles (PPP) to the Privacy by Design principles** 54
Annex D (informative) **Exclusions to the scope of ISO/IEC 15944-17** 58
Annex E (informative) **Fair Information Principles / Fair Information Practices** 60
Annex F (informative) **Aspects currently not addressed** 61
Bibliography 62

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

Foreword

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

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

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

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

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

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

This document is intended to be used in conjunction with ISO/IEC 14662, ISO/IEC 15944-1, ISO/IEC 15944-4, ISO/IEC 15944-5, ISO/IEC 15944-8 and ISO/IEC 15944-12.

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

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

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

Introduction

0.1 Purpose and overview

The ISO/IEC 14662 and the ISO/IEC 15944 Business Operational View (BOV) series of standards focus on electronic data interchange (EDI) and “collaboration space” among Persons. Modelling business transactions using scenarios and scenario components includes specifying the applicable constraints on the data using explicitly stated rules. The ISO/IEC 14662 Open-edi Reference Model identifies two basic classes of constraints, "internal constraints" and "external constraints".

Jurisdictional domains are the primary source of external constraints on business transactions. Privacy protection is addressed as a common set of external constraint requirements coming from jurisdictional domains. Jurisdictional domains, such as UN member states and/or their administrative sub-divisions (see further 5.2 on sources of requirements), 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 used for the recording of personal information and/or its communication to other Persons.

The overall purpose of the PbD[2] approach is two folds: (1) to ensure that privacy protection requirements (as stated in applicable legal and/or regulatory requirements) are identified as early as possible in the business operational process; (2) are specified in a systematic and rule-based manner for those developing any IT systems within their organization.

The PbD approach has always been supported and embedded in ISO/IEC 15944 development work. The need for the multipart ISO/IEC series of standards to comply with and support privacy protection requirements was already incorporated in the1st edition of ISO/IEC 15944-1. The development of the multipart series of ISO/IEC 15944 eBusiness standards and relevant parts of the multipart ISO/IEC standard that focus on privacy protection requirements fully supports the seven (7) foundational principles of the PbD approach. [2] In particular, it provides the detailed rules, definitions and related guidelines necessary 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 for any personal information interchanged via EDI among parities to a particular business transaction.

This document highlights the requirements of ISO/IEC 14662 and ISO/IEC 15944 that focus on addressing commonly definable aspects of external constraints that relate to Privacy by Design in a privacy protection requirements (PPR) context when the source is a jurisdictional domain.[1)] 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.

This document also extends the requirements of ISO/IEC 14662 and ISO/IEC 15944 where relevant and describes the added business semantic descriptive techniques needed to support PbD aspects beyond privacy protection requirements (PPR) when modelling business transactions. PbD aspects are central to ensuring that PPR are embedded early on in the design, passed on and supported throughout the lifecycle of the personal information, among all the parties to a business transaction using EDI.

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

0.2.1 ISO/IEC 14662 "Open-edi Reference Model"[2)]

ISO/IEC 14662 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

1) See further sublause 0.2 below which identifies and summarizes the relevance of ISO/IEC 14662 and specific parts of the multipart ISO/IEC 15944 standard to this document.

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

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

related views of the business transaction. 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.

The delivery of Privacy by Design and 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 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. This is 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.

The first is the Business Operational View (BOV). The second is the Functional Service View (FSV). ISO/IEC 14662:2010, Figure 1 illustrates the realm to which PbD aligns with the Open-edi environment.

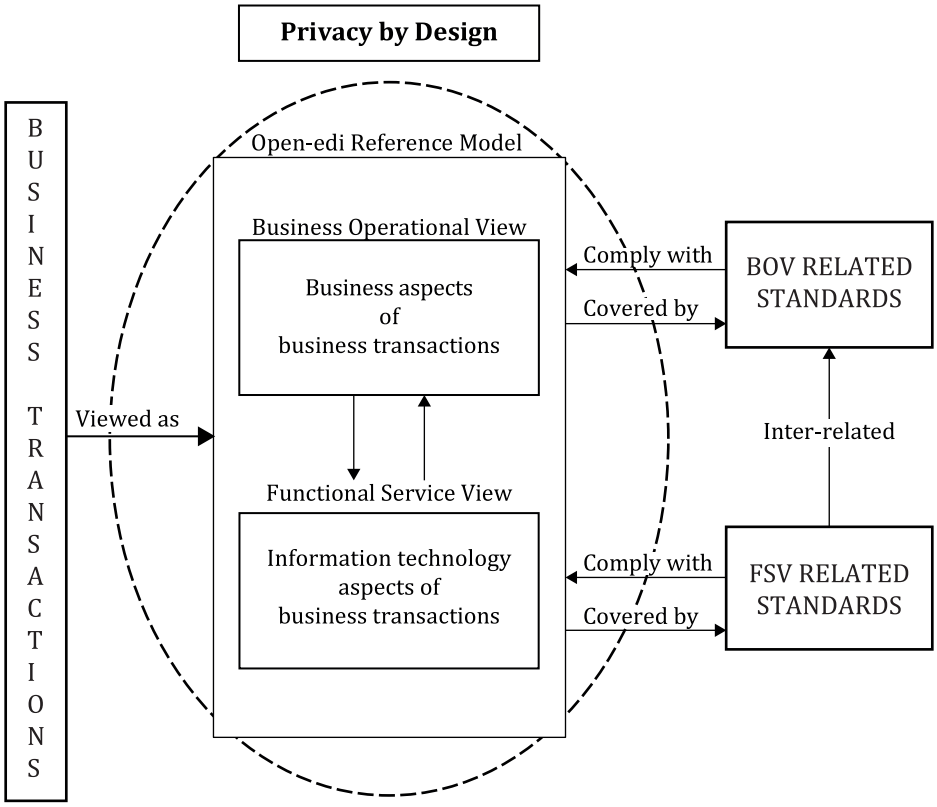

Figure 1 — Privacy by Design and Open-edi reference model environment

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 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, accessibility and human rights (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). One needs the ability to distinguish,

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

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 shows an integrated view of these business operational requirements. Since the focus of this document on Open-edi and Privacy by Design is that of external constraints for which jurisdictional domains are the primary source, these primary sources have been shaded (see 5.2 for sources of requirements).

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

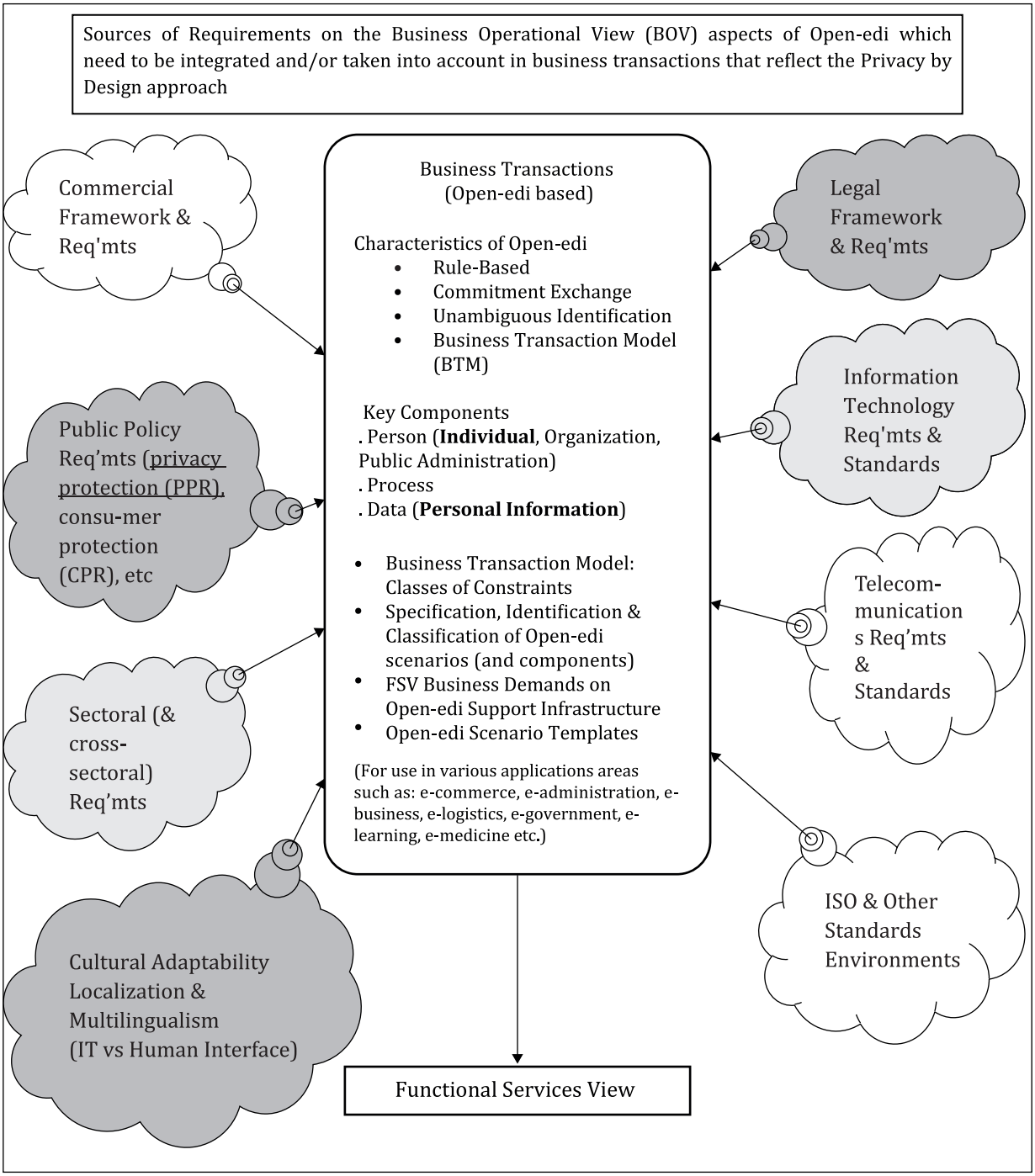

Figure 2 — Integrated view of business operational requirements with a focus on external constraints relevant to Privacy by Design

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[3)].

0.2.3 Links to ISO/IEC 15944-5, ISO/IEC 15944-8, ISO/IEC 15944-4 and ISO/IEC 15944-12

3) The text in this section is based on existing text in Section "0.3" in ISO/IEC 15944-1 and ISO/IEC 14662 (3rd edition). ISO/IEC 15944-7 "… eBusiness vocabulary" standard

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

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 identifies 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 uses ISO/IEC 15944-8 as the basis for establishing the fundamental privacy protection principles and rules that carry over to Privacy by Design. (Refer to Annex C.)

ISO/IEC 15944-4 helps to define the context in which PPP and PbD rules apply which is to the collaboration space. ISO/IEC 15944-4 provides the independent and the trading partner perspectives in the Open EDI ontology. In ISO/IEC 15944-1:2011, 6.1.3, Rule 1 states: *"Business transactions require both information exchange and commitment exchange."* REA firmly agrees with and helps give definition to this assertion. Reciprocal commitments are exchanged in REA via economic contracts that govern exchanges, while information exchange is tracked via business events that govern the state transitions of business transaction entities that represent various economic phenomena. (See further 7.2 for REA and collaboration space). It is the requirement for information exchange and more specifically, information exchange with an individual within a business transaction that will trigger privacy protection rules in an Open EDI environment.

ISO/IEC 15944-12 is based on both ISO/IEC 15944-5 and ISO/IEC 15944-8 and integrates applicable concepts and definitions, principles, rules, etc., found in both (as well as applicable elements of the Open-edi reference model and other parts of the ISO/IEC 15944 series). The focus is on information life cycle management (ILCM) aspects at a more granular level, i.e. that are required to be able to support implementation of the same. The focus 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. It describes the added business semantic descriptive techniques needed to support information life cycle management_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. ILCM is an important aspect of privacy protection and PbD.

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

The ISO/IEC 15944 series sets out the processes for achieving a common understanding of the BOV from commercial, legal, ICT, public policy and cross-sectoral perspectives. It is 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 associated terms, each definition and its associated term has been made available in at least one language other than English in the document in which it is introduced. In this context, it is noted that ISO/IEC 15944-7 already also contains human interface equivalents (HIEs) in Chinese, French, and Russian.

0.4 Basic rules and guidelines

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

---

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

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

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 for which there is mutual agreement. 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.

0.5 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";

— 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.

0.6 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.

0.7 Use of "jurisdictional domain" in the context of privacy protection requirements and Privacy by Design

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.

0.8 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

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

of Person are that they are required to be an identifiable, living individual. As a consequence, this can only apply to some proportion of the specific role players in a business transaction (including their personae) and not others.

0.9 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.

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 an SRI is of the nature of personal information or contains personal information, privacy protection requirements (PPR) apply. Within the context of PPR and with the focus of PbD the concept and definition of SPI applies:

set of personal information (SPI)

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

This document focuses on PbD in support of PPR and as such "set of personal information (SPI)" is used throughout this document.

0.10 Aspects currently not addressed

The first edition of this document focuses on the essential and basic PbD aspects in an EDI and collaboration space context. Other aspects identified in the development of this document remain to be addressed. For detailed information, see Annex F.

0.11 IT-systems environment neutrality

This document, like all the other parts of ISO/IEC 15944, does not assume or 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.

0.12 Organization and description of this document

The focus of this document is on any kind of recorded personal information concerning individuals as buyers in a business transaction or whose personal information is used in a business transaction or any type of commitment exchange. (Refer to the exclusion of Publicly Available Personal Information (PAPI) in Annex D).

This document applies to any organization which receives, creates, process, maintains, communicates, etc. personal information (PI) of a consumer 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.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

This document is intended for use by organizations 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 design management 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.

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 context of PbD requirements.

The purpose and focus of Clause 6 is to apply the seven PbD requirements in Open-edi business transaction context using the ISO/IEC 15944 rule-based approach as they apply to any organization (or public administration) in their interaction with any individual (outside of their organization) in the role of that individual as a buyer, i.e. consumer, in its interaction with the organization.

The importance of the concept of "collaboration space" introduced in ISO/IEC 15944-4 is carried forward and adapted in the privacy protection context in Clause 7, as the "privacy collaboration space (PCS)".

Clause 8 summarizes the Information Lifecycle Management (ILCM) aspects of PbD as part of privacy protection requirements when modelling business transactions using the external constraints of jurisdictional domains defined in detail in ISO/IEC 15944-12:2020.

Clause 9 provided the conformance requirements for this document.

Annex A provides the HIEs for all the terms and definitions newly defined in this document in addition to other parts of ISO/IEC 15944.

Annex B provides a consolidated set of rules defined in ISO/IEC 15944 relevant to this document.

Annex C provides the mapping of Privacy Protection Principles (PPP) to the Privacy by Design principles.

Annex D is a further description to the scope to clarify the exclusions that this document is not specifying.

Annex E introduces the concept of Fair Information Principles/Fair Information Practices in more detail.

Annex F provides additional information to the scope, stating those aspects that are yet addressed by the content of this document.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

Documents
Document Sharing Hub

Information technology — Business operational view —

Part 17: Fundamental principles and rules governing Privacy-by-Design (PbD) requirements in an EDI and collaboration space context

1 Scope

This document:

a) focuses on PbD aspects of privacy protection requirements as external constraints on any type of Person, (e.g. organization or public administration) involved in any kind of business transaction among such Persons which involves the electronic data interchange (EDI) of any personal information;

b) establishes a fundamental set of privacy principles known as Privacy by Design and assumptions based on primary sources;

c) integrates existing normative elements in support of PbD as are already identified in ISO/IEC 14662 and ISO/IEC 15944-1, ISO/IEC 15944-5, ISO/IEC 15944-8, ISO 15944-12;

d) provides overarching operational 'best practice' statements for associated (and not necessarily automated) processes, procedures, practices and governance requirements that need to act in support of implementing and enforcing technical mechanisms that support PbD in Open-edi transaction and collaboration space environments;

e) focuses on PbD related aspects of the life cycle management of and accountability for the 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.

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

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

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 15944-1:2011, *Information technology — Business operational view — Part 1: Operational aspects of open-edi for implementation*

ISO/IEC 15944-4:2015, *Information technology — Business operational view — Part 4: Business transaction scenarios — Accounting and economic ontology*

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

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

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

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

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)*

3 Terms and definitions

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

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

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

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

3.1
agent
Person (3.41) acting for another *Person* in a clearly specified capacity in the context of a *business transaction* (3.4)

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 15944-1:2011, 3.1]

3.2
business
series of *processes* (3.51), each having a clearly understood purpose, involving more than one *Person* (3.41), realized through the exchange of *recorded information* (3.57) and directed towards some mutually agreed upon goal, extending over a period of time

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

3.3
Business Operational View
BOV
perspective of *business transactions* (3.4) limited to those aspects regarding the making of *business* (3.2) decisions and *commitments* (3.9) among *Persons* (3.41), which are needed for the description of a *business transaction*

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

3.4
business transaction
predefined set of activities and/or *processes* of *Persons* (3.41) which is initiated by a *Person* to accomplish an explicitly shared *business* (3.2) 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]

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

3.5
business transaction identifier
BTI
identifier assigned by a *seller* (3.63) or a *regulator* (3.58) to an instantiated *business transaction* (3.4) among the *Persons* (3.41) involved

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

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

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

Note 4 to entry: As and where required by the applicable jurisdictional domain(s), the recorded information associated with the business transaction identifier (BTI) can 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]

3.6
buyer
Person (3.41) 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 15944-1:2011, 3.8]

3.7
coded domain
domain for which: (1) the boundaries are defined and explicitly stated as a rulebase of a coded domain Source Authority; and, (2) each *entity* (3.19) which qualifies as a member of that domain is identified through the assignment of a unique *ID code* (3.24) in accordance with the applicable Registration Schema of that *Source Authority* (3.66)

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 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: 3 A coded domain is a data set for which the content values of the data element 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; and/or, (b) one and/or more equivalent representations especially those in the form of human interface equivalent (HIE) (linguistic) expressions.

Note 5 to entry: In a coded domain the rules for assignment and structuring of the ID codes must 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 must 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”.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

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]

3.8
collaboration space
business (3.2) 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]

3.9
commitment
making or accepting of a right, obligation, liability or responsibility by a *Person* (3.41) that is capable of enforcement in the *jurisdictional domain* (3.34) in which the *commitment* (3.9) is made

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

3.10
constraint
rule (3.61), explicitly stated, that prescribes, limits, governs or specifies any aspect of a *business transaction* (3.4)

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 15944-1:2011, 3.11]

3.11
consumer
buyer (3.6) who is an *individual* (3.27) to whom *consumer protection* (3.13) requirements are applied as a set of *external constraints* (3.21) on a *business transaction* (3.4)

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 can be peculiar to a specified jurisdictional domain.

[SOURCE: ISO/IEC 15944-1:2011, 3.12]

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

3.12
consumer information profile
CIP
any one or more, *personal information profiles (PIPs)* (3.44) and any related *personal information* (3.42) on or about an identifiable *individual* (3.27) to which *consumer protection* (3.13) requirements apply, i.e., in addition to applicable *privacy protection* (3.48) requirements

[SOURCE: ISO/IEC 15944-12:2020, 3.25]

3.13
consumer protection
set of *external constraints* (3.21) of a *jurisdictional domain* (3.34) as rights of a *consumer* (3.11) and thus as obligations (and possible liabilities) of a *vendor* (3.71) in a *business transaction* (3.4) which apply to the good, service and/or right forming the object of the *business transaction* including associated information management and interchange requirements including applicable *set(s) of recorded information (SRIs)* (3.65)

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 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 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]

3.14
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]

3.15
data element
unit of *data* (3.14) for which the definition, *identification* (3.25), representation and permissible values are specified by means of a set of attributes

[SOURCE: ISO/IEC 15944-1:2011, 3.15]

3.16
Decision Making Application
DMA
model of that part of an Open-edi system that makes decisions corresponding to the *role(s)* (3.60) that the Open-edi Party plays as well as the originating, receiving and managing *data* (3.14) values contained in the instantiated *Information Bundles* (3.29) which is not required to be visible to the other Open-edi Parties (OeP)

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

3.17
eBusiness
business transaction (3.4), involving the making of *commitments* (3.9), in a defined *collaboration space* (3.8), among *Persons* (3.41) using their *IT Systems* (3.32), according to *Open-edi standards* (3.37)

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

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

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 15944-7:2015, 3.06]

3.18
Electronic Data Interchange
EDI
automated exchange of any predefined and structured *data* (3.14) for *business* (3.2) purposes among information systems of two or more *Persons* (3.41)

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

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

3.19
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]

3.20
expungement
process of ensuring complete elimination, wiping out, destroying, or obliteration of any *recorded information* (3.57) (or *sets of recorded information (SRIs))* (3.65), often including the *medium* on which it is recorded, so that there can be no reconstruction of any its contents in whole or in part

[SOURCE: ISO/IEC 15944-12:2020, 3.44]

3.21
external constraint
constraint (3.10) which takes precedence over *internal constraints* (3.36) in a *business transaction* (3.4), i.e., is external to those agreed upon by the parties to a *business transaction*

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

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

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

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

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

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

EXAMPLE 3 Hazardous wastes can 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.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

EXAMPLE 4 There can 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 15944-1:2011, 3.23]

3.22
Functional Service View
FSV
perspective of *business transactions* (3.4) limited to those information technology interoperability aspects of *IT Systems* (3.32) needed to support the execution of *Open-edi transactions*

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

3.23
Human Interface Equivalent
HIE
representation of the *unambiguous* (3.69) and IT-enabled semantics of an IT interface equivalent (in a *business transaction* (3.4)), often the *ID code* of a *coded domain* (or a composite identifier, in a formalized manner suitable for communication to and understanding by humans

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

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

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

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

3.24
ID code
identifier assigned by the *coded domain* (3.7) Source Authority (cdSA) to a member of a *coded domain* ID

Note 1 to entry: ID codes must 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; (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 must be specified as the pivot ID code.

Note 4 to entry: A coded domain may contain ID codes pertaining to entities which are not members as peer entities, i.e., have the same properties and behaviours, such as ID codes which pertain to predefined conditions other than member entities. If this is the case, the rules governing such exceptions must 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 modeling notation, an ID code is viewed as an instance of an object class.

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

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024

3.25
identification
rule-based *process*, explicitly stated, involving the use of one or more attributes, i.e., *data element(s)* (3.15), whose value (or combination of values) are used to identify uniquely the occurrence or existence of a specified *entity* (3.19)

[SOURCE: ISO/IEC 15944-1:2011, 3.26]

3.26
identifier (in a business transaction)
unambiguous (3.69), unique and a linguistically neutral value, resulting from the application of a rule-based *identification* (3.25) *process* (3.51)

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 19135-1:2015, 4.1.5}

[SOURCE: ISO/IEC 15944-1:2011, 3.27]

3.27
individual
Person (3.41) who is a human being, i.e., a natural person, who acts as a distinct indivisible *entity* (3.19) or is considered as such

[SOURCE: ISO/IEC 15944-1:2011, 3.28]

3.28
individual accessibility
set of *external constraints* (3.21) of a *jurisdictional domain* (3.34) as rights of an *individual* (3.27) with disabilities to be able to use *IT Systems* (3.32) at the human, i.e., user, interface and the concomitant obligation of a *seller* (3.63) 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]

3.29
Information Bundle
IB
formal description of the semantics of the *recorded information* (3.57) to be exchanged by Open-edi parties playing *roles* (3.60) in an Open-edi scenario

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

3.30
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* (3.57), 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]

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 15944-17:2024