TECHNICAL SPECIFICATION

ISO/IEC TS 38505-3

First edition
2021-12

Information technology — Governance of data —

Part 3: Guidelines for data classification

Technologies de l'information — Gouvernance des technologies de l'information —

Reference number
ISO/IEC TS 38505-3:2021(E)

© ISO/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

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

© ISO/IEC 2021 – All rights reserved

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Foundations **4**
4.1 Context 4
4.1.1 The data deluge 4
4.1.2 The strategic value of data 4
4.1.3 The risks associated with data 4
4.1.4 Consequences of failure 4
4.2 Data classification 5
4.3 Purpose of classification: 5
4.4 Engage and empower staff 6
4.5 Structure of this document 6

5 Roles and responsibilities **6**
5.1 General 6
5.2 Role of governing body 8
5.2.1 General 8
5.2.2 Understanding the role of data 8
5.2.3 Governance of data 8
5.2.4 Data classification approach 8
5.2.5 Data classification and risk management 8
5.2.6 Direct according to policy 9
5.2.7 Monitor conformance and performance 9
5.3 Role of management 9
5.3.1 General 9
5.3.2 Setting the scope of data classification 9
5.3.3 Propagating and implementing policy 9
5.3.4 Defining roles and responsibilities 10
5.3.5 Mobilizing the organization in support of the policy 10
5.3.6 Operation 11
5.3.7 Feedback from management to the governing body 11
5.3.8 Levels, discovery and attribution 11
5.4 Changing classifications 11
5.5 Defining the requirements: key considerations 12

6 Data classification framework **12**
6.1 Context 12
6.2 Identification 13
6.3 Implementation 13
6.4 Monitor/Improve 14

7 Guiding principles **14**
7.1 Simplicity 14
7.2 Default classifications 14
7.3 Interoperability 14
7.4 Equivalence 14
7.5 Use of data classification for processor and controller 15
7.6 Auditing, controls and compliance 15
7.7 Customer data 15
7.8 Assessment and reporting 16
7.9 Learning, maintaining and improving 16
7.10 Data protection 16

© ISO/IEC 2021 – All rights reserved

Bibliography **17**

© ISO/IEC 2021 – All rights reserved

Foreword

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

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

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 https://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. 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 40, *IT Service Management and IT Governance*.

A list of all parts in the ISO/IEC 38505 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 2021 – All rights reserved

Introduction

This document complements the existing International Standards on IT governance (ISO/IEC 38500) and data governance (ISO/IEC 38505-1). It is designed to provide practical guidance for organizations including governing bodies and management to allow them to:

— maintain an oversight of their data portfolio,

— understand the business context, value, sensitivity and risk associated with the data, and

— apply mechanisms that are both proportionate and appropriate, ensuring that data is protected, and is only used for intended purposes consistent with the organization's obligations.

© ISO/IEC 2021 – All rights reserved

Information technology — Governance of data —

Part 3:
Guidelines for data classification

1 Scope

This document provides essential guidance for members of governing bodies of organizations and management on the use of data classification as a means to support the organization's overall data governance policy and associated systems. It sets out important factors to be considered in developing and deploying a data classification system.

2 Normative references

There are no normative references in this document.

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
big data
extensive datasets, primarily in the data characteristics of volume, variety, velocity and/or variability, that require scalable technology for efficient storage, manipulation, management and analysis

Note 1 to entry: Big data is commonly used in many different ways, for example as the name of the scalable technology used to handle big data extensive datasets.

[SOURCE: ISO/IEC 20546:2019, 3.1.2, modified.]

3.2
customer data
data held on file about customers

Note 1 to entry: This comprises the information customers provide while interacting with the organization via their website, mobile applications, surveys, social media, marketing campaigns and other online and offline avenues.

3.3
data controller
person or organization who determines the purposes for which and the manner in which any data are to be processed, stored and used

[SOURCE: ISO 10667-1:2020, 3.10, modified.]

© ISO/IEC 2021 – All rights reserved

3.4
data processor
person [other than an employee of the *data controller* (3.3)] or organization that processes the data on behalf of the data controller.

[SOURCE: ISO 10667-1:2020, 3.11, modified.]

3.5
data quality owner
senior level employee accountable for the quality of one or more datasets

3.6
data sensitivity
property of data that reflects the potential harm of unauthorized disclosure

Note 1 to entry: The potential harm is to an individual or organization.

Note 2 to entry: Different levels of data protection can be used to account for varying levels of data sensitivity.

Note 3 to entry: Data sensitivity can be applied to specific categories of data such as healthcare, finance, *personal data* (3.12).

3.7
data sharing
access to or processing of the same data by more than one authorized entity

3.8
data stakeholder
natural or legal person that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to the processing of data

3.9
data steward
role within an organization responsible for ensuring that data-related work is performed according to policies and practices as established through data governance

Note 1 to entry: Typically, data stewards are responsible for business controls, data content and meta-data management related to a set of data assets, utilizing an organization's data governance processes to ensure fitness of data elements, both the content and metadata.

[SOURCE: ISO/TR 14872:2019, 3.5, modified.]

3.10
data taxonomy
scheme for organizing data based upon relationships and common characteristics

Note 1 to entry: A data taxonomy can include data categorization and data classification; it represents a convenient way to organize data.

3.11
organizational data
class of data objects under the control, by legal, contractual or other reasons, of an organization.

Note 1 to entry: Organizational data are all business information and data that are accessed, collected, used, processed, stored, shared, distributed, transferred, disclosed, destroyed or disposed of by any of the business units. Organization data can include, for example, financial records, business strategy documents, governing body and governance papers, staff information (employees, contractors, consultants), business analysis and intelligence, and executive information.

Note 2 to entry: Organizational protected data, or OPD, is organizational data for which protection is required based on the policies established by the governance of data process.

© ISO/IEC 2021 – All rights reserved

Note 3 to entry: Organizations have policies that govern the data under their control. ISO/IEC 38505-1 identifies and examines higher level governance concerns regarding the use of data which is relevant from the perspective of governance of data.

Note 4 to entry: Organizational data can contain OPD and PII.

[SOURCE: ISO/IEC 19944-1:2020, 3.4.2, modified.]

3.12
personally identifiable information
PII
personal data
any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person.

Note 1 to entry: The "natural person" in the definition is the *PII principal* (3.13). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd1:2018, 2.9, modified.]

3.13
PII principal
natural person to whom the *personally identifiable information (PII)* (3.12) relates

Note 1 to entry: Depending on the jurisdiction and the particular PII protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.14
semi-structured data
aggregate datatype whose components' datatypes and their labels are not pre-determined

Note 1 to entry: Semi-structured data are forms of *structured data* (3.15) that do not follow the formal structure of data models related to relational databases or other forms of databases.

Note 2 to entry: Examples of semi-structured data include the data that contain HTML tags or other markers to separate semantic elements and to represent hierarchies of records and fields within the data.

[SOURCE: ISO/IEC 20944-1:2013, 3.21.12.21, modified.]

3.15
structured data
data which are organized based on a pre-defined (applicable) set of rules.

Note 1 to entry: The predefined set of rules governing the basis on which the data are structured needs to be clearly stated and made known.

Note 2 to entry: A pre-defined data model is often used to govern the structuring of data.

Note 3 to entry: Examples of structured data are the data contained in relational databases.

[SOURCE: ISO/IEC 20546:2019, 3.1.35, modified.]

© ISO/IEC 2021 – All rights reserved