
**Information technology — Governance
of data —**

**Part 3:
Guidelines for data classification**

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





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

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

Bibliography	17
---------------------------	-----------

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.

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.

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.