BS ISO/IEC 38505-1:2017

BSI Standards Publication

Information technology — Governance of IT — Governance of data —

Part 1: Application of ISO/IEC 38500 to the governance of data

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 38505-1:2017

National foreword

This British Standard is the UK implementation of ISO/IEC 38505-1:2017.

The UK participation in its preparation was entrusted to Technical Committee IST/60/1, Governance of Information Technology.

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 2017.
Published by BSI Standards Limited 2017

ISBN 978 0 580 92321 0

ICS 35.020

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 30 April 2017.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 38505-1:2017

INTERNATIONAL STANDARD

ISO/IEC 38505-1

First edition
2017-04

Information technology — Governance of IT — Governance of data —

Part 1: Application of ISO/IEC 38500 to the governance of data

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

Partie 1: Application de l'ISO/IEC 38500 à la gouvernance des données

Reference number
ISO/IEC 38505-1:2017(E)

Documents
Document Sharing Hub
© ISO/IEC 2017

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 38505-1:2017

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **2**
4 Good governance of data **4**
4.1 Benefits of good governance of data 4
4.2 Responsibilities of the governing body 5
4.3 Governing body and oversight mechanisms 5
5 Principles, model and aspects for good governance of data **5**
6 Data accountability **6**
6.1 General 6
6.2 Collect 7
6.3 Store 8
6.4 Report 8
6.5 Decide 9
6.6 Distribute 9
6.7 Dispose 10
7 Guidance for the governance of data — Principles **10**
7.1 General 10
7.2 Principle 1 — Responsibility 10
7.3 Principle 2 — Strategy 11
7.4 Principle 3 — Acquisition 11
7.5 Principle 4 — Performance 11
7.6 Principle 5 — Conformance 11
7.7 Principle 6 — Human behaviour 12
8 Guidance for the governance of data — Model **12**
8.1 Applying the model 12
8.2 Internal requirements 13
8.3 External pressures 13
8.4 Evaluate 13
8.5 Direct 14
8.6 Monitor 14
9 Guidance for the governance of data — Data-specific aspects **15**
9.1 General 15
9.2 Value 15
9.2.1 General 15
9.2.2 Quality 15
9.2.3 Timeliness 16
9.2.4 Context 16
9.2.5 Volume 16
9.3 Risk 16
9.3.1 General 16
9.3.2 Management 16
9.3.3 Data classification schemes 17
9.3.4 Security 17
9.4 Constraints 17
9.4.1 General 17
9.4.2 Regulation and legislation 17
9.4.3 Societal 17
9.4.4 Organizational policy 18

© ISO/IEC 2017 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO/IEC 38505-1:2017

10 Application of the data accountability map **18**
Bibliography **20**

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 38505-1:2017

Foreword

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

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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC/JTC 1, *Information technology*, Subcommittee SC 40, *IT Service Management and IT Governance*.

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 38505-1:2017

Introduction

The objective of this document is to provide principles, definitions and a model for governing bodies to use when evaluating, directing and monitoring the handling and use of data in their organizations.

This document is a high level, principles-based advisory standard. In addition to providing broad guidance on the role of a governing body, it encourages organizations to use appropriate standards to underpin their governance of data.

All organizations use data, and the major proportion of this data is stored electronically across IT systems. With the advent of cloud computing, the realization of the potential of the "internet of things" and the increasing use of "big data" analytics, data is becoming easier to generate, gather, store and mine for useful information. This flood of data brings with it an urgent requirement and responsibility for governing bodies to ensure that valuable opportunities are leveraged and sensitive data is protected and secured.

This document has been prepared to provide guidelines to the members of governing bodies to apply a principles-based approach to the governance of data so as to increase the value of the data while decreasing the risks associated with this data. ISO/IEC 38500 provides principles and model for the governing bodies of organizations to guide their current use and to plan for their future use of Information technology (IT), and it is that document that is applied here.

As with ISO/IEC 38500, this document is addressed primarily to the governing body of an organization, and will equally apply regardless of the size of the organization or its industry or sector. Governance is distinct from management and thus we are concerned with evaluating, directing and monitoring the use of data, rather than the mechanics of storing, retrieving or managing the data. That being said, an understanding of some data management and techniques is outlined in order to enunciate the possible strategies and policies that could be directed by the governing body.

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 38505-1:2017

INTERNATIONAL STANDARD ISO/IEC 38505-1:2017(E)

Information technology — Governance of IT — Governance of data —

Part 1: Application of ISO/IEC 38500 to the governance of data

1 Scope

This document provides guiding principles for members of governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of data within their organizations by

— applying the governance principles and model of ISO/IEC 38500 to the governance of data,

— assuring stakeholders that, if the principles and practices proposed by this document are followed, they can have confidence in the organization's governance of data,

— informing and guiding governing bodies in the use and protection of data in their organization, and

— establishing a vocabulary for the governance of data.

This document can also provide guidance to a wider community, including:

— executive managers,

— external businesses or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies,

— internal and external service providers (including consultants), and

— auditors.

While this document looks at the governance of data and its use within an organization, guidance on the implementation arrangement for the effective governance of IT in general is found in ISO/IEC/TS 38501. The constructs in ISO/IEC/TS 38501 can help to identify internal and external factors relating to the governance of IT and help to define beneficial outcomes and identify evidence of success.

This document applies to the governance of the current and future use of data that is created, collected, stored or controlled by IT systems, and impacts the management processes and decisions relating to data.

This document defines the governance of data as a subset or domain of the governance of IT, which itself is a subset or domain of organizational, or in the case of a corporation, corporate governance.

This document is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. This document is applicable to organizations of all sizes from the smallest to the largest, regardless of the extent of their dependence on data.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes 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 38500, *Information technology — Governance of IT for the organization*

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 38505-1:2017

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 38500 and the following apply.

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

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

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

3.1
anonymization
process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

[SOURCE: ISO/IEC 29100:2011, 2.2]

3.2
big data
data set(s) with characteristics (e.g. volume, velocity, variety, variability, veracity, etc.) that for a particular problem domain at a given point in time cannot be efficiently processed using current/existing/established/traditional technologies and techniques in order to extract value

Note 1 to entry: The term 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:—[1)], 3.2.1]

3.3
cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

[SOURCE: ISO/IEC 17788:2014, 3.2.5]

3.4
data accountability
accountability for data and its use

Note 1 to entry: The "use" of data includes all activities associated with data.

3.5
de-identification
general term for any process of removing the association between a set of identifying data and the data subject

[SOURCE: ISO/TS 25237:2008, 3.18]

1) Under preparation.

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 38505-1:2017