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)

Contents

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*.

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.

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*

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.

国际标准

ISO/IEC 38505-1

第一版
2017-04

信息技术 • IT 治理 • 数据治理 | 第 1 部分: ISO/IEC 38500在数据治理中的应用

信息技术 • 信息技术治理 • 数据治理

第 1部分:ISO /IEC38500应用于数据治理

参考编号
ISO/IEC 38505-1:2017(E)

国际标准化组织 **发布**

ISO 版权局
布兰多内特Ch. 8 - CP 401
CH-
1214韦尔尼尔,日内瓦,瑞士电话。+4
1 22 749 0111
传真+41 22 749 09 47
copyright@iso.org
www.iso.org

内容

页面

前言

ISO(国际标准化组织)和IEC(国际电工委员会)构成了全球标准化的专门系统。作为ISO或IEC成员的国家机构参与国际通过相关组织设立的技术委员会制定国家标准来处理与特殊字段技术活动。ISO 和 IEC 技术委员会在共同感兴趣的领域开展协作。其他国际组织、政府和非政府机构在与ISO和IEC联络下也参与了这项工作。在信息技术领域,ISO和IEC设立了一个联合技术委员会,即ISO/IEC JTC 1。

ISO/IEC 指令第 1 部分介绍了用于开发本文档 d 的过程,这些程序用于进一步维护。特别是,应注意到不同类型的文件所需的不同批准标准。本文件是根据《关于起草的e我SO/我欧共体Directives,Part2(se e www.i所以.org g/directis).

提请注意本文件的某些内容可能是专利权的主题。ISO 和 IEC 不负责识别任何或所有此类专利权。在文件开发过程中确定的任何专利权的详细信息将在Intr ooton an 中d/o o on n r r r nei Oo lsofp在entdeclar在ionsreceived(se e www.i所以.org g/pat恩ts).

本文档中使用的任何商号都是为方便用户和不构成背书。

关于 ISO与符合性评估相关的特定术语和表达式的含义的解释,如以及有关ISO遵守世界贸易组织(WTO)原则的信息在Tec hncal Barrirrsto tad e (TBT) se e th following gURL:www.iso.org g/iso/foreword.html.

ths oou www as rredbyTechnicalCo毫米ittee我SO/我EC/JTC1,*我nformat约ntechnolog gy,* 小组委员会SC40,*它服务服务管理和它治理.*

介绍

本文件的目的是为理事机构提供原则、定义和模式,供其评估、指导和监测其组织中数据的处理和使用时使用。

本文档是一个高层次的、基于原则的咨询标准。除了提供广泛的指导上角色的a治理身体,它鼓励组织到使用适当标准以支撑他们的治理的数据。

所有组织都使用数据,并且这些数据的大部分以电子方式存储在 IT 系统中。与出现的云计算,实现的潜力的"互联网的事情"和越来越多地使用"大数据"分析,数据越来越容易生成,收集,存储和挖掘对于有用信息。这洪水的数据带来与它a紧急要求和责任治理身体到确保有价值的机会是杠杆和敏感数据是保护和安全。

编写本文件是为了向理事机构成员提供指导方针,以便对数据治理采用基于原则的办法,以提高数据的价值,同时减少相关风险智慧这个数据。ISO/IEC 38500为各组织的理事机构提供了原则和模式,以指导其当前使用,并规划其未来信息的使用技术(它),和它是文档是应用在这里。

与 ISO/IEC 38500 一样,本文档主要针对组织的理事机构,并同样适用,无论组织或其行业的规模如何,或部门。治理是独特的从管理和因此我们是关注与评估,导演和监测使用的数据,而比机械师的存储,检索或管理数据。那.被说,理解的一些数据管理和技术是概述在订单到名词可能战略和政策可以被定向由治理身体。

信息技术 • IT 治理 • 数据治理 |

第 1 部分:
ISO/IEC 38500 在数据治理中的应用

1 范围

本文件为各组织理事机构的成员提供了指导原则(该组织可包括所有者、董事、合作伙伴、执行经理或类似)在其组织内有效、高效和可接受的使用数据由

- 将 ISO/IEC 38500的治理原则和模型应用于数据治理,
- 向利益相关者保证,如果遵循本文件提出的原则和做法,他们可以对组织的数据治理,
- 通知和指导理事机构在其组织中使用和保护数据,以及
- 建立数据治理的词汇表。

本文档还可以为更广泛的社区提供指导,包括:

- 执行经理,
- 外部企业或技术专家,如法律或会计专家、零售或行业协会或专业机构,
- 内部和外部服务提供商(包括顾问),以及
- 核数师。

虽然本文档着眼于数据的治理及其在组织中的使用,但指南关于一般IT有效治理的实施安排在ISO/IEC/TS38501. ISO/IEC/TS 38501 中的构造有助于确定与IT和帮助定义有益的结果,并认同成功的证据。

本文档适用于当前和将来使用的数据的治理,由IT系统创建、收集、存储或控制,并影响管理流程和决策相关到数据。

本文档将数据的治理定义为 IT 治理的子集或域,而IT治理本身是组织的子集或域,或就公司而言,是公司治理。

本文档适用于所有组织,包括公共和私营公司、政府实体和非营利组织。本文档适用于从最小到最大的各种规模的组织,无论它们对数据的依赖程度如何。

2 规范参考

案文中提及的下列文件的方式,即部分或全部内容构成本文件的要求。对于日期参考,只有引用的版本适用。对于未注明日期参考,最新版的the引用文档(包括任何修正)适用。

ISO/IEC 38500,*信息技术与组织的 IT 治理*

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2）也可通过客服电话咨询 **025-85307007**。