International Standard

ISO/IEC 38500

Information technology — Governance of IT for the organization

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

Third edition
2024-02

Reference number
ISO/IEC 38500:2024(en)

© ISO/IEC 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

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Good governance of IT **3**
4.1 Outcomes of good governance of IT 3
4.1.1 Overview 3
4.1.2 Effective performance 3
4.1.3 Responsible stewardship 4
4.1.4 Ethical behaviour 4
4.2 Principles, model and framework 4
5 Principles for the governance of IT **5**
5.1 Overview 5
5.2 Purpose 6
5.2.1 Principle 6
5.2.2 Governance implications for use of IT 6
5.2.3 Outcomes 7
5.3 Value generation 7
5.3.1 Principle 7
5.3.2 Governance implications for use of IT 7
5.3.3 Outcomes 7
5.4 Strategy 8
5.4.1 Principle 8
5.4.2 Governance implications for use of IT 8
5.4.3 Outcomes 8
5.5 Oversight 8
5.5.1 Principle 8
5.5.2 Governance implications for use of IT 8
5.5.3 Outcomes 9
5.6 Accountability 9
5.6.1 Principle 9
5.6.2 Governance implications for use of IT 9
5.6.3 Outcomes 10
5.7 Stakeholder engagement 10
5.7.1 Principle 10
5.7.2 Governance implications for use of IT 10
5.7.3 Outcomes 10
5.8 Leadership 11
5.8.1 Principle 11
5.8.2 Governance implications for use of IT 11
5.8.3 Outcomes 11
5.9 Data and decisions 11
5.9.1 Principle 11
5.9.2 Governance implications for use of IT 11
5.9.3 Outcomes 12
5.10 Risk governance 12
5.10.1 Principle 12
5.10.2 Governance implications for use of IT 12
5.10.3 Outcomes 13
5.11 Social responsibility 13
5.11.1 Principle 13
5.11.2 Governance implications for use of IT 13

© ISO/IEC 2024 – All rights reserved

5.11.3 Outcomes 13
5.12 Viability and performance over time 13
5.12.1 Principle 13
5.12.2 Governance implications for use of IT 14
5.12.3 Outcomes 14
6 Model for the governance of IT 14
6.1 Introduction 14
6.2 Governance of IT practice 15
6.2.1 Engage stakeholders 15
6.2.2 Evaluate 15
6.2.3 Direct 16
6.2.4 Monitor 16
6.3 Management of IT practice 16
6.4 Framework for the governance of IT 16
7 Framework for the governance of IT 16
7.1 General 16
7.2 Elements of the framework 17
7.2.1 General 17
7.2.2 Direction 18
7.2.3 Capability 18
7.2.4 Policy 18
7.2.5 Delegation 19
7.2.6 Performance 19
7.2.7 Accountability 20
Bibliography 21

© ISO/IEC 2024 – 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).

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 had 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 40, *IT service management and IT governance*.

This third edition cancels and replaces the second edition (ISO/IEC 38500:2015), which has been technically revised.

The main changes are as follows:

— the principles for governance of IT and alignment to the principles of governance in ISO 37000 have been elaborated;

— the model has been updated to include "engage stakeholders";

— a framework for the governance of IT has been updated from ISO/IEC TR 38502.

A list of all parts in the ISO/IEC 38500 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

Introduction

The use of information technology (IT) is critical to the success of most organizations, not only as a supporting function, but also as part of the organization's capability to transform the organization. IT enables new business models and can substantially improve the organization's outcomes to meet the organization's stakeholder needs and expectations. The growing threat of cybersecurity and risks emanating from emerging technologies increases this focus.

The increasing potential of current and future IT requires the appropriate application of governance of IT to ensure that it fulfils the purpose of the organization in an effective, responsible and ethical manner, and that it aligns with the organization's strategic direction.

The objective of this document is to provide guidance to governing bodies on the responsible, innovative, sustainable and strategic use of IT, data and digital capabilities, so their organizations can fulfil their purpose in a manner expected by their stakeholders. This document provides principle-based guidelines and therefore does not include specific implementation detail.

It utilizes three tools for the governing body and associated governance and management practices to achieve good governance of IT:

1) Principles for the governance of IT — applying these principles to the responsible and strategic use of IT can lead to an organization that is more agile and adaptive.

2) Model for the governance of IT — the model shows the main governance tasks and interactions throughout the organization, leading to a clarity of decision-making and responsibilities for all aspects of the use of IT.

3) Framework for the governance of IT — the framework describes the elements through which the organization's governance of IT arrangements operate, which helps to ensure the critical actions of governance are considered and applied to the use of IT by the organization.

As the governance of IT is a domain of the governance of organizations, this document aligns to ISO 37000 and its principles of governance. This document can also be used in conjunction with other governance codes and principles for effective governance. This document can be used independently or to upgrade current governance based on the previous edition of ISO/IEC 38500.

This document is addressed primarily to the governing body but recognizes that governance occurs throughout the organization. It therefore provides guidance on the practice of governance of IT across the organization including the interaction and collaboration of all personnel, regardless of their job description.

© ISO/IEC 2024 – All rights reserved

Information technology — Governance of IT for the organization

1 Scope

This document provides guiding principles for members of governing bodies of organizations and those that support them on the effective, efficient and acceptable use of information technology (IT) within their organizations.

This document is applicable to:

— the governance of the organization's current, and future, use of IT;

— the governance of IT as a domain of governance of organizations.

In terms of audience, this document is applicable to:

— all organizations, including public and private companies, government entities, and not-for-profit organizations;

— organizations of all sizes, from the smallest to the largest, regardless of the extent of their use of IT.

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 37000, *Governance of organizations — Guidance*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 37000 and the following 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
direct
communicate desired purposes and outcomes

Note 1 to entry: Within the context of the governance of IT, directing involves setting objectives, strategies and policies to be adopted by the members of the organization, to ensure that the use of IT meets business objectives.

Note 2 to entry: Objectives, strategies and policies can be set by management if they have the relevant authority delegated to them by the governing body.

© ISO/IEC 2024 – All rights reserved