INTERNATIONAL STANDARD

ISO/IEC 38503

First edition
2022-01

Information technology — Governance of IT — Assessment of the governance of IT

Technologies de l'information — Gouvernance des TI — Évaluation de la gouvernance des TI

Reference number
ISO/IEC 38503:2022(E)

© ISO/IEC 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

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 2022 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Benefits of the assessment of the governance of IT ... **2**
4.1 Context ... 2
4.2 Benefits of assessing the governance of IT ... 2
5 Assessment scope and approach ... **3**
5.1 Establish scope ... 3
5.2 Assessment approach and involved parties ... 4
5.3 Roles, responsibilities and competencies ... 5
5.3.1 Roles associated with the assessment of the governance of IT ... 5
5.3.2 Governing body ... 6
5.3.3 Sponsor ... 6
5.3.4 Executive management ... 7
5.3.5 Assessment expert (assessor) ... 7
5.3.6 Business expert ... 7
5.3.7 Technical expert ... 8
6 Assessment of the governance of IT ... **8**
6.1 Assessment overview ... 8
6.2 Reference model for the governance of IT ... 9
6.2.1 Governance of IT practice areas ... 9
6.2.2 Governance of IT characteristics ... 9
6.2.3 Measurement model for the governance of IT ... 10
6.2.4 Assessment framework for the governance of IT ... 11
6.3 Assessment of the governance of IT ... 12
6.4 Governance of IT maturity model ... 12
7 Assessment activities ... **14**
7.1 Plan the assessment ... 14
7.2 Perform the assessment ... 15
7.2.1 Collect the data ... 15
7.2.2 Conduct the assessment ... 15
7.3 Report the assessment ... 16
Annex A (Informative) **Assessment framework — Governance of IT practice areas** ... **17**

© ISO/IEC 2022 – 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 documents 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 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*.

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 2022 – All rights reserved

Introduction

As part of their accountability for an organization, governing bodies are responsible and accountable for the current and future use of IT (information technology) within an organization. To meet this obligation, it is recommended that members of the governing body ensure that there is effective governance of IT within the organization, involving both their own activities in setting the direction for the organizational use of IT, as well as their oversight and evaluation of the management of IT within the organization.

ISO/IEC 38500 provides principles, definitions and a model for governing bodies to use when evaluating, directing and monitoring the use of IT in their organizations. This document provides guidance on how to assess an organization's governance of IT arrangements based on ISO/IEC 38500, ISO/IEC TS 38501 and ISO/IEC TR 38502.

The specific arrangements for the governance of IT vary from organization to organization. The variation depends on various factors including the organization's level of reliance on IT, both strategically and operationally, as well as the size and nature of the organization.

Governing bodies should seek continual improvement of the governance of IT as part of their overall accountability for organization governance and they should assess whether the current arrangements meet the needs of the organization. They should use such an assessment to improve the effectiveness of the governance of IT in a structured way, with a planned approach. The assessment should address not only management's approach to supporting the governance of IT but also the effectiveness of their own approach to evaluating, directing and monitoring management activities.

The purpose of this document is to assist governing bodies, authorized subcommittees and other key stakeholders in assessing the capability and maturity of the arrangements for the governance of IT in the organization.

It provides an objective approach for determining whether the governing body is appropriately governing IT, as well as examples of the practices and outcomes (referred to as 'characteristics' in this document) of the good governance of IT (see Tables A.1 to A.7 in Annex A). The outcomes of the assessment can be used to assist the governing body to determine where and how the governance of IT can be improved in the organization.

The primary audiences for this document are the governing body and its subcommittees, executive managers and assessors, who will also derive benefit from this document when planning and conducting an assessment of the organization's governance of IT.

© ISO/IEC 2022 – All rights reserved

Information technology — Governance of IT — Assessment of the governance of IT

1 Scope

This document provides guidance on the assessment of governance of information technology (IT) based on the principles, definitions and model for the governance of IT outlined in ISO/IEC 38500 and ISO/IEC TR 38502 and the implementation considerations outlined in ISO/IEC TS 38501.

This document includes approaches for conducting the assessment, the criteria against which the assessment can be made, guidance on the evidence that can be used for the assessment, as well as a method for determining the maturity of the organization's governance of IT.

This document is applicable to organizations of all sizes, 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/IEC 38500, *Information technology — Governance of IT for the organization*

ISO/IEC TS 38501, *Information technology — Governance of IT — Implementation guide*

ISO/IEC TR 38502, *Information technology — Governance of IT — Framework and model*

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
beneficial outcome
achievement of a high-level objective of the organization, related to the successful deployment and use of information technology

3.2
evidence of success
observable and measurable deliverables from information technology functions/processes that support and enable the achievement of beneficial outcomes

© ISO/IEC 2022 – All rights reserved