PD ISO/IEC TS 38501:2015

BSI Standards Publication

Information technology — Governance of IT — Implementation guide

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/IEC TS 38501:2015.

The UK participation in its preparation was entrusted by Technical Committee IST/60, IT Service Management and IT Governance, to Subcommittee 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.

Published by BSI Standards Limited 2015

ISBN 978 0 580 72038 3
ICS 35.080

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2015.

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL SPECIFICATION

ISO/IEC TS 38501

First edition
2015-04-01

Information technology — Governance of IT — Implementation guide

Technologies de l'information — Gouvernance des technologies de l'information — Guide d'implémentation

Reference number
ISO/IEC TS 38501:2015(E)

Published in Switzerland

Contents

Page

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 WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

This committee responsible for this document is ISO/IEC JTC 1, *Information Technology,* Subcommittee SC 40, *IT Service Maintenance and IT Governance.*

Introduction

Information technology (IT) has become pervasive in supporting and enabling the strategy of organizations and this prevalence mandates the governance of IT as an organizational imperative.

Organizations have made significant investments in IT to automate business processes and to communicate and transact electronically with their customers and suppliers. The benefits from these investments have unfortunately not always materialised and in some instances, organizations have incurred significant financial and reputational damage as a result of IT failures. This has further heightened governing body awareness of the need for the governance of IT and of their responsibilities in this regard.

It might be, however, that some governing bodies are uncertain of what arrangements they need to have in place for the governance of IT.

This Technical Specification has therefore been developed to provide guidance on the implementation of governance of IT within organizations. It considers governance, both from the perspective of gaining assurance that the risks associated with the use of IT are appropriately managed, as well as ensuring that the organization maximizes the value from its investments in IT.

It expands on the model and principles for good governance of IT described in ISO/IEC 38500 and ISO/IEC/TR 38502, and provides guidance on a methodology for implementing principles-based governance of IT.

Information technology — Governance of IT — Implementation guide

1 Scope

1.1 Overview

This Technical Specification provides guidance on how to implement arrangements for effective governance of IT within an organization.

1.2 Purpose

This Technical Specification identifies the key activities that an organization has to undertake to implement governance of IT, in accordance with ISO/IEC 38500.

It provides guidance on the design and establishment of the arrangements for the governance of IT, clarifying roles and responsibilities of key stakeholders within the organization, as well as providing examples of matters to consider in the design of the governance of IT.

1.3 Audience

This Technical Specification can be used by individuals responsible for governance of IT within an organization and individuals supporting in the governance of organizations. This Technical Specification is applicable to organizations of all sizes and types.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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, *Corporate governance of information technology*

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

3 Implementation approach

The implementation of the governance of IT should be based on a cyclic approach considering the model presented in ISO/IEC 38500, Figure 1. The first cycle of activities involves the establishment of the initial "implementation" or baseline, with subsequent cycles of the activities being used to support and enhance the governance of IT implementation by means of continual improvement. The duration of cycles will be different for each organization, depending on a number of factors including the organization's size, its industry, as well as the maturity of the governance of IT in the organization.

The implementation cycle comprises the following main activities which are expanded in the clauses below.

— **Establish and sustain enabling environment:** Commence by establishing an enabling environment which ensures that all stakeholders are appropriately identified and made aware of their roles and responsibilities. Subsequent cycles will ensure that the enabling environment is sustained.

— **Govern IT:** Progress to the evaluate, direct, and monitor activities to perform the governance of IT.

