PD ISO/IEC TR 38502:2014

BSI Standards Publication

Information technology — Governance of IT — Framework and model

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/IEC TR 38502:2014.

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

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 2014

ISBN 978 0 580 72039 0
ICS 35.020

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 28 February 2014.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/IEC TR 38502:2014

TECHNICAL REPORT

ISO/IEC TR 38502

First edition
2014-02-01

Information technology — Governance of IT — Framework and model

Technologies de l'information — Gouvernance des TI — Cadre général et modèle

Reference number
ISO/IEC TR 38502:2014(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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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.

ISO/IEC TR 38502 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Introduction

The measure of success for any investment in the use of information technology (IT), whether for new initiatives or on-going operations, is the benefit that it brings to the organization making the investment.

Benefits from investment in IT are typically not derived directly from the actual IT acquired or supported. Rather, realized benefits are a result of changes in business activities enabled by the use of the technology to meet organizational needs or requirements. Organizations need strategies and support arrangements for IT which maximize the value from such investments while managing the risks associated with the use of IT. Risks comprise such things as the failure to deliver required capabilities, failure of the business to achieve the required benefits, and the impact on the organization from IT failures leading to business disruption, breach of obligations, regulatory non-compliance, failures of security, loss of data, down time, etc.

One of the challenges for organizational investment in IT is ensuring that such investment and acquisition decisions are based on business strategies, priorities and needs. Those responsible for governance of the organization should therefore have appropriate oversight and involvement in decisions related to the use of IT in the business, to ensure that such decisions are based on business strategies, risk appetite, priorities and needs. The effort required to derive the expected benefits should be identified and understood.

ISO/IEC 38500[2] recognizes that the proper balance of demand and supply of IT is a requirement of good governance and management, which must be driven from the top of an organization. The objective of ISO/IEC 38500 is to provide guidance for the governing body of organizations when evaluating, directing and monitoring the use of IT in their organizations.

There is evidence of confusion in the market place regarding the use of the term *governance* when it applies to IT. For instance, there is often inappropriate application of the term *governance* to *management systems*, *control frameworks* and *information systems* that are not, in themselves, governance, but which are both outcomes of, and necessary enablers for, effective governance. As a result, there is often confusion about the respective roles of governance and management, and this has hindered the development of consistent guidance in respect of governance and the effective implementation of governance practices.

This Technical Report has been developed to clarify the distinction between the concepts of governance and management in respect of IT. It provides a model that illustrates the relationship between governance and management, and identifies the responsibilities associated with each.

Information technology — Governance of IT — Framework and model

1 Scope

This Technical Report provides guidance on the nature and mechanisms of governance and management together with the relationships between them, in the context of IT within an organization.

The purpose of this Technical Report is to provide information on a framework and model that can be used to establish the boundaries and relationships between governance and management of an organization's current and future use of IT.

This Technical Report provides guidance for:

— governing bodies;

— managers who have to work within the authority and accountability established by governance;

— advisors or those assisting in the governance of organizations of all sizes and types; and

— developers of standards in the areas of governance of IT and management of IT.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
acceptable
meets stakeholder expectations that are capable of being shown as reasonable or merited

2.2
accountable
answerable for actions, decisions and performance

2.3
accountability
state of being accountable

Note 1 to entry: Accountability relates to an allocated responsibility. The responsibility may be based on regulation or agreement or through assignment as part of delegation.

2.4
corporate governance
system by which corporations are directed and controlled

Note 1 to entry: Corporate governance is organizational governance applied to corporations.

Note 2 to entry: From Cadbury 1992 and OECD 1999.

Note 3 to entry: Definition is included to clarify changes in terminology from previous edition.

2.5
direct
communicate desired purposes and outcomes to

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