

[This is a preview - click here to buy the full publication](#)

INTERNATIONAL
STANDARD

**ISO/IEC
38500**

First edition
2008-06-01

Corporate governance of information technology

Gouvernance des technologies de l'information par l'entreprise

Reference number
ISO/IEC 38500:2008(E)



© ISO/IEC 2008

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents	Page
1 SCOPE, APPLICATION AND OBJECTIVES	1
1.1 Scope	1
1.2 Application	1
1.3 Objectives	1
1.4 Benefits of Using This Standard	1
1.5 Referenced Documents	3
1.6 Definitions.....	3
2 FRAMEWORK FOR GOOD CORPORATE GOVERNANCE OF IT	6
2.1 Principles	6
2.2 Model	7
3 GUIDANCE FOR THE CORPORATE GOVERNANCE of IT	9
3.1 General.....	9
3.2 Principle 1: Responsibility	9
3.3 Principle 2: Strategy	11
3.4 Principle 3: Acquisition	12
3.5 Principle 4: Performance	13
3.6 Principle 5: Conformance.....	14
3.7 Principle 6: Human Behaviour.....	15

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.

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 38500 was prepared by Standards Australia (as AS8015:2005) and was adopted, under a "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

ISO/IEC 38500 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 IT.

At the time of publication of this standard, JTC1 is continuing efforts to develop further documents relating to governance of Information Technology. These documents, which are likely to be released in the future as ISO/IEC Technical Reports and, possibly, as Standards, are expected to address a range of topics including:

- Governance of Projects involving IT Investment
- Governance of IT used in ongoing Business Operations

Introduction

The objective of this standard is to provide a framework of principles for Directors to use when evaluating, directing and monitoring the use of information technology (IT) in their organizations.

Most organizations use IT as a fundamental business tool and few can function effectively without it. IT is also a significant factor in the future business plans of many organizations.

Expenditure on IT can represent a significant proportion of an organization's expenditure of financial and human resources. However, a return on this investment is often not realized fully and the adverse effects on organizations can be significant.

The main reasons for these negative outcomes are the emphasis on the technical, financial and scheduling aspects of IT activities rather than emphasis on the whole business context of IT use.

This standard provides a framework for effective governance of IT, to assist those at the highest level of organizations to understand and fulfil their legal, regulatory, and ethical obligations in respect of their organizations' use of IT. The framework comprises definitions, principles and a model.

This standard is aligned with the definition of Corporate Governance that was published as a Report of the Committee on the Financial Aspects of Corporate Governance (the Cadbury Report) in 1992. The Cadbury Report also provided the foundation definition of Corporate Governance in the OECD Principles of Corporate Governance in 1999 (revised in 2004). Users of this standard are encouraged to familiarise themselves with the Cadbury Report and the OECD Principles of Corporate Governance.

Governance is distinct from management, and for the avoidance of confusion, the two concepts are clearly defined in the standard.

While this standard is addressed primarily to the governing body, which may in turn direct that certain actions be taken by the management of the organization, it also allows that, in some (typically smaller) organizations, the members of the governing body may also occupy the key roles in management. In this way, it ensures that the standard is applicable for all organizations, from the smallest, to the largest, regardless of purpose, design and ownership structure.

The standard is also intended to inform and guide those involved in designing and implementing the management system of policies, processes, and structures that support governance.

Corporate governance of information technology

1 SCOPE, APPLICATION AND OBJECTIVES

1.1 Scope

This standard provides guiding principles for directors of organizations (including owners, board members, directors, partners, senior executives, or similar) on the effective, efficient, and acceptable use of Information Technology (IT) within their organizations.

This standard applies to the governance of management processes (and decisions) relating to the information and communication services used by an organization. These processes could be controlled by IT specialists within the organization or external service providers, or by business units within the organization.

It also provides guidance to those advising, informing, or assisting directors. They include:

- senior managers;
- members of groups monitoring the resources within the organization;
- external business or technical specialists, such as legal or accounting; specialists, retail associations, or professional bodies;
- vendors of hardware, software, communications and other IT products;
- internal and external service providers (including consultants);
- IT auditors.

1.2 Application

This standard is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. The standard is applicable to organizations of all sizes from the smallest to the largest, regardless of the extent of their use of IT.

1.3 Objectives

The purpose of this standard is to promote effective, efficient, and acceptable use of IT in all organizations by:

- assuring stakeholders (including consumers, shareholders, and employees) that, if the standard is followed, they can have confidence in the organization's corporate governance of IT;
- informing and guiding directors in governing the use of IT in their organization; and
- providing a basis for objective evaluation of the corporate governance of IT.

1.4 Benefits of Using This Standard

1.4.1 General

This standard establishes principles for the effective, efficient and acceptable use of IT. Ensuring that their organisations follow these principles will assist

directors in balancing risks and encouraging opportunities arising from the use of IT.

This standard establishes a model for the governance of IT. The risk of directors not fulfilling their obligations is mitigated by giving due attention to the model in properly applying the principles.

The standard establishes a vocabulary for the Governance of IT.

1.4.2 Conformance of the organization

Proper corporate governance of IT may assist directors in assuring conformance with obligations (regulatory, legislation, common law, contractual) concerning the acceptable use of IT.

Inadequate IT systems can expose the directors to the risk of not complying with legislation. For example, in some jurisdictions, directors could be held personally accountable if an inadequate accounting system results in tax not being paid.

Processes dealing with IT incorporate specific risks that must be addressed appropriately. For example, directors could be held accountable for breaches of:

- security standards;
- privacy legislation;
- spam legislation;
- trade practices legislation;
- intellectual property rights, including software licensing agreements;
- record keeping requirements;
- environmental legislation and regulations;
- health and safety legislation;
- accessibility legislation;
- social responsibility standards.

Directors using the guidelines in this standard are more likely to meet their obligations.

1.4.3 Performance of the organization

Proper corporate governance of IT assists directors to ensure that IT use contributes positively to the performance of the organization, through:

- appropriate implementation and operation of IT assets;
- clarity of responsibility and accountability for both the use and provision of IT in achieving the goals of the organization;
- business continuity and sustainability;
- alignment of IT with business needs;
- efficient allocation of resources;
- innovation in services, markets, and business;
- good practice in relationships with stakeholders;
- reduction in the costs for an organization; and
- actual realization of the approved benefits from each IT investment.

1.5 Referenced Documents

The following documents are referred to in this Standard:

Report of the Committee on the Financial Aspects of Corporate Governance, Sir Adrian Cadbury, London, 1992 ISBN 0 85258 913 1

OECD Principles of Corporate Governance, OECD, 1999 and 2004

ISO Guide 73 2002 - Risk management — Vocabulary — Guidelines for use in standards.
