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)

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.

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.

1.6 Definitions

For the purpose of this Standard, the definitions below apply.

It is expected that an organization will adapt the terminology used within this standard to suit their circumstances or structure.

1.6.1 Acceptable

Meeting stakeholder expectations that are capable of being shown as reasonable or merited.

1.6.2 Corporate governance

The system by which organizations are directed and controlled. (adapted from Cadbury 1992 and OECD 1999)

1.6.3 Corporate governance of IT

The system by which the current and future use of IT is directed and controlled.

Corporate governance of IT involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organization.

1.6.4 Competent

Having the combination of knowledge, formal and informal skills, training, experience and behavioural attributes required to perform a task or role.

1.6.5 Director

Member of the most senior governing body of an organization. Includes owners, board members, partners, senior executives or similar, and officers authorized by legislation or regulation.

1.6.6 Human behaviour

The understanding of interactions among humans and other elements of a system with the intent to ensure well being and systems performance. Human

behaviour includes culture, needs and aspirations of people as individuals and as groups.

Note: In respect of IT, there are numerous groups or communities of humans, each with their own needs, aspirations and behaviours. For example, people who use information systems might exhibit needs relating to accessibility and ergonomics, as well as availability and performance. People whose job roles are changing because of the use of IT might exhibit needs relating to communication, training, and reassurance. People involved in building and operating IT capabilities might exhibit needs relating to working conditions and development of skills.

1.6.7 Information technology (IT)

Resources required to acquire, process, store and disseminate information. This term also includes "Communication Technology (CT)" and the composite term "Information and Communication Technology (ICT)".

1.6.8 Investment

Allocation of human, capital and other resources to achieve defined objectives and other benefits.

1.6.9 Management

The system of controls and processes required to achieve the strategic objectives set by the organisation's governing body. Management is subject to the policy guidance and monitoring set through corporate governance.

1.6.10 Organization

Any company, corporation, government, not-for-profit or other legally constituted body including associations, clubs, partnerships, government agencies, publicly listed companies, private companies and sole traders that has its own function(s) and administration.

1.6.11 Policy

Clear and measurable statements of preferred direction and behaviour to condition the decisions made within an organization.

1.6.12 Proposal

Compilation of benefits, costs, risks, opportunities, and other factors applicable to decisions to be made. Includes business cases.

1.6.13 Resources

People, procedures, software, information, equipment, consumables, infrastructure, capital and operating funds, and time.

1.6.14 Risk

Combination of the probability of an event and its consequence (ISO/IEC Guide 73).

Note: The consequences are impacts upon the organization. They can be negative, as in common usage, or 'opportunities' in common usage.

1.6.15 Risk management

Coordinated activities to direct and control an organization with regard to risk (ISO/IEC Guide 73).

1.6.16 Stakeholder

Any individual, group or organization who may affect, be affected by, or perceive themselves to be affected by, a decision or activity (adapted from ISO/IEC Guide 73).

1.6.17 Strategy

An organization's overall plan of development, describing the effective use of resources in support of the organization in its future activities. It involves setting objectives and proposing initiatives for action.

1.6.18 Use of IT

The planning, design, development, deployment, operation, management, and application of IT to meet the needs of the business. It includes both the demand for, and the supply of, IT services by internal business units, specialist IT units, or external suppliers and utility services (such as those providing software as services).

2 FRAMEWORK FOR GOOD CORPORATE GOVERNANCE OF IT

2.1 Principles

This section sets out six principles for good corporate governance of IT. The principles are applicable to most organizations.

The principles express preferred behaviour to guide decision making. The statement of each principle refers to what should happen, but does not prescribe how, when or by whom the principles would be implemented – as these aspects are dependent on the nature of the organization implementing the principles. Directors should require that these principles are applied.

2.1.1 Principle 1: Responsibility

Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.

2.1.2 Principle 2: Strategy

The organization's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy.

2.1.3 Principle 3: Acquisition

IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.

2.1.4 Principle 4: Performance

IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.

2.1.5 Principle 5: Conformance

IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.

2.1.6 Principle 6: Human Behaviour

IT policies, practices and decisions demonstrate respect for Human Behaviour, including the current and evolving needs of all the 'people in the process'.

2.2 Model

Directors should govern IT through three main tasks:

a) Evaluate the current and future use of IT.

b) Direct preparation and implementation of plans and policies to ensure that use of IT meets business objectives.

c) Monitor conformance to policies, and performance against the plans.

Figure 1 shows the IT Governance model of the cycle of Evaluate-Direct-Monitor. The text following Figure 1 explains the elements and relationships depicted.

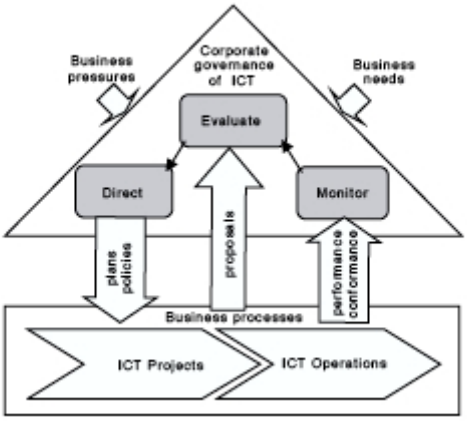

Figure 1 Model for Corporate Governance of IT

Evaluate

Directors should examine and make judgement on the current and future use of IT, including strategies, proposals and supply arrangements (whether internal, external, or both).

In evaluating the use of IT, directors should consider the external or internal pressures acting upon the business, such as technological change, economic and social trends, and political influences.

Directors should undertake evaluation continually, as pressures change.

Directors should also take account of both current and future business needs — the current and future organizational objectives that they must achieve, such as maintaining competitive advantage, as well as the specific objectives of the strategies and proposals they are evaluating.

Direct

Directors should assign responsibility for, and direct preparation and implementation of plans and policies. Plans should set the direction for investments in IT projects and IT operations. Policies should establish sound behaviour in the use of IT.

Directors should ensure that the transition of projects to operational status is properly planned and managed, taking into account impacts on business and operational practices as well as existing IT systems and infrastructure.

Directors should encourage a culture of good governance of IT in their organization by requiring managers to provide timely information, to comply with direction and to conform with the six principles of good governance.

If necessary, directors should direct the submission of proposals for approval to address identified needs.

Monitor

Directors should monitor, through appropriate measurement systems, the performance of IT. They should reassure themselves that performance is in accordance with plans, particularly with regard to business objectives.

Directors should also make sure that IT conforms with external obligations (regulatory, legislation, common law, contractual) and internal work practices.

> Note: Responsibility for specific aspects of IT may be delegated to managers within the organization. However, accountability for the effective, efficient and acceptable use and delivery of IT by an organization remains with the directors and cannot be delegated.

3 GUIDANCE FOR THE CORPORATE GOVERNANCE of IT

3.1 General

The following sections provide guidance for the general principles of good IT governance and the practices required to implement the principles.

The practices described are not exhaustive but provide a starting point for discussion of the responsibilities of Directors for the governance of IT. That is, the practices described are suggested guidance for IT Governance.

It is the responsibility of each organization, individually, to identify the specific actions required to implement the principles, giving due consideration to the nature of the organization, and appropriate analysis of the risks and opportunities of the use of IT.

As a basis for illustration, the practices described are applicable to most organizations (large or small), most of the time. Any variation should be well considered.

3.2 Principle 1: Responsibility

Evaluate
Directors should evaluate the options for assigning responsibilities in respect of the organization's current and future use of IT. In evaluating options, directors should seek to ensure effective, efficient, and acceptable use and delivery of IT in support of current and future business objectives. Directors should evaluate the competence of those given responsibility to make decisions regarding IT. Generally, these people should be business managers who are also responsible for the organization's business objectives and performance, assisted by IT specialists who understand business values and processes.
Direct
Directors should direct that plans be carried out according to the assigned IT responsibilities. Directors should direct that they receive the information that they need to meet their responsibilities and accountability.

Monitor
Directors should monitor that appropriate IT governance mechanisms are established. Directors should monitor that those given responsibility acknowledge and understand their responsibilities. Directors should monitor the performance of those given responsibility in the governance of IT (for example, those people serving on steering committees or in presenting proposals to directors).

3.3 Principle 2: Strategy

Evaluate

Directors should evaluate developments in IT and business processes to ensure that IT will provide support for future business needs.

In considering plans and policies, directors should evaluate IT activities to ensure they align with the organization's objectives for changing circumstances, take consideration of better practices and satisfy other key stakeholder requirements.

Directors should ensure that IT use are subject to appropriate risk assessment and evaluation, as described in relevant international and national standards.

Direct

Directors should direct the preparation and use of plans and policies that ensure the organization does benefit from developments in IT.

Directors should also encourage the submission of proposals for innovative uses of IT that enable the organization to respond to new opportunities or challenges, undertake new businesses or improve processes.

Monitor

Directors should monitor the progress of approved IT proposals to ensure that they are achieving objectives in required timeframes using allocated resources.

Directors should monitor the use of IT to ensure that it is achieving its intended benefits.

3.4 Principle 3: Acquisition

Evaluate
Directors should evaluate options for providing IT to realize approved proposals, balancing risks and value for money of proposed investments.
Direct
Directors should direct that IT assets (systems and infrastructure) be acquired in an appropriate manner, including the preparation of suitable documentation, while ensuring that required capabilities are provided. Directors should direct that supply arrangements (including both internal and external supply arrangements) support the business needs of the organization.
Monitor
Directors should monitor IT investments to ensure that they provide the required capabilities. Directors should monitor the extent to which their organization and suppliers maintain the shared understanding of the organization's intent in making any IT acquisition.

3.5 Principle 4: Performance

Evaluate
Directors should evaluate the means proposed by the managers to ensure that IT will support business processes with the required capability and capacity. These proposals should address the continuing normal operation of the business and the treatment of risk associated with the use of IT.
Directors should evaluate the risks to continued operation of the business arising from IT activities.
Directors should evaluate the risks to the integrity of information and the protection of IT assets, including associated intellectual property and organizational memory.
Directors should evaluate options for assuring effective, timely decisions about use of IT in support of business goals.
Directors should regularly evaluate the effectiveness and performance of the organization's system for Governance of IT.
Direct
Directors should ensure allocation of sufficient resources so that IT meets the needs of the organization, according to the agreed priorities and budgetary constraints.
Directors should direct those responsible to ensure that IT supports the business, when required for business reasons, with correct and up-to-date data that is protected from loss or misuse.
Monitor
Directors should monitor the extent to which IT does support the business.
Directors should monitor the extent to which allocated resources and budgets are prioritised according to business objectives.
Directors should monitor the extent to which the policies, such as for data accuracy and the efficient use of IT, are followed properly.

3.6 Principle 5: Conformance

Evaluate
Directors should regularly evaluate the extent to which IT satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines. Directors should regularly evaluate the organization's internal conformance to its system for Governance of IT.
Direct
Directors should direct those responsible to establish regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines. Directors should direct that policies are established and enforced to enable the organization to meet its internal obligations in its use of IT. Directors should direct that IT staff follow relevant guidelines for professional behaviour and development. Directors should direct that all actions relating to IT be ethical.
Monitor
Directors should monitor IT compliance and conformance through appropriate reporting and audit practices, ensuring that reviews are timely, comprehensive, and suitable for the evaluation of the extent of satisfaction of the business. Directors should monitor IT activities, including disposal of assets and data, to ensure that environmental, privacy, strategic knowledge management, preservation of organizational memory and other relevant obligations are met.

3.7 Principle 6: Human Behaviour

Evaluate

Directors should evaluate IT activities to ensure that human behaviours are identified and appropriately considered.

Direct

Directors should direct that IT activities are consistent with identified human behaviour.

Directors should direct that risks, opportunities, issues and concerns may be identified and reported by anyone at any time. These risks should be managed in accordance with published policies and procedures and escalated to the relevant decision makers.

Monitor

Directors should monitor IT activities to ensure that identified human behaviours remain relevant and that proper attention is given to them.

Directors should monitor work practices to ensure that they are consistent with the appropriate use of IT.