

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*

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 38502:2014

Reference number
ISO/IEC TR 38502:2014(E)



© ISO/IEC 2014

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 38502:2014



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014

All rights reserved. Unless otherwise specified, 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
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
Foreword	iv
Introduction	v
1 Scope	1
2 Terms and definitions	1
3 The Model and Framework	4
3.1 The Model for governance of IT	4
3.2 Relationship between Governance and Management of IT	6
3.3 Key elements of a governance framework for IT	6
4 Guidance on the application of the model	8
4.1 Responsibilities of the Governing Body	8
4.2 Strategy Formulation and Oversight	9
4.3 Delegation	9
4.4 Responsibilities of Managers	10
4.5 Governance and Internal Control	11
Annex A (informative) Principles of good governance of IT	13
Bibliography	14

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 38502:2014

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.

Note 2 to entry: Objectives, strategies and policies may be set by managers if they have authority from the governing body.

2.6
evaluate

consider and make informed judgements

Note 1 to entry: In the context of governance of IT, evaluate involves judgements about the internal and external, current and future circumstances and opportunities relating to the organization's current and future use of IT.

2.7
executive manager

person who has authority delegated by the governing body for implementation of strategies and policies to fulfil the purpose of the organization

Note 1 to entry: Executive managers can include roles which report to the governing body or the head of the organization or have overall accountability for major reporting function, for example Chief Executive Officers (CEOs), Heads of Government Organizations, Chief Financial Officers (CFOs), Chief Operating Officers (COOs), Chief Information Officers (CIOs), and like roles.

Note 2 to entry: In management standards, executive managers may be referred to as top management.

2.8
governance

system of directing and controlling

2.9
governing body

person or group of people who are accountable for the performance and conformance of the organization

2.10
governance framework

strategies, policies, decision-making structures and accountabilities through which the organization's governance arrangements operate

2.11
governance of IT

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

Note 1 to entry: Governance of IT is a component or a subset of organizational governance.

Note 2 to entry: This term is equivalent to the terms "corporate governance of IT", "enterprise governance of IT" and "organizational governance of IT".

2.12
internal control

policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected

2.13
information technology

IT
resources used to acquire, process, store and disseminate information

Note 1 to entry: This term also includes "Communications Technology (CT)" and the composite term "Information and Communications Technology (ICT)".

2.14
investment

allocation of resources to achieve defined objectives and other benefits

2.15**management**

exercise of control and supervision within the authority and accountability established by governance

Note 1 to entry: This term is often used as a collective term for those with responsibility for controlling an organization or parts of an organization. The term “managers” is used to avoid confusion with management systems.

2.16**management system**

set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: Management systems have to operate within the strategies, structures, responsibilities and accountabilities specified within the organization’s governance framework.

[SOURCE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2013, Annex SL, Appendix 2, 3.04, modified – Note 2 has been added.]

2.17**managers**

group of people responsible for supervision of an organization or parts of an organization

Note 1 to entry: Executive managers are a category of managers.

2.18**monitor**

review as a basis for appropriate decisions and adjustments

Note 1 to entry: Monitor involves routinely obtaining information about progress against plans as well as the periodic examination of overall achievements against agreed strategies and outcomes to provide a basis for decision making and adjustments to plans.

Note 2 to entry: Monitor includes reviewing compliance with relevant legislation, regulations and organizational policies.

2.19**organization**

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2013, Annex SL, Appendix 2, 3.01]

2.20**organizational governance**

system by which organizations are directed and controlled

2.21**policy**

intentions and direction of an organization as formally expressed by its governing body or executive managers acting with appropriate authority

2.22**proposal**

compilation of benefits, costs, risks, opportunities, and other factors applicable to decisions to be made

2.23

resources

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

[SOURCE: ISO/IEC 38500:2008, 1.6.13]

2.24

responsibility

obligation to act and take decisions to achieve required outcomes

2.25

risk

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected — positive and/or negative.

[SOURCE: ISO Guide 73:2009, 1.1, modified — NOTES 2 to 5 have been deleted.]

2.26

risk appetite

amount and type of risk that an organization is willing to pursue or retain

[SOURCE: ISO Guide 73:2009, 3.7.1.2]

2.27

stakeholder

any individual, group or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

[SOURCE: ISO Guide 73:2009, 3.2.1.1, modified — The NOTE has been deleted.]

2.28

use of IT

planning, design, development, deployment, operation, management, and application of IT to fulfil business objectives and create value for the business

Note 1 to entry: The use of IT includes both the demand for, and the supply of, IT.

Note 2 to entry: The use of IT includes both current and future use.

3 The Model and Framework

3.1 The Model for governance of IT

3.1.1 Governing Body Responsibilities and Accountabilities

The governing body is responsible and accountable for the current and future use of IT within an organization as part of their overall responsibility for organizational governance.

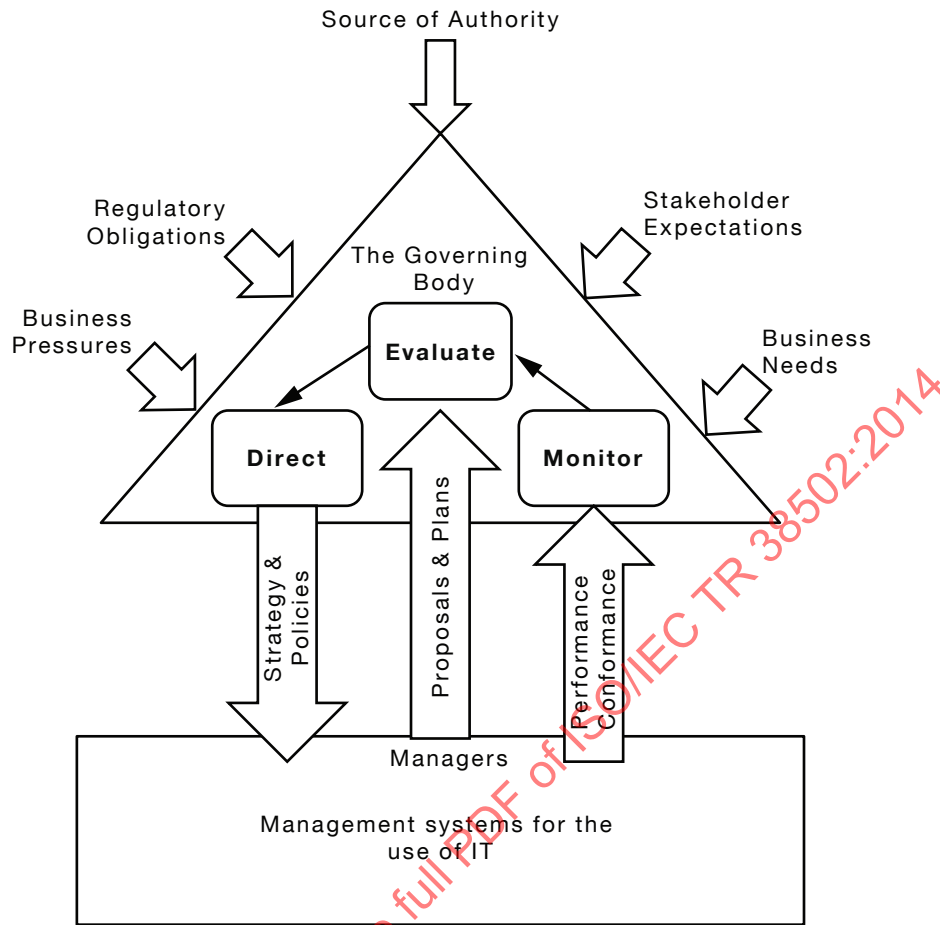


Figure 1 — Model for governance of IT (adapted from ISO/IEC 38500:2008)

The governing body's authority, responsibility and accountability will depend on its source of authority such as the legislative arrangement under which it operates. The agreed level of authority and boundaries on the scope of the organization will generally be documented. Depending on the size, type of the organization, and legislative framework applicable to the organization, this will be in the form of a constitution or charter for the organization or a simple agreement between the parties.

In many public companies, the governing body is a board e.g. board of directors. There are jurisdictions in which a two-tier board structure is utilized, with both a supervisory and executive board.

3.1.2 Governance Tasks

ISO/IEC 38500[2] recommends that the governing body govern the use of IT through the tasks of:

- Evaluate
- Direct
- Monitor

The tasks evaluate, direct and monitor are carried out in close cooperation between the governing body and managers to enable the governing body to direct and control the use of IT to fulfil the business objectives.

While undertaking governance activities, the governing body should take into account regulatory obligations and the legitimate expectations of stakeholders in its decisions as well as the impact of the business environment including business pressures and business needs.

3.1.3 Managers' Responsibilities and Accountabilities

Managers are responsible for ensuring the achievement of the objectives of the organization within the strategies and policies established by the governing body. Managers are accountable to the governing body in respect to assigned responsibilities.

Organizations may operate through a management hierarchy, with the CEO having overall responsibility and with the organization's other managers reporting either directly or indirectly as appropriate. In some organizations, nominated executive managers may be part of the governing body.

3.1.4 Applicability of the Model

The model for governance of IT described in this section can also be used to consider governance requirements in organizations in which a formal governing body such as a board of directors does not exist. This may include government organizations, where authority, responsibility and accountability rests within the political arm of government. In such situations, the authority and responsibility for governance may be delegated directly to one or more executive managers of the organization. This will generally be the CEO (or equivalent) of the organization who will exercise the responsibilities of the governing body. In small businesses, the same individual might undertake the role of governing body and CEO.

3.2 Relationship between Governance and Management of IT

The key elements of the relationship between governance and management of IT as reflected in the model are as follows:

- a) **Responsibilities of the Governing Body.** Members of the governing body are responsible for the governance of IT and are accountable for the effective, efficient and acceptable use of IT within the organization;
- b) **Strategy Formulation and Oversight.** Governance provides the means through which the governing body sets the direction for the organization in respect of the use of IT and monitors the state of the organization and the performance of its managers in achieving required outcomes;
- c) **Delegation.** Aspects of governance of IT may be undertaken by managers if they have appropriate responsibility assigned to them by the governing body together with delegated authority ;
- d) **Responsibilities of Managers.** Managers are responsible for achieving organizational strategic objectives within the strategies and policies for use of IT set by the governing body; and
- e) **Governance and Internal Control.** Effective governance of IT requires the establishment of an effective system of internal control as part of the organization's management systems.

Each of these elements is discussed in [Clause 4](#): Guidance on the application of the model.

3.3 Key elements of a governance framework for IT

An organization's management systems for IT, and its use of IT, should be based on a governance framework established for the organization.

The actual governance framework will be determined by the organization itself, and depend on the size and function of the organization and decisions by the governing body as to boundaries of responsibility but the key elements should be as shown in [Figure 2](#). The shaded area shows the associated management elements.

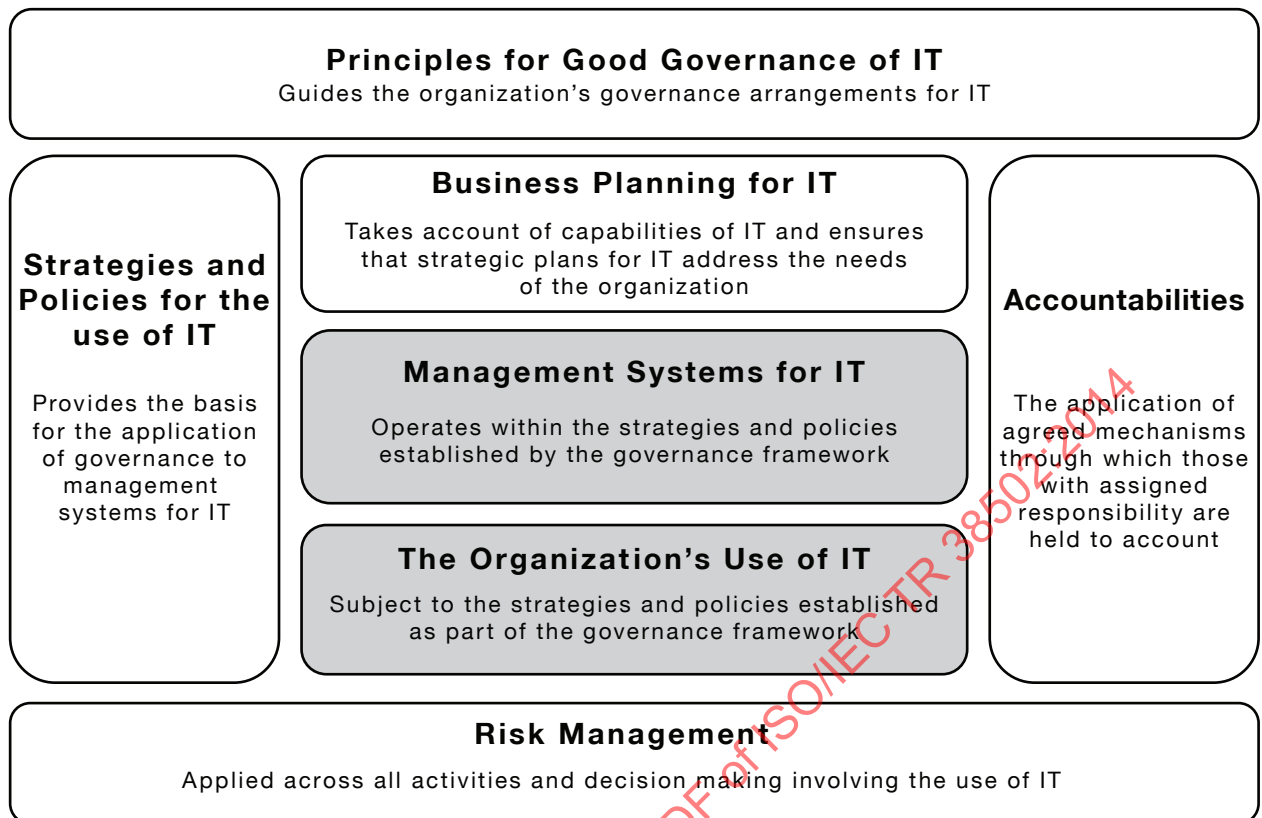


Figure 2 — Key Elements of a Governance framework for IT

The key elements of a governance framework for IT should involve:

- a) **Principles for Good Governance of IT.** The governance framework should be based on the principles for good governance of IT as outlined in ISO/IEC 38500. [Annex A]. The principles should guide how organizations establish the governance arrangements for the use of IT.
- b) **Strategies and Policies for Use of IT.** The strategies and policies for the use of IT set by the governing body and communicated to managers should provide the basis for the application of governance to the management systems of the organization. While based in part on mandatory requirements set by legislation and regulations in different jurisdictions, or by policy directives for public-sector organizations, strategies and policies should address organizational specific requirements set by governing bodies and managers. Strategies and policies that take account of the principles of behaviour outlined in ISO/IEC 38500 should be defined, communicated and outcomes monitored. They may include:
 - Business objectives for the use of IT;
 - Priorities and resource allocation;
 - Level of authority and decision-making rights including what decision-making rights are reserved for the governing body;
 - Required arrangements for decision-making based on agreed strategies and policies for the use of IT, including responsibilities, boundaries, authority, exception arrangements and reporting arrangements;
 - Risk appetite relating to the use of IT and specific control requirements; and
 - Policies that define required behaviours in respect of the use of IT.

- c) **Business Planning for IT.** Business planning processes should take into account the current and future capabilities of IT to ensure that the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy. This includes business innovations enabled by the use of IT. Business planning for IT is therefore an integral part of an organization's governance framework for IT.
- d) **Risk Management.** The governance framework for IT should involve robust risk management practices across all IT activities and decision-making. Risk management for the use of IT should be based upon the application of the organization's risk management processes.
- e) **Accountabilities.** The mechanisms through which those with assigned responsibility are held to account should be defined and agreed. This may include such things as the ongoing evaluation of performance (both performance and conformance) of IT strategies, plans and business units across the organization.
- f) **Management Systems for IT.** Management systems for IT should operate within the strategies and policies set by the governing body to achieve the organization's strategic and operational objectives. This includes systems dealing with the demand for, and the supply of, IT by internal business units, specialist IT units, or external suppliers and utility services. The responsibility for implementing management systems to achieve the objectives of the organizations rests with the managers of the organization.
- g) **The Organization's Use of IT.** The focus of a governance framework for IT is the organization's use of IT. The use of IT to meet the needs of the business should be subject to the strategies and policies defined as part of a governance framework as well as the organization's management systems for IT.

The governance framework should enable managers to operate on a day-to-day basis with as much autonomy as possible. Governance requires the development of shared values and purpose, setting direction, providing resources and delegated authority to enable managers to act with autonomy and appropriate responsiveness in changing environment.

4 Guidance on the application of the model

4.1 Responsibilities of the Governing Body

4.1.1 General

Members of the governing body are responsible for the governance of IT and are accountable for the effective, efficient and acceptable use of IT within the organization. [3.2 a)]

The governing body's authority, responsibility and accountability for the effective, efficient and acceptable use of IT arise from its overall responsibility for governance of the organization.

The key focus of the governing body's role in the governance of IT is to ensure that the organization obtains value from investments in IT while managing risk.

4.1.2 Governing Body and Oversight Mechanisms

- a) The governing body should establish oversight mechanisms for governance of IT that are appropriate to the level of business dependency on IT.
- b) The governing body should have a clear understanding of the importance of IT to the organization's business strategies as well as the potential strategic risk to the organization from the use of IT. The level of attention that a governing body gives to IT should be based on those factors.
- c) The governing body may establish a subcommittee to assist the governing body in overseeing the organization's use of IT from a strategic point of view. The need for a subcommittee will depend on the importance of IT to the organization and its size.

- d) The governing body should ensure that its members and associated governance mechanisms (such as Audit, Risk and IT committees) have the requisite knowledge and understanding of the use of IT and future trends and directions of IT, as well as the appropriate authority to address their responsibilities.
- e) The governing body should monitor the effectiveness of the mechanisms for the governance of IT by requiring processes such as audit and independent assessments to gain assurance that governance is effective. For example, the governing body should ensure that there is adequate audit coverage of IT related risk management, control, and governance processes as part of the audit approach.

4.2 Strategy Formulation and Oversight

4.2.1 General

Governance provides the means through which the governing body sets the direction for the organization in the use of IT and monitors the state of the organization and the performance of its managers in achieving required outcomes. [3.2 b)]

Overall, the governing body acts to guide the organization through strategy formulation and through oversight of managers' performance in implementing the strategy. In many organizations this requires that the governing body works with and is advised by executive managers. Together they must have a clear vision of how IT can be best utilized for the benefit of the organization both in the present and future.

4.2.2 The Governing Body's Role in Strategy Formulation

- a) The governing body working with and advised by executive managers should provide leadership in developing strategies for obtaining value from the use of IT.
- b) The governing body should approve the organization's business strategy for IT taking into account the implications of the strategy for achieving business objectives and any associated risks that might arise.
- c) The governing body should ensure that the organization's external and internal environment are regularly monitored and analysed to determine if there is a need to review and, when appropriate, revise the strategy for IT and any associated policies. This includes its customers' needs and expectations, the competitive situation, its strengths, weaknesses and opportunities, new technologies, regulatory demands, political changes, economic forecasts and sociological factors.
- d) The governing body should ensure that policies are developed to guide organizational behaviour. Such policies should support the achievement of business objectives including requirements of mandatory legislation and regulations. Others will be based on best practices and will guide the organization in terms of risk management or improvements in efficiency and effectiveness.
- e) The governing body should ensure that there are mechanisms to clarify and interpret objectives, strategies and policies as emergent issues arise.
- f) The governing body should understand the business readiness for any major changes proposed as part of the business strategy for IT and ensure that there is a commitment and capability within the organization to undertake required changes.

4.3 Delegation

4.3.1 General

Aspects of governance of IT may be undertaken by managers if they have appropriate responsibility assigned to them by the governing body together with delegated authority. [3.2 c)]

The governing body achieves the objectives of the organization by working through and with the managers of the organization. A governing body may delegate authority to one or more managers subject to the constitution of the organization and relevant applicable laws and regulations.

Governance of IT will be generally exercised by both the governing body and managers. In many organizations, the responsibility for the use of IT is allocated to managers together with the delegated authority to run an organization to achieve business objectives rather than there being an explicit delegated authority for IT.

In principle, there are no restrictions as to what can be delegated to executive managers and what will continue to be undertaken by the governing body. The governing body remains accountable for the performance and conformance of the organization, even when aspects of governance and management such as decision-making are delegated. This includes the impact of the success or failure of the use of IT.

4.3.2 Delegation by the Governing Body

- a) The governing body may delegate aspects of governance of IT to managers of the organization.
- b) When delegating the authority for the governance of IT, the governing body should establish:
 - Clearly defined and agreed responsibilities and boundaries for decision-making;
 - Commensurate authority with appropriate resources; and
 - Mechanisms to ensure conformance with strategies and policies and that performance in achieving objectives is monitored and/or assessed.
- c) The governing body should ensure that those to whom authority is delegated have the requisite competence and that the governing body retains appropriate oversight of key decisions.
- d) The governing body should determine and make clear what decisions are required to be referred to the governing body rather than being taken by managers without referral.
- e) The governing body should ensure that the extent to which authority for governance of IT is delegated to managers is clearly articulated in governance policies. In respect of IT, the governing body typically retains involvement in such things as:
 - Approval of objectives, strategies and policies for the use of IT;
 - Approval of major investments involving the use of IT;
 - Oversight of programs and projects with a major impact on the business; and
 - Approval of key risk management practices such as those relating to security and business continuity.
- f) The governing body should ensure that the appropriateness of delegated authority is subject to review on an ongoing basis.

4.4 Responsibilities of Managers

4.4.1 General

Managers are responsible for achieving organizational strategic objectives within the strategies and policies for use of IT set by the governing body. [3.2 d)]

Managers are responsible for ensuring that the organization achieves required outcomes within the boundaries established by the strategies and policies for IT as stipulated or agreed by the governing body. Managers are accountable to the governing body for the outcomes. Managers' responsibilities,

authority and accountability are determined by the governing body. In some jurisdictions, there may be specific accountability and reporting requirements applied to some organizational roles.

Managers are responsible for the strategy and policy implementation, as well as the implementation and oversight of the management systems required to achieve the objectives established by the governing body.

4.4.2 The Role of Managers

- a) Managers should ensure the achievement of the required outcomes for the business within the strategies and policies for the use of IT, as set by the governing body.
- b) Managers should implement strategies, policies and management systems to achieve the business objectives established by governing bodies. This may include:
 - Developing and communicating policies, guidelines and standards for IT based on principles and policies as stipulated or set by the governing body;
 - Strategic planning for IT as an integral part of business strategic planning if the authority is delegated by the governing body;
 - Establishing mechanisms for managing demand and supply of IT in support of business change initiatives;
 - Establishing mechanisms for managing demand and supply of IT for existing business operations;
 - Applying risk management (integrated with the organizational risk management system) to the use of IT;
 - Ensuring IT related investments will be managed as a portfolio with the full scope of activities that are required to achieve business value; and
 - Monitoring and assessing organizational performance and conformance and reporting to the governing body.
- c) Managers should make decisions in the context of the strategies and policies set by the governing body.

4.5 Governance and Internal Control

4.5.1 General

Effective governance of IT requires the establishment of an effective system of internal control as part of the organization's management systems. [3.2 e)]

Effective governance of IT relies on the establishment of an effective system of internal control as part of the establishment of management systems to support the achievement of the organization's business objectives.

Managers have the responsibility for assessing the risks to the organization and implementing an appropriate system of internal control. The governing body sets policies on internal control taking account of what is an acceptable risk to the organization, including legislative requirements. Risk management is a key element of the governance model since risk has to be considered during evaluating, directing and monitoring.

4.5.2 Establishing Internal Control