TECHNICAL REPORT

# ISO/IEC TR 38502

Second edition
2017-12

# Information technology — Governance of IT — Framework and model

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



Reference number
ISO/IEC TR 38502:2017(E)



ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

# 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 voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, SC 40 *IT Service Management and IT Governance.*

This second edition cancels and replaces the first edition (ISO/IEC TR 38502:2014) of which it constitutes a minor revision comprising the following changes:

— in Clause 1 “Scope” and the definition 3.3 “Note 2 to entry” the inappropriate words “have to” have been deleted;

— a new Clause 2 “Normative references” has been inserted stating that there are no normative references in this document with the following clauses and sub-clauses appropriately renumbered as a consequence;

— at the beginning of Clause 3 “Terms and definitions” the applicability of “the terms and definitions given in ISO/IEC 38500:2015” is stated in addition and the standard referral to the ISO and IEC terminological databases is also given;

— in Clause 3 “ Terms and definitions” all definitions given in ISO/IEC 38500:2015 have been deleted and the remaining definitions renumbered;

— Figure 1 has been updated to include an ampersand in the Performance/Conformance arrow making it identical with Figure 1 in ISO/IEC 38500:2015 and the caption has been updated to reflect this;

— in the Bibliography reference [1] to ISO/IEC 38500 has been updated to reflect its current title “*Information technology — Governance of IT for the organization*”.



# 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[1] 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 document 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 document 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 document 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 document provides guidance for:

— governing bodies;

— managers who 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 Normative references

There are no normative references in this document.

## 3 Terms and definitions

For the purposes of this document the terms and definitions given in ISO/IEC 38500 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

**3.1**
**governance framework**
strategies, policies, decision-making structures and accountabilities through which the organization's governance arrangements operate

**3.2**
**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

**3.3**
**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 operate within the strategies, structures, responsibilities and accountabilities specified within the organization's governance framework.

[SOURCE: ISO 9000:2015, 3.5.3, modified - The notes to entry have been modified.]

**3.4**
**risk appetite**
amount and type of risk that an organization is willing to pursue or retain

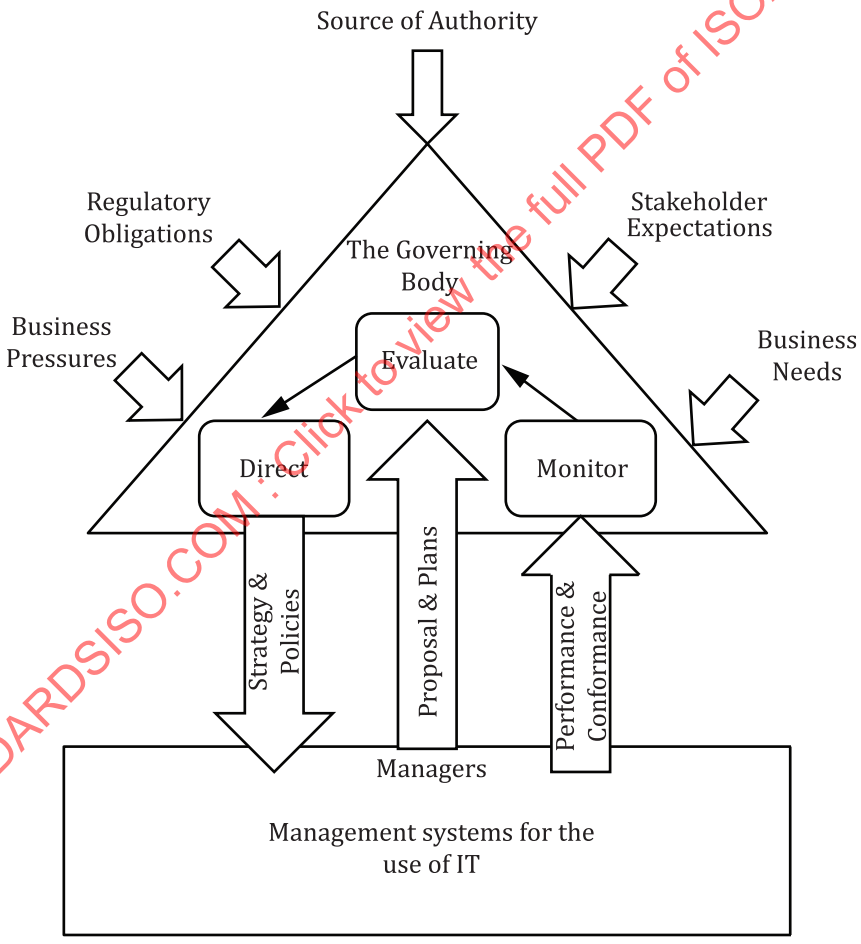
[SOURCE: ISO Guide 73:2009, 3.7.1.2]

# 4 Model and framework

## 4.1 Model for governance of IT

### 4.1.1 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.




NOTE SOURCE: ISO/IEC 38500.

**Figure 1 — Model for governance of IT**

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.

#### 4.1.2 Governance tasks

ISO/IEC 38500[1] 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.

#### 4.1.3 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.

#### 4.1.4 Applicability of the model

The model for governance of IT described in this clause 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.

### 4.2 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 5: Guidance on the application of the model.

## 4.3 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.

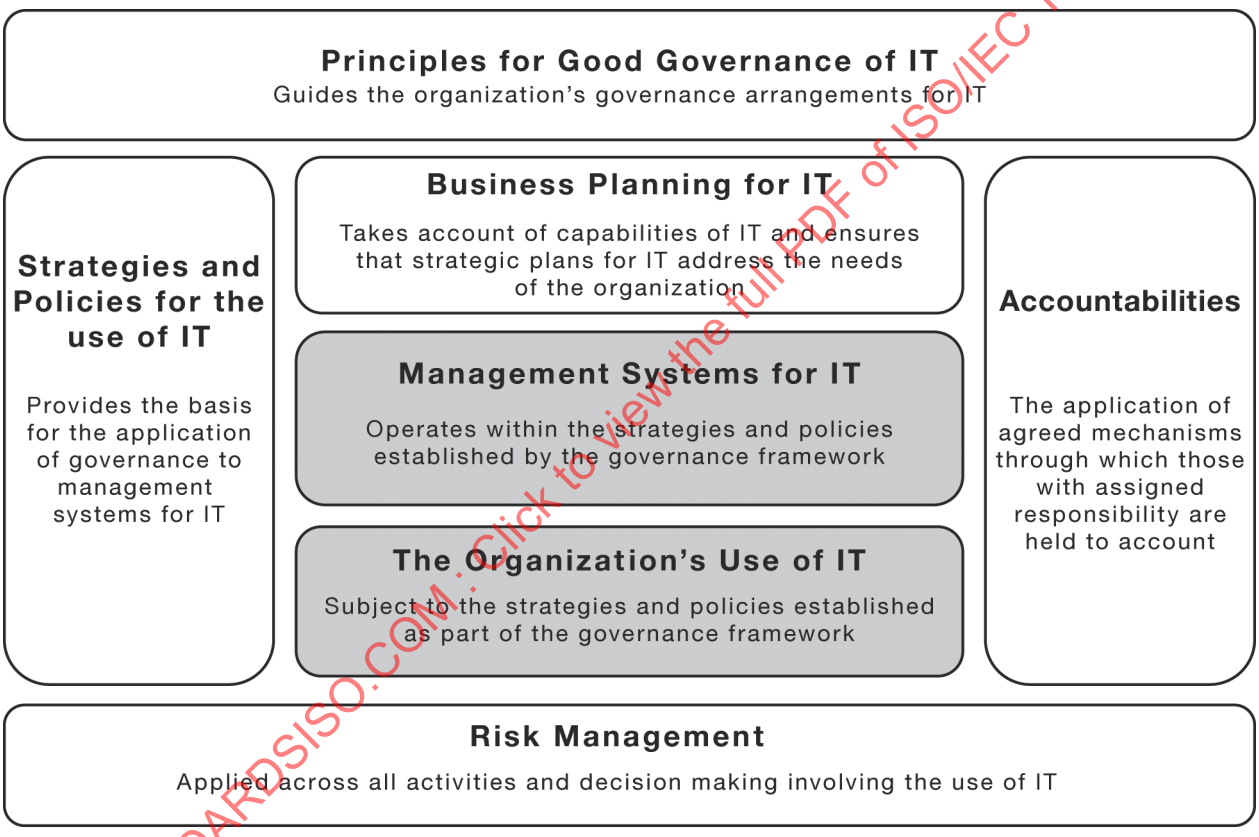



**Figure 2 — Key elements of a governance framework for IT**



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 and in Annex A of this document. The principles should give guidance on 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.



# 5 Guidance on the application of the model

## 5.1 Responsibilities of the governing body

### 5.1.1 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. [4.2 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.

### 5.1.2 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.

## 5.2 Strategy formulation and oversight

### 5.2.1 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. [4.2 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.

### 5.2.2 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.

## 5.3 Delegation

### 5.3.1 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. [4.2 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 IT.

### 5.3.2 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.

## 5.4 Responsibilities of managers

### 5.4.1 General

Managers are responsible for achieving organizational strategic objectives within the strategies and policies for use of IT set by the governing body. [4.2 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.

### 5.4.2 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.

