ISO/IEC JTC 1
Information technology
Secretariat: ANSI (USA)

Document type:	Text for PDTR ballot or comment
Title:	Text of 2nd PDTR 38502, Governance of IT - Framework and Model
Status:	Please submit your vote via the online balloting system.
Date of document:	2012-02-17
Source:	WG 6 Secretariat
Expected action:	VOTE
Action due date:	2012-05-18
Email of secretary:	lrajchel@ansi.org
Committee URL:	http://isotc.iso.org/livelink/livelink/open/jtc1

ISO/IEC JTC 1/WG 6
Corporate Governance of IT
Secretariat: SA

Document type: Text for PDTR ballot or comment

Title: JTC 1 WG6 PDTR 2 38502 Jan 2012

Status: For the action of the JTC 1 Secretariat. Please distribute to JTC 1 Member Bodies for 2 month PD ballot.

Date of document: 2012-02-06

Source: JTC 1/WG 6 Project Editor ISO/IEC PDTR 38500

Expected action: ACT

Action due date: 2012-02-10

No. of pages: 19

Email of secretary: andrew.mckay@standards.org.au

Committee URL: http://isotc.iso.org/livelink/livelink/open/jtc1wg6

ISO/IEC JTC 1/WG 6 N

Date: 2012-01-29

ISO/IEC WDTR 38502

ISO/IEC JTC 1 WG 6

Secretariat: SA

Governance of IT - Framework and Model

Error! AutoText entry not defined.

Document type: Technical Report
Document subtype:
Document stage: (20) Preparatory Draft
Document language: E

Contents

Pag

Figures & Tables

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 IT, 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.

Technical Reports are subject to review within three years of publication, to decide whether they can be transformed into International Standards. 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, which is a Technical Report, was prepared by Joint Technical Committee ISO/IEC JTC 1.

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, realised benefits are a result of changes in business activities enabled by the use of the technology to meet a specific organizational need or requirement. This requires that the organization has 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, 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 such decisions are based on business strategies, priorities and needs. The full scope of effort required to derive the expected benefits should be identified and understood.

ISO/IEC 38500 recognises that the proper balance of demand and supply of IT is a requirement of sound 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 and the managers 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* which 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 to 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 with respect to IT. It provides a model illustrating the relationship between governance and management identifying the responsibilities associated with each.

Governance of IT – framework and model

1 Scope, Purpose, Audience

1.1 Scope

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

1.2 Purpose

This Technical Report provides 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.

1.3 Audience

This Technical Report provides guidance for those responsible for governance of IT within organizations and those involved in advising or assisting in the governance of organizations of all sizes and types. The technical report also provides guidance for those involved in development of standards in the areas of governance of IT and the management of IT. It does this by providing a model that can be used to assist in the understanding of the various components of, and the inter-relationship between, governance of IT and management of IT.

2 Normative References

The following referenced documents are indispensable for the application of this Technical Report. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- ISO/IEC 38500– Corporate Governance of IT
- ISO Guide 73:2009 Risk management – Vocabulary

3 Definitions

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

3.1
accountable
may be expected to justify decisions and performance

Note. Accountability relates to an allocated responsibility. The responsibility may be based on regulation or agreement or through delegation

3.2
corporate governance
the system by which corporations are directed and controlled. (Cadbury 1992 [1] and OECD 1999 [2]).

Note. Corporate governance is organizational governance applied to corporations.

3.3
delegation
the act of entrusting a responsibility to another person or group

3.4
direct
set and articulate the objectives, strategies and policies
.
3.5
evaluate
consider and make informed judgement on the internal, external current and future circumstances and opportunities

3.6
executive managers
person or group of people who have delegated responsibility from the governing body for implementation of strategies and policies to fulfil the purpose of the organization

Note 1. Executive managers form part of top management: For clarity of roles, this standard distinguishes between two groups within top management: the governing body and executive managers.

Note 2. Executive managers can include Chief Executive Officers (CEOs), Heads of Government Organizations, Chief Financial Officers (CFOs), Chief Operating Officers (COOs), Chief Information Officers (CIOs), and like roles.

3.7
governance
the action or manner of directing or controlling

3.8
governing body
the person or group of people who are accountable to stakeholders for the performance and conformance of the organization.

Note. The governing body forms part of top management: For clarity of roles, this standard distinguishes between two groups within top management: the governing body and executive managers.

3.9
governance framework
The policies, decision making structures and accountabilities through which the organization's governance arrangements operate

3.10
governance of IT
the system through which an organization's current and future use of IT is directed and controlled

Note 1. The governance of IT is a component or a subset of organization governance.

Note 2. The term governance of IT is equivalent to the terms corporate governance of IT, enterprise governance of IT, organizational governance of IT, governance of Enterprise IT and governance of IT for an Enterprise etc.

3.11
internal control
the 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

3.12
Information technology (IT)
resources required to acquire process, store and disseminate information. (ISO/IEC 38500)

Note. This term also includes "Communication Technology (CT)" and the composite term "Information and communication Technology (ICT)".

3.13
management systems
the system of controls and processes required to achieve the strategic objectives set by the organization's governing body.

3.14
management
the exercise of control and supervision within the constraints of a governance framework

3.15
managers
person or group of people responsible for controlling an organization or parts of an organization

Note 1. The term *management* is often used as a collective term for those with delegated responsibility for controlling an organization or parts of an organization. This Technical report uses the term *managers* to avoid confusion with management systems.

Note 2. Executive Managers are a category of managers.

3.16
monitor
obtain appropriate information regarding performance, conformance and circumstances of the organization in order to make decisions and adjustments as necessary

3.17
Organizational Governance
the system by which organisations are directed and controlled

3.18
policy
clear and measurable statements of preferred direction and behaviour to guide the decisions made within an organization (ISO/IEC 38500)

3.19
resources
people, procedures, software, information, equipment, consumables, infrastructure, capital and operating funds, and time (ISO/IEC 38500)

3.20
responsibility
the opportunity or ability to act independently and take decisions within a delegated authority

3.21
stakeholder
individual or group that has ownership of the organizations or an interest in decisions or activities of an organization

3.22
strategy
a logically structured plan or method for achieving objectives, especially over a long period of time

4 The Model and Framework

4.1 The Model for governance of IT

ISO/IEC 38500 provides guidance for the governing body and executive managers on the governance of IT. It explains their duty to direct and control the use of IT, and, through its model and principles, gives guidance to assist them in making appropriate decisions. ISO/IEC 38500 recommends that the governing body should govern the current and future use of IT through the following three main tasks:

(a) Evaluate.

(b) Direct.

(c) Monitor.

The tasks evaluate, direct and monitor are carried out in close cooperation between the governing body and the managers in a way so that the governing body fully can direct and control the use of IT to fulfil the business objectives.

While undertaking governance activities, in addition to considering the impact of the business environment (business pressures and business needs), the governing body has also to take into account regulatory obligations and the legitimate expectations and interests of other stakeholders in its decisions.

In respect to IT, the key focus of governance of IT is to ensure that the organization obtains value from investments in IT while managing risk. This requires that the use of IT provides appropriate support to business to either enhance outcomes or to remove constraints – thereby facilitating improved business outcomes.

In many public companies, the governing body is a board (e.g. board of directors, et al). There are countries in which a two-tier board structure is utilised, with both a supervisory and executive board.

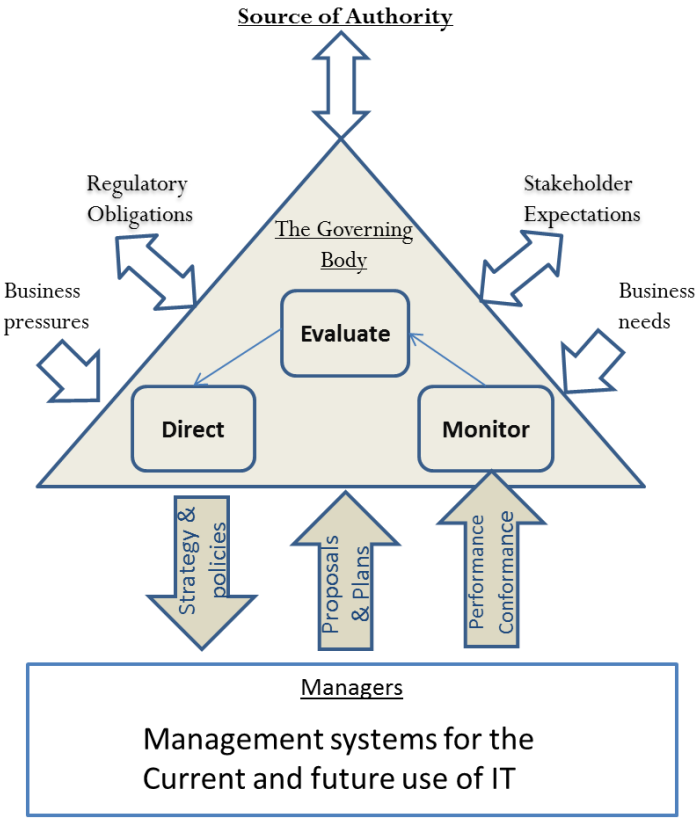

Figure 1. Model for governance of IT (adapted from ISO/IEC 38500: 2008)

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

Some organizations may operate through a management hierarchy, with one executive manager (sometimes called the CEO or Managing Director) having overall responsibility and with the organization's other managers reporting either directly or indirectly as appropriate. In some organizations, managers (generally called executive directors) may be part of the governing body.

4.2 Relationship between Governance and Management of IT as part of the model

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

1. 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.

2. Aspects of governance of IT may be undertaken by managers if they are given the delegation by the governing body;.

3. Governance provides the processes through which members of the governing body act to protect stakeholders' interests by setting the direction for the organization and monitoring the state of the organization and the performance of its managers in achieving the objectives of the organization;

4. Managers are responsible for ensuring the achievement of the required outcomes for the business within the strategies and policies for IT use agreed by the governing body and are accountable to the governing body; and.

5. Effective governance of IT requires the establishment by management of an effective system of internal control as part of the organisation's management systems

Each of these elements is discussed at section 5 Guidance on the application of the model.

4.3 Governance Principles for IT

In establishing the relationships between Governance and Management of IT, the governing body should ensure that consideration is given to the principles outlined in ISO/IEC 38500. [Appendix A]

The role of these principles in the implementation of governance is not addressed in the technical report.

4.4 The Governance Framework

Core to establishing effective governance is the specification of a governance framework which defines the structure (strategies, policies, structures, responsibilities and accountability mechanisms) within which management systems operate.

The governance framework is the tool through which an organisation embeds the principles of governance of IT as outlined in ISO/IEC38500 together with required practices of governance and management into the organisation. The actual arrangements required for governance and management will be determined by the organisation itself, and depend on the size and function of the organisation and the decision by the governing body as to boundaries of responsibility

The key elements of the governance framework are as shown in figure 2.

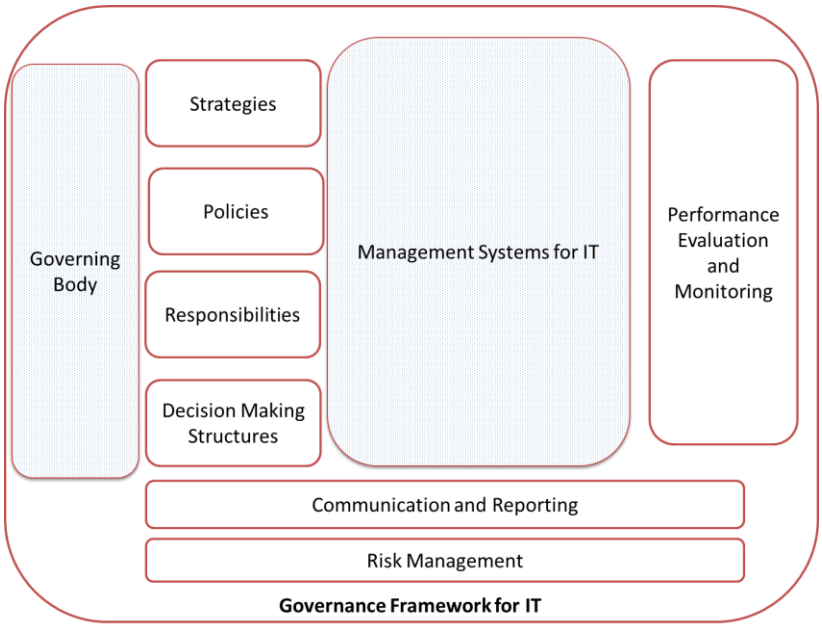

Figure 2 Key Elements of a Governance Framework for IT

While based in part on mandatory requirements set by legislation and regulations in different jurisdictions, (or by policy directives for public-sector organizations), a governance framework should address organizational specific requirements set by governing bodies and managers

4.5 Use of IT

Governance of IT should address both current and future use of IT. This involves processes for both governance and management of demand and supply of the IT. This includes the IT needed to support an organization's continued functioning as a business on a day-to-day basis with the required level of performance as well as the delivery of changes to the business that are enabled and supported by the use of new or improved IT.

The use of IT includes organizational processes for managing demand and supply when external providers provide such IT service or support. Even, when the responsibility for service delivery is transferred, the accountability for ensuring continued delivery of value from the service provider and the management of risks to the organizations are not.

5 Guidance on the application of the model

5.1 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.

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

The governing body's authority and accountability will depend on an organization's size, type and the sources 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 in a simple agreement between the parties.

A governing body should have a clear understanding of the level of risk associated with the organizations use of IT as well as the opportunities for business that could arise from the use of IT. The level of attention that a governing body gives to IT should be based on those factors. Depending on the importance of IT to the organization and its size, consideration should also be given to the establishment of a subcommittee to assist the governing body in overseeing the organization's IT usage from the strategic point of view.

A governing body should ensure that it and associated governance subcommittees (such as Audit, or Audit and Risk Committees) have the requisite knowledge and understanding of the use of IT to address their responsibilities, as well as the appropriate authority.

The governing body should also monitor the performance of the governance of IT, and, by requiring processes such as audit and independent assessments gain assurance that governance processes are effective. For example, the governing body should ensure that there is an adequate program of audit coverage of IT related risk management, control, and governance processes as part of the audit approach. In some jurisdictions, there is a legislative requirement for oversight of such a program by an Audit Committee.

5.2 Delegation

Aspects of governance of IT may be undertaken by managers if they are given the delegation by the governing body.

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

Governance of IT will be generally exercise by both the governing body and managers. In many organizations, the responsibility for the current and future use of IT is delegated to managers as part of a delegated authority to run an organization to achieve business objectives rather than there being an explicit delegation of responsibilities.

Effective delegation requires:

- Clearly defined and agreed responsibilities and boundaries for decision making;
- Commensurate authority and appropriate resourcing; and

- Mechanisms to ensure conformance with policies and performance in achieving goals is monitored and/or assessed.

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.

Note. In some jurisdictions there are specific legal obligations and constraints around delegations from the governing body. This Technical Report does not deal with those obligations and constraints.

However, even when the governing body delegates (implicitly or explicitly) certain aspects of decision making or responsibility for organizational performance, the governing body remains accountable for the performance and conformance of the organization. This includes the impact of the success or failure of the use IT.

Because it is accountable for the performance and conformance of the organization, the governing body should ensure that those to whom responsibility is delegated have the requisite competence and that the governing body has appropriate oversight of key decisions.

The governing body should determine and make clear what decisions that are required to be referred to the governing body rather than being taken by management without referral. The extent to which responsibilities for IT are delegated to managers should be clearly articulated in governance policies. In respect to IT, this typically will include the governing body retaining involvement in such things as:

- Approval of strategies and policies for the use if IT;
- Approval of major investments involving the use if IT;
- Level of 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.

5.3 Strategy Formulation and Oversight

Governance provides the processes through which members of the governing body act to protect stakeholders' interests by setting the direction for the organization and monitoring the state of the organization and the performance of its managers in achieving the objectives of the organization.

Overall, the governing body acts to guide the organization through:

- Strategy Formulation;
- Policy making;
- Risk Management;
- Oversight of managers' performance; and
- Accountability to stakeholders

In respect to IT, the governing body, together with executive managers, has a key role in providing leadership in developing strategies for obtaining value from current and future use of IT. In many organizations this requires that the governing body working with and advised by executive managers,

has a clear vision of how IT can be best utilised for the benefit of the organization both in the present and future.

While, the strategy for the delivery of IT will generally be developed by managers, the governing body should approve the strategy taking accounting of the implications of the strategy for achieving business objectives and any associated risks that might arise.

The governing body should ensure that the organization's environment is regularly monitored to determine if there is a need to review and (when appropriate) revise the strategy for IT and any associated policies. In order to establish, adopt and sustain an effective strategy and appropriate policies for IT, the organization should have processes to continually monitor and regularly analyse the organization's environment. This includes its customers' needs and expectations, the competitive situation, its strengths and, weaknesses and opportunities, new technologies, regulatory demands, political changes, economic forecasts, sociological factors,

With increasing dependence of organizations on IT and associated organizational risk from IT related failures, a governing body should, following the principles of behaviour outlined in ISO/IEC 38500, ensure that the following are defined, communicated and outcomes are monitored:

- 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 principles and policies for IT, including responsibilities, boundaries, authority, exception arrangements and reporting arrangements for IT;
- Risk Appetite relating to the current and future use of IT and specific control requirements; and
- Principles and policies that define required behaviours with respect to IT.

5.4 Responsibilities of Managers

Managers are responsible for ensuring the achievement of the required outcomes for the business within the strategies and policies for IT use agreed by the governing body and are accountable to the governing body.

Managers of an organization are responsible for ensuring that the organization achieves required outcomes within the boundaries established by the strategies and policies for IT agreed by the governing body. Managers are accountable to the governing body for the outcomes. Managers' authority and accountability is determined by the governing body. In some jurisdictions, there may be specific accountability and reporting requirements applied to some management 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.

Managers make decisions in the context of the strategies and policies established by the governing body. However, managers, under the guidance of the governing body, will actively participate in the formulation of strategies and policies. They will assist the governing body to make appropriate decisions and provide practicable guidance to the business and setting clear direction upon which managers should act.

Managers should develop and implement strategies, policies and management systems to achieve organizational objectives established by governing bodies. This may include;

- Developing and communicating policies, guidelines and standards for IT (based on principles and policies agreed by the governing body);
- Strategic planning for IT as an integral part of business strategic planning;
- Establishing mechanisms for managing demand and supply of IT in support of business change initiatives;
- Establish mechanisms for managing demand and supply of IT for existing business operations;
- Applying risk management (integrated with the organizational risk management system) to the current and future 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 assessment of organizational performance and conformance and reporting to the governing body.

5.5 Governance and Internal control

Effective governance of IT requires the establishment by management of an effective system of internal control as part of the organisation's management systems

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 objectives.

The specific requirements for internal control will be based on the achievement of business objectives and external regulatory requirements.

The internal control requirements are generally implemented through management systems. ***"..a****n effective internal control system is an essential part of the efficient management of a company*." [1] Executive managers are required to establish appropriate management systems that operate within the rules established through a governance framework which embeds the principles and practices of governance and control into the organization.

The system of internal control will derive from the governance framework with:

- Clear definition of responsibilities for IT within the organisation. This includes the responsibilities, boundaries of responsibilities, accountability, authority and reporting arrangements.
- Communication of relevant and reliable information to enable appropriate exercise of responsibilities;
- Risk Management to identify and analyse the IT risks in relation to the achievement of the organisations' objectives and policies and for ensuring that procedures exist for managing those risks; and
- On-going monitoring of the internal control system together with regular reviews of the way internal control for IT is operating.

Control activities appropriate for the level of risk should designed to reduce the risks associated with each process that could affect the organisations ability to achieve its Business Objectives.

Although managers have the responsibility for assessing the risks to the organization and implementing an appropriate system of internal control, the governing body, as part of governance, 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 it has to be considered during evaluating, directing and monitoring.

An organization's system of internal control should provide an organization with reasonable assurance that the business objectives will be achieved and that external regulatory requirements will be satisfied. While internal control cannot prevent bad judgements or decisions from being made, or affect external events that will cause the business to fail to achieve its goals, it should provide reasonable assurance that managers and the governing body will be provided with timely information on the extent that the organization is moving away from the objectives so that corrective action can be taken.

6 Bibliography

[1] Report Of The Committee On The Financial aspects Of Corporate Governance, UK 1992 (Cadbury Report)

[2] OECD Principles of Corporate Governance, OECD, 1999

Appendix A

Principles of Good Governance of IT

(Informative)

ISO/IEC 38500 outlines six principles for good governance of IT. The principles are applicable to most organizations. This Appendix lists these principles and provides basic details. For more information see ISO/IEC 38500.

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. The governing body should require that these principles are applied.

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.

Principle 2—Strategy

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

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.

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.

Principle 5—Conformance

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

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'.