

Board Briefing on IT Governance

“IT governance is the term used to describe how those persons entrusted with governance of an entity will consider IT in their supervision, monitoring, control and direction of the entity. How IT is applied within the entity will have an immense impact on whether the entity will attain its vision, mission or strategic goals.”

— ROBERT S. ROUSSEY, CPA, PROFESSOR,
UNIVERSITY OF SOUTHERN CALIFORNIA

“The board of directors of my company is well aware its role is to oversee the company’s organisational strategies, structures, systems, staff and standards. However, as president of the company, it is my responsibility to ensure that they extend that oversight to the company’s IT as well. In today’s economy, and with our reliance on IT for competitive advantage, we simply cannot afford to apply to our IT anything less than the level of commitment we apply to overall governance.”

— MICHAEL CANGEMI, PRESIDENT AND CHIEF OPERATING OFFICER,
ETIENNE AIGNER GROUP INC.

The IT Governance Institute appreciates the support the following organisations have provided to this project:



*American Institute
for Certified
Public Accountants*



*Association Française de L'Audit
et du Conseil Informatiques*



ANDERSEN

Andersen



**The Canadian Institute
of Chartered Accountants**

*The Canadian Institute
of Chartered Accountants*



The Center for Internet Security



The Gartner Group



**The Institute of
Chartered Accountants**
in England & Wales



*International Federation
of Accountants*



PricewaterhouseCoopers



JICPA

*Japanese Institute of
Certified Public Accountants*



SANS Institute

Acknowledgements

The IT Governance Institute wishes to recognise:

- **The development team, for its leadership of the project**

Erik Guldentops, CISA, SWIFTsc, Belgium (Leader, Development Team)
 John W. Lainhart IV, CISA, PricewaterhouseCoopers, USA (Chair, IT Governance Board)
 Gary Hardy, Arthur Andersen, UK
 Eddy Schuermans, CISA, PricewaterhouseCoopers, Belgium

- **The expert reviewers, whose comments helped shape the final document**

Everett C. Johnson Jr., CPA, Deloitte & Touche, USA
 Nils Kandelin, Ph.D., CISA, Holt & Kandelin Group, USA
 William Malik, The Gartner Group, USA
 Doug McPhie, CA, Ernst & Young, Canada
 Robert G. Parker, CISA, FCA, CMC, Deloitte & Touche LLP, Canada
 Hugh A. Parkes, CISA, FCA, Stanton Consulting, Australia
 Vernon R. Poole, Deloitte & Touche, UK
 Daniel Fernando Ramos, CISA, CPA, SAFE Consulting Group, Argentina
 Robert S. Roussey, CPA, University of Southern California, USA
 Deepak Sarup, CISA, FCA, ALLTEL, Singapore
 Gustavo Solis, CISA, Grupo Cynthus, Mexico
 Wim van Grembergen, Ph.D., UFSIA, Belgium
 Tom Wallace, KPMG, USA

- **The Board of Directors/Trustees, for their support of the project**

Paul A. Williams, FCA, MBCS, Arthur Andersen, UK, International President
 J. Manuel Aceves, CISA, CISSP, Cambridge Technology Partners, Mexico, Vice President
 Marios Damianides, CISA, CA, CPA, Ernst & Young, USA, Vice President
 Lynn C. Lawton, CISA, BA, FCA, FIIA, PIIA, KPMG, UK, Vice President
 Jae Woo Lee, Ph.D., Dongguk University, IAI, Korea, Vice President
 Michael J. A. Parkinson, CISA, CIA, KPMG, Australia, Vice President
 Robert S. Roussey, CPA, University of Southern California, USA, Vice President
 Ronald Saull, CSP, Great-West and Investors Group, Canada, Vice President
 Patrick Stachtchenko, CISA, CA, Deloitte & Touche, France, Past International President
 Akira Matsuo, CISA, CPA, Chuo Audit Corporation, Japan, Past International President
 Erik Guldentops, CISA, SWIFTsc, Belgium, Trustee
 Emil G. D'Angelo, CISA, Marsh and McLennan, Inc., USA, Trustee

- **The IT Governance Board, for its contribution to the development and review of the document**

IT Governance Institute™

The IT Governance Institute (ITGI), founded by the Information Systems Audit and Control Association and its affiliated foundation in 1998, strives to assist enterprise leadership in ensuring long-term, sustainable enterprise success and increased stakeholder value by expanding awareness of the need for and benefits of effective IT governance. The institute develops and advances understanding of the vital link between IT and enterprise governance, and offers best practice guidance on the management of IT-related risks.

Information Systems Audit and Control Foundation™

The Information Systems Audit and Control Foundation (ISACF™) was created in 1976 to undertake large-scale research efforts to expand the knowledge and value of the IT governance and control field. The role of the foundation is to evaluate the latest guidelines for implementation of emerging technologies and their applications. The research conducted by ISACF not only informs and guides the profession, it also forms the basis of many of the products and services—such as education, technical articles and publications, conferences, standards and professional certification—the association offers members and other constituents.

Information Systems Audit and Control Association®

The Information Systems Audit and Control Association (ISACA™) is an international professional, technical and educational organisation dedicated to being a single source provider for those concerned with the effective governance of information and its related technologies. With members in more than 100 countries, ISACA is uniquely positioned to fulfill the role of a central harmonising source of IT control practice standards the world over. Its strategic alliances with other organisations in the financial, accounting, auditing and IT professions ensure an unparalleled level of integration and commitment by business process owners.

This publication is based on the IT Governance Institute's *Control Objectives for Information and related Technology (COBIT) 3rd Edition*, which is an open standard and is available from the ISACA web site. This publication is considered one of the COBIT family of products, an international and generally accepted IT control framework enabling organisations to implement an IT governance structure throughout the enterprise.

Disclaimer

The IT Governance Institute, Information Systems Audit and Control Foundation, Information Systems Audit and Control Association and the authors of *Board Briefing on IT Governance* have designed this publication primarily as an educational resource for boards of directors, executive management and information technology control professionals. The IT Governance Institute, Information Systems Audit and Control Foundation and Information Systems Audit and Control Association make no claim that use of this publication will assure a successful outcome. This document should not be considered inclusive of any inquiries, proper procedures and tests or exclusive of other inquiries, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific inquiries, procedures or tests, the users should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

Disclosure

Copyright © 2001 by the Information Systems Audit and Control Foundation (ISACF). Reproduction of selections of this publication for academic use is permitted and must include full attribution of the material's source. Reproduction or storage in any form for commercial purpose is not permitted without ISACF's prior written permission. No other right or permission is granted with respect to this work.

Information Systems Audit and Control Foundation

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: jseago@isaca.org
Web sites: www.isaca.org and
www.ITgovernance.org

ISBN 1-893209-27-X (*Board Briefing on IT Governance*)

Printed in the United States of America

Table of Contents

EXECUTIVE SUMMARY	6
BOARD BRIEFING ON IT GOVERNANCE	
1. WHAT IS IT GOVERNANCE?	9
2. WHY IS IT GOVERNANCE IMPORTANT?	12
3. WHOM DOES IT CONCERN?	13
4. WHAT CAN THEY DO ABOUT IT?	14
4.1 <i>How Should the Board Address the Challenges?</i>	14
4.2 <i>How Should Executive Management Address the Expectations?</i>	15
5. WHAT DOES IT COVER?	17
5.1 <i>IT Strategic Alignment</i>	18
5.2 <i>IT Value Delivery</i>	19
5.3 <i>Performance Measurement</i>	21
5.4 <i>Risk Management</i>	23
6. WHAT QUESTIONS SHOULD BE ASKED?	24
7. HOW IS IT ACCOMPLISHED?	25
8. HOW DOES YOUR ORGANISATION COMPARE?	27
9. WHAT REFERENCE MATERIAL EXISTS?	28
APPENDICES	
APPENDIX A. IT Governance Checklist	30
APPENDIX B. Board Action Plan	32
APPENDIX C. Management Action Plan	34
APPENDIX D. IT Governance Maturity Model	36
APPENDIX E. The Emerging Enterprise Model	39
APPENDIX F. Regulatory Reports and Emerging Standards on Governance	40
REFERENCES	44

Executive Summary

Would you like to know whether your organisation's information technology (IT) is:

- Likely to achieve its objectives?
- Resilient enough to learn and adapt?
- Judiciously managing the risks it faces?
- Appropriately recognising opportunities and acting upon them?

A number of organisations are becoming successful in understanding the risks and exploiting the benefits of IT, and are finding ways to deal with:

- Aligning IT strategy with the business strategy
- Cascading strategy and goals down into the enterprise
- Providing organisational structures that facilitate the implementation of strategy and goals
- Insisting that an IT control framework be adopted and implemented
- Measuring IT's performance

Effective and timely measures aimed at addressing these top management concerns need to be promoted by the governance layer of an enterprise. Hence, boards and executive management need to extend governance to IT and provide the leadership, organisational structures and processes that ensure that the organisation's IT *sustains and extends the organisation's strategies and objectives*. IT governance is not an isolated discipline. It must become an integral part of overall enterprise governance, similar to the need for IT to become an integral part of the enterprise rather than something being practiced in remote corners or ivory towers.

An increasingly educated and assertive set of stakeholders has raised concerns about the sound management of their interests. This has led to the emergence of corporate governance regulations and standards for overall enterprise governance. These regulations establish board responsibilities and demand that board directors exercise due diligence in their roles of setting strategy and ensuring management implements it.

Enterprise governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

While governance developments primarily have been driven by the need for transparency on enterprise risks and the protection of shareholder value, the pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT governance.

IT is essential to manage transactions, information and knowledge necessary to initiate and sustain economic and social activities. These activities increasingly rely on globally cooperating entities to be successful. In many organisations, IT has become an integral part of the business and is fundamental to support, sustain and grow the business.

Many organisations recognise the potential benefits that technology can yield. Successful organisations understand and manage the risks associated with implementing new technologies. Too often, however, there is lack of understanding of how strategically important IT is to the organisation. Executive management needs to have an appreciation for and a basic understanding of the risks and constraints of IT to provide effective direction and adequate controls. The board of directors needs to put IT firmly on its agenda. Although this has not always been the case, Y2K, the Internet, e-commerce and the networked economy have changed the board's awareness and IT governance is slowly moving onto the board's agenda.

Advice to boards on how to operate traditionally has been long on board structure, composition, size and independence, but short on risk management and practical IT governance. This *Board Briefing on IT Governance* therefore specifically addresses IT governance, how it has become a critical part of enterprise governance, and how boards and management need to address:

- IT's enabling capacity for new business models and changing business practices
- IT's increasing costs and information's increasing value
- The risks of doing business in an interconnected digital world and the dependence on entities beyond the direct control of the enterprise
- IT's impact on business continuity due to increasing reliance on information and IT in all aspects of the enterprise
- IT's ability to build and maintain knowledge essential to sustain and grow the business
- The failures of IT, increasingly impacting reputation and enterprise value

The overall objectives of IT governance activities are therefore to understand the issues and the strategic importance of IT, to ensure that the enterprise can sustain its operations and to ascertain that it can implement the strategies required to extend its activities into the future. IT governance practices aim at ensuring that expectations for IT are met and IT risks are mitigated.

Boards and executive management generally expect their organisation's IT to deliver business value, i.e., provide fast, secure, high-quality development; generate maximum return on investment; and move from efficiency and productivity gains toward value creation and business effectiveness.

While some have been successful, in many organisations expectations and reality often do not match. Boards are often met with:

- Business losses, reputational damage and a weakened competitive position
- The failure of IT initiatives to bring the innovation and benefits they promised
- Technology that is inadequate or even obsolete
- Deadlines that are not met and budgets that are overrun

Boards exercising proper IT governance often uncover and address problems in advance simply by asking the right questions, such as:

- How critical is IT to sustaining the enterprise? How critical is IT to growing the enterprise?
- How far should the enterprise go in risk mitigation and is the cost justified by the benefit?
- Is IT a regular item on the agenda of the board and is it addressed in a structured manner?
- Is the reporting level of the most senior IT manager commensurate with the importance of IT?

This *Board Briefing on IT Governance*:

- Will help you understand why IT governance is important, what the issues are and what your responsibility is for managing them
- Is addressed to boards of directors, supervisory boards, audit committees, chief executive officers, chief information officers and other executive management
- Was developed by the IT Governance Institute, a not-for-profit organisation founded in 1998, with the mission to develop and advance understanding, promote good practice and positively influence effective IT governance from the board level through executive management to IT specialist practitioners
- Is based on *Control Objectives for Information and related Technology* (COBIT), an international and generally accepted IT control framework, enabling organisations to implement an IT governance structure throughout the enterprise
- Was developed in response to the finding that the complexity of IT and the intangible value of information make IT a more difficult area to govern
- Covers:
 - A summarised background on governance
 - Where IT governance fits in the larger context of enterprise governance
 - A simple framework with which to think about IT governance
 - Questions board members should ask
 - Good practices as well as critical success factors
 - Performance measures board members can track
 - A maturity model against which to benchmark your own organisation

1. What Is IT Governance?

Why do we, in our enterprises, get into governance? We actually do it when preparing major decisions like acquisitions, joint ventures and outsourcing. When selecting a major supplier or product, or acquiring a company, we often perform due diligence. We look at the productive functions and infrastructure of the supplier or acquisition entity. We request information on skills, culture and operating environment. We want to know about key issues such as capabilities, risks, process knowledge and customer information. When outsourcing, we insist on service levels and aggressively define processes and responsibilities.

All of this has to do with getting comfort about the ability of the other entity to deliver against our expectations, now and in the future. We should be equally inquisitive about our own organisations.

The Report of the Committee on the Financial Aspects of Corporate Governance (Cadbury Report, 1992) focused global thinking on the issue of governance. While the report is aimed at financial reporting and auditing, it alludes to wider concepts of governance. It recommends openness, integrity and accountability to improve standards of corporate behavior, strengthening controls over enterprises and their public accountability while retaining the essential spirit of enterprise. It identifies various board governance responsibilities, such as setting strategic aims, providing leadership, supervising management and reporting to shareholders on their stewardship. That stewardship is extending to IT as boards investigate the depth of their enterprise's reliance on IT.

IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.

Several entities have put forward definitions of governance. A useful and pragmatic definition is provided by the Bank for International Settlements (BIS) in *Enhancing Corporate Governance in Banking Organisations* (1999). It defines the governance arrangements as encompassing the set of relationships between the entity's management and its governing body, its owners and its other stakeholders and providing the structure through which:

- The entity's overall objectives are set
- The method of attaining those objectives is outlined
- The manner in which performance will be monitored is described

At the heart of the governance responsibilities of setting strategy, managing risks, delivering value and measuring performance, are the stakeholder¹ values, which drive the enterprise and IT strategy. Sustaining the current business and growing into new business models are certainly stakeholder expectations and can be achieved only with adequate governance of the enterprise's IT infrastructure.

IT governance, like other governance subjects, is the responsibility of executives and shareholders (represented by the board of directors²). It is not an isolated discipline or activity, but rather is integral to enterprise governance. It consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.

The purpose of IT governance is to direct IT endeavours, to ensure that IT's performance meets the following objectives:

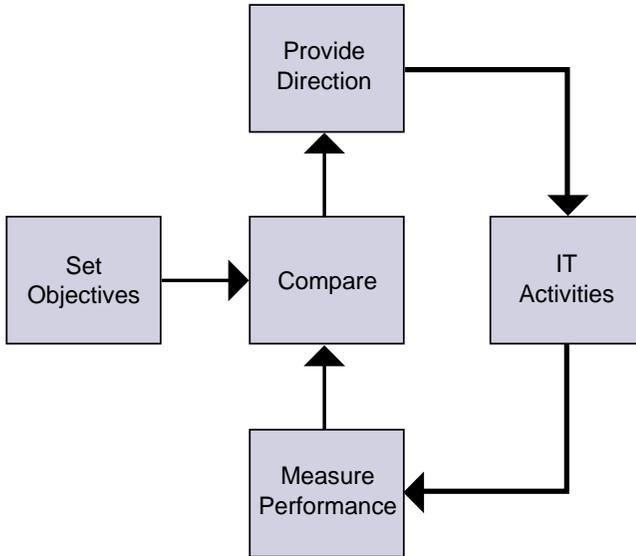
- For IT to be aligned with the enterprise and realise the promised benefits
- For IT to enable the enterprise by exploiting opportunities and maximising benefits
- For IT resources to be used responsibly
- For IT-related risks to be managed appropriately

IT governance usually occurs at different layers, with team leaders reporting to and receiving direction from their managers, with managers reporting up to the executive, and the executive to the board of directors. Reports that indicate deviation from targets usually will already include recommendations for action to be endorsed by the governing layer. Clearly this will not be effective unless strategy and goals have first been cascaded down into the organisation. The illustration on the next page presents conceptually the interaction of objectives and IT activities from an IT governance perspective and can be applied among the different layers within the enterprise.

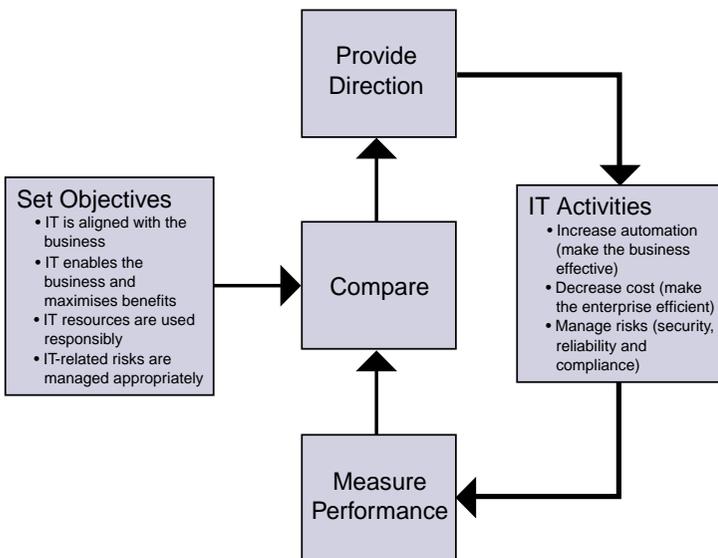
The governance process starts with setting objectives for the enterprise's IT, providing the initial direction. From then on, a continuous loop is established of performance that is measured and compared to objectives, resulting in redirection of activities where necessary and change of objectives where appropriate. While objectives are primarily the responsibility of the board and performance measures that of management, it is evident they should be developed in concert so that the objectives are achievable and the measures represent the objectives correctly.

¹ In this document, "stakeholder" is used to indicate anyone who has either a responsibility for or an expectation from the enterprise's IT, e.g., shareholders, directors, executives, business and technology management, users, employees, governments, suppliers, customers and the public.

² In this document, "board of directors" and "board" are used to indicate the body that is ultimately accountable to the stakeholders of the enterprise.



In response to the direction received, the IT function needs to focus on realising benefits by increasing automation and making the enterprise more effective, and by decreasing cost and making the whole enterprise more efficient; and on managing risks (security, reliability and compliance). The IT governance framework can then be completed as indicated below:



2. Why Is IT Governance Important?

The use of IT will be the major driver of economic wealth in the 21st century. While IT is already critical to enterprise success, serves as a competitive advantage and offers a means for increasing productivity, it will be even more so in the future. Leveraging IT successfully to transform the enterprise and create value-added products and services has become a universal business competency. IT is fundamental for enterprise resource management; it is indispensable for customer relationship management; it enables increasingly global and dematerialised transactions; and is key for recording and disseminating business knowledge.

Since IT is such a critical function in supporting and enabling enterprise goals, effective IT governance generates real business benefits, such as reputation, trust, product leadership, time-to-market and reduced costs, all of which increase stakeholder value.

While IT is fundamental to sustain what may be unglamorous and taken-for-granted business operations, it is equally essential to grow and innovate the business. Those with a strict commercial focus may challenge the latter but should be aware that unwillingness to innovate will limit the prospects of achieving future goals and long-term sustainability.

IT also carries risks. It is clear that in these days of doing business on a global scale around the clock, system and network downtime has become far too costly for any enterprise to afford. In some industries, IT is a necessary competitive resource to differentiate and provide a competitive advantage while in many others it determines survival, not just prosperity.

The networked economy has brought more efficient markets, enabled streamlining of processes and optimised supply chains. It has also created new technology and business risks and new information and resilience requirements. These new requirements and risks mandate that management of IT be more effective and transparent.

With IT now so intrinsic and pervasive within enterprises, governance needs to pay special attention to IT, reviewing how strongly the enterprise relies on IT and how critical IT is for the execution of the business strategy. While boards usually look at business strategy and strategic risks, IT is different in many ways, which may have resulted in it not receiving the attention it merits, despite the fact that it involves large investments and huge risks:

- IT requires more technical insight than do other disciplines to understand how it enables the enterprise and creates risks and opportunities
- IT has traditionally been treated as an entity separate to the business
- IT is complex, even more so in the extended enterprise operating in a networked economy

The ultimate reason IT governance is important is that expectations and reality often do not match. Boards usually expect management to:

- Deliver quality IT solutions on time and on budget
- Harness and exploit IT to return business value
- Leverage IT to increase efficiency and productivity while managing IT risks

However boards frequently experience:

- Business losses, damaged reputations or weakened competitive positions
- Deadlines that are not met, costs higher than expected and quality lower than anticipated
- Enterprise efficiency and core processes negatively impacted by poor quality of IT deliverables
- Failures of IT initiatives to bring innovation or deliver the promised benefits

3. Whom Does It Concern?

While IT governance is the responsibility of executives and shareholders, and while it usually occurs at different layers in the organisation, there are indications that it should be an important item on any audit committee agenda. For example, *Internal Control: Guidance for Directors on the Combined Code (Turnbull Report, 1999)* calls for increasing emphasis on a broader corporate governance role for audit committees. The report calls for the board to assure that there are appropriate and effective processes to monitor risk and that the system of internal control is effective in reducing those risks to an acceptable level.

From this it is clear that IT governance, like most other governance activities, intensively engages both board and executive management in a cooperative manner. However, due to complexity and specialisation, this governance layer must rely heavily on the lower layers in the enterprise to provide the information needed in its decision-making and evaluation activities. To have effective IT governance in the enterprise, the lower layers need to apply the same principles of setting objectives, providing and getting direction, and providing and evaluating performance measures. As a result, good practices in IT governance need to be applied throughout the enterprise.

4. What Can They Do About It?

IT governance responsibilities form part of a broad framework of corporate governance. This framework is well covered in the *Principles of Corporate Governance* issued by the Organisation for Economic Co-operation and Development (OECD, 1998), which focuses on the rights, roles and equitable treatment of shareholders; disclosure and transparency; and the responsibilities of the board. The report further calls for the governance framework to ensure sound strategic guidance of the company, for effective monitoring of management by the board, and for the board to be accountable for the company and to the shareholders. Among the board's responsibilities are reviewing and guiding corporate strategy, setting and monitoring achievement of management's performance objectives, and ensuring the integrity of the organisation's systems.

Apart from the fact that IT governance should be addressed like any other strategic agenda item of the board, the BIS has stated in simple terms that for critically dependent IT systems, governance should be effective, transparent and accountable. This means that the board should be very clear about its own and management's responsibilities, and should have a system in place to enforce those responsibilities which generally relate to IT's alignment and use within all activities of the enterprise, the management of technology-related business risks and the verification of the value delivered by the use of IT across the enterprise. Boards begin to do that by asking the right questions.

4.1 How Should the Board Address the Challenges?

The board should drive enterprise alignment by:

- Ascertaining that IT strategy is aligned with enterprise strategy
- Ascertaining that IT delivers against the strategy through clear expectations and measurement
- Directing IT strategy to balance investments between supporting and growing the enterprise
- Making considered decisions about where IT resources should be focused

The board should direct management to deliver measurable value through IT by:

- Delivering on time and on budget
- Enhancing reputation, product leadership and cost efficiency
- Providing customer trust and competitive time-to-market

The board should also measure performance by:

- Defining and monitoring measures together with management to verify that objectives are achieved and to measure performance to eliminate surprises
- Leveraging a system of balanced business scorecards maintained by management that form the basis for executive management compensation

The board should manage enterprise risk by:

- Ascertaining that there is transparency about the significant risks to the organisation
- Being aware that the final responsibility for risk management rests with the board
- Being conscious that risk mitigation can generate cost-efficiencies
- Considering that a proactive risk management approach can create competitive advantage
- Insisting that risk management be embedded in the operation of the enterprise
- Ascertaining that management has put processes, technology and assurance in place for information security to ensure that:
 - Business transactions can be trusted
 - IT services are usable, can appropriately resist attacks and recover from failures
 - Critical information is withheld from those who should not have access to it

4.2 How Should Executive Management Address the Expectations?

The executive's focus is generally on cost-efficiency, revenue enhancement and building capabilities, all of which are enabled by information, knowledge and the IT infrastructure. Because IT is an integral part of the enterprise, and as its solutions become more and more complex (outsourcing, third-party contracts, networking, etc.), adequate governance becomes a critical factor for success. To this end, management should:

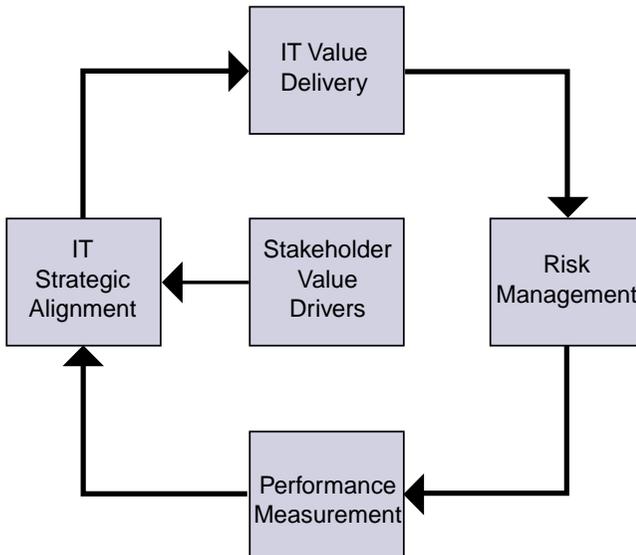
- *Embed clear accountabilities* for risk management and control over IT into the organisation, based on a clear risk policy and comprehensive control framework
- *Cascade strategy, policies and goals* down into the enterprise and *align the IT organisation* with the enterprise goals
- *Provide organisational structures* to support the implementation of IT strategies and an *IT infrastructure* to facilitate the creation and sharing of business information

- *Measure performance* by having outcome measures³ for business value and competitive advantage that IT delivers and performance drivers to show how well IT performs
- *Focus on core business competencies IT must support*, which are those business processes that add customer value, differentiate the enterprise's products and services in the marketplace, and add value across multiple products and services over time
- *Focus on important IT processes* that improve business value, such as change, applications and problem management. Management must become aggressive in defining these processes and their associated responsibilities.
- *Focus on core IT competencies* that usually relate to planning and overseeing the management of IT assets, risks, projects, customers and vendors
- *Create a flexible and adaptive enterprise* that leverages information and knowledge: an enterprise that *senses* what is happening in the market, *uses* knowledge assets to *learn* from that and *innovates* new products, services, channels and processes, then *mutates* rapidly to bring innovation to market or to repel challenges and *measures* results and performance. At the heart of this emerging model is knowledge. IT is the enabling factor to collect, build and distribute knowledge. This emerging enterprise model is depicted in detail in Appendix E.
- *Have clear external sourcing strategies*. The extended enterprise and the need to acquire outside IT resources and services render the management of third-party contracts and associated service level agreements critical in providing the information the enterprise needs. It also requires trust to be built between organisations, often entailing interconnectivity and information sharing that require adopting mutual IT control and governance practices.

³ The COBIT control framework refers to key goal indicators (KGIs) and key performance indicators (KPIs) for the Kaplan/Norton concepts of outcome measures and performance drivers.

5. What Does It Cover?

Fundamentally, IT governance is concerned about two things: that IT delivers value to the business and that IT risks are mitigated. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need measurement, for example, by a balanced scorecard. This leads to the four main focus areas for IT governance, all driven by stakeholder value. Two of them are outcomes: value delivery and risk mitigation. Two of them are drivers: strategic alignment and performance measurement.



IT governance entails a number of activities for the board and for executive management, such as being informed of the role and impact of IT on the enterprise, assigning responsibilities, defining constraints within which to operate, measuring performance, managing risk and obtaining assurance.

Typical subjects covered by these activities include the objectives of IT, the opportunities and risks of new technologies, and the key processes and core competencies.

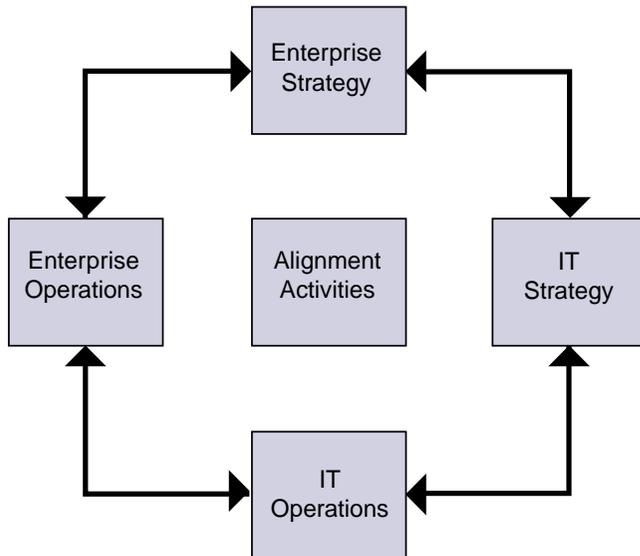
See the action plans in Appendices B and C for a full listing of IT governance activities and subjects.

The four focus areas on which the IT governance activities concentrate are briefly explained hereafter. In section 7, a number of practices and critical success factors⁴ are introduced that elaborate further on how these activities are performed and what elements will increase their success.

5.1 IT Strategic Alignment

The key question is whether a firm's investment in IT is in harmony with its strategic objectives (intent, current strategy and enterprise goals) and thus building the capabilities necessary to deliver business value. This state of harmony is referred to as "alignment." It is complex, multifaceted and never completely achieved. It is about continuing to move in the right direction and being better aligned than competitors. This may not be attainable for many enterprises because enterprise goals change too quickly, but is nevertheless a worthwhile ambition because there is real concern about the value of IT investment.

Alignment of IT has been synonymous with IT strategy, i.e., does the IT strategy support the enterprise strategy? For IT governance, alignment encompasses more than strategic integration between the (future) IT organisation and the (future) enterprise organisation. It is also about whether IT operations are aligned with the current enterprise operations (illustration below). Of course, it is difficult to achieve IT alignment when enterprise units are misaligned.



“IT alignment is a journey, not a destination.”

⁴ In this document, critical success factors are conditions, capabilities, competencies and behaviours not always under one's own control to obtain.

Hence the board should drive business alignment by:

- Ascertaining that IT strategy is *aligned* with business strategy
- Ascertaining that IT *delivers* against the strategy (delivering on time and within budget, with appropriate functionality and the intended benefits, is a fundamental building block of alignment and value delivery) through clear expectations and measurement (e.g., balanced business scorecard)
- Directing IT strategy to *balance* investments between systems that support the enterprise as is, transform the enterprise or create an infrastructure that enables the business to grow and compete in new arenas
- Making considered decisions about *focus* of IT resources: break into new markets, drive competitive strategies, increase overall revenue generation, improve customer satisfaction, assure customer retention

Alignment requires planned and purposeful management processes, such as:

- Creating and sustaining awareness of the strategic role of IT at the top management level
- Clarifying what role IT should play, utility vs. enabler
- Creating IT guiding principles from business maxims. For example, “develop partnerships with customers worldwide” can lead to “consolidate customer database and order processing processes.”
- Monitoring the business impact of the IT infrastructure and applications portfolio
- Evaluating, post-implementation, benefits delivered by IT projects

5.2 IT Value Delivery

The basic principles of IT value are delivery on time, within budget and with the benefits that were promised. In business terms, this is often translated into: competitive advantage, elapsed time for order/service fulfillment, customer satisfaction, customer wait time, employee productivity and profitability. Several of these elements are either subjective or difficult to measure, something all stakeholders need to be aware of.

The value that IT adds to the business is a function of the degree to which the IT organisation is aligned with the business and meets the expectations of the business. The business has expectations relative to the contents of the IT deliverable:

- Fit for purpose, meeting business requirements
- Flexibility to adopt future requirements
- Throughput and response times
- Ease of use, resiliency and security
- Integrity, accuracy and currency of information

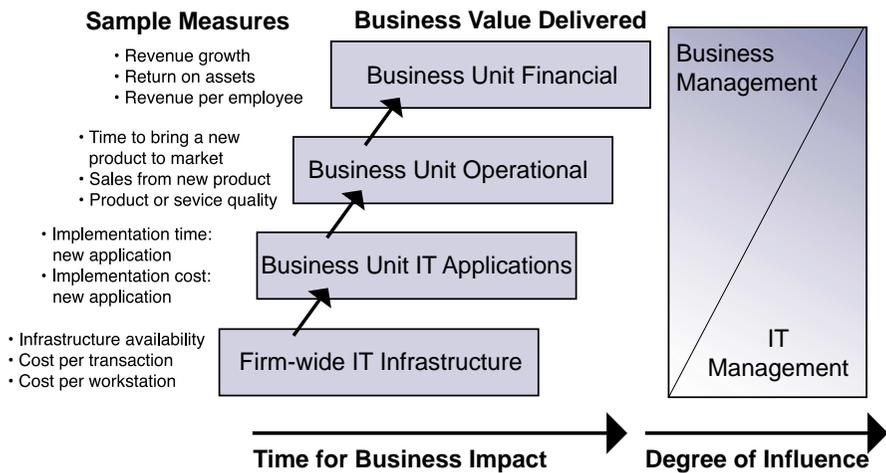
“IT value is in the eye of the beholder.”

The business also has expectations regarding the method of working:

- Time-to-market
- Cost and time management
- Partnering success
- Skill set of IT staff

To manage these expectations, IT and the business should use a common language for value which translates business and IT terminology and is based wholly on fact.

Different levels of management and users will perceive the value of IT differently, as illustrated below.⁵ The following illustration also shows that the higher one goes in the measurement hierarchy, the more dilution will occur (i.e., the less influence IT management can exercise). This also means that measuring the impact of an IT investment is much easier at the bottom of the hierarchy than at the top.



Therefore, IT needs to be aligned to deliver value so that it *supports the enterprise* as is by delivering on time, with appropriate functionality and the intended benefits, and by delivering infrastructures that *enable the enterprise to grow* by breaking into new markets, increasing overall revenue, improving customer satisfaction, assuring customer retention and driving competitive strategies.

To do that implies:

- Timely, usable and reliable information about customers, processes, markets, etc.

⁵ Peter Weill and Marianne Broadbent, *Leveraging the New Infrastructure: How Market Leaders Capitalize on Information Technology*, Harvard Business School Press, 1998

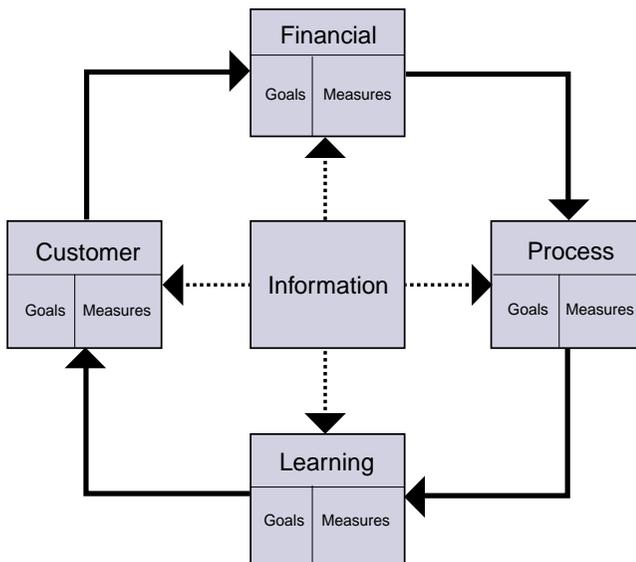
- Productive and effective practices (performance measurement, knowledge management, etc.)
- The ability to integrate technology

To be successful, enterprises need to be aware that different strategic contexts require different indicators of value. They will have to assign explicit responsibility in the organisation for each value measure and establish the value measures in concert between the business and IT. This implies, as is recommended in section 5.4, that the IT balanced scorecard should cover these measures and be developed with input and approval from business management.

5.3 Performance Measurement

Strategy has taken on a new urgency as enterprises mobilise intangible and hidden assets to compete in an information-based global economy. Balanced scorecards translate strategy into action to achieve goals with a performance measurement system that goes beyond conventional accounting, measuring those relationships and knowledge-based assets necessary to compete in the information age: *customer* focus, *process* efficiency and the ability to *learn* and grow.

At the heart of these scorecards is management information supplied by the IT infrastructure (illustration below).



**“In IT,
if you are
playing the
game
and not
keeping
score, you
are only
practising.”**

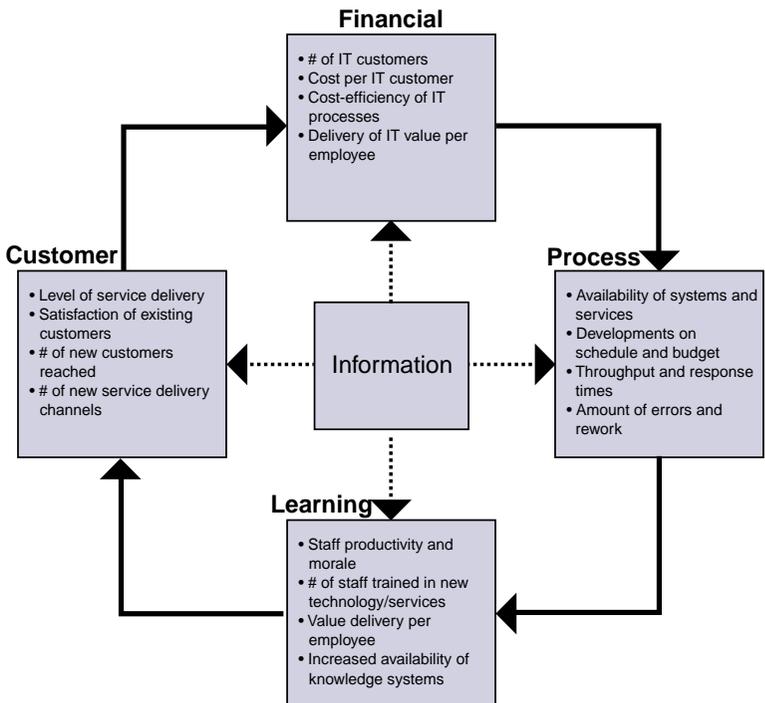
But IT does more than provide information to obtain a global picture of where the organisation is and where it is going. It also enables and sustains solutions for the actual goals set in the financial (enterprise resource management), customer (customer relationship manage-

ment), process (intranet and workflow tools) and learning (knowledge management) dimensions of the scorecard.

IT not only contributes information to the business scorecards and tools to the different dimensions being measured, but also, because of the criticality of IT itself, needs its own scorecard. Defining clear goals and good measures that unequivocally reflect the business impact of the IT goals is a challenge and needs to be resolved in co-operation among the different governance layers within the enterprise.

It is also vital to note that the linkage between the business balanced scorecard and the IT balanced scorecard is a strong method of alignment. Many of the outcome measures of IT influence how well the enterprise is doing and are therefore performance measures for the enterprise. It is equally vital to stress that the balanced scorecard should demonstrate the value that IT delivers to the enterprise.

The following illustration depicts some examples of outcome and performance measures for the different dimensions of the IT balanced scorecard. Section 7 in this document lists more extensive IT measures for management and for those responsible for IT governance.



5.4 Risk Management

The introduction of the *Turnbull Report* internal control requirements (specifically in the UK, but used as a reference model elsewhere) and the universal need to demonstrate good corporate governance to shareholders and customers are the drivers for increased risk management activities in large organisations. Enterprise risk comes in many varieties, not only financial risk. Regulators are specifically concerned about operational and systemic risk, within which technology risk and information security issues are prominent. The BIS, for example, supports that view because all major past risk issues studied in the financial industry were caused by breakdowns in internal control, oversight and IT. Infrastructure protection initiatives in the US and the UK point to the utter dependence of all enterprises on IT infrastructures and the vulnerability to new technology risks. The first recommendation these initiatives make is for risk awareness of senior corporate officers.

Therefore, the board should manage enterprise risk by:

- Ascertaining that there is *transparency* about the significant risks to the organisation and clarifying the risk-taking or risk-avoidance policies of the enterprise
- Being aware that the final *responsibility* for risk management rests with the board so, when delegating to executive management, making sure the constraints of that delegation are communicated and clearly understood
- Being conscious that the system of internal control put in place to manage risks often has the capacity to generate *cost-efficiency*
- Considering that a transparent and proactive risk management approach can create *competitive advantage* that can be exploited
- Insisting that risk management is *embedded in the operation* of the enterprise, responds quickly to changing risks and reports immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how)

“It’s the IT alligators you don’t see that will get you.”

6. What Questions Should Be Asked?

While it is not the most efficient IT governance process, asking tough questions is an effective way to get started. Of course, those responsible for governance want good answers to these questions. Then they want action. Then they need follow-up. It is essential to determine, along with the action, *who* is responsible to deliver *what* by *when*. Here are some sample questions. A more extensive checklist is provided in Appendix A. The questions focus on three objectives: questions asked to discover IT issues, to find out what management is doing about them, and to self-assess the board's governance over them.

To Uncover IT Issues

- How often do IT projects fail to deliver what they promised?
- Are end users satisfied with the quality of the IT service?
- Are sufficient IT resources, infrastructure and competencies available to meet strategic objectives?
- What has been the average overrun of IT operational budgets? How often and how much do IT projects go over budget?
- How much of the IT effort goes to firefighting rather than enabling business improvements?

To Find Out How Management Addresses the IT Issues

- How well are enterprise and IT objectives aligned?
- How is the value delivered by IT being measured?
- What strategic initiatives has executive management taken to manage IT's criticality relative to maintenance and growth of the enterprise, and are they appropriate?
- Is the enterprise clear on its position relative to technology: pioneer, early-adopter, follower or laggard? Is it clear on risk: risk-avoidance or risk-taking?
- Is there an up-to-date inventory of IT risks relevant to the enterprise? What has been done to address these risks?

To Self-assess IT Governance Practices

- Is the board regularly briefed on IT risks to which the enterprise is exposed?
- Is IT a regular item on the agenda of the board and is it addressed in a structured manner?
- Does the board articulate and communicate the business objectives for IT alignment?
- Does the board have a clear view on the major IT investments from a risk and return perspective? Does the board obtain regular progress reports on major IT projects?
- Is the board getting independent assurance on the achievement of IT objectives and the containment of IT risks?

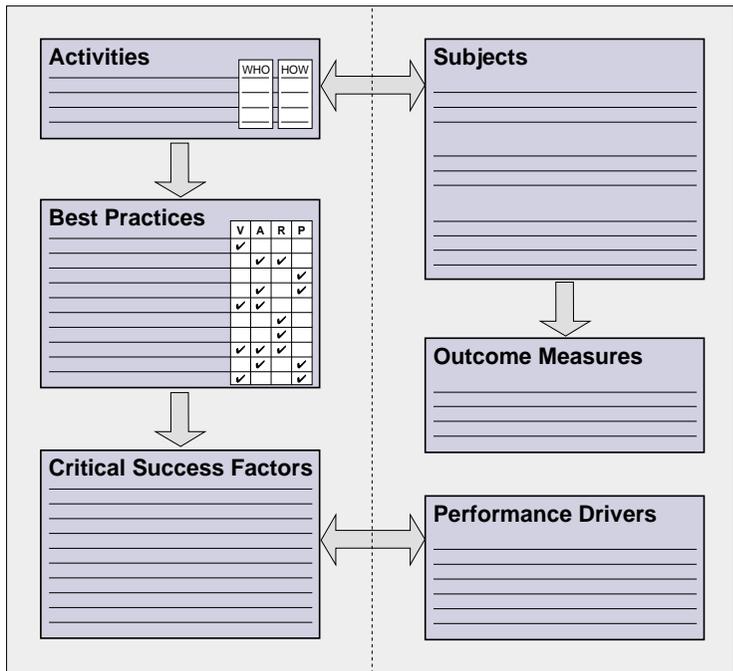
7. How Is It Accomplished?

Action plans for implementing effective IT governance, from both a board and an executive management point of view, are provided in Appendices B and C, respectively. These plans consist of various elements:

- *Activities* list what is done to exercise the IT governance responsibilities and the *subjects* identify those items that typically get onto an IT governance agenda.
- *Outcome measures* relate directly to the subjects of IT governance, such as the alignment of business and IT objectives, cost-efficiencies realised by IT, capabilities and competencies generated and risks and opportunities addressed. Examples include:
 - Enhanced performance and cost management
 - Measurable contribution from IT to fast introduction of innovative products and services
 - Actual availability of systems and services and increasing level of service delivery
 - Absence of integrity and confidentiality risks
- *Best practices* then list examples of how the activities are being performed by those who have established leadership in governance of technology. Examples include:
 - Embedding into the enterprise an IT governance structure that is accountable, effective and transparent, with defined activities and purposes and with unambiguous responsibilities
 - Establishing an audit committee that considers what the significant risks are and assesses how they are identified, evaluated and managed, i.e., the effectiveness of the system of internal control in managing significant risks
 - Aggressively aligning enterprise and IT strategies and objectives
 - Enabling a growing knowledge base on customers, products, markets and processes
- *Critical success factors* are conditions, competencies and attitudes that are critical to being successful in the practices. Examples include:
 - Sensitivity to the fact that IT is integral to the enterprise and not something to be relegated to a technical function
 - Awareness of IT's criticality to the enterprise and ensuing formal acceptance of responsibility by management who engage specialists to assist them
 - Management that is goal-focused and has the appropriate information on markets, customers and internal processes

- A business culture that establishes accountability, encourages cross-divisional co-operation and teamwork, promotes continuous process improvement and handles failure well
- *Performance drivers* provide indicators on “how” IT governance is achieving, as opposed to the outcome measures that measure “what” is being achieved. They often relate to the critical success factors. Examples include:
 - The extent and frequency of risk and control reporting to the board
 - Improved cost-efficiency of IT processes (costs vs. deliverables)
 - System downtime
 - Throughput and response times

Appendices B and C include a full set of action plans for board and management, organised as shown below. The plans list IT governance activities and link a set of subjects and practices to them. Practices have been classified to reflect the IT governance area(s) to which they provide the greatest contribution: value delivery, strategic alignment, risk management and/or performance (V, A, R, P). A list of critical success factors is provided in support of the practices. Finally, two sets of measures are listed: outcome measures that relate to the IT governance subjects and performance drivers that relate to how activities are performed and the associated practices and critical success factors.

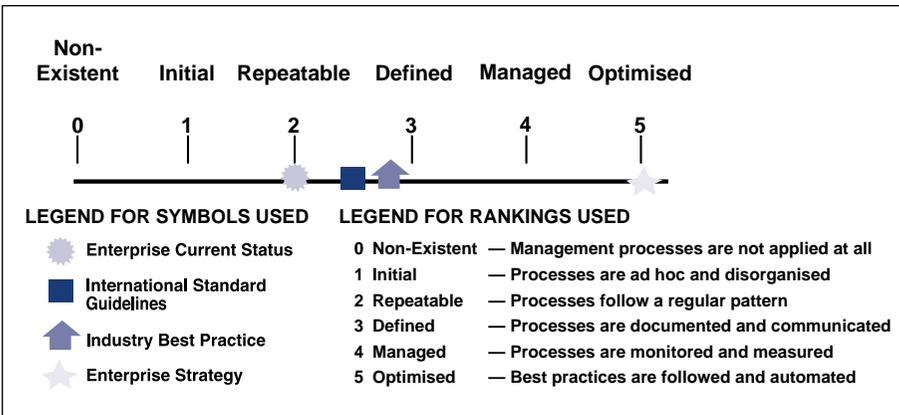


8. How Does Your Organisation Compare?

For effective governance of IT to be implemented, organisations need to assess how well they are currently performing and be able to identify where and how improvements can be made. This applies to both the IT governance process itself and to all the processes that need to be managed within IT.

The use of maturity models greatly simplifies this task and provides a pragmatic and structured approach for measuring how well developed your processes are against a consistent and easy-to-understand scale.

The maturity scales are shown below, and the models provide descriptive characteristics that would be expected to be seen at each level for governance and the processes that need to be governed.



Using this technique the organisation can:

- Build a view of current practices by discussing them in workshops and comparing to example models
- Set targets for future development by considering model descriptions higher up the scale and comparing to best practices
- Plan projects to reach the targets by defining the specific changes required to improve management
- Prioritise project work by identifying where the greatest impact will be made and where it is easiest to implement

A maturity model showing descriptions of the different levels of maturity for IT governance is provided in Appendix D.

9. What Reference Material Exists?

Various regulatory bodies, such as the Bank for International Settlements and the Organisation for Economic Co-operation and Development, have issued reports on corporate governance since the early 1990s. Each of these reports makes recommendations on good practice for effective governance for boards and executive management. Stakeholder value, transparency of risk and internal control are common themes emphasised by all.

COBIT (*Control Objectives for Information and related Technology*), issued by the Information Systems Audit and Control Foundation and the IT Governance Institute, is increasingly internationally accepted as good practice for control over information, IT and related risks. Its guidance enables an organisation to implement effective governance over the IT that is pervasive and intrinsic throughout the enterprise.

IT governance, as a critical element of—not isolated from—corporate governance, incorporates the elements proposed in these seminal documents, and adds the component of focus on the alignment between the business and IT strategies.

For a summary of major regulatory reports dealing with corporate and IT governance, see Appendix F.

APPENDICES

Appendix A—IT Governance Checklist

V = IT Value Delivery; A = IT Strategic Alignment; R = Risk Management; P = Performance

<i>Questions to Ask to Uncover IT Issues</i>	V	A	R	P
Is it clear what IT is doing?		✓		
How often do IT projects fail to deliver what they promised?	✓	✓		
Are end users satisfied with the quality of the IT service?	✓			
Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives?	✓	✓		
Are IT core competencies maintained at a sufficient level to meet required enterprise strategic objectives?	✓	✓		
How well are IT outsourcing agreements being managed?	✓		✓	✓
What has been the average overrun of IT operational budgets?				✓
How often and how much do IT projects go over budget?				✓
How long does it take to make major IT decisions?		✓	✓	
Are the total IT effort and investments transparent?	✓			✓
How much of the IT effort goes to firefighting rather than enabling business improvements?	✓	✓		
Is the enterprise's internal IT skill set decreasing and how successfully are skilled IT resources attracted to the organisation?		✓	✓	
How well do the enterprise and IT align their objectives?		✓		

<i>Questions to Ask to Find Out How Management Addresses the IT Issues</i>	V	A	R	P
How critical is IT to sustaining the enterprise? How critical is IT to growing the enterprise?	✓	✓	✓	
What strategic initiatives has executive management taken to manage IT's criticality relative to maintenance and growth of the enterprise, and are they appropriate?		✓		
What is the organisation doing about leveraging its knowledge to increase shareholder value?	✓			
What IT assets are there and how are they managed?			✓	✓
Are suitable IT resources, infrastructures and skills available to meet the required enterprise strategic objectives?		✓		
Is the enterprise clear on its position relative to technology: pioneer, early-adopter, follower or laggard?	✓	✓		
Is IT participating in overall corporate change setting and strategic direction? Do IT practices and IT culture support and encourage change within the enterprise?		✓		
Does the enterprise research technology, process and business prospects to set direction for future growth?		✓		
Are enterprise and IT objectives linked and synchronised?		✓		

<i>Questions to Ask to Find Out How Management Addresses the IT Issues, continued</i>	V	A	R	P
Is the enterprise clear on its position relative to risk: risk-avoidance or risk-taking?			✓	
Is there an up-to-date inventory of IT risks relevant to the enterprise?			✓	
What has been done to address these risks?			✓	
How far should the enterprise go in risk mitigation and is the cost justified by the benefit?			✓	
What are other organisations doing, and how is the enterprise placed in relation to them?		✓		✓
What is industry best practice and how does the enterprise compare?	✓			✓
What is management doing to address risks?		✓		
Is the board regularly briefed on risks to which the enterprise is exposed?			✓	
Based on these questions, can the enterprise be said to be taking “reasonable” precautions relative to technology risks?		✓	✓	

<i>Questions to Ask to Self-assess IT Governance Practices</i>	V	A	R	P
How certain is the board about the answers provided to the above questions?				✓
Is the board aware of the latest developments in IT from a business perspective?		✓		
Is IT a regular item on the agenda of the board and is it addressed in a structured manner?		✓		
Does the board articulate and communicate the business direction to which IT should be aligned?		✓		
Is the board aware of potential conflicts between the enterprise divisions and the IT function?		✓	✓	
Does the board have a view on how and how much the enterprise invests in IT compared to its competitors?	✓			✓
Is the reporting level of the most senior IT manager commensurate with the importance of IT?		✓		
Does the board have a clear view on the major IT investments from a risk and return perspective?	✓		✓	
Does the board obtain regular progress reports on major IT projects?	✓			✓
Does the board obtain IT performance reports illustrating the value of IT from a business driver’s perspective (customer service, cost, agility, quality, etc.)?	✓			✓
Is the board regularly briefed on IT risks to which the enterprise is exposed, including compliance risks?			✓	
Is the board assured of the fact that suitable IT resources, infrastructures and skills are available (including external resourcing), to meet the required enterprise strategic objectives?		✓		
Is the board getting independent assurance on the achievement of IT objectives and the containment of IT risks?	✓		✓	✓

Appendix B—Board Action Plan

IT Governance Activities	Board and/or Management	Activity Type
Become informed of role and impact of IT on the enterprise	B/M	Plan
Set direction and expected return	B	Direct
Determine required capabilities and investments	M	Plan
Assign responsibilities	B/M	Direct
Sustain current operations	M	Organise
Make transformation happen	B/M	Direct
Define constraints within which to operate	B	Direct
Acquire and mobilise resources	M	Organise
Measure performance	B	Control
Manage risk	B/M	Control
Obtain assurance	B	Control



Best Practices	V	A	R	P
Embedding into the enterprise an IT governance structure that is accountable, effective and transparent, with defined activities and purposes and with unambiguous responsibilities	✓	✓	✓	✓
Establishing an audit committee that considers what the significant IT risks are; assesses how they are identified, evaluated and managed; commissions IT and security audits and rigorously follows up closure of subsequent recommendations	✓		✓	
Appointing and overseeing an internal audit function with a direct reporting line to the chief executive and the audit committee, and possibly an independent external auditor as well as other third-party reviewers	✓	✓	✓	✓
Coordinating and reviewing charter, budget and plans using risk-based planning, scope, coverage and quality of work of IT auditors and other providers of IT assurance	✓	✓	✓	✓
Defining the scope and charter of audit committee, securing annual opinion letters, management control assertions and compliance letters, also covering IT and security	✓		✓	
Monitoring how management determines what IT resources are needed to achieve strategic objectives	✓		✓	
Paying special attention to IT control failures and weaknesses in internal control and their actual and potential impact, while considering whether management acts promptly on them and whether more monitoring is required	✓		✓	✓
Evaluating the scope and quality of management's ongoing monitoring of IT risks and controls	✓		✓	✓
Creating an IT strategy committee of the board that reviews major investments on behalf of the full board and advises management on strategic directions	✓	✓		
Developing a process for making the return vs. risk balance explicit and measurable while accepting a balanced failure/success ratio in the portfolio of innovation projects	✓		✓	✓
Assessing senior management's performance on strategies in operation and whether they are strongly and clearly communicated across the enterprise and are understood		✓		✓
Getting involved in defining useful strategic IT metrics and IT performance measures	✓	✓		✓

V = IT Value Delivery; A = IT Strategic Alignment; R = Risk Management; P = Performance



Critical Success Factors
Consideration of IT as an integral part of the enterprise, not something to be relegated to a technical function; IT strategy as an integral part of enterprise strategy; and IT governance as an integral part of enterprise governance
Awareness of IT's criticality to the enterprise and ensuing formal acceptance of responsibility by management who engage specialists to assist them
IT governance activities are defined with a clear purpose, documented and implemented, based on enterprise needs and with unambiguous accountabilities
Audit committee members with relevant background and exposure in technology risk
Ability to work well with partners and suppliers in support of the extended enterprise
Focus on the enterprise goals, strategic initiatives, the use of technology to enhance the enterprise and on the availability of sufficient resources and capabilities to keep up with the business demands
Informal channels of communications with management and external auditors to create a culture of openness
A code of conduct established in co-operation between management and board, that is reviewed for compliance and formally signed off by senior management
Implementation of a strategic management system that provides visibility to the IT governance issues of IT strategic alignment, value delivery, risk management and service performance



IT Governance Subjects
<i>The objectives of IT—how it:</i>
• Improves cost-efficiencies
• Creates revenue enhancement
• Supports the building of new capabilities
• Enables core business processes (typically, those that differentiate and add value over products and services in the marketplace and over time)
• Enables new business models
<i>The opportunities and risks of new technology:</i>
• Internet and intranet
• E-commerce
• Mobile computing
• Workflow technology
• Knowledge systems, etc.
<i>The key processes and core competencies:</i>
• The return on investment of IT projects and initiatives, and how they deliver against expectations
• Performance of IT services against service level agreements
• IT risks, asset protection and information security
• IT acquisition and outsourcing strategies
• Important IT processes such as change, application and problem management
• Core IT competencies: planning, support, operations, project management, knowledge management
• Ethical behavior, data privacy and fraud prevention

Outcome Measures
Enhanced performance and cost management
Measurable contribution from IT to fast introduction of innovative products and services
Improved return on major IT investments
Appropriately integrated and standardised enterprise processes
Reaching new and satisfying existing customers
Meeting stakeholder requirements and expectations on budget and on time
Adherence to laws, regulations, industry standards and contractual commitments
Transparency on risk taking and adherence to the agreed organisational risk profile
Creation of new service delivery channels
Business cases that demonstrate a high potential return on investment

Performance Drivers
The extent and frequency of risk and control reporting to the board
Improved cost-efficiency of IT processes (costs vs. deliverables)
Increased number of enterprise transformation projects enabled by IT
Increased utilisation of IT infrastructure
Increased satisfaction of stakeholders (survey and number of complaints)
Improved staff productivity (number of deliverables) and morale (survey)
Increased availability of knowledge and information for managing the enterprise
Increased linkage between IT and enterprise governance
Improved performance as measured by IT balanced scorecards
Benchmarking comparisons of IT governance maturity

Appendix C—Management Action Plan

IT Governance Activities	Board and/or Management	Activity Type
Become informed of role and impact of IT on the enterprise	B/M	Plan
Set direction and expected return	B	Direct
Determine required capabilities and investments	M	Plan
Assign responsibilities	B/M	Direct
Sustain current operations	M	Organise
Make transformation happen	B/M	Direct
Define constraints within which to operate	B	Direct
Acquire and mobilise resources	M	Organise
Measure performance	B	Control
Manage risk	B/M	Control
Obtain assurance	B	Control

Best Practices	V	A	R	P
Aggressively aligning enterprise and IT strategies and objectives		✓		
Enabling a growing knowledge base on customers, products, markets and processes	✓			
Communicating goals and objectives strongly and clearly across the enterprise and ensuring they are understood and provide clarity of purpose to all stakeholders		✓		
Establishing an IT council, involving the chief information officer and senior business managers, that sets priorities for IT initiatives and assigns ownership for IT-enabled business opportunities	✓	✓		
Developing and applying control practices that increase transparency, reduce complexity, promote learning and provide flexibility	✓		✓	✓
Measuring IT performance along different dimensions: financial aspects, customer satisfaction, process effectiveness and future capability; and reward IT management based on measures that usually include: scheduled up time, service levels, transaction throughput and response times, and application availability.				✓
Instituting control practices that avoid breakdowns in internal control and oversight, increase efficient and optimal use of resources and increase the effectiveness of IT processes	✓		✓	✓
Integrating and providing smooth interoperability of the more complex IT processes such as problem, change and configuration management	✓	✓		
A general manager (chief executive officer) who mediates between imperatives of the business and of the technology		✓		
Managing supplier risk through relationship management, escrow, second sourcing or by acquiring an interest in the supplier organisation			✓	
Extensive automated monitoring practices, leveraging IT to measure its own performance, tracking performance measures, effectiveness of internal control systems and status of improvement activities	✓		✓	✓
Embed clear accountabilities for control over IT and for risk management into the organisation, balancing disciplinary action and reward, enabling fast and professional response to IT governance issues	✓		✓	✓
Providing an infrastructure to facilitate the creation and sharing of business information that: <ul style="list-style-type: none"> • Is flexible and able to be integrated and maintained • Is functional, cost-effective, timely, secure and resilient to failure • Logically extends, maintains and manages disparate legacy systems and new applications • Ensures standard, reusable and modular applications and components 	✓		✓	

V = IT Value Delivery; A = IT Strategic Alignment; R = Risk Management; P = Performance

Critical Success Factors
Management that is goal-focused and has the appropriate information on markets, customers and internal processes
A business culture that establishes accountability, encourages cross-divisional co-operation and teamwork, promotes continuous process improvement and handles failure well
Organisational practices that enable sound oversight, a control culture, risk assessment as standard practice and appropriate adherence to established standards
Rigorous monitoring of and follow-up on control deficiencies and risks
User involvement in IT initiatives and IT managers' involvement in business initiatives
Ability to work well with outside parties
Understanding that building complex systems is very hard and prone to failure
IT managers with a "compulsion for completion"
Cognisance that value chains do not remain static, that components do not "plug and play" and that bandwidth is not free
Sensitivity to the fact that IT architectures remain inflexible and difficult to integrate
Awareness that skilled IT resources are the working capital of successful IT operations and that IT skills demand and supply frequently will not be in balance
Ability to acquire and manage knowledge about customers, products, channels, services, competitors, complementors and processes
Understanding of the complexity of IT, especially for the extended enterprise operating in the networked economy

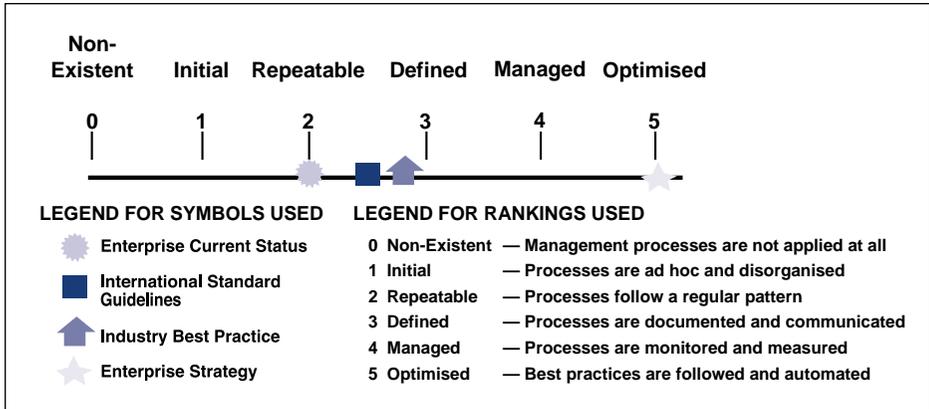
IT Governance Subjects
<i>The objectives of IT—how it:</i>
<ul style="list-style-type: none"> • Improves cost-efficiencies • Creates revenue enhancement • Supports the building of new capabilities • Enables core business processes (typically, those that differentiate and add value over products and services in the marketplace and over time) • Enables new business models
<i>The opportunities and risks of new technology:</i>
<ul style="list-style-type: none"> • Internet and intranet • E-commerce • Mobile computing • Workflow technology • Knowledge systems, etc.
<i>The key processes and core competencies:</i>
<ul style="list-style-type: none"> • The return on investment of IT projects and initiatives, and how they deliver against expectations • Performance of IT services against service level agreements • IT risks, asset protection and information security • IT acquisition and outsourcing strategies • Important IT processes such as change, application and problem management • Core IT competencies: planning, support, operations, project management, knowledge management • Ethical behavior, data privacy and fraud prevention



Outcome Measures
Actual availability of systems and services and increasing level of service delivery
Absence of integrity and confidentiality risks
Availability of appropriate bandwidth, computing power and IT delivery mechanisms
Confirmation of reliability and effectiveness
Adherence to development cost and schedule
Deviation between estimated and actual costs
Staff productivity and morale
Number of timely changes to processes and systems
Improved productivity (e.g., delivery of value per employee, number of customers and cost per customer served)
Cost efficiency of processes and operations

Performance Drivers
System downtime
Throughput and response times
Amount of errors and rework
Increased satisfaction of IT users and stakeholders
Number of staff trained in new technology and customer service skills
Benchmark comparisons
Number of non-compliance reportings
Reduction in development and processing time
Increased number of IT action plans for process improvement initiatives
Improved performance as measured by IT balanced scorecards

Appendix D—IT Governance Maturity Model



0 Non-existent There is a complete lack of any recognisable IT governance process. The organisation has not even recognised that there is an issue to be addressed and hence there is no communication about the issue.

Governance, such as it is, is predominantly centralised within the IT organisation, and IT budgets and decisions are made centrally. Business unit input is informal and done on a project basis. In some cases, a steering committee may be in place to help make resource decisions.

1 Initial /Ad Hoc The organisation has recognised that IT governance issues exist and need to be addressed. There are, however, no standardised review processes, but instead management considers IT management issues on an individual or case-by-case basis. Management's approach is unstructured and there is inconsistent communication on issues and approaches to address the problems that arise. Although it is recognised that the performance of the IT function ought to be measured, there are no proper metrics in place—reviews are based on individual managers' requests. IT monitoring is implemented only reactively to an incident that has caused some loss or embarrassment to the organisation.

Governance is difficult to initiate and the central IT organisation and business units may even have an adversarial relationship. The organisation is trying to increase trust between IT and the business and there are normally periodic joint meetings to review operational issues and new projects. Upper management is involved only when there are major problems or successes.

2 Repeatable but Intuitive There is awareness of IT governance objectives, and practices are developed and applied by individual managers. IT governance activities are becoming established within the organisation's change management process, with active senior management involvement and oversight. Selected IT processes have been identified for improvement that would impact key business processes. IT management is beginning to define standards for processes and technical architectures. Management has identified basic IT governance measurements, assessment methods and techniques, but the process has not been adopted across the organisation. There is no formal training and communication on governance standards and responsibilities are left to the individual.

An IT steering committee has begun to formalise and establish its roles and responsibilities. There is a draft governance charter (e.g., participants, roles, responsibilities, delegated powers, retained powers, shared resources and policy). Small and pilot governance projects are initiated to see what works and what does not. General guidelines are emerging for standards and architecture that make sense for the enterprise and a dialogue has started to sell the reasons for their need in the enterprise.

3 Defined Process The need to act with respect to IT governance is understood and accepted. A baseline set of IT governance indicators is developed, where linkages between outcome measures and performance drivers are defined, documented and integrated into strategic and operational planning and monitoring processes. Procedures have been standardised, documented and implemented. Management has communicated standardised procedures and informal training is established. Performance indicators over all IT governance activities are being recorded and tracked, leading to enterprise-wide improvements. Although measurable, procedures are not sophisticated, but are the formalisation of existing practices. Tools are standardised, using currently available techniques. IT balanced business scorecard ideas are being adopted by the organisation. It is, however, left to the individual to get training, to follow the standards and to apply them. Root cause analysis is only occasionally applied. Most processes are monitored against some (baseline) metrics, but any deviation, while mostly being acted upon by individual initiative, would unlikely be detected by management. Nevertheless, overall accountability of key process performance is clear and management is rewarded based on key performance measures.

The IT steering committee is formalised and operational, with defined participation and responsibilities agreed to by all stakeholders. The governance charter and policy is also formalised and documented. The governance organisation beyond the IT steering committee is established and staffed.

4 Managed and Measurable There is full understanding of IT governance issues at all levels, supported by formal training. There is a clear understanding of who the customer is and responsibilities are defined and monitored through service level agreements. Responsibilities are clear and process ownership is established. IT processes are aligned with the enterprise and with the IT strategy. Improvement in IT processes is based primarily upon a quantitative understanding and it is possible to monitor and measure compliance with procedures and process metrics. All process stakeholders are aware of risks, the importance of IT and the opportunities it can offer. Management has defined tolerances under which processes must operate. Action is taken in many, but not all cases where processes appear not to be working effectively or efficiently. Processes are occasionally improved and best internal practices are enforced. Root cause analysis is being standardised. Continuous improvement is beginning to be addressed. There is limited, primarily tactical, use of technology, based on mature techniques and enforced standard tools. There is involvement of all required internal domain experts. IT governance evolves into an enterprise-wide process. IT governance activities are becoming integrated with the enterprise governance process.

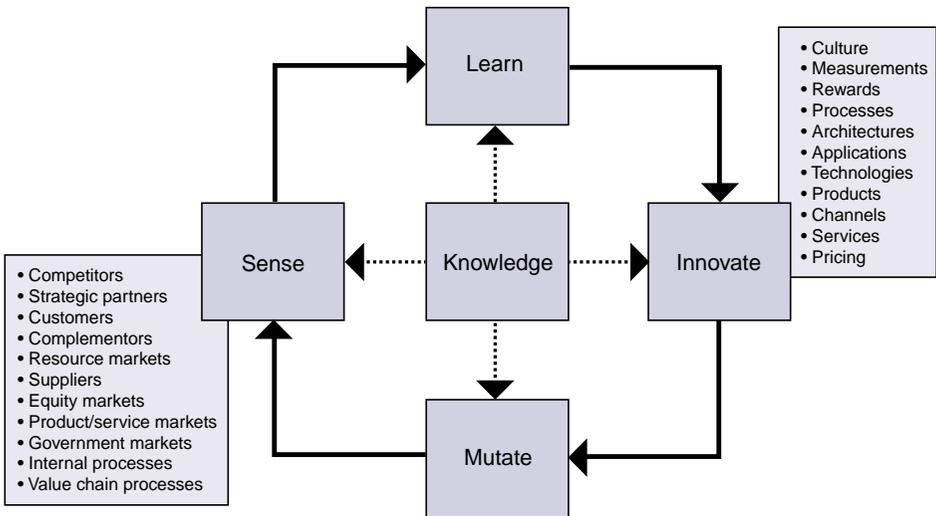
There is a fully operational governance structure that addresses a consistent architecture for re-engineering and interoperation of business processes across the enterprise, and ensures competition for enterprise resources and ongoing incremental investments in the IT infrastructure. IT is not solely an IT organisational responsibility but is shared with the business units.

5 Optimised There is advanced and forward-looking understanding of IT governance issues and solutions. Training and communication is supported by leading-edge concepts and techniques. Processes have been refined to a level of external best practice, based on results of continuous improvement and maturity modeling with other organisations. The implementation of these policies has led to an organisation, people and processes that are quick to adapt and fully support IT governance requirements. All problems and deviations are root cause analysed and efficient action is expediently identified and initiated. IT is used in an extensive, integrated and optimised manner to automate the workflow and provide tools to improve quality and effectiveness. The risks and returns of the IT processes are defined, balanced and communicated across the enterprise. External experts are leveraged and benchmarks are used for guidance. Monitoring, self-assessment and communication about governance expectations are pervasive within the organisation and there is optimal use of technology to support measurement, analysis, communication and training. Enterprise governance and IT governance are strategically linked, leveraging technology and human and financial resources to increase the competitive advantage of the enterprise.

The governance concept and structure forms the core of the enterprise IT governing body including provisions for amending the structure for changes in enterprise strategy, organisation or new technologies.

Appendix E—The Emerging Enterprise Model

Successful enterprises monitor their IT environment on a continuous basis. They then leverage the information and knowledge they gain from their monitoring to adapt and innovate. This even further stresses the need for boards and management to effectively direct and control IT.



The new and fast-moving economy requires agile and adaptable enterprises: enterprises that *sense* what is happening in the market, use knowledge assets to *learn* from that and *innovate* new products, services, channels and processes, then *mutate* rapidly to bring innovation to market or to repel challenges and measure results and performance. At the heart of this emerging model is knowledge. IT is the enabling factor to collect, build and distribute knowledge.

Appendix F—Regulatory Reports and Emerging Standards on Governance

Report of the Committee on the Financial Aspects of Corporate Governance (Cadbury Report, 1992)

The *Cadbury Report* makes recommendations on good practice covering the responsibilities of executive and non-executive directors in reviewing and reporting information to shareholders. It covers the rationale for and composition of audit committees, the responsibilities of auditors and the extent and value of the audit, and the links between shareholders, boards and auditors.

It recommends a Code of Best Practice based on openness, integrity and accountability to improve standards of corporate behavior, strengthen controls over businesses and their public accountability while retaining the essential spirit of the enterprise. It identifies board responsibilities for governance, including setting strategic aims, providing leadership, supervising management and reporting to shareholders on their stewardship. The audit role defined is to provide an effective external and objective check on the reporting to shareholders. All entities are encouraged to have an audit committee. The report stresses the need for balanced and understandable reporting of present and future prospects in both numerical and explanatory terms.

The recommendations in this report have been profoundly influential in establishing corporate governance in the UK and many other countries, and while the report was aimed at financial reporting and auditing, it alludes to wider concepts of governance.

Internal Control: Guidance for Directors on the Combined Code (Turnbull Report, 1999)

The *Turnbull Report* calls for increasing emphasis on a broader corporate governance role for audit committees. It reiterates that the board should maintain a sound system of internal control to safeguard the shareholders' investments in the company's assets.

This system of internal control is all the policies and practices that together support a company's effective and efficient operation. It also enables the organisation to respond to significant risks (operational, financial, compliance, etc.). Even though it is delegated to management, the board is ultimately responsible for this system of internal control.

To exercise that responsibility, the board should assure that (1) there are appropriate and effective processes to monitor risks and (2) the system of internal control is effective in reducing those risks to an acceptable level. In doing so, the board has to determine what is acceptable and not acceptable risk; what is likely and less likely to happen; what is the company's ability to deal with it when it does happen; and what is the cost/benefit of risk mitigation.

Organisation for Economic Co-operation and Development, Principles of Corporate Governance (1998)

The Organisation for Economic Co-operation and Development's principles draw heavily on governance concepts currently in the literature and are presented in five areas:

- The rights of shareholders
- The equitable treatment of shareholders
- The role of stakeholders
- Disclosure and transparency
- The responsibilities of the board

The last area should be of interest to board members and also has applicability to IT governance as illustrated by the following excerpts from the OECD principles:

The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the Board, and the Board's accountability to the company and the shareholders.

The Board should ensure compliance with applicable law and take into account the interests of stakeholders.

The Board should fulfill certain key functions, including:

- *Reviewing and guiding corporate strategy, major plans of action, risk policy, annual budgets and business plans; setting performance objectives; monitoring implementation and corporate performance; and overseeing major capital expenditures, acquisitions and divestitures.*
- *Ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for monitoring risk, financial control, and compliance with the law.*

In order to fulfill their responsibilities, Board members should have access to accurate, relevant and timely information.

Bank for International Settlements, Enhancing Corporate Governance in Banking Organisations (1999)

The BIS, representing the Central Banks of the G10, establishes policy and guidelines for the financial industry and particularly focuses on systemic and operational risk. The BIS states that for highly critical systems governance arrangements should be effective, accountable and transparent. While not all enterprises face this type of IT criticality, these guidelines are instructive about good governance practices relative to IT systems and services.

The BIS defines the governance arrangements as encompassing the set of relationships between the entity's management and its governing body, its owners and its other stakeholders and providing the structure through which the entity's overall objectives are set, the method of attainment is outlined and the measures of performance are defined.

The BIS maintains that effective governance provides proper incentives for management to pursue objectives that are in the interests of the entity and its stakeholders. It also ensures that management has the appropriate tools and abilities to achieve the entity's objectives. Governance arrangements should provide accountability to stakeholders, so that they can influence its overall objectives and performance. An essential aspect of achieving accountability is to ensure that governance arrangements are transparent, so that all affected parties have access to information about decisions affecting the entity and how they are taken.

The BIS also suggests the use of commonly available governance tools for these high risk systems:

- Written strategic objectives and plans for achieving them
- Reporting arrangements that assess the actions of senior management against the strategic objectives
- Clear lines of responsibility and accountability within the organisation and appropriate management controls together with arrangements for their enforcement
- Requirements that management at all levels be appropriately qualified and supervise the system and its operations competently
- Risk management and audit functions independent of those responsible for day-to-day operations.

To achieve transparency the BIS recommends disclosure to the stakeholders of the enterprise's:

- Governance, senior management and basic organisational structure
- Design of risk management (policies, rules, etc.)
- Design of the internal control system

and recommends that:

- Major decisions be made promptly, with proper consultation, and communicated clearly
- Relevant information about the system and its performance be made readily available

Information Systems Audit and Control Foundation/IT Governance Institute, Control Objectives for Information and related Technology (COBIT®)

Developed and promoted by the Information Systems Audit and Control Foundation and the IT Governance Institute (3rd edition), COBIT starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives. In addition to promoting process focus and process ownership, COBIT looks at fiduciary, quality and security needs of enterprises and provides for seven information criteria that can be used to generically define what the business requires from IT: effectiveness, efficiency, availability, integrity, confidentiality, reliability and compliance.

COBIT further divides IT into 34 processes belonging to four domains (Planning and Organisation, Acquiring and Implementing, Delivery and Support, Monitoring). For each of these processes, a high-level control objective is defined:

- Identifying which information criteria are most important in that IT process
- Listing which resources will usually be leveraged
- Providing considerations on what is important for controlling that IT process

The more detailed elements of COBIT provide some 300 detailed control objectives for management and IT practitioners who are looking for best practices in control implementation, and extensive audit guidelines building on these objectives. The latter are geared toward those needing to evaluate and audit the degree of control and governance over IT processes.

Recent COBIT developments added a management and governance layer, providing management with a toolbox containing:

- Performance measurement elements (outcome measures and performance drivers for all IT processes)
- A list of critical success factors that provides succinct non-technical best practices for each IT process
- A maturity model to assist in benchmarking and decision-making for control over IT

References

IT Governance Institute, COBIT (Control Objectives for Information and related Technology) 3rd Edition, 2000, www.ITgovernance.org and www.isaca.org

Peter Weill and Marianne Broadbent, *Leveraging the New Infrastructure: How Market Leaders Capitalize on Information Technology*, Harvard Business School Press, 1998

Robert S. Kaplan and David P. Norton, *The Balanced Scorecard: Translating Strategy into Action*, Harvard Business School Press, 1996

Robert S. Kaplan and David P. Norton, *The Strategy-Focused Organization*, Harvard Business School Press, 2001

S. Mingay et al, *The Five Pillars of IS Organisational Effectiveness*, Gartner Group, 1998

Various Gartner research notes on IT Alignment and IT Value Delivery, 1996 - 2000

J. Luftman, P. Lewis and S. Oldach, "Transforming the Enterprise: The Alignment of Business and Information Technology Strategies," *IBM Systems Journal*, 32,1, pp. 198-221, 1993

PricewaterhouseCoopers and The Institute of Internal Auditors Research Foundation, *Corporate Governance and the Board—What Works Best*, 2000