

Board Briefing on IT Governance

SECOND
EDITION



Board Briefing on IT Governance

SECOND
EDITION

“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*



CA The Canadian Institute
of Chartered Accountants



ERNST & YOUNG
Quality In Everything We Do



*International
Federation of
Accountants*



*Japanese Institute of
Certified Public
Accountants*



The Institute of
Chartered Accountants
in England & Wales



PRICEWATERHOUSECOOPERS

Board Briefing on IT Governance, 2nd Edition

IT Governance Institute®

The IT Governance Institute (ITGI) strives to assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals. Its goals are to raise awareness and understanding among and provide guidance and tools to boards of directors, executive management and chief information officers (CIOs) such that they are able to ensure within their enterprises that IT meets and exceeds expectations, and its risks are mitigated.

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 recognised global leader in IT governance, control and assurance. 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.

Disclaimer

The IT Governance Institute, Information Systems Audit and Control Association and the authors of *Board Briefing on IT Governance, 2nd Edition* have designed this product primarily as an educational resource for boards of directors, executive management and information technology control professionals. The IT Governance Institute and Information Systems Audit and Control Association make no claim that use of this product will assure a successful outcome. This product should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the controls professional should apply his or her own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

Disclosure

Copyright © 2003 by the IT Governance Institute. 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 ITGI's prior written permission. No other right or permission is granted with respect to this work.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web sites: www.itgi.org and www.isaca.org

ISBN 1-893209-64-4
Printed in the United States of America

Acknowledgements

The IT Governance Institute wishes to recognise:

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

Erik Guldentops, CISA, University of Antwerp Management School, Belgium (Chair)
 Steven De Haes, University of Antwerp Management School, Belgium (Project Manager)
 Gary Hardy, ITWinners Ltd, UK
 Jacqueline Ormsby, Deloitte & Touche, UK
 Daniel Fernando Ramos, CISA, CPA, SAFE Consulting Group, Argentina
 Jon Singleton, CISA, CA, Office of the Auditor General, Province of Manitoba, Canada
 Paul A. Williams, FCA, MBCS, Paul Williams Consulting, UK

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

Georges Ataya, CISA, CISSP, Solvay Business School, Belgium
 Marios Damianides, CISA, CA, CPA, Ernst & Young, USA
 John Court, Institute of Chartered Accountants in England and Wales, UK
 John W. Lainhart IV, CISA, CISM, IBM, USA
 Hugh Parkes, CISA, FCA, The Q Alliance, Australia
 Vernon Poole, Deloitte & Touche, UK
 Robert S. Roussey, CPA, University of Southern California, USA
 Ronald Saull, CSP, Great-West and Investors Group, Canada
 Michael Schirnbrand, CISM, CISA, CPA, Ernst & Young, Austria
 Lily Shue, CISA, CPP, Sony Corporation of America, USA
 Wim Van Grembergen, University of Antwerp Management School, Belgium

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

Robert S. Roussey, CPA, University of Southern California, USA, International President
 Marios Damianides, CISA, CA, CPA, Ernst & Young, USA, Vice President
 Abdul Hamid Bin Abdullah, CISA, CPA, FIIA, Auditor-General's Office, Singapore,
 Vice President
 Everett C. Johnson, CPA, Deloitte & Touche, USA, Vice President
 Dean R. E. Kingsley, CISA, CISM, CA, Deloitte & Touche, Australia, Vice President
 Ronald Saull, CSP, Great-West and Investors Group, Canada, Vice President
 Eddy Schuermans, CISA, PricewaterhouseCoopers, Belgium, Vice President
 Johann Tello, CISA, Banco del Istmo, Panama, Vice President
 Paul A. Williams, FCA, MBCS, Paul Williams Consulting, UK, Past International President
 Patrick Stachtchenko, CISA, CA, Deloitte & Touche, France, Past International President
 Emil G. D'Angelo, CISA, Bank of Tokyo-Mitsubishi, USA, Trustee

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

Table of Contents

EXECUTIVE SUMMARY6

1. WHAT IS IT GOVERNANCE?10

2. WHY IS IT GOVERNANCE IMPORTANT?13

3. WHOM DOES IT CONCERN?14

4. WHAT CAN THEY DO ABOUT IT?15

 4.1 *How Should the Board Address the Challenges?*16

 4.2 *How Should Executive Management Address the Expectations?*....18

5. WHAT DOES IT GOVERNANCE COVER?19

 5.1 *Strategic Alignment.*22

 5.2 *Value Delivery*24

 5.3 *Risk Management*.....26

 5.4 *Resource Management*.....28

 5.5 *Performance Measurement*29

6. WHAT QUESTIONS SHOULD BE ASKED?32

7. HOW IS IT ACCOMPLISHED?33

8. HOW DOES YOUR ORGANISATION COMPARE?35

9. WHAT REFERENCE MATERIAL EXISTS?.....36

10. CONCLUSIONS37

 10.1 *IT Governance Should Be Integrated within Enterprise Governance*37

 10.2 *IT Governance Roles and Responsibilities Need To Be Defined*.....37

 10.3 *An IT Governance Implementation Plan Is Required*.....38

APPENDIX A—IT Governance Checklist42

APPENDIX B—Board IT Governance Tool Kit44

APPENDIX C—Management IT Governance Tool Kit46

APPENDIX D—IT Governance Maturity Model.....48

APPENDIX E—Roles and Responsibilities for IT Governance50

APPENDIX F—IT Strategy Committee53

APPENDIX G—Regulatory Reports and Emerging Standards on Governance.....58

APPENDIX H—The Emerging Enterprise Model63

Executive Summary

Increasingly, top management is realising the significant impact that information technology (IT) can have on the success of the enterprise. Management hopes for heightened understanding of the way IT is operated and the likelihood of its being leveraged successfully for competitive advantage. In particular, top management needs to know if its IT management 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?

Successful enterprises understand the risks and exploit the benefits of IT, and find ways to deal with:

- Aligning IT strategy with the business strategy
- Cascading IT strategy and goals down into the enterprise
- Providing organisational structures that facilitate the implementation of strategy and goals
- Creating constructive relationships and effective communications between the business and IT, and with external partners
- Insisting that an IT control framework be adopted and implemented
- Measuring IT's performance

Boards and executive management need to extend governance to IT and provide the leadership, organisational structures and processes that ensure that the enterprise's IT *sustains and extends the enterprise's strategies and objectives*. IT governance is not an isolated discipline. It is an integral part of overall enterprise governance. The need to integrate IT governance with overall governance is similar to the need for IT to be an integral part of the enterprise rather than something practiced in remote corners or ivory towers.

An increasingly educated and assertive set of stakeholders is concerned about the sound management of its interests. This has led to the emergence of governance principles and standards for overall enterprise governance. Furthermore, regulations establish board responsibilities and require that the board of directors exercise due diligence in its roles. Investors have also realised the importance of governance, because they are willing to pay a premium of more than 20 percent on shares of enterprises that have shown to have good governance practices in place (McKinsey's Investors Opinion Survey, June 2000).

Enterprise governance is a 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 have primarily been driven by the need for the transparency of 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 the transactions, information and knowledge necessary to initiate and sustain economic and social activities. In most enterprises, IT has become an integral part of the business and is fundamental to support, sustain and grow the business. Successful enterprises understand and manage the risks and constraints of IT. As a consequence, boards of directors understand the strategic importance of IT and have put IT governance firmly on their agenda.

Usually, advice to boards on how to operate is long on board structure, composition, size and independence, but short on risk management and practical IT governance. This *Board Briefing on IT Governance, 2nd Edition* specifically addresses IT governance. Boards and management need to assess their capacity to:

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

The overall objective of IT governance, therefore, is to understand the issues and the strategic importance of IT, so that the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. IT governance aims at ensuring that expectations for IT are met and IT risks are mitigated.

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

In many enterprises, expectations of IT and reality often do not match and boards are faced with:

- Business losses, reputational damage and a weakened competitive position
- Inability to obtain or measure a return from IT investments
- Failure of IT initiatives to bring the innovation and benefits they promised
- Technology that is inadequate or even obsolete
- Inability to leverage available new technologies
- 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:

- How critical is IT to sustaining the enterprise and 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?

Other aspects of an effective IT governance framework can be explored by asking questions like:

- Does the board of the organisation occasionally ask questions about IT?
- Is the board regularly informed of major IT initiatives, their status and issues?
- Does the board approve IT strategy?
- Does the board have a standing IT strategy committee with representation from the business as well as IT?

This *Board Briefing on IT Governance, 2nd Edition*:

- 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
- Will help in understanding why IT governance is important, what the critical issues are and what frameworks and models are available for management of IT resources
- 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 assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals
- Is based on *Control Objectives for Information and related Technology* (COBIT®), an international and generally accepted IT control framework,

which provides metrics and critical success factors thereby enabling organisations to implement an IT governance structure throughout the enterprise

- 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 and the different domains it covers:
 - Strategic alignment of IT with the business
 - Value delivery of IT
 - Management of IT risks
 - IT resource management
 - Performance measurement of IT
 - Questions that should be asked
 - Good practices as well as critical success factors
 - Performance measures board members can track
 - A maturity model against which to benchmark the enterprise

1. What Is IT Governance?

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 IT¹ sustains and extends the organisation's strategies and objectives.

Two major publications stress the importance of governance:

1. 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 behaviour, strengthening controls over enterprises and their public accountability while retaining the essential spirit of the enterprise. It identifies various board governance responsibilities, such as setting strategic aims, providing leadership, supervising management and reporting to shareholders on their stewardship.

In practice, that stewardship is extending to IT as boards investigate the depth of their enterprise's reliance on IT.

2. The Bank for International Settlements (BIS), in *Enhancing Corporate Governance in Banking Organisations* (1999), defines 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 way that 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 stakeholder² 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.

¹ In this document, "IT" is understood to encompass the infrastructure as well as the capabilities and organisation that establish and support it.

² "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.

IT governance, like other governance subjects, is the responsibility of the board³ and executives. 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 enterprise's IT sustains and extends the enterprise's strategies and objectives. Critical to the success of these structures and processes is effective communication among all parties based on constructive relationships, a common language and a shared commitment to addressing the issues.

IT governance responsibilities form part of a broad framework of enterprise governance and should be addressed like any other strategic agenda item of the board. In simple terms, 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 deliver on those responsibilities. The responsibilities 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.

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

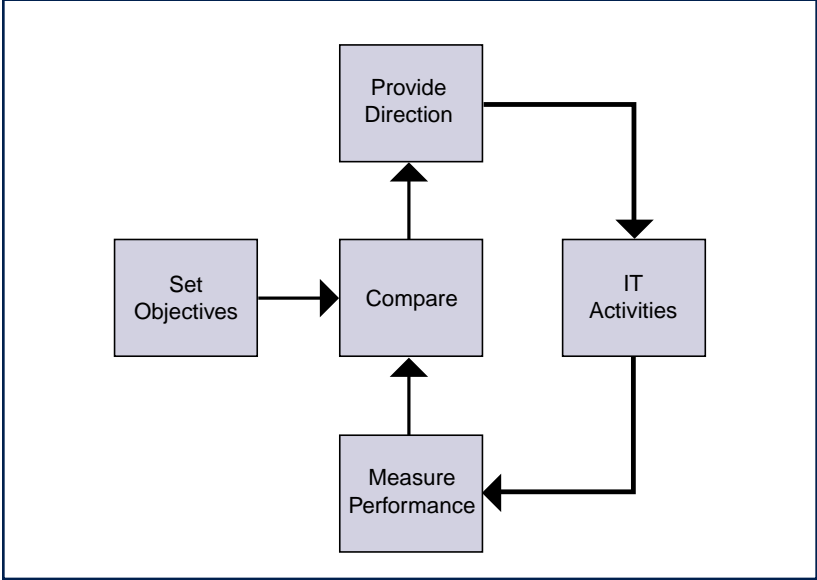
- Alignment of IT with the enterprise and realisation of the promised benefits
- Use of IT to enable the enterprise by exploiting opportunities and maximising benefits
- Responsible use of IT resources
- Appropriate management of IT-related risks

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 will usually include recommendations for action to be endorsed by the governing layer. Clearly, this approach will not be effective unless strategy and goals have first been cascaded down into the organisation. The illustration in **figure 1** 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 for measuring performance, comparing to objectives, and resulting in the redirection of activities where necessary and a 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.

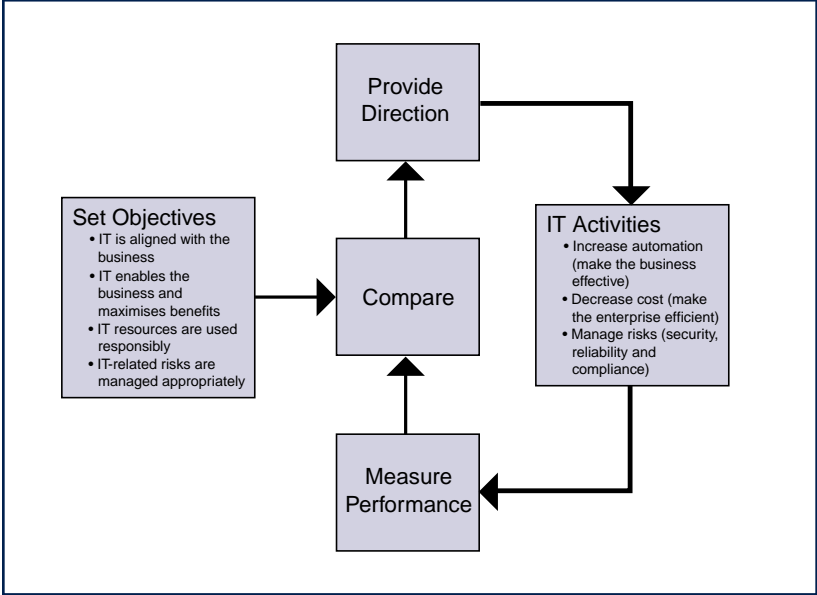
³ "Board of directors" and "board" are used to indicate the body that is ultimately accountable to the stakeholders of the enterprise.

Figure 1—Interaction of Objectives and IT Activities



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 in **figure 2**.

Figure 2—IT Governance Framework



2. Why Is IT Governance Important?

The use of IT has the potential to be the major driver of economic wealth in the 21st century. While IT is already critical to enterprise success, provides opportunities to obtain a competitive advantage and offers a means for increasing productivity, it will do all this 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 managing enterprise resources, dealing with suppliers and customers, and enabling increasingly global and dematerialised transactions. IT also is key for recording and disseminating business knowledge.

An ever larger percentage of the market value of enterprises has transitioned from the tangible (inventory, facilities, etc.) to the intangible (information, knowledge, expertise, reputation, trust, patents, etc.). Many of these assets revolve around the use of IT. Moreover, a firm is inherently fragile if its value emanates more from conceptual, as distinct from physical, assets. Good governance of IT therefore is critical in supporting and enabling enterprise goals.

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 limits 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, since:

- IT is critical in supporting and enabling enterprise goals.
- IT is strategic to the business (growth and innovation).
- Due diligence is increasingly required relative to the IT implications of mergers and acquisitions.

While boards usually look at business strategy and strategic risks, few boards have focused on IT, despite the fact that it involves large investments and huge risks. Why is that? Among the reasons:

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

Ineffective IT governance is likely to be a root cause of the negative experiences many boards have had with IT:

- Business losses, damaged reputations or weakened competitive positions
- Deadlines 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 board members, governance activities must flow through various levels of the enterprise. 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.

IT governance, like most other governance activities, intensively engages both board and executive management in a cooperative manner. However, due to complexity and specialisation, the board and executive must set direction and insist on control, while needing to rely on the lower layers in the enterprise to provide the information required in 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 and especially between the IT function and the business units. The business units have a responsibility to work in partnership with IT to ensure that their business requirements are met.

To help enable this:

- Board members should take an active role in IT strategy or similar committees.
- CEOs should provide organisational structures to support the implementation of IT strategy.
- CIOs must be business-oriented and provide a bridge between IT and the business.
- All executives should become involved in IT steering or similar committees.

4. What Can They Do About It?

IT governance responsibilities form part of a broad framework of enterprise 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 enterprise, for effective monitoring of management by the board, and for the board to be accountable for the enterprise 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 enterprise's systems.

The BIS has stated that IT should be addressed like any other strategic agenda item of the board, and 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. It 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 about:

- The strategy and its integration throughout the enterprise
- How IT investment improves quality of service
- Investment in and proper allocation of IT resources
- Policies and procedures for IT risk management
- Learning from failures and successes

Board members, particularly nonexecutive directors, should ensure they are satisfied that adequate answers can be provided to each of the above issues to:

- Assess the status of IT
- Obtain a clearer understanding of the potential for using IT to improve business objectives
- Promote more integrated business solutions through the application of IT
- Ensure resources are used wisely and effectively on projects and conducted to professional standards

Many boards carry out their governance duties through committees that oversee critical areas such as audit, compensation and acquisitions. Taking the criticality of IT into account, IT should be managed with the same commitment and accuracy. The setup of an IT committee at the board level—an IT strategy committee—can be an important mechanism to achieve this goal. The IT strategy committee, composed of board and non-board members, should assist the board in governing and overseeing the enterprise's IT-related matters. It should ensure that IT governance is addressed in a structured manner and the board has the information it needs to achieve the ultimate objectives of IT governance. More details on the IT strategy committee can be found in appendix F, IT Strategy Committee.

Similarly, executive management increasingly delegates certain responsibilities to committees. The most widely known is the IT steering committee, which usually focuses on tracking IT investments, setting priorities and allocating scarce resources. More recently, enterprises have begun to establish IT architecture and technology committees. The roles and responsibilities of the different committees are covered in appendix E, Roles and Responsibilities for IT Governance.

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 by addressing the level and allocation of investments, balancing the investments between supporting and growing the enterprise and by making considered decisions about where IT resources should be focused
- Ensuring a culture of openness and collaboration among the business, geographical and functional units of the enterprise

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

- Delivering solutions and services with the appropriate quality, on time and on budget
- Enhancing reputation, product leadership and cost-efficiency
- Providing customer trust and competitive time-to-market

The board should manage enterprise risk by:

- Ascertaining that there is transparency about the significant risks to the enterprise
- 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

Boards should support learning and growth and manage resources by:

- Maintaining awareness of new IT developments and opportunities
- Ensuring that IT resources are able to support current and expected business requirements
- Committing to improving the efficiency and effectiveness of the IT infrastructure
- Sustaining an adequate investment in staff education, development and training for IT operations and developments

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

Pragmatic practices in support of the board's governance requirements are listed in appendix B, Board IT Governance Tool Kit.

4.2 How Should Executive Management Address the Expectations?

The executive's focus generally is 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:

- *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. To achieve this, co-responsibility between business and IT for the commercial and technical success of IT investments needs to be promoted. In this context, the CIO needs to be the bridge between IT and the business, and business management needs to be more involved in decision-making around IT.
- *Embed clear accountabilities* for risk management and control over IT into the organisation, based on a clear risk policy and comprehensive control framework
- *Measure performance* by having outcome measures⁴ for business value and competitive advantage that IT delivers and performance drivers to show how well IT performs. Use few but precise performance measures, directly and demonstrably linked to strategy.
- *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 (also supported by an IT steering committee)
- *Create a flexible and adaptive enterprise* that leverages information and knowledge. This is 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 finally 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 model is depicted in appendix H, The Emerging Enterprise Model.

⁴ 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.

- *Strengthen value delivery* through technology standardisation (technology councils and architecture review boards), disciplined project management and clarifying value of IT
- *Focus on the optimisation of IT costs* to obtain the right value from IT resources at a reasonable cost
- *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 parties, often entailing interconnectivity and information sharing that necessitate adopting mutual IT control and governance practices.

Pragmatic practices in support of management's governance requirements are listed in appendix C, Management IT Governance Tool Kit.

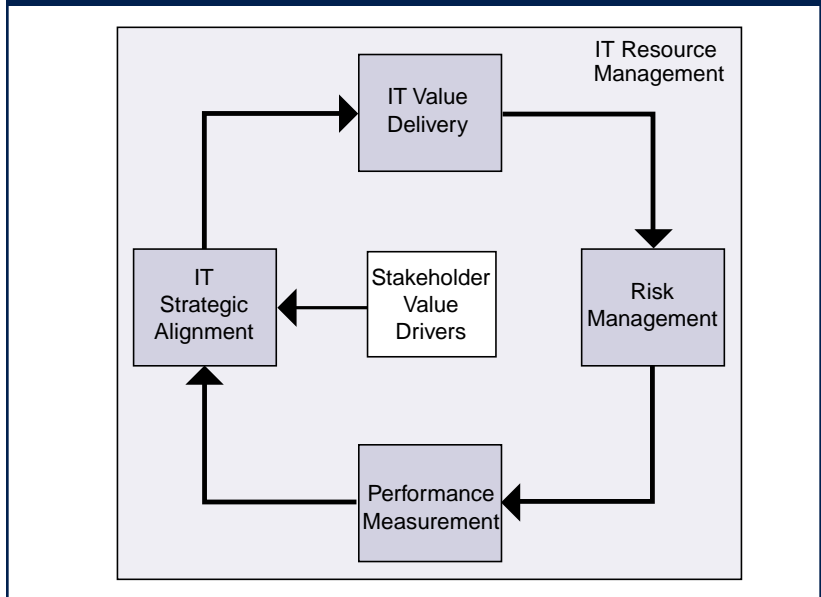
5. What Does IT Governance Cover?

Fundamentally, IT governance is concerned about two things: IT's delivery of value to the business and mitigation of IT risks. The first is driven by strategic alignment⁵ of IT with the business. The second is driven by embedding accountability into the enterprise. Both need to be supported by adequate resources and measured to ensure that the results are obtained.

This leads to the five main focus areas for IT governance, all driven by stakeholder value. Two of them are outcomes: value delivery and risk management. Three of them are drivers: strategic alignment, resource management (which overlays them all) and performance measurement (**figure 3**).

IT governance is also a continuous life cycle, which can be entered at any point. Usually one starts with the strategy and its alignment throughout the enterprise. Then implementation occurs, delivering the value the strategy promised and addressing the risks that need mitigation. At regular intervals (some recommend continuously) the strategy needs to be monitored and the results measured, reported and acted upon. Generally on an annual basis, the strategy is reevaluated and realigned, if needed.

⁵ Value delivery and strategic alignment are often combined in professional and academic literature.

Figure 3—Focus Areas of IT Governance

This life cycle does not take place in a vacuum. Each enterprise operates in an environment that is influenced by:

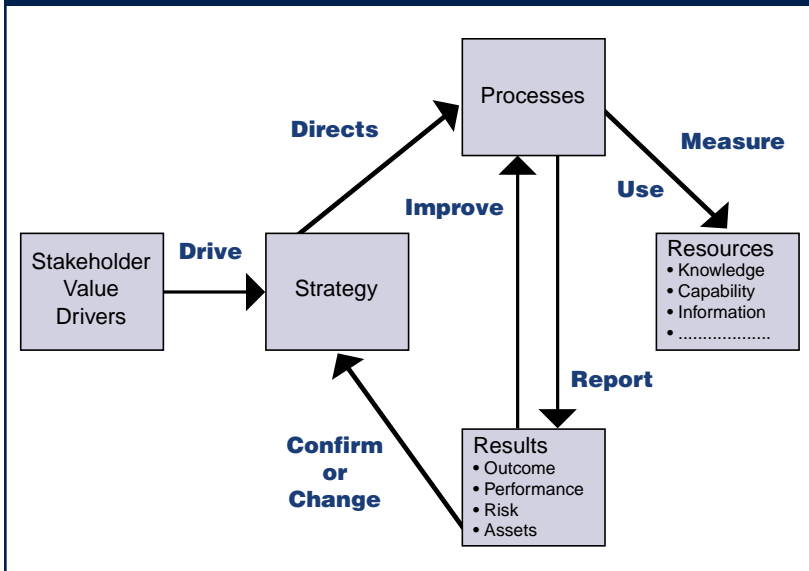
- Stakeholder values
- The mission, vision and values of the enterprise
- The community and company ethics and culture
- Applicable laws, regulations and policies
- Industry practices

IT governance is also a process in which the IT strategy drives the IT processes, which obtain resources necessary to execute their responsibilities. The IT processes report against these responsibilities on process outcome, performance, risks mitigated and accepted, and resources consumed. These reports should either confirm that the strategy is properly executed or provide indications that strategic redirection is required (**figure 4**).

IT governance entails a number of activities for the board and for executive management, such as becoming 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.

Figure 4—IT Governance Process



See the board and management IT governance tool kits in appendices B and C, respectively, for a full listing of IT governance activities and subjects.

Review of the predictions of reputable market analysts such as Gartner, Compass, Giga and CSC reveal that the top issues for IT management have moved from the technology- to the management-related arenas. These issues clearly map onto the IT governance areas:

- **Strategic alignment**, with focus on aligning with the business and collaborative solutions
- **Value delivery**, concentrating on optimising expenses and proving the value of IT
- **Risk management**, addressing the safeguarding of IT assets, disaster recovery and continuity of operations
- **Resource management**, optimising knowledge and IT infrastructure

Furthermore, none of these factors can be managed appropriately without:

- **Performance measurement**, tracking project delivery and monitoring IT services

Each of these focus areas is outlined below. In section 7, a number of practices and critical success factors⁶ are introduced that elaborate further on how these activities are performed and what elements increase their success.

⁶ In this document, critical success factors are conditions, capabilities, competencies and behaviours not always under one's own control to obtain.

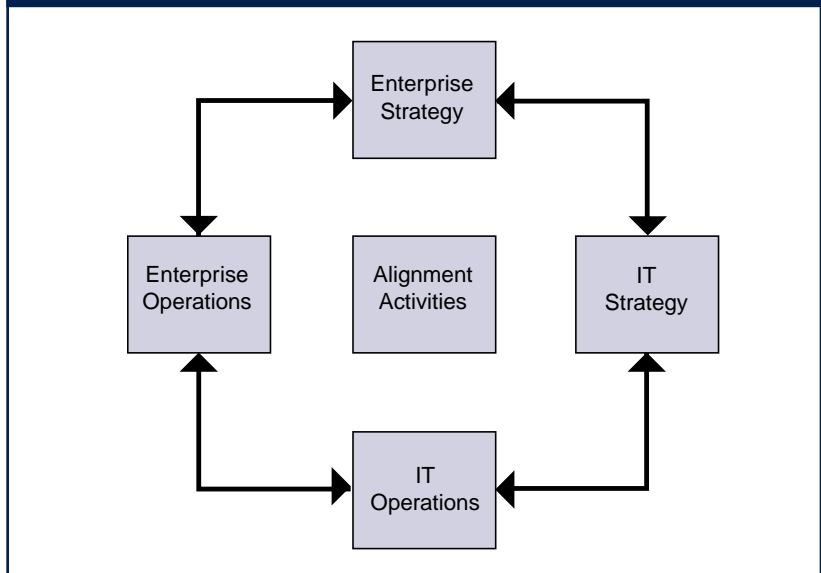
**“IT alignment
is a journey,
not a
destination.”**

5.1 IT Strategic Alignment (focusing on aligning with the business and collaborative solutions)

The key question is whether an enterprise’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 it 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 also is about whether IT operations are aligned with the current enterprise operations (**figure 5**). Of course, it is difficult to achieve IT alignment when enterprise units are misaligned.

Figure 5—IT/Enterprise Alignment



IT often is seen as a “necessary evil,” but considered strategically it can provide enterprises with the opportunity to:

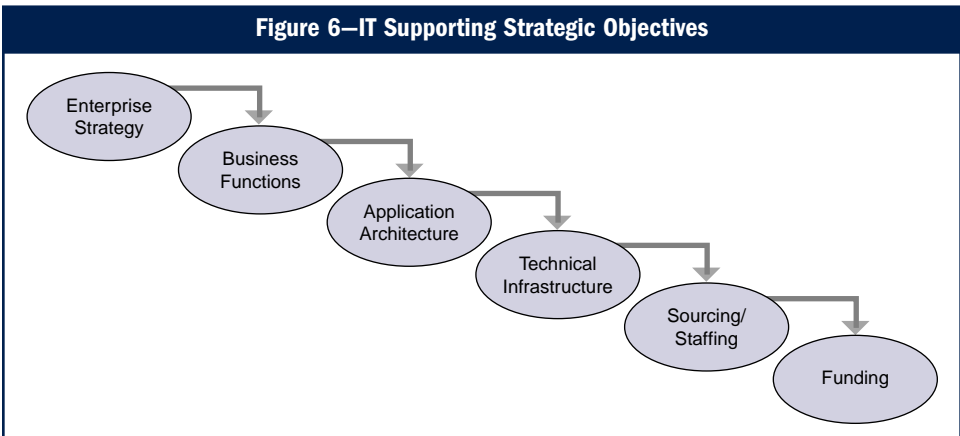
- Add value to products and services
- Assist in competitive positioning
- Contain costs and improve administrative efficiency
- Increase managerial effectiveness

The IT strategy articulates the enterprise's intention to use IT for some or all of these reasons, based on business requirements. Linkage to the business aims is essential for IT to deliver recognisable value to the enterprise.

When formulating the IT strategy, the enterprise must consider:

- Business objectives and the competitive environment
- Current and future technologies and the costs, risks and benefits they can bring to the business
- The capability of the IT organisation and technology to deliver current and future levels of service to the business, and the extent of change and investment this might imply for the whole enterprise
- Cost of current IT and whether this provides sufficient value to the business
- The lessons learned from past failures and successes

Once these issues are clearly understood, the IT strategy can be developed to ensure all elements of the IT environment support the strategic objectives, as demonstrated in **figure 6**.



It is important that the plan for implementing the strategy be endorsed by all relevant parties. It is also important that the implementation plans be broken down into manageable parts, each with a clear business case incorporating a plan for achieving outcomes and realising benefits. The board should ensure that the strategy is reviewed regularly in the light of technological and operational change.

Hence the board, or a dedicated IT strategy committee of the board, should drive business alignment by:

- Ensuring that IT strategy is *aligned* with business strategy and that distributed IT strategies are consistent and integrated

- Ensuring that IT *delivers* against the strategy (delivering on time and within budget, with appropriate functionality and the intended benefits—a fundamental building block of alignment and value delivery) through clear expectations and measurement (e.g., balanced business scorecard)
- Balancing 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, that is, their use to break into new markets, drive competitive strategies, increase overall revenue generation, improve customer satisfaction and/or assure customer retention

Alignment requires planned and purposeful management processes, such as:

- Creating and sustaining awareness of the strategic role of IT at 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

As IT becomes more critical for enterprise survival in addition to enabling growth, IT strategy committees need to broaden their scope. Not only should they offer advice on strategy when assisting the board in its IT governance responsibilities, but also they should focus on IT value, risks and performance. In appendix F, the roles and responsibilities of this committee are further elaborated.

5.2 Value Delivery (*concentrating on optimising expenses and proving the value of IT*)

The basic principles of IT value are the on-time and within-budget delivery of appropriate quality, which achieves the benefits that were promised. In business terms, this is often translated into: competitive advantage, elapsed time for order/service fulfilment, 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 understand. Often, top management and boards fear to start major IT investments because of the size of investment and the uncertainty of the outcome. For effective IT value delivery to be achieved, both the actual costs and the return on investment need to be managed.

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

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 should set 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

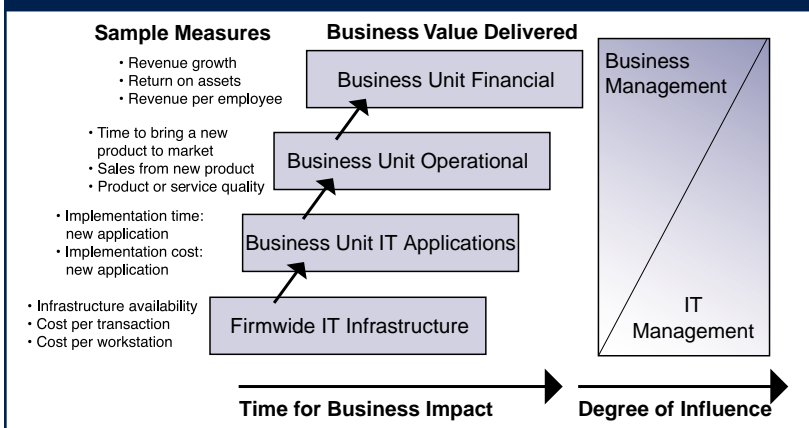
The business should also set expectations regarding the method of working:

- 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 perceive the value of IT differently, as illustrated in **figure 7**.⁷ Figure 7 also shows that the higher one goes in the measurement hierarchy, the more dilution occurs (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. However, successful investments in IT have a positive impact on all four levels of the business value hierarchy. Furthermore, there is an increasing separation between the creation of value and its subsequent realisation. Therefore, it is important not only to focus on measurements based on value realisation (i.e., financial measures), but also to take into account the enterprise's performance in creating value.

Figure 7—Views of IT Value (Weill and Broadbent)



⁷ Weill, Peter; Marianne Broadbent; *Leveraging the New Infrastructure: How Market Leaders Capitalize on Information Technology*, Harvard Business School Press, 1998

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 achievement of the intended benefits. Alignment of IT also provides value 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.

The capacity to deliver is dependent on:

- Timely, usable and reliable information about customers, processes, markets, etc.
- 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. This means that it is important to establish the value measures in concert between the business and IT. This implies, as is recommended below, that the IT balanced scorecard should cover these measures and be developed with input and approval from business management. It should also be mentioned that the public sector has different value drivers/indicators than the private sector. In the public sector, measures like compliance and due diligence take prominence over financial measures such as profitability.

5.3 Risk Management (*addressing the safeguarding of IT assets and disaster recovery*)

The universal need to demonstrate good enterprise governance to shareholders and customers is the driver 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.

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

Therefore, the board should manage enterprise risk by:

- Ascertaining that there is *transparency* about the significant risks to the enterprise and clarifying the risk-taking or risk-avoidance policies of the enterprise (i.e., determining the enterprise’s appetite for risk)
- 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 be *embedded in the operation* of the enterprise, respond quickly to changing risks and report immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how)

Effective risk management begins with a clear understanding of the enterprise’s appetite for risk and a brainstorming session on the high-level risk exposures of the enterprise. This focuses all risk management effort and, in an IT context, impacts future investments in technology, the extent to which IT assets are protected and the level of assurance required.

Having defined risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Dependent on the type of risk and its significance to the business, management and the board may choose to:

- Mitigate—Implement controls (e.g., acquire and deploy security technology to protect the IT infrastructure)
- Transfer—Share risk with partners or transfer to insurance coverage
- Accept—Formally acknowledge that the risk exists and monitor it

As a minimum, risk should at least be analysed, because even if no immediate action is taken, the awareness of risk will influence strategic decisions for the better. Often, the most damaging IT risks are those that are not well understood.

“I cannot imagine any condition which could cause this ship to founder. I cannot conceive of any vital disaster happening to this vessel.”—Captain of the Titanic, 1912

“A good craftsman is recognised by the quality of his tools.”

5.4 Resource Management *(optimising knowledge and infrastructure)*

A key to successful IT performance is the optimal investment, use and allocation of IT resources (people, applications, technology, facilities, data) in servicing the needs of the enterprise. Most enterprises fail to maximise the efficiency of their IT assets and optimise the costs relating to these assets. In addition, the biggest challenge in recent years has been to know where and how to outsource and then to know how to manage the outsourced services in a way that delivers the values promised at an acceptable price.

Boards need to address appropriate investments in infrastructure and capabilities by ensuring that:

- The responsibilities with respect to IT systems and services procurement are understood and applied
- Appropriate methods and adequate skills exist to manage and support IT projects and systems
- Improved workforce planning and investment exist to ensure recruitment and, more important, retention of skilled IT staff
- IT education, training and development needs are fully identified and addressed for all staff
- Appropriate facilities are provided and time is available for staff to develop the skills they need

Boards need to ensure that IT resources are used wisely by ensuring that:

- Appropriate methods and adequate skills exist in the organisation to manage IT projects
- The benefits accruing from any service procurement are real and achievable

In most enterprises, the biggest portion of the IT budget relates to ongoing operations. Effective governance of IT operational spending requires effective control of the cost base: the IT assets and their focus where they are needed most. Enterprises should align and prioritise the existing IT services that are required to support business operations based on clear service definitions. These definitions and related performance metrics enable business-oriented service level agreements providing a basis for effective oversight and monitoring of both internal and outsourced IT services. The IT assets should be organised optimally so that the required quality of service is provided by the most cost-effective delivery infrastructure. Companies that achieve this not only realise great cost savings but also are well placed to take on the next new IT initiative, judiciously introducing new technologies and replacing or updating obsolete systems.

IT assets are complex to manage and continually change due to the nature of technology and changing business requirements. Effective management of the life cycle of hardware, software licences, service contracts and

permanent and contracted human resources is a critical success factor not only for optimising the IT cost base, but also for managing changes, minimising service incidents and assuring a reliable quality of service.

Of all the IT assets, human resources represent the biggest part of the cost base and, on a unit basis, the one most likely to increase. It is essential to identify and anticipate the required core competencies in the workforce. When these are understood, an effective recruitment, retention and training programme is necessary to ensure that the organisation has the skills to utilise IT effectively to achieve the stated objectives.

The ability to balance the cost of infrastructure assets with the quality of service required (including those services provided by outsourced external service providers) is critical to successful value delivery. It is also a powerful reason for adopting sound performance measurement systems like the balanced scorecard.

5.5 Performance Measurement (*tracking project delivery and monitoring IT services*)

Strategy has taken on a new urgency as enterprises mobilise intangible and hidden assets to compete in an information-based global economy. The means of value creation has shifted from tangible to intangible assets, and intangible assets generally are not measurable through traditional financial means. 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*.

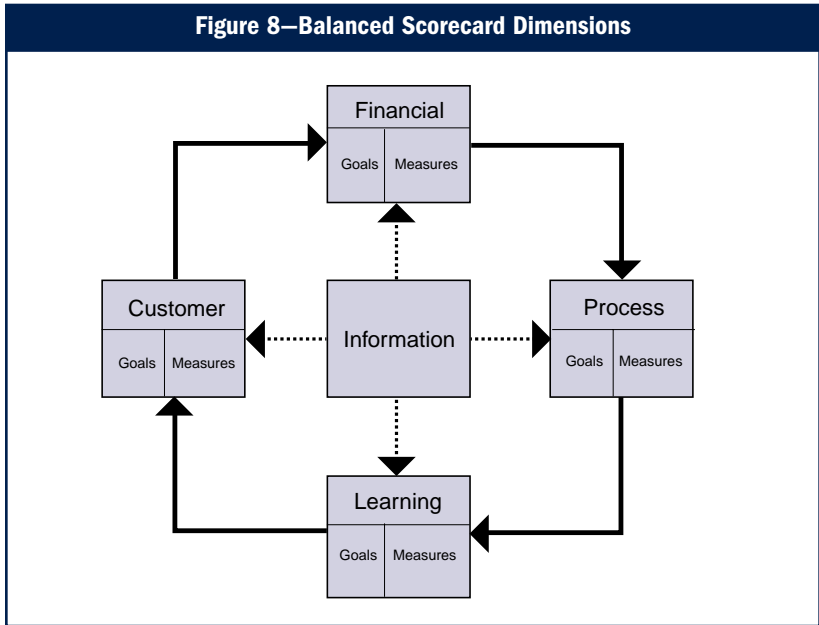
Each perspective is designed to answer one question about the enterprise's way of doing business:

- Financial perspective—To satisfy our stakeholders, what financial objectives must we accomplish?
- Customer perspective—To achieve our financial objectives, what customer needs must we serve?
- Internal process perspective—To satisfy our customers and stakeholders, in which internal business processes must we excel?
- Learning perspective—To achieve our goals, how must our organisation learn and innovate?

By using the balanced scorecard, managers rely on more than short-term financial measures as indicators of the company's performance. They also take into account such intangible items as level of customer satisfaction, streamlining of internal functions, creation of operational efficiencies and development of staff skills. This unique and more holistic view of business operations contributes to linking long-term strategic objectives with short-term actions.

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

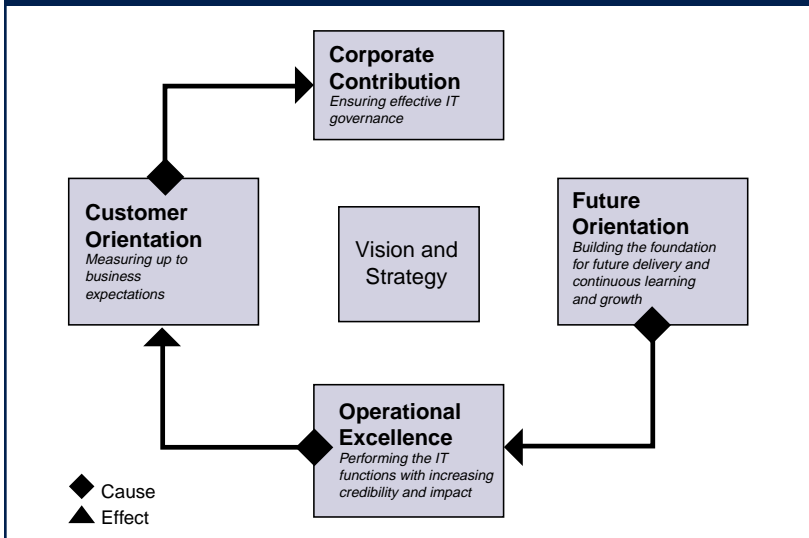
At the heart of these scorecards is management information supplied by relevant stakeholders and supported by a sustainable reporting system (figure 8).



But IT does more than provide information to obtain a global picture as to where the enterprise 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 management), 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.

Use of an IT balanced scorecard (IT BSC) is one of the most effective means to aid the board and management to achieve IT and business alignment. The objectives are to establish a vehicle for management reporting to the board, to foster consensus among key stakeholders about IT's strategic aims, to demonstrate the effectiveness and added value of IT and to communicate about IT's performance, risks and capabilities.

Figure 9—Cause and Effect Relationships Between Scorecard Dimensions

To apply the balanced scorecard concepts to the IT function, the four perspectives need to be redefined. An IT BSC template can be developed by considering the following questions:

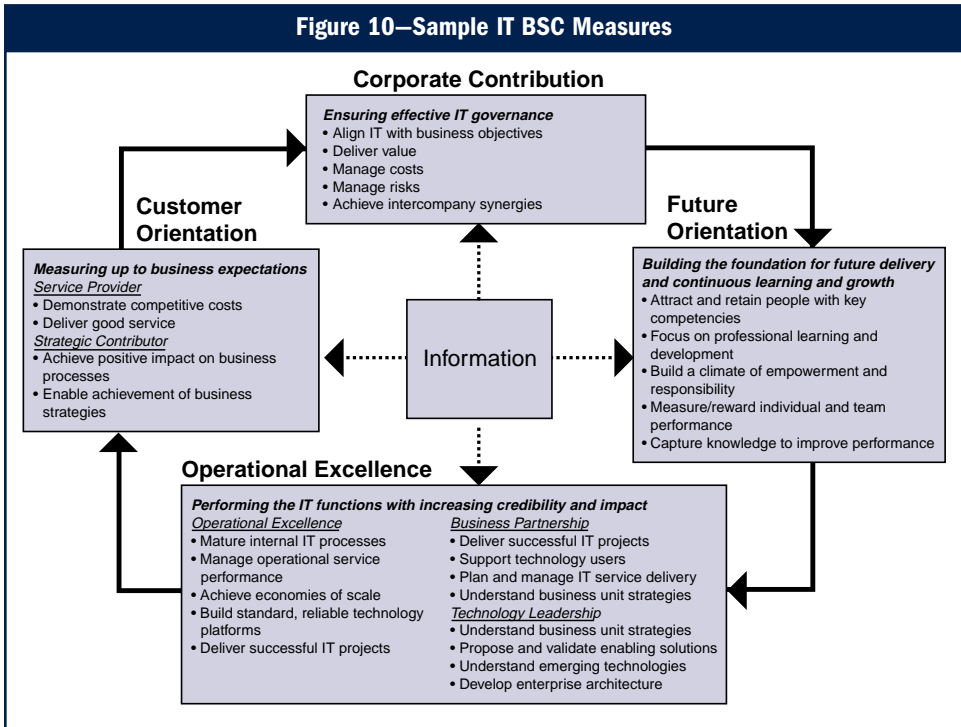
- Enterprise contribution—How do business executives view the IT department?
- User orientation—How do users view the IT department?
- Operational excellence—How effective and efficient are the IT processes?
- Future orientation—How well is IT positioned to meet future needs?

To demonstrate the value IT delivers to the business requires cause-and-effect relationships between two types of measures throughout the scorecard (see **figure 9**):⁸ outcomes measures (measuring what you have done) and performance drivers (measuring how you are doing). A well-developed IT BSC contains a good mix of these two types of measures, and should link to the higher-level business scorecards.

⁸ Van Grembergen, W.; Ronald Saull; Steven De Haes; "Linking the IT Balanced Scorecard to the Business Objectives at a Major Canadian Financial Group," *Strategies for Information Technology Governance*, ed. Van Grembergen, 2003

Figure 10 summarises the objectives of each specific area from which measures can be derived, and section 7 provides some example measures for management and those responsible for IT governance.

Figure 10—Sample IT BSC Measures



6. What Questions Should Be Asked?

Asking tough questions is an effective way to get started in implementing IT governance. 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, not just the action, but also *who* is responsible to deliver *what* by *when*. Here are some sample questions. A more extensive checklist is provided in appendix A, IT Governance Checklist. The questions focus on three objectives.

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?

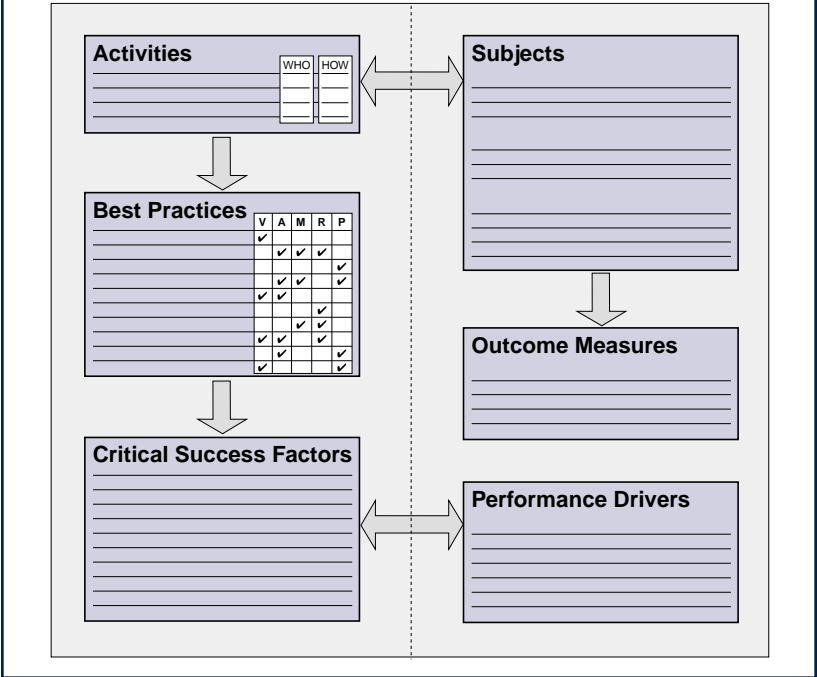
7. How Is It Accomplished?

Tool kits for supporting the implementation of effective IT governance, from both a board and an executive management point of view, are provided in appendices B and C, respectively. These consist of various elements (**figure 11**):

- *Activities* comprise actions that should be carried out to exercise the IT governance responsibilities and the *subjects* comprise those items that typically get onto an IT governance agenda (objectives, opportunities, risks, key processes and core competencies).
- *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* comprise examples of how the activities are being performed by those who have established leadership in governance of technology. These practices have been classified to reflect the IT governance area(s) to which they provide the greatest contribution: value delivery, strategic alignment, resource management, risk management and/or performance (V, A, M, R, P). 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, mitigated and residual risk 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 best 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

Figure 11—IT Governance Action Plan



8. How Does Your Organisation Compare?

For effective IT governance to be implemented, enterprises 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 all the processes that need to be managed within IT.

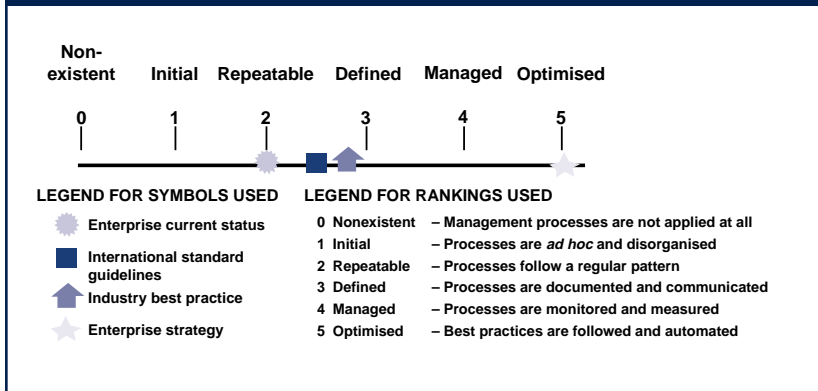
The use of maturity models greatly simplifies this task and provides a pragmatic and structured approach for measuring how well developed an enterprise's processes are against a consistent and easy-to-understand scale.

Maturity models provide maturity scales (**figure 12**) and a description of the observable characteristics of each level.

Using this technique the enterprise 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

Figure 12—Maturity Scales



A maturity model showing descriptions of the different levels of maturity for IT governance is provided in appendix D, IT Governance Maturity Model.

9. What Reference Material Exists?

Various regulatory bodies, such as the Treadway Commission, BIS and OECD, 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.

In addition, advisory initiatives and emerging international standards, such as Cadbury, Turnbull and COBIT, have produced guidance on responsibilities of boards and executives relative to risk and control.

COBIT (*Control Objectives for Information and related Technology*), issued by the IT Governance Institute, is increasingly accepted internationally as good practice for control over information, IT and related risks. Its guidance enables an enterprise to implement effective governance over the IT that is pervasive and intrinsic throughout the enterprise. In particular, COBIT's *Management Guidelines* component contains a framework responding to management's need for control and measurability of IT by providing tools to assess and measure the enterprise's IT capability for the 34 COBIT IT processes. The tools include:

- Performance measurement elements (outcome measures and performance drivers for all IT processes)
- A list of critical success factors that provides succinct, nontechnical best practices for each IT process
- Maturity models to assist in benchmarking and decision-making for capability improvements

IT governance incorporates the principles proposed in these influential documents, summary of which can be found in appendix G, Regulatory Reports and Emerging Standards on Governance.

10. Conclusions

10.1 IT Governance Should Be Integrated within Enterprise Governance

An IT governance framework helps boards and management understand the issues and strategic importance of IT, and assists in ensuring that the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. It provides assurance that expectations for IT are met and IT risks are addressed.

IT governance fits in the broader governance arrangements that cover relationships between the entity's management and its governing body, its owners and its other stakeholders. It provides the structure through which the entity's overall objectives are set, the method of attaining those objectives is outlined and the manner in which performance will be monitored is described.

In summary, IT governance ensures that IT goals are met and IT risks are mitigated such that IT delivers value to sustain and grow the enterprise. IT governance drives strategic alignment between IT and the business and must judiciously measure performance.

IT is an integral part of the business. IT governance is an integral part of enterprise governance.

10.2 IT Governance Roles and Responsibilities Need to be Defined

This document extensively points out the responsibilities of the board, executive and IT strategy committee. Appendix F (IT Strategy Committee), which further documents the workings of the IT strategy committee, also covers the IT steering committee, which operates at executive level and usually focuses on priority setting, resource allocation and project tracking. A more complete picture of the roles of the business and IT executives, and for the two other committees that typically support the CEO and the CIO in setting and controlling technology (technology council) and architecture standards (architecture review board), is provided in appendix E, Roles and Responsibilities for IT Governance.

These two committees drive the standardisation, reuse and optimisation of IT resources. Together with the IT strategy and IT steering committees, they complete the emerging best practice of a three-tier IT governance structure: strategy, steering and standards.

Appendix E provides an overview of roles and responsibilities for board of directors, IT strategy committee, CEO, business executives, CIO, IT steering committee, technology council and architecture review board, defined for each of the five IT governance domains:

- Strategic alignment
- Value delivery
- Risk management
- Resource management
- Performance measurement

These suggested roles and responsibilities are useful when implementing IT governance in the enterprise.

10.3 An IT Governance Implementation Plan Is Required

To get its IT governance initiatives headed in the right direction, the enterprise needs an effective action plan that suits its particular circumstances and needs.

First, it is important for the board to take ownership of IT governance and set the direction management should follow. This is best done by making sure that the board operates with IT governance in mind:

- Making sure IT is on the board agenda
- Challenging management's activities with regard to IT, to make sure IT issues are uncovered
- Guiding management by helping it to align IT initiatives with real business needs, and ensuring that it appreciates the potential impact on the business of IT-related risks
- Insisting that IT performance be measured and reported to the board
- Establishing an IT strategy committee with responsibility for communicating IT issues between the board and management
- Insisting that there be a management framework for IT governance based on a common approach (e.g., COBIT)

With this mandate and direction in place, management then can initiate and put into action an IT governance approach. To help management decide where to begin and to ensure that the IT governance process delivers positive results where they are needed most, the following steps are suggested:

1. **Set up a governance organisational framework** that will take IT governance forward and own it as an initiative, with clear responsibilities and objectives and participation from all interested parties.

2. **Align IT strategy with business goals.** What are the current business concerns and issues where IT has a significant influence, e.g., cost reduction, competitive advantage and/or merger/acquisition? Obtain a good understanding of the business environment, risk appetite and business strategy as they relate to IT. Identify the top IT issues on management's agenda.
3. **Understand/define the risks.** Given top management's business concerns, what are the risk indicators relating to IT's ability to deliver against these concerns? Consider:
 - Previous history and patterns of performance
 - Current IT organisational factors
 - Complexity and size/scope of the existing or planned IT environment
 - Inherent vulnerability of the current and planned IT environment
 - Nature of the IT initiatives being considered, e.g., new systems projects, outsourcing considerations, architectural changes
4. **Define target areas.** Identify the process areas in IT that are critical to managing these risk areas. Use the COBIT process framework as a guide.
5. **Analyse current capability and identify gaps.** Perform a maturity capability assessment to find out where improvements are needed most. Use COBIT's management guidelines as a guide.
6. **Develop improvement strategies.** Decide which are the highest priority projects that will help improve the management and governance of these significant areas. This decision should be based on most potential benefit and ease of implementation, and a focus on important IT processes and core competencies. Define specific IT governance projects as the first step in the IT governance continuous improvement initiative.
7. **Measure results.** Establish a balanced scorecard mechanism for measuring current performance. Monitor the results of new improvements considering, as a minimum, the following key considerations:
 - Will the organisational structures support strategy implementation?
 - Are responsibilities for risk management embedded in the organisation?
 - Do infrastructures exist that will facilitate and support the creation and sharing of vital business information?
 - Have strategies and goals been communicated effectively to everyone who needs to know within the organisation?
8. **Repeat steps 2-7 on a regular basis.**

There are also some obvious but pragmatic rules that management ought to follow:

- Treat the IT governance initiative as a project activity with a series of phases rather than a “one-off” step.
- Remember that IT governance involves cultural change as well as new processes, and therefore a key success factor is the enablement and motivation of these changes.
- Make sure there is a clear understanding of the objectives.
- Manage expectations. In most enterprises, achieving successful oversight of IT will take some time and is a continuous improvement process.
- Focus first on where it is easiest to make changes and deliver improvements. Build from there one step at a time.

A more complete description of the IT governance implementation road map can be found in *IT Governance Implementation Guide* (IT Governance Institute, 2003).

APPENDICES

Appendix A—IT Governance Checklist

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

<i>Questions to Ask to Uncover IT Issues</i>	V	A	M	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? How successfully are skilled IT resources attracted to the organisation?		✓	✓	✓	
What is the percentage of revenue (revenue can be replaced by budget for the public sector) spent on IT compared to the industry average?					
How has it evolved over the years?	✓				✓
What is the amount spent on IT compared to the enterprise's entire profit (profit can be replaced by budget for the public sector)?	✓				✓
Does IT support the enterprise in complying with regulations and service levels?		✓			✓
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	M	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 stakeholder 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?		✓	✓		

<i>Questions to Ask to Find Out How Management Addresses the IT Issues, continued</i>	<i>V</i>	<i>A</i>	<i>M</i>	<i>R</i>	<i>P</i>
Are enterprise and IT objectives linked and synchronised?		✓			
Is the enterprise clear on its position relative to risks: risk-avoiding or risk-taking?				✓	
Is there an up-to-date inventory of 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 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?		✓	✓	✓	
What are other similar organisations doing, and how is the enterprise placed in relation to them, relative to value, risk and resource management?					✓
What is industry best practice and how does the enterprise compare, relative to value, risk and resource management?					✓

<i>Questions to Ask to Self-Assess IT Governance Practices</i>	<i>V</i>	<i>A</i>	<i>M</i>	<i>R</i>	<i>P</i>
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 other like organisations?	✓		✓		✓
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 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 IT Governance Tool Kit

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

Best Practices	V	A	M	R	P
Asking the right questions (nonexecutive board members do not need to know the answers, they need to know the questions)	✓	✓	✓	✓	✓
Understanding the answers to their questions to ask appropriate follow-ups and understand the implications for the enterprise	✓	✓	✓	✓	✓
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; 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	✓	✓		✓	✓
Defining the scope and charter of the 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	✓		✓	✓	
Ensuring major IT development projects are aligned with the business strategy and have an approved business case which clearly demonstrate value and how it will be measured	✓	✓			✓
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		✓			✓
Ascertaining that risk analysis is part of management's strategic planning process and considers the vulnerabilities of the IT infrastructure and the exposure of intangible assets				✓	
Getting involved in defining useful strategic IT metrics and IT performance measures	✓	✓			✓

V = IT Value Delivery; A = IT Strategic Alignment; M = IT Resource Management; 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
Definition of IT governance activities with a clear purpose, and their documentation and implementation, based on enterprise needs; no ambiguous 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, which 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 IS strategic alignment, value delivery, risk management, resource management and service performance

IT Governance Subjects*The objectives of IT—how it:*

- Improves cost-efficiencies
- Creates revenue enhancement
- Supports the building of new capabilities
- Enables core business processes (typically, those that differentiate and add value to products and services in the marketplace and over time)
- Enables new business models

The opportunities and risks of new technology:

- Internet and intranet
- E-commerce
- Mobile computing
- Workflow technology
- Knowledge systems, etc.

The key processes and core competencies:

- 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

Outreach to new and satisfaction of existing customers

Adherence to 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

Increased satisfaction of stakeholders (survey and number of complaints)

Business cases that demonstrate a high potential return on investment

Performance Drivers

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

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 IT Governance Tool Kit

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

Best Practices	V	A	M	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 CIO 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	✓			✓	✓
Establishing an IT balanced scorecard (including its approval by key stakeholders) to measure 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 uptime, 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			✓		
Having a general manager (CEO) who mediates/reconciles 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			✓	✓	
Using extensive automated monitoring practices, leveraging IT to measure its own performance; tracking performance measures, effectiveness of internal control systems and status of improvement activities	✓			✓	✓
Embedding 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	✓			✓	✓
Cascading business and IT goals down into the organisation and translating them into actions for the people at each level in their terms of responsibility, all the way down to the individual		✓			✓
Taking co-responsibility of business and IT for success and return of business value of IT endeavors	✓	✓			✓
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; M = IT Resource Management; 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 successful 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*The objectives of IT—how it:*

- 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

The opportunities and risks of new technology:

- Internet and intranet
- E-commerce
- Mobile computing
- Workflow technology
- Knowledge systems, etc.

The key processes and core competencies:

- 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

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

Increased satisfaction of IT users and stakeholders

Improved productivity (e.g., delivery of value per employee, number of customers and cost per customer served)

Number of noncompliance reports

Cost-efficiency of processes and operations

Performance Drivers

System downtime

Throughput and response times

Amount of errors and rework

Availability of appropriate bandwidth, computing power and IT delivery mechanisms

Number of staff trained in new technology and customer service skills

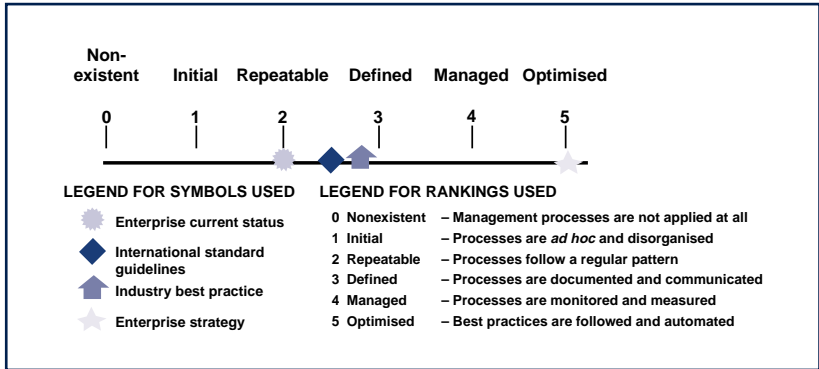
Benchmark comparisons

Reduction in development and processing time

Increased number of IT action plans for process improvement initiatives

Improved performance measurement process by use of IT balanced scorecards

Appendix D—IT Governance Maturity Model



0 Nonexistent

There is no senior management oversight of IT-related activities to ensure that the enterprise's IT goals add value to the organisation and to ensure that IT-related risks are appropriately managed.

1 Initial/*Ad Hoc*

The concept of IT governance does not exist formally and oversight is based mostly on management's consideration of IT-related issues on a case-by-case basis. The governance of IT depends on the initiative and experience of the IT management team, with limited input from the rest of the organisation. Upper management is involved only when there are major problems or successes. The measurement of IT performance is typically limited to technical measures and only within the IT function.

2 Repeatable but Intuitive

There is a realisation that more formalised oversight of IT is required and it needs to be a shared management responsibility requiring the support of top management. Regular governance practices such as review meetings, creation of performance reports, and investigation into problems take place, but rely mostly on the initiative of the IT management team, with voluntary or co-opted participation by key business stakeholders, depending on current IT projects and priorities. Problems identified are tackled on a project basis with teams formed as necessary to undertake improvements.

3 Defined Process

An organisational and process framework has been defined for oversight and management of IT activities and is being introduced to the organisation as the basis for IT governance. The board has issued guidance, which has been

developed into specific procedures for management covering key governance activities. These include regular target-setting, reviews of performance, assessments of capability against planned needs, and project planning and funding for any necessary IT improvements. Previous informal but successful practices have been institutionalised and the techniques followed are relatively simple and unsophisticated.

4 Managed and Measurable

Target-setting has developed to a fairly sophisticated stage with relationships between outcome goals in business terms, and IT process improvement measures now well understood. Real results have been communicated to management in the form of a balanced scorecard. The enterprise's management team is now working together for the common goal of maximising IT value delivery and managing IT-related risks. There have been regular assessments of IT capabilities and projects have been completed that have delivered real improvements to IT's performance. Relationships among the IT function, its users in the business community and external service providers are now based on service definitions and service agreements.

5 Optimised

The IT governance practices have developed into a sophisticated approach using effective and efficient techniques. There is true transparency of IT activities, and the board feels in control of the IT strategy. IT activities have been optimally directed toward real business priorities, and the value being delivered to the enterprise can be measured and steps taken on a timely basis to correct significant deviations or problems. The balanced scorecard approach has evolved into one that is focused on the most important measures relevant to the enterprise's overall business strategy. The effort spent on risk management (and on IT management activities generally) has been streamlined through adoption of standardised and, where possible, automated processes. The practice of continuous improvement of IT capability is embedded in the culture and this includes regular external benchmarking and independent audits providing positive assurance to management. Overall, the cost of IT is monitored effectively and the organisation is able to achieve optimal IT spending through continuous internal improvements, the effective outsourcing of selected services and effective negotiation with vendors. When dealing with external business partners or service providers, the organisation is able to demonstrate first-class performance and demand best practices from others.

Appendix E—Roles and Responsibilities for IT Governance

1. Board of directors

	Strategic Alignment	Value Delivery	IT Resource Management	Risk Management	Performance Management
Board of Directors	<ul style="list-style-type: none"> Ensure management has put in place an effective strategic planning process Ratify the aligned business and IT strategy Ensure the IT organisational structure complements the business model and direction 	<ul style="list-style-type: none"> Ascertain that management has put processes and practices in place that ensure IT delivers provable value to the business Ensure IT investments represent a balance of risk and benefit and that budgets are acceptable 	<ul style="list-style-type: none"> Monitor how management determines what IT resources are needed to achieve strategic goals Ensure a proper balance of IT investments for sustaining and growing the enterprise 	<ul style="list-style-type: none"> Be aware about IT risk exposures and their containment Evaluate the effectiveness of management's monitoring of IT risks 	<ul style="list-style-type: none"> Assess senior management's performance on IT strategies in operation Work with the executive to define and monitor high-level IT performance
IT Strategy Committee	<ul style="list-style-type: none"> Provide strategy direction and the alignment of IT and the business Issue high-level policy guidance (e.g., risk, funding, sourcing, partnering) Verify strategy compliance (e.g., achievement of strategic goals and objectives) 	<ul style="list-style-type: none"> Confirm that the IT/business architecture is designed to drive maximum business value from IT Oversee the delivery of value by IT to the enterprise Take into account return and competitive aspects of IT investments 	<ul style="list-style-type: none"> Provide high-level direction for sourcing and use of IT resources, e.g., strategic alliances Oversee the aggregate funding of IT at the enterprise level 	<ul style="list-style-type: none"> Ascertain that management has resources in place to ensure proper management of IT risks Take into account risk aspects of IT investments Confirm that critical risks have been managed 	<ul style="list-style-type: none"> Verify strategy compliance, i.e., achievement of strategic IT objectives Review the measurement of IT performance and the contribution of IT to the business (i.e., delivering the promised business value)

2. Executive management

	Strategic Alignment	Value Delivery	IT Resource Management	Risk Management	Performance Management
CEO	<ul style="list-style-type: none">Align and integrate IT strategy with business goalsAlign IT operations with business operationsCascade strategy and goals down into the organisationMediate between imperatives of the business and of the technology	<ul style="list-style-type: none">Direct the optimisation of IT costsEstablish co-responsibility between the business and IT for IT investmentsEnsure the IT budget and investment plan is realistic and integrate into the overall financial planEnsure that financial reporting has accurate accounting of IT	<ul style="list-style-type: none">Ensure the organisation is in the best position to capitalise on its information and knowledgeEstablish business priorities and allocate resources to enable effective IT performanceSet up organisational structures and responsibilities that facilitate IT strategy implementationDefine and support the CIO's role, ensuring the CIO is a key business player and part of executive decision-making	<ul style="list-style-type: none">Adopt a risk, control and governance frameworkEmbed responsibilities for risk management in the organisationMonitor IT risk and accept residual IT risks	<ul style="list-style-type: none">Obtain assurance of the performance, control and risks of IT and independent comfort about major IT decisionsWork with the CIO on developing an IT balanced scorecard ensuring it is properly linked to business goals
Business Executives	<ul style="list-style-type: none">Understand the enterprise's IT organisation, infrastructure and capabilitiesDrive the definition of business requirements and own themAct as sponsor for major IT projects	<ul style="list-style-type: none">Approve and control service levelsAct as customer for available IT servicesIdentify and acquire new IT servicesAssess and publish operational benefits of owned IT investments	<ul style="list-style-type: none">Allocate business resources required to ensure effective IT governance over projects and operations	<ul style="list-style-type: none">Provide business impact assessments to the enterprise risk management process	<ul style="list-style-type: none">Sign off on the IT balanced scorecardMonitor service levelsProvide priorities for addressing IT performance problems and corrective actions
CIO	<ul style="list-style-type: none">Drive IT strategy development and execute against it, ensuring measurable value is delivered on time and budget, currently and in the futureImplement IT standards and policiesEducate executives on dependence on IT, IT-related costs, technology issues and insights, and IT capabilities	<ul style="list-style-type: none">Clarify and demonstrate the value of ITProactively seek ways to increase IT value contributionLink IT budgets to strategic aims and objectivesManage business and executive expectations relative to ITEstablish strong IT project management disciplines	<ul style="list-style-type: none">Provide IT infrastructures that facilitate creation and sharing of business information at optimal costEnsure the availability of suitable IT resources, skills and infrastructure to meet the strategic objectivesEnsure that roles critical for driving maximum value from IT are appropriately defined and staffedStandardise architectures and technology	<ul style="list-style-type: none">Assess risks, mitigate efficiently and make risks transparent to the stakeholdersImplement an IT control frameworkEnsure that roles critical for managing IT risks are appropriately defined and staffed	<ul style="list-style-type: none">Ensure the day-to-day management and verification of IT processes and controlsImplement an IT balanced scorecard with few but precise performance measures directly and demonstrably linked to the strategy

3. Committees supporting the executives and the CIO, usually coordinated by the CIO project office,⁹ chief architect, chief technology officer, etc.

	Strategic Alignment	Value Delivery	IT Resource Management	Risk Management	Performance Management
IT Steering Committee	<ul style="list-style-type: none">• Define project priorities• Assess strategic fit of proposals• Perform portfolio reviews for continuing strategic relevance	<ul style="list-style-type: none">• Review, approve and fund initiatives, assessing how they improve business processes• Ensure identification of all costs and fulfillment of cost/benefit analysis• Perform portfolio reviews for cost optimisation	<ul style="list-style-type: none">• Balance investments between supporting and growing the enterprise	<ul style="list-style-type: none">• Ensure all projects have a project risk management component• Act as sponsor of the control, risk and governance framework• Make key IT governance decisions	<ul style="list-style-type: none">• Define project success measures• Follow progress on major IT projects• Monitor and direct key IT governance processes
Technology Council	<ul style="list-style-type: none">• Provide technology guidelines• Monitor relevance of latest developments in IT from a business perspective	<ul style="list-style-type: none">• Consult/advise on the selection of technology within standards• Assist in variance review	<ul style="list-style-type: none">• Advise on infrastructure products• Direct technology standards and practices	<ul style="list-style-type: none">• Ensure vulnerability assessments of new technology occur	<ul style="list-style-type: none">• Verify compliance with technology standards and guidelines
IT Architecture Review Board	<ul style="list-style-type: none">• Provide architecture guidelines	<ul style="list-style-type: none">• Consult/advise on the application of architecture guidelines	<ul style="list-style-type: none">• Direct IT architecture design	<ul style="list-style-type: none">• Ensure that the IT architecture reflects the need for legislative and regulatory compliance, the ethical use of information and business continuity	<ul style="list-style-type: none">• Verify compliance with architecture guidelines

⁹ The project office (PO) is a staff function supporting the CIO, developed in response to complex project management requirements in larger organisations. The PO manages the project portfolio and the project managers, sets and enforces project management standards, manages priority and resource conflicts, reviews project deliverables and reports on consolidated project results.

Appendix F—IT Strategy Committee

Many boards carry out their governance duties through committees that oversee critical areas such as audit, compensation and acquisitions. Boards also need to assess the criticality of IT in the enterprise for which they are responsible. One of the most effective mechanisms for establishing governance over IT is the IT strategy committee. This committee is charged with considering how the board should become involved in IT governance, how to integrate the board's role in IT and business strategy, and the extent to which the committee has an ongoing role in IT governance.

However, boards and executive management may be reluctant to deploy an IT strategy committee for a variety of reasons:

- Top management is not as well versed in technical issues as it is in other aspects of the business.
- IT is seen only as an expense and there is insufficient awareness of the actual importance/criticality of IT.
- Budget and/or time restrictions exist, i.e., there is reluctance to participate in “yet another” committee.
- CEOs may wish to avoid inviting additional board involvement in enterprise affairs.
- Boards may not wish to undermine the authority of the CEO and CIO.

The establishment of a well-balanced IT strategy committee with ex-officio representation of key executives and composed of informed members of the board, assisted as necessary with external expertise, will help overcome these obstacles.

How To Get Started

IT strategy committees often limit their scope to providing direction to ensure that IT is aligned with current and future business strategies. However, the IT strategy committee is well placed to assist the board on all aspects of IT governance, notably the monitoring of the successful implementation of the strategic plans. This is best achieved by performance measurement—for example, through an IT balanced scorecard—enabling management and the board to correct deviations and adjust the strategy as needed.

The following pages describe—through a charter, a generic approach and some guidelines—how to initiate an effective IT strategy committee.

IT Strategy Committee Charter

Name

IT Strategy Committee of the Board of Directors

Purpose

To assist the board in governing and overseeing the enterprise's IT-related matters

Goal

The committee needs to ensure that IT is a regular item on the board's agenda and that it is addressed in a structured manner. In addition, the committee must ensure that the board has the information it needs to make informed decisions that are essential to achieve the ultimate objectives of IT governance. Those objectives are:¹⁰

- The alignment of IT and the business
- The delivery of value by IT to the business
- The sourcing and use of IT resources
- The management of IT-related risks
- The measurement of IT performance

These goals are interdependent and complementary. Achievement of one can be undone by failure on another.

Responsibility

The board must receive sound information to make informed decisions. While it is the responsibility of management to provide that information, it is the responsibility of the IT strategy committee to ensure that management is following through on its obligation. More specifically, the committee needs to offer expert insight into and timely advice and direction on topics such as:

- The relevance of the latest developments in IT from a business perspective
- The alignment of IT with the business direction
- The achievement of strategic IT objectives
- The availability of suitable IT resources, skills and infrastructure to meet the strategic objectives
- Optimisation of IT costs
- The role and the value delivery of external IT sourcing
- Risk, return and competitive aspects of IT investments
- Progress on major IT projects
- The contribution of IT to the business (i.e., delivering the promised business value)
- Exposure to IT risks, including compliance risks
- Containment of risks

¹⁰ The IT governance framework, as addressed by the IT Governance Institute in the *Board Briefing on IT Governance*, June 2001

Authority

The IT strategy committee operates at the board level but neither assumes the board's governance accountability nor makes final decisions. Neither does it play a role in day-to-day management. It acts solely as an advisor to the board and management on current and future IT-related issues.

The IT strategy committee must work in partnership with the other board committees and management to provide input to, review and amend the aligned corporate and IT strategies. Possible partnerships are with:

- The audit committee, on major IT risks
- The business strategy committee, on value delivery and alignment
- The compensation committee, on performance measurement
- The finance committee, for major IT resource investments

Executive management drives strategy development and takes responsibility for implementing the strategy after obtaining input and approval from the board and the relevant committees.

The detailed implementation of the IT strategy is the responsibility of executive management, assisted by one or more IT steering committees. Typically, such steering committees have the specific responsibility for overseeing a major project or managing IT priorities and IT resource allocation. To illustrate the important distinctions between the IT strategy committee and IT steering committees, see **table 1**, Comparison of Typical IT Strategy Committee and IT Steering Committee Responsibilities.

The responsibilities of these committees need to be aligned and integrated with:

- The overall responsibility of the board for approving the strategy and overseeing management's execution of it
- The overall management responsibilities for strategy development, management of IT risks and the evaluation of IT performance

Also, in practice, the distribution of responsibilities among these committees, the board of directors, executive management and the CIO may differ depending on the organisation's culture, history and structure, as well as particular circumstances.

Membership

The IT strategy committee is composed of a chairman, several board and nonboard members and ex-officio representation of key executives. The chairman should be a board member. The members should be selected on the basis of their knowledge and expertise in understanding the business impacts of information and related technology. (The selection criteria need to be customised depending on the business context in which the enterprise operates.)

To ensure that there is enough technical expertise in the committee, the board may choose to select IT experts to serve as external advisors. Regardless of the number of specialist members, it is important that at least two board members remain active in the committee so the board is adequately represented.

The success of the IT strategy committee depends on an objective and business-oriented understanding of the organisation's IT issues. An effective mix of members who understand the business operations and can challenge IT assumptions is likely to increase the IT strategy committee's success in achieving its goals. For this reason, the committee should be encouraged to seek and capitalise on external expertise while remaining mindful of confidentiality requirements.

Meetings

The IT strategy committee should meet when needed and as often as needed to accomplish its duties. The committee should report its findings and recommendations to the board. In addition, the committee's meeting agenda, minutes and supporting documents should be provided to the board so that board members not sitting on the committee may submit their comments to the committee chairman.

Table 1: Comparison of Typical IT Strategy Committee and IT Steering Committee Responsibilities

	IT Strategy Committee	IT Steering Committee
Level	<ul style="list-style-type: none"> • Board level 	<ul style="list-style-type: none"> • Executive level
Responsibility	<ul style="list-style-type: none"> • Provides insight and advice to the board on topics such as: <ul style="list-style-type: none"> — The relevance of developments in IT from a business perspective — The alignment of IT with the business direction — The achievement of strategic IT objectives — The availability of suitable IT resources, skills and infrastructure to meet the strategic objectives — Optimisation of IT costs, including the role and value delivery of external IT sourcing — Risk, return and competitive aspects of IT investments — Progress on major IT projects — The contribution of IT to the business (i.e., delivering the promised business value) — Exposure to IT risks, including compliance risks — Containment of IT risks • Provides direction to management relative to IT strategy • Is driver and catalyst for the board's IT governance practices 	<ul style="list-style-type: none"> • Decides the overall level of IT spending and how costs will be allocated • Aligns and approves the enterprise IT architecture • Approves project plans and budgets, setting priorities and milestones • Acquires and assigns appropriate resources • Ensures projects continuously meet business requirements, including reevaluation of the business case • Monitors project plans for delivery of expected value and desired outcomes, on time and within budget • Monitors resource and priority conflict between enterprise divisions and the IT function, and between projects • Makes recommendations and requests for changes to strategic plans (priorities, funding, technology approaches, resources, etc.) • Communicates strategic goals to project teams • Is a major contributor to management's IT governance responsibilities
Authority	<ul style="list-style-type: none"> • Advises the board and management on IT strategy • Is delegated by the board to provide input to the strategy and prepare its approval • Focuses on current and future strategic IT issues 	<ul style="list-style-type: none"> • Assists the executive in the delivery of the IT strategy • Oversees day-to-day management of IT service delivery and IT projects • Focuses on implementation
Membership	<ul style="list-style-type: none"> • Board members and (specialist) nonboard members 	<ul style="list-style-type: none"> • Sponsoring executive • Business executive (key users) • CIO • Key advisors as required (IT, audit, legal, finance)

Appendix G—Regulatory Reports and Emerging Standards on Governance

Committee of Sponsoring Organisations of the Treadway Commission (COSO)

The National Commission on Fraudulent Financial Reporting, known as the Treadway Commission, was created in 1985 by the joint sponsorship of the American Institute of Certified Public Accountants (AICPA), American Accounting Association, Financial Executives International (FEI), Institute of Internal Auditors (IIA) and Institute of Management Accountants (IMA, formerly the National Association of Accountants). The Treadway Commission had as its major objectives to identify the causal factors of fraudulent financial reporting and make recommendations to reduce its incidence.

Based on the Treadway recommendations, a task force under the auspices of the Committee of Sponsoring Organisations of the Treadway Commission (COSO) undertook a project to provide practical, broadly accepted criteria for establishing internal control and evaluating its effectiveness. In 1992 *Internal Control—Integrated Framework* was issued. This report is commonly referred to as the COSO framework.

COSO broadly defines internal control as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

The COSO framework has been adopted by many private sector and government organisations. The framework has also influenced the development of other control and management frameworks, such as COBIT.

Most recently, the COSO framework has been identified as meeting the framework requirements of Section 404 of the Sarbanes-Oxley Act. Under these rules, management must disclose any material weakness and is unable to conclude that the company's internal control over financial reporting is effective if there are one or more material weaknesses in such control. Furthermore, the framework on which management's evaluation is based must be a suitable, recognised control framework that is established by a body or group that has followed due process procedures, including the broad distribution of the framework for public comment.

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 nonexecutive 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 behaviour and 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 of profound influence 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 if 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 among 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 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

IT Governance Institute, Control Objectives for Information and related Technology (COBIT)

Developed by the IT Governance Institute, 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 seven information criteria that can be used to define generically 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 (plan and organise, acquire and implement, deliver and support, monitor and evaluate). For each of these 34 IT 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

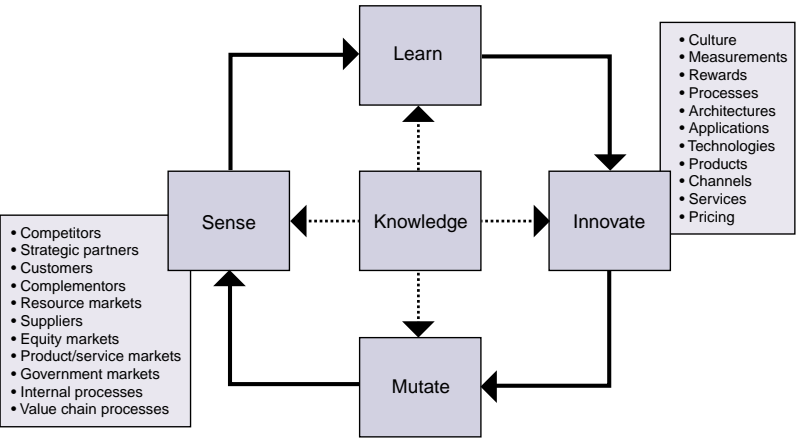
The more detailed elements of COBIT provide some 300 detailed control objectives for management and IT practitioners who are looking for best practices in control implementation, and extensive audit guidelines building on these objectives. The latter are geared toward those needing to evaluate and audit 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 each IT process)
- A list of critical success factors that provides succinct nontechnical best practices for each IT process
- A maturity model to assist in benchmarking and decision-making for control over each IT process

Appendix H—The Emerging Enterprise Model

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.



Successful enterprises monitor their 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.



IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: www.itgi.org