Unlocking Value: An Executive Primer on the Critical Role of IT Governance
IT Governance Institute®

The IT Governance Institute (ITGI™) (www.itgi.org) is a non-profit, independent research entity that provides guidance for the global business community on issues related to the governance of IT assets. ITGI was established by the non-profit membership association ISACA in 1998 to help ensure that IT delivers value and its risks are mitigated through alignment with enterprise objectives, IT resources are properly managed, and IT performance is measured. ITGI developed Control Objectives for Information and related Technology (CobiT®) and Val IT™, and offers original research and case studies to help enterprise leaders and boards of directors fulfill their IT governance responsibilities and help IT professionals deliver value-adding services.

Disclaimer

ITGI has designed Unlocking Value: An Executive Primer on the Critical Role of IT Governance (the ‘Work’) primarily as an educational resource for executives. ITGI makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of all proper procedures and tests or exclusive of other proper procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, control professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or IT environment.

Reservation of Rights

© 2008 ITGI. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of ITGI. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and non-commercial use and for consulting/advisor y engagements, and must include full attribution of the material’s source. 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: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: www.itgi.org

ISBN 978-1-933284-79-8
Unlocking Value: An Executive Primer on the Critical Role of IT Governance
Printed in the United States of America
Acknowledgements

The IT Governance Institute wishes to recognise:

Researchers
Gary Hardy, CGEIT, IT Winners, South Africa
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG, Austria
John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada
Paul Williams, FCA, CITP, Paul Williams Consulting, UK

Expert Reviewers
Max Blecher, Virtual Alliance, South Africa
W. Krag Brotby, CISM, Brotby & Associates, USA
Sushil Chatterji, Edutech, Singapore
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Alison Holt, Concrete Campus, New Zealand
Anil K. Jogani, Avon Consulting Ltd., UK
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India
John W. Lainhart IV, CISA, CISM, CGEIT, IBM, USA
Amarit Laorakpong, D. Eng., Siam Commercial Bank, Thailand
Lynn Lawton, CISA, FBCS CITP, FCA, FIAs, PIIAs, KPMG LLP, UK
Jean-Louis Leignel, Benchmarking Governance of IS (BGIS), France
Debbie A. Lew, CISA, Ernst & Young LLP, USA
William J. Malik, CISA, Malik Consulting LLC, USA
Akira Matsuo, CISA, CPA, KPMG (AZSA)/Aoyama Gakuin University, Japan
Lucio Augusto Molina Focazzio, CISA, Colombia
Kamesh Namuduri, Ph.D., CISA, CISM, CISSP, Sun Certified J2EE Architect, Wichita State University, USA
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia
Hugh Parkes, CISA, FCA, Parkes & Parkes, Australia
Max Shanahan, CISA, FCPA, MIIA (Aust.), Max Shanahan & Associates, Australia
Patrick Stachtchenko, CISA, CA, Stachtchenko & Associates, France
Wim Van Greembergen, Ph.D., University of Antwerp Management School, and IT Alignment and Governance (ITAG) Research Institute, Belgium
Vatsaraman Venkatakrishnan, CISA, CISM, CGEIT, Emirates Airline, UAE

ITGI Board of Trustees
Lynn Lawton, CISA, FBCS CITP, FCA, FIAs, PIIAs, KPMG LLP, UK, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control sa-nv, Belgium, Vice President
Yonosuke Harada, CISA, CISM, CAIS, InfoCom Research Inc., Japan, Vice President
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, CGEIT, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Frank Yam, CISA, FHKCS, FHKIod, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Acknowlegements (cont.)

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Sushil Chatterji, Edutech Enterprises, Singapore
Kyung-Tae Hwang, CISA, Dongguk University, Korea
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Hugh Penri-Williams, CISA, CISM, CCSA, CIA, Glaniad 1865 EURL, France
Eddy Schuermans, CISA, PricewaterhouseCoopers, Belgium
Gustavo Adolfo Solis Montes, CISA, CISM, Grupo Cynthus, Mexico
Robert E. Stroud, CA Inc., USA
John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp Management School, and IT Alignment and Governance (ITAG) Research Institute, Belgium

COBIT Steering Committee
Robert E. Stroud, CA Inc., USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Rafael Eduardo Fabius, CISA, Republica AFAP SA, Uruguay
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Jimmy Heschl, CISA, CISM, CGEIT, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Greet Volders, Voquals, Belgium

Val IT Steering Committee
John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada, Chair
George Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
Kris Budnik, ITIL, Deloitte & Touche, South Africa
Peter Harrison, FCPA, Fujitsu Consulting, Australia
Paul Williams, CITP, FCA, MBCS, Paul Williams Consulting, UK

ITGI Affiliates and Sponsors
ISACA chapters
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systemes d’Information
Institute of Management Accountants Inc.
ISACA
ITGI Japan
Norwich University
Socitm Performance Management Group
Acknowledgements (cont.)

Solvay Brussels School of Economics and Management
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
Analytix Holdings Pty. Ltd.
B Wise B.V.
CA Inc.
Consult2Comply
Hewlett-Packard
IBM
ITpreneurs Nederlands B.V.
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corporation
TruArx Inc.
Wolcott Group LLC
World Pass IT Solutions
Table of Contents

1. **Introduction: Why IT Governance Is So Critical** .......................................7
   - IT: A Principal Driver of Business Value ..................................................8
   - The Significant Cost of IT .....................................................................8
   - IT Risk .................................................................................................9
   - Ensuring That IT’s Value Is Achievable ..................................................9
   - Achieving Business Value Through IT Governance ..........................10

2. **What Exactly Is IT Governance?** ...................................................11
   - A Best-practice-based Definition .........................................................11
   - What IT Governance Should Deliver .....................................................11
   - A Dynamic, Continuous Process .........................................................12

3. **Key Players in IT Governance** ......................................................13
   - The Board of Directors .................................................................13
   - Executive Management .................................................................14
   - The Chief Information Officer ........................................................14
   - Business Unit Executives .................................................................15

4. **How Is Effective IT Governance Best Accomplished?** ...............16
   - Asking—and Answering—Four Fundamental Questions ..................16
   - Using a Comprehensive IT Governance Framework .....................17
   - Making IT Governance Work in Practice ......................................18
   - Avoiding Pitfalls When Implementing Best Practices ..................19

5. **How Does the Enterprise Currently Measure Up?** ......................20
   - Setting Objectives and Measuring Performance ...............................20
   - Knowing the Current Status and Where Gaps Exist ......................21
   - Using Benchmarks for Performance Comparisons to Peers ...........21

6. **The Critical Steps: How to Improve IT Governance** .................23
   - Ten Fundamental Steps ..................................................................23

Appendix—Maturity Model ......................................................................25

Other Publications ....................................................................................27
1. Introduction: Why IT Governance Is So Critical

We live in a rapidly changing world. Investment in information technology (IT) is no longer just about implementing technology itself; it is about ensuring that value is realised from business and organisational changes enabled by IT. Globally, enterprises—whether public or private, large or small—increasingly understand that information is a strategic asset and IT is an important contributor to economic success.

Enterprises that figure out how to govern IT-enabled change are more likely to realise value—but those that do not may experience serious and visible failures. The vast majority, however, fall somewhere between these two extremes: pursuing the promise of IT-enabled change but unwittingly leaving much, and sometimes most, of its rewards unclaimed.

Proven practices in realising value from IT and delivering reliable and secure IT services have been available for more than a decade, and embracing them does not have to be complex or expensive. Opportunity, cost and risk make IT operationally critical and strategic to enterprise success, so implementing good professional management practices should be a management imperative.

From business improvement to strategic transformation initiatives, executives appreciate that IT can be a powerful tool to help their enterprise achieve its most important objectives. For example, IT can represent a core driver of cost savings for large-scale transactions across mergers, acquisitions and divestitures. Additionally, IT is often the key interface with the customer and is therefore, the public face of the enterprise. IT can also enable complete automation of key processes, such as the supply chain.

Executives need to feel confident that investments in IT are likely to realise value in the enterprise. They should consider these questions regarding the enterprise’s IT:

• Are we doing the right things?
• Are we doing them the right way?
• Are we getting them done well?
• Are we getting the benefits?

Many executives regard anything related to IT as mysterious, technical and risky. As a result, they fail to apply known and proven techniques to address these questions when managing investment in IT.

This guide helps board members and executive management better understand how to govern their investments in IT to optimise benefits at an affordable cost, with a known and acceptable level of risk. Gaining this understanding will enable them to unlock and maximise value from these investments and

1 Based on the ‘Four Ares’ as described by John Thorp in his book The Information Paradox, written jointly with Fujitsu, first published by McGraw Hill, USA, in 1998 and a revised in 2003
Unlocking Value: An Executive Primer on the Critical Role of IT Governance

enhance their business operations. The guide is based on the experiences of many enterprises and experts around the world. It is not, however, intended to be a full implementation guide. More comprehensive implementation guidance, including the IT Governance Implementation Guide Using COBIT® and Val IT, 2nd Edition; COBIT QuickStart, 2nd Edition; and Enterprise Value: Governance of IT Investments, Getting Started With Value Management, is available at www.itgi.org.

IT: A Principal Driver of Business Value

IT is not only critical in its support of key business processes, but also transformational. Consider the expanding scope of IT’s impact not just on the performance of individual organisations, but on entire industries. IT does not just reduce cost through, for example, aggregating information across previously independent business units. By helping executives use this information to acquire a comprehensive, 360-degree view of their customers, IT has also triggered a quantum shift in the business model from one focused on specific services to one intent on capturing the much more rewarding, long-term benefits inherent in a relationship-based approach to customer service. This new model has the potential to change ‘the game’—enabling a networked economy that cuts through geographic locations, time zones and organisational silos to provide new and innovative ways of creating value.

The Significant Cost of IT

At the same time, investing in IT can consume enormous resources, especially for large, global enterprises. IT is often the largest category of expenditure after staffing costs, and it can be a difficult task to acquire a clear and complete picture of exactly how much is being spent, on what types of technology assets and processes, and where in the enterprise. In far too many cases, IT costs are not understood and budgets are spread across business units and functions with no overall oversight.

Unfortunately for most enterprises, the greatest portion of this spending is typically committed to post-implementation maintenance and operational costs for non-value-adding legacy system technologies—a draining commitment that often leaves far too little money available for technologies to support more strategic initiatives or game-changing opportunities. Compounding this, when funds are spent on strategic initiatives, they all too often fail to deliver the expected outcomes.

As a result—and not surprisingly—even after enterprises have spent handsomely on IT, many still fail to demonstrate concrete, measurable business value for the investment. In fact, every day billions of pounds are lost or wasted as a result of poor business oversight and decision making regarding IT investments.²

Far too many enterprises discuss IT at the board level on just two occasions: during annual budget discussions and when IT-related failures have already resulted in financial losses or corporate embarrassment.

The most common red flags of poor IT oversight are listed in figure 1.

**Figure 1—Red Flags of Common Examples of Poor IT Oversight**

- Board members or senior managers are reluctant to engage with IT.
- Business executives and IT executives communicate amongst themselves poorly or infrequently.
- IT leaders and experts do not ‘get’ the business requirements.
- Business leaders do not understand the potential for IT-enabled innovation.
- Potential senior-level sponsors fail to take ownership.
- IT is bureaucratic and slow to respond to add value.
- IT-enabled changes frequently fail to meet business needs and are delivered late and over budget.
- IT risks are not understood or managed effectively in conjunction with business risks.
- The enterprise fails to comply with regulatory or contractual requirements.
- Metrics to measure IT’s success are not relevant to the business users.

**IT Risk**

The networked economy creates new technology and business opportunities, but also involves increasing risk in areas such as business continuity, information security, and failure to recognise or successfully implement the organisational changes that are necessary for an enterprise to prosper or even survive in such an economy. While many of these risks are not new, in these days of doing business on a global scale around the clock, the non-availability of business systems, particularly those that are customer facing, has become far too visible and costly for any enterprise to ignore.

With IT now so intrinsic and pervasive within enterprises, business management 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 processes (operational)
- IT is a key enabler of business strategy and change (growth and innovation), and the risk of not recognising or making the business changes necessary to utilise IT capability to deliver value must be recognised, understood and managed
- Due diligence is increasingly required relative to the IT implications of mergers and acquisitions

Remember that risk is not always to be avoided; informed and conscious risk taking is also an essential element of business strategy. Management of risk is as much about grasping an opportunity as it is about dealing with undesirable events.

**Ensuring That IT’s Value Is Achievable**

Successful enterprises strive to avoid serious failures through effective governance. They plan and execute a strategic undertaking with oversight at the highest levels to avoid the risk of failure. They also make sure controls are in place to avoid operational risks when new services are delivered.
Enterprises that have implemented effective IT governance have put in place business-led structures such as IT executive committees to provide enhanced direction and gain better control of IT-related activities. They are adopting and adapting best practices in areas such as portfolio management, service delivery and risk management. They are able to monitor IT’s performance using business-oriented reporting.

Successful enterprises are hiring chief information officers (CIOs) with business insight. They are requiring business case rationales for new acquisitions and they are tying funding approval to a clear demonstration of measurable business value.

Getting better business value from IT requires the right leadership; well-defined processes with clear roles, responsibilities and accountabilities; appropriate structures; and supporting metrics, information, and tools. In short, an effective approach to enterprise governance of IT is required.

**Achieving Business Value Through IT Governance**

While boards usually look at business strategy and strategic risks, few boards have focused on IT, despite the fact that it involves perhaps the largest investments they will ever make and huge risks. Why is that? Possible reasons include the following:

- Within many enterprises, IT has traditionally been treated as an entity separate from the business function, and anything to do with IT is perceived as a technology issue.
- IT is complex, even more so in the extended enterprise operating in a networked economy.
- The business and organisational changes that have to be recognised and managed if enterprises are to realise value using IT capabilities further add to the complexity.

To be effective and drive value, IT needs to be recognised as a strategic business asset, with business executives owning IT-enabled business changes and the management of operational risks.

Good governance requires active, continued and committed involvement from all business leaders, and their working understanding of the role of IT and how it contributes to value. In fact, without such commitment, value will not be created. The business executives will need to take accountability for the delivery of business value from IT and for the management of the associated risks.

Board members are also facing increasing regulatory pressures and must demonstrate that effective IT controls are in place. Good IT governance will ensure that there are no IT control surprises.

One of the most effective means of continually ensuring that IT contributes measurable value to the enterprise’s objectives is a strategic, leadership-sponsored commitment to establishing a comprehensive IT governance capability.
2. What Exactly Is IT Governance?

Governance—as both a concept and a term—is often employed casually these days to support a wide range of agendas. To avoid stakeholder confusion, directors and executive leaders should be clear and consistent in how they define IT governance and communicate its primary goal, always remembering that IT governance is not, in itself, the endgame. IT governance is merely a necessary means of achieving optimum value from, and control over, IT within the enterprise.

A Best-practice-based Definition

ITGI defines IT governance as:

*The responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise’s IT sustains and extends the organisation’s strategies and objectives.*

This definition of IT governance departs in an important way from traditional definitions, which typically focus more narrowly on the sole domain of IT—IT services, the supporting infrastructures and the organisations that deliver applications, connectivity and information.

The definition clearly positions IT governance not as an isolated discipline but as an integral part of enterprise governance. This is a vital distinction because it reflects the fact that, while the need for governance at an enterprise level has been driven primarily by demand for transparency across enterprise risks and protection of shareholder value, the enormous costs, risks and opportunities associated with IT call for a dedicated, yet integrated, focus on IT governance.

What IT Governance Should Deliver

Fundamentally, IT governance is concerned with two outcomes: IT’s delivery of value to the business and the mitigation of IT risks. Both are enabled by strategic alignment of IT with the business, and the availability of adequate resources. Management then needs to measure performance to monitor progress toward desired goals.

In this respect, IT governance can be pictured as focusing primarily on five main areas:

1. **Strategic alignment**—Achieving the goals and strategies of an enterprise through the coherent undertaking of activities by the different governance structures or management levels within an organisation. A culture of business and IT partnership should be developed, supported by IT’s interest and understanding of the business, and sharing of technology-related issues and opportunities. This culture will enable a collaborative approach to strategy development and a shared focus on high-value IT investments.

2. **Value delivery**—Creating new value for the enterprise, maintaining and extending existing value, and eliminating initiatives and assets that are not creating sufficient value.

---

What is value?

*The result of subtracting costs from benefits and adjusting the total to account for two things: risk and the time value of money.*

What is the principal goal of IT governance?

*To ensure that IT creates value for the enterprise in alignment with its strategic objectives, while managing IT-related risks.*
3. **Risk management**—Addressing IT-related risks and using IT to assist in managing business risks

4. **Resource management**—Having the right capability to execute the strategic plan, and providing sufficient, appropriate and effective resources

5. **Performance measurement**—Tracking the achievement of the objectives of the enterprise and compliance with specific external requirements

**A Dynamic, Continuous Process**

IT governance functions as a continuous process and, as an integral part of enterprise governance, focuses on strategic objectives. Executives and directors should regularly assess whether their organisation is delivering the value that the strategy promised and addressing the risks that require mitigation. At regular intervals—and on a continual basis in large enterprises—performance should be monitored and the results measured, reported and acted upon. At least annually, the strategy should be re-evaluated and realigned with the business as necessary.
3. Key Players in IT Governance

IT governance is the direct responsibility of board members and executive management, and governance-related roles and activities need to be carried out by executives, managers and staff in almost every function and business unit across the enterprise. To help focus on IT aspects, this chapter provides a brief description of the primary responsible parties and a summary overview of their roles.3

The Board of Directors

At the most strategic level, board members have overall responsibility for enterprise governance. As defined in Principles of Corporate Governance, issued by the Organisation for Economic Co-operation and Development (OECD) in 1998, board members must:

• Ensure that a sound framework exists to provide strategic guidance for the enterprise
• Monitor management
• Oversee the integrity of the enterprise’s systems and information

As an extension of these enterprise governance responsibilities, board members are also accountable for the performance of IT. In fact, as the Bank for International Settlements (BIS)4 has pointed out, board members should address IT like any other strategic board agenda item.

Specifically, this means that the board must be clear about its own and management’s responsibilities and have a system in place to allocate accountabilities. This will ensure that:

• IT is creating value for the business in alignment with its strategic objectives
• There are appropriate and effective processes to monitor risk, and the system of internal control is effective in reducing those risks to an acceptable level5
• Information assets are safeguarded, their integrity is ensured, and they are used effectively and efficiently to grow the business and enhance shareholder value

Part of this process involves ensuring that sound governance principles are in place, communicated, understood, accepted and followed. To achieve effective IT governance, directors, managers and staff at every level of the enterprise must collaborate in applying the same principles, which can range from setting objectives and clarifying direction, to providing and evaluating performance measures. Examples of these principles are provided in ITGI’s COBIT® and Val IT™ frameworks, which are discussed in detail in chapter 4.

3 Further detail on how board members and senior management address these expectations is provided in chapter 4.
4 BIS, ‘Enhancing Corporate Governance in Banking Organisations’, 1999
5 Turnbull Report, Internal Control: Guidance for Directors on the Combined Code, 1999
6 IT Governance Institute, COBIT® 4.1, USA, 2007, www.itgi.org/cobit
7 IT Governance Institute, Enterprise Value: Governance of IT Investments, The Val IT™ Framework 2.0, USA, 2008, www.itgi.org/valit
The board must also be guided by management and have the means to gain the required assurance through independent expertise as appropriate. Typically, an IT strategy committee or executive committee might play a key role in directing and monitoring IT activities on behalf of the board.

Further assurance can be gained from the activities of an audit committee and internal audit function. Independent reports from experts, including internal auditors, can also be commissioned.

The key to good governance and to obtaining assurance is having a proper understanding of the enterprise’s objectives and associated opportunities and risks, an ability to ask the right people the right questions at the right time, the ability to properly interpret the answers, and the ability to ‘drill down’ to obtain full and proper explanations.

**Executive Management**

Although members of executive management collaborate closely with the board in carrying out an effective IT governance programme, they play a different role from the board. Unlike the board, executive management has day-to-day responsibility for embedding processes that provide information to support governance and practices throughout the enterprise and communicating their importance to the enterprise’s employees, including any outsourced functions.

Executive management is also responsible for reporting to the board on IT performance and plays a central role in ensuring that IT governance objectives are carried out.

**The Chief Information Officer**

Above all, CIOs must be adept and agile at understanding the opportunities and risks that IT provides in support of the enterprise’s objectives and initiatives, and must act as the bridge between IT and the business. CIOs must also ensure a secure and reliable delivery of IT services.

This role requires specialised knowledge and a particular set of skills. From his/her position at the centre of the enterprise, the CIO should have an overview of the business strategy, the business drivers and the processes that deliver value to the organisation. The CIO should understand how technology can contribute to business value by enabling the delivery of business change through innovation and delivering services to support critical business processes. He/she should also understand how to manage and mitigate the associated risks.

In addition, the CIO should help the business executives understand the process and organisational changes they will need to make to ensure that the target value is realised. No CIO can deliver this alone; the overall business change and the ongoing operation of the business process is the business executives’ responsibility. The CIO should foster close collaboration and partnership with the business. A culture of trust and mutual respect between IT and the business is essential.
Business Unit Executives

It may be tempting for business leaders charged with managing business unit performance or non-IT functions to assume that IT governance duties are solely the board’s or management’s responsibility—or worse, that IT governance is merely a technology-related challenge that sits beyond their scope of duties. In fact, the opposite is true: functional and business unit executives—not the board, management or any IT managers—bear the majority of the day-to-day responsibilities in operating within the governance framework and processes. They and their teams are the ones who sponsor the investments and are accountable for, and live with, the results.

One of the best ways to meet these challenges and expectations, of course, is to be highly informed about the IT investment and operational service objectives as well as governance-related policies and procedures.

The most effective IT investments stand out in part because, rather than merely reacting to these activities, functional and business unit executives take a much more proactive approach and leadership role in the entire investment life cycle. Successful business executives accept accountability, sponsor and drive investments affecting their function, and provide critical stakeholder input.

Business unit executives must also ensure that their operations are aligned with the overall enterprise strategy, and the IT strategy and operational services that support it.

The most successful business changes enabled by IT are those initiated, championed and directed by the business executive. Conversely, an IT initiative for a business unit that does not have the business executive’s support will likely fail.
4. How Is Effective IT Governance Best Accomplished?

In addition to ensuring that policies and procedures are defined, IT governance-related roles and responsibilities are understood, and the right organisational structures are in place, adoption of good IT governance practices will enable:

- Board members and senior executives to ask the right questions and interpret the answers
- An appropriate IT governance framework to be adopted
- Critical success factors to be addressed

**Asking—and Answering—Four Fundamental Questions**

Board members and executive managers in business and IT need to consider regularly the following four questions (figure 2).

1. **The strategic question: Are we doing the right things?**
   Answering this question requires asking:
   - Are our investments in line with our vision?
   - Are our investments consistent with our business principles?
   - Are our investments contributing to our strategic objectives, both individually and collectively, such that we are getting optimal benefits, at an affordable cost, at an acceptable level of risk?
   - Are our IT services, assets and other resources resulting from our investments focused on real business needs and priorities?
   - Do we know/understand our total investment in/spent on IT?

2. **The architecture question: Are we doing these things the right way?**
   Answering this question requires asking:
   - Are our investments in line with our enterprise’s architecture?
   - Are our investments consistent with our architectural principles and our standards?
   - Are we leveraging synergies between our investments?
   - Are our IT services delivered based on optimal use of IT infrastructure and other assets and resources?

3. **The delivery question: Are we getting these things done well?**
   Answering this question requires asking:
   - Do we have effective and disciplined management, delivery and change management processes?
   - Do we have competent and available technical and business resources to deliver the required capabilities and the organisational changes required to leverage them?
   - Are services delivered reliably, available when and where required, and secure?

4. **The value question: Are we getting the benefits?**
   Answering this question requires asking:
   - Do we have a clear and shared understanding of what constitutes value for our enterprise?
• Do we have a clear and shared understanding of the expected benefits from new investments, and resulting IT services, assets, and other resources?
• Do we have clear and accepted accountability and relevant metrics for realising the benefits?
• Do we have an effective benefits realisation process over the full economic life cycle of our investments to ensure that we are getting optimal business value?

Using a Comprehensive IT Governance Framework
Implementing good IT governance is almost impossible without engaging an effective governance framework. Such a framework must define which decisions have to be made, who is involved in making them, how they are made, and exactly what the process is for ensuring that these decisions are carried out in the appropriate manner. The framework should also ensure that results are monitored and that corrective actions are taken when expected results are not realised.

Two IT governance frameworks have been developed by ITGI: Control Objectives for Information and related Technology (COBIT) and Val IT. The intelligent application of processes defined by COBIT and Val IT can help enterprises significantly improve IT governance and the return on their investments. While COBIT sets high-level objectives for all four of the questions depicted in figure 2, Val IT focuses on two: Are we doing the right things? Are we getting the benefits?

![Figure 2—Is IT Creating Value? Make Sure to Ask the Right Questions.](image)

**COBIT**
COBIT is a globally accepted set of tools organised into a framework that executives at all enterprises can use to ensure that their IT is helping them achieve their goals and objectives. Many executives need to make decisions based on diverse opinions from IT managers, auditors and others. COBIT cuts through these barriers by providing a common language for executives to communicate goals, objectives and expected results. Based on industry standards and best practices, COBIT enables executives to direct their IT for optimal advantage, reduce IT-related risks and increase confidence in the information provided by IT. COBIT enables clear policy development and good practice for
Unlocking Value: An Executive Primer on the Critical Role of IT Governance

IT management, increases the value enterprises can attain from IT, and helps manage compliance. The tools are used by many enterprises, government agencies, academic institutions and other entities around the world.

**Val IT**

The Val IT framework is an IT governance framework based on COBIT that helps boards and executive management ensure that IT investments in IT-enabled change are managed throughout their full economic life cycle, and that they continue to deliver optimal benefits at an affordable cost, with acceptable levels of risk. Val IT consists of a set of guiding principles and a number of processes conforming to those principles that are further defined as a set of key management practices. The framework addresses outcomes, assumptions, costs and risks related to a balanced portfolio of IT-enabled business investments.

**Making IT Governance Work in Practice**

In addition to preparing the board and managers to ask hard, pointed questions—and putting a guiding framework in place—effective implementation of an IT governance programme also depends on several changes to both culture and behaviour.

Strong leadership, of course, is imperative, particularly from leaders in addition to the CIO, such as senior executives, all of whom must be visibly committed to championing the value that IT and IT governance can deliver to the enterprise. At the same time, the governance objectives targeted by the board and management must be clearly defined, realistic and communicated. There has to be a change in culture driven by example from the top, down to the workforce.

A trusting business and IT partnership should be developed, supported by IT’s interest in and understanding of the business, and sharing of technology-related issues and opportunities. This will enable a collaborative approach to strategy development and a shared focus on creating value from high-value IT investments and managing risks.

Processes need to be supported with carefully prescribed roles, responsibilities and accountabilities. They also require an appropriate set of guiding principles, organisational structures and processes that fit the style, skills, and operational norms specific to the enterprise.

Suitable analysis, communications tools, performance metrics and other benchmarks will help make the business’s and IT’s performance more transparent and enable direction and control.

COBIT provides a performance measurement framework based on business goals, which can be used to improve IT performance reporting. **Figure 3** lists examples of business goals that are aligned to a balanced scorecard.

A well-recognised governance framework will enable a common language and a shared commitment. It will generally be acceptable to all stakeholders, including stock market analysts who increasingly are monitoring IT investment performance to provide guidance to potential investors and divestors.
Avoiding Pitfalls When Implementing Best Practices

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

- Treat the implementation initiative as an improvement programme with a series of phases, rather than a ‘one-off’ step.
- Ensure that the improvements are sustained and adopted as ‘business as usual’.
- Remember that implementation involves cultural change as well as new processes. 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 governance of IT takes time and is a continuous improvement process.
- Focus first on where it is easiest to make changes and deliver improvements, and build from there one step at a time.
- Obtain top management buy-in and ownership. This needs to be based on the principles of best management of the IT investment.
- Avoid the initiative becoming perceived as a purely bureaucratic exercise.
- Avoid the unfocused checklist approach.⁸

---

⁸ This section is quoted from Aligning COBIT 4.1, ITIL v3 and ISO 27002 for Business Benefit, ITGI, USA, 2008.
5. How Does the Enterprise Currently Measure Up?

To implement effective governance of IT, enterprises need to assess how well they are currently performing and identify precisely where and how improvements can be made—not just to the IT governance process itself but also to all processes that need to be managed within and around IT.

Setting Objectives and Measuring Performance
Setting clear strategic objectives and using metrics to monitor results ensures that the drivers for governance have been recognised, any improvements are measured, and the expected benefits are realised.

Which metrics should be used? That depends, of course, on many factors, such as the enterprise’s particular priorities and business drivers as well as its risk tolerance and culture. Frameworks such as CoBIT and Val IT provide extensive guidance on the use of metrics and other measuring techniques, utilising tools such as balanced scorecards and IT or business dashboards, as shown in figure 4.

As the IT governance programme evolves, metrics will grow increasingly broader and more granular, and will shift from an IT-centric focus to a business-centric one over time. As shown in figure 4, at the IT-focused end of the spectrum, metrics such as infrastructure availability or cost per transaction can help measure the performance of enterprise-wide IT infrastructure. As alignment of IT investments with business objectives is progressively improved, IT’s contribution to business value should be assessed with more business-centric metrics such as
revenue growth and cost reduction, improved competitive products and services, and improved customer orientation and service.⁹

Knowing the Current Status and Where Gaps Exist
A maturity model provides a pragmatic and structured means of measuring how well developed the processes are against a consistent and easy-to-understand scale. By engaging a maturity scale such as the one depicted in figure 5, enterprise can:

• Build a view of current practices by discussing them in workshops and comparing them to the COBIT and Val IT models
• Set targets for future development by considering model descriptions higher up the scale and comparing them to best practices
• Set targets that are attainable and that have the potential, once reached, of adding value and reducing risk. This helps avoid unnecessary expenditures on trying to attain a higher level than can properly be justified.
• Plan process improvement projects to reach internally mandated targets by defining the specific changes required to improve management
• Prioritise project work by identifying where the greatest impact will be made and where this impact is easiest to implement

Using Benchmarks for Performance Comparisons to Peers
One of the questions most commonly asked by boards and executives is ‘How does our use of IT compare with that of our competitors?’

As a result, more and more enterprises today—particularly those that are most heavily dependent on IT—are undertaking valuable benchmarking initiatives. While external competitive benchmarking is probably the most useful approach, there is also much to be gained from internal benchmarking within a group of enterprises to identify the attributes of successful and less successful IT-related business strategies within the same group.

---
⁹ Examples from COBIT’s business goals
ⁱ⁰ Op. cit., COBIT 4.1
It is important that the benchmarking initiative be truly focused on improving stakeholder value over time. It should not be a tactical initiative intended to make a particular IT project’s sponsor look good or an exercise in assigning blame.

Benchmarking is most useful when it is designed and managed as part of a total business and IT improvement strategy. Benchmarking alone will not provide all the answers, but, together with qualitative analysis and other tools, it should help management ask the right questions, identify key attributes of success and failure, and enhance stakeholder value over time.
6. The Critical Steps: How to Improve IT Governance

Once the awareness of the need for an effective approach to IT governance has been realised, the next step involves putting together an IT governance implementation plan.

Ten Fundamental Steps

Every enterprise will have a different plan or road map, depending, of course, on factors such as its industry and business environment and its culture and objectives. Equally important will be the current starting point. Few enterprises will have no IT governance structures or processes in place, even if they are not recognised as such currently. Therefore, the emphasis needs to be on building on what the enterprise already has. At some level, however, all IT governance plans should address the following 10 fundamental steps:

1. **Define and demonstrate the enterprise’s need for IT governance.** Set clear objectives and specify the desired outcomes expected based on business need. Consider the risks of not addressing the objectives. Inform and engage relevant stakeholders, and identify and assign sponsors. Make it easy for all stakeholders to understand—from the beginning—that implementing an effective IT governance programme is also about embracing cultural change and nurturing commitment at all levels of the enterprise, from the board to the ‘shop floor’.

2. **Integrate IT governance with enterprise governance.** Remember that IT governance should never be a stand-alone programme. To build business value, it must be positioned and approached as an integral component of a broader enterprise governance programme.

3. **Define the scope for the programme.** This is not just about deciding which objectives are long-term and which are short-term. It is also about defining the deliverables associated with these goals, agreeing on deadlines and priorities, and communicating the proposed plan to the stakeholders.

4. **Determine the risks and adjust the programme’s scope accordingly.** Every enterprise’s tolerance for risk, as defined by its board and senior executives, is different. And this tolerance often changes—not just over time but also by project. Identify which risks need to be managed and adjust the scope of the programme to mitigate them.\(^{12}\)

5. **Set up the enterprise to execute the programme and processes needed to support it.** This means defining and adopting a governance framework. Specify who will make decisions and who will approve them. Provide and communicate guiding principles; create appropriate organisational structures, processes and practices; and define key participants (including a dedicated IT governance manager or facilitator) as well as their roles and responsibilities. Clearly draft and communicate policies, standards and processes.

---

\(^{11}\) Based on *IT Governance Implementation Guide: Using COBIT and Val IT. 2nd Edition*, ITGI, USA, 2007

\(^{12}\) IT Governance Institute, *COBIT Quickstart, 2nd Edition*, USA, 2007
6. **Assess the current situation.** Take a frank look at the enterprise’s present capabilities. Ask pointed questions such as ‘How do we currently perform—and how should we perform? What are we aiming for?’ Make sure to clearly identify the ‘pain points’ as well as the gaps in the IT governance approach.

7. **Agree on an improvement strategy.** Use information gathered on the needs and capability gaps to identify improvement opportunities. Then prioritise projects in alignment with the strategic business objectives. Finally, plan, fund and approve the projects that promise the best investment return.

8. **Implement improvements.** Expect the programme to evolve and improve. Adopt and adapt best practices. Build on strengths and focus on key weaknesses. Work diligently with process owners. Building on a base of good practices, be creative in adopting innovative ways to enable organisational change.

9. **Measure and monitor results.** It is difficult to improve without a clear, quantitative baseline. Set metrics aligned with the original goals and provide top management with scorecards and tailored, easy-to-read reports. Measure benefit realisation. Review programme effectiveness continuously, and never miss an opportunity to communicate success.

10. **Sustain the programme.** As the business and IT strategy evolves, so should the IT governance programme. If the enterprise’s vision and mission change, the governance programme may need to adapt. Ensure accountability for IT throughout the enterprise by defining appropriate organisational structures; drafting and clearly communicating policies, standards and processes; and effecting enterprise-wide cultural change.

In summary, as long as IT remains critical to realising business value—and it is hard to imagine this changing—the single most effective means of continually ensuring that IT contributes measurable value to the organisation’s objectives is a strategic, leadership-sponsored commitment to establishing a comprehensive IT governance capability.

For further guidance on how to adopt and implement effective IT governance practices in a smaller enterprise, refer to COBIT® Quickstart™, 2nd Edition. For guidance on how to begin the implementation of value management processes, refer to the Val IT publication Enterprise Value: Governance of IT Investments, Getting Started With Value Management.
Appendix— Maturity Model

0 Non-existent
There is no senior management oversight of IT-related activities to ensure that the enterprise’s IT goals add value to the organisation and 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 that IT needs to be a shared management responsibility with the support of top management. Regular governance practices such as review meetings, creation of performance reports, and investigation into problems take place, but they 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
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 amongst 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, including 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, 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 good practices from others.
Other Publications

Many publications issued by ITGI and ISACA contain detailed assessment questionnaires and work programmes. For further information, please visit www.isaca.org/bookstore or e-mail bookstore@isaca.org.

Assurance
• **ITAF™**: A Professional Practices Framework for IT Assurance, 2008
• **Stepping Through the IS Audit, 2nd Edition**, 2004

ERP Series:

Specific Environments:
• **Electronic and Digital Signatures: A Global Status Report**, 2002
• **Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment**, 2004
• **Linux: Security, Audit and Control Features**, 2005
• **Oracle® Database Security, Audit and Control Features**, 2004
• **OS/390—z/OS: Security, Control and Audit Features**, 2003
• **Risks of Customer Relationship Management: A Security, Control and Audit Approach**, 2003
• **Security Provisioning: Managing Access in Extended Enterprises**, 2002

IT Governance
• **Board Briefing on IT Governance, 2nd Edition**, 2003
• **IT Governance Global Status Report**—2008, 2008

COBIT® and Related Publications
• **COBIT® 4.1**, 2007
• **COBIT® Quickstart™, 2nd Edition**, 2007
• **IT Assurance Guide: Using COBIT®**, 2007
• **IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance**, 2007
COBIT Mapping Series:
• Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit, 2008
• COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0, 2007
• COBIT® Mapping: Mapping of ITIL With COBIT® 4.0, 2007
• COBIT® Mapping: Mapping of NIST SP800-53 With COBIT® 4.1, 2007
• COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0, 2006
• COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0, 2007
• COBIT® Mapping: Mapping of SEI’s CMM for Software With COBIT® 4.0, 2006
• COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0, 2007

IT Governance Domain Practices and Competencies:
• Information Risks: Whose Business Are They?, 2005
• Optimising Value Creation From IT Investments, 2005
• Measuring and Demonstrating the Value of IT, 2005
• Governance of Outsourcing, 2005
• IT Alignment: Who Is in Charge?, 2005

Val IT:
• Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0, 2008
• Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0 Extract, 2008
• Enterprise Value: Governance of IT Investments, Getting Started With Value Management, 2008
• Enterprise Value: Governance of IT Investments, The Business Case, 2006

Security
• Cybercrime: Incident Response and Digital Forensics, 2005
• Information Security Harmonisation—Classification of Global Guidance, 2005
• Managing Enterprise Information Integrity: Security, Control and Audit Issues, 2004
• Security Awareness: Best Practices to Serve Your Enterprise, 2005
• Stepping Through the InfoSec Program, 2007