

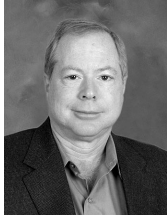
March 29, 2005

IT Governance Framework

by Craig Symons

BEST PRACTICES

BEST PRACTICES



March 29, 2005

IT Governance Framework

Structures, Processes, And Communication

This is the third document in the “IT Governance” series.

by Craig Symons

with Mark Cecere, G. Oliver Young, and Natalie Lambert

EXECUTIVE SUMMARY

With IT at the core of most 21st century businesses, and with today’s focus on compliance and risk management as a result of legislation like Sarbanes Oxley, organizations can no longer afford to have IT governance by default or bad IT governance by design. IT governance at its most basic is the process of making decisions about IT. By this simple definition, every organization has some form of IT governance. Good IT governance ensures that IT investments are optimized, aligned with business strategy, and delivering value within acceptable risk boundaries — taking into account culture, organizational structure, maturity, and strategy.

TABLE OF CONTENTS

2 What Is Good IT Governance?

IT Governance Defined

3 Establishing A Foundation

IT Governance Maturity

Structural Issues In IT Governance

The Four Objectives Of IT Governance

7 Existing Frameworks

COBIT

ITIL

ISO 17799

11 Constructing Your Framework

Governance Structures

Governance Processes

Governance Communications

RECOMMENDATIONS

14 Good IT Governance Is Straightforward

NOTES & RESOURCES

Forrester reviewed hundreds of related client inquiries and interviewed several vendors and end user companies.

Related Research Documents

“IT Governance And The Balanced Scorecard”
August 20, 2004, Quick Take

“IT Governance: Steering Committee Do’s And Don’ts”
July 9, 2003, IdeaByte

“CIOs: IT Governance Best Practices”
October 10, 2002, Brief

WHAT IS GOOD IT GOVERNANCE?

Forrester's Business Technographics® November 2004 United States SMB Benchmark Study found that enterprises spend an average of 4.9% of revenues on IT. In 2005, we expect IT budgets to grow 7% over last year.¹ IT is now at the core of most organizations' ability to execute strategy. Recent legislation, such as the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX), have elevated demands for improved compliance and risk management across the enterprise, and on IT organizations specifically. The result is a "perfect storm" of pressure on CIOs and their IT organizations for better IT governance.

IT Governance Defined

At its most basic definition, IT governance is the process by which decisions are made around IT investments. How decisions are made, who makes the decisions, who is held accountable, and how the results of decisions are measured and monitored are all parts of IT governance. Based on this definition, everyone has some form of IT governance. Unfortunately for many firms, the governance process is ad hoc and informal. There is no consistency across the enterprise, accountability is weak — if present at all — and there are no formal mechanisms to measure and monitor the outcomes of the decisions.

There is just too much at stake today for organizations to leave IT governance to chance or legacy processes. Optimizing IT investments must become a priority. There is a growing trend on the part of large organizations to elevate IT performance to the board of directors level. In addition to the traditional audit committee and compensation committee, boards are adding an IT oversight committee to become more involved in the role that IT plays in enabling and executing the enterprise's strategy. For example, FedEx has established the Information Technology Oversight Committee to oversee major IT-related projects and technology architecture decisions.²

Such executive commitments are only natural. IT governance can not exist in isolation but must be a subset of enterprise governance. It is the responsibility not just of IT management but of the board of directors and executive management. According to the IT Governance Institute, IT governance "is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."³

Implementing good IT governance requires a framework based on three major elements:

- **Structure.** Who makes the decisions? What structural organizations will be created, who will take part in these organizations, and what responsibilities will they assume?
- **Process.** How are IT investment decisions made? What are the decision-making processes for proposing investments, reviewing investments, approving investments, and prioritizing investments?

- **Communication.** How will the results of these processes and decisions be monitored, measured, and communicated? What mechanisms will be used to communicate IT investment decisions to the board of directors, executive management, business management, IT management, employees, and shareholders?

ESTABLISHING A FOUNDATION

With a working definition of good IT governance at hand, the next step is to establish a foundation on which to build an IT governance framework. The foundation consists of three parts: understanding the governance maturity, knowing how structural issues impact governance, and understanding the four objectives of IT governance.

IT Governance Maturity

Forrester recommends that organizations in the process of developing or evolving their current IT governance framework conduct an IT governance maturity assessment. Understanding where you are is extremely helpful in trying to formulate an IT governance strategy. Forrester's IT Governance Maturity Model is comprised of four stages (see Figure 1):

- **Stage 1: Ad hoc.** There are no formal IT governance processes, and it's not recognized by management as being a necessity. IT investments are made on a completely ad hoc basis. This scenario is almost always found in highly decentralized organizations, but it is not limited to them.
- **Stage 2: Fragmented.** Here there is an attempt to formalize IT governance processes but on a fragmented basis. These formalized processes may exist in one or more business units and IT decisions within those business units may be optimized, but there is no enterprisewide effort to coordinate investment decisions or examine tradeoffs between business units or enterprisewide investments versus BU investments.
- **Stage 3: Consistent.** At the third level of maturity, IT governance processes have been consistently applied across the enterprise. All business units/entities conform to the same set of IT governance processes. IT investment decisions are based on the enterprise view.
- **Stage 4: Best practices.** At the fourth level of maturity, IT governance processes are fully evolved and optimized across the enterprise. A strong IT portfolio management process is in place to ensure that all IT investment decisions are themselves optimized, the CEO and executive team are active participants in the governance process, and IT strategy is part of the enterprise strategy.

Figure 1 IT Governance Maturity Model

IV	Best practices	IT governance has been practiced for some time and has evolved to represent best practices. Companies employing IT governance best practices tend to have an optimized IT portfolio.
III	Consistent	There is a formal IT governance process in place and practiced consistently across the enterprise.
II	Fragmented	There has been some effort to formalize IT governance practices, but they are fragmented across the enterprise.
I	Ad hoc	Ad hoc governance practices are just that. There are no formal processes or mechanisms, it's essentially everyone for themselves.

Source: Forrester Research, Inc.

Structural Issues In IT Governance

Any attempt at developing and enforcing IT governance requires an understanding of the structural, or organizational, pieces of the framework. Forrester has identified four major types of IT organizational structures. These four include: centralized, decentralized, federated, and project-based organizations (see Figure 2). Each organizational structure presents a different challenge in implementing IT governance as characterized by its decision-making process.

- **Centralized.** In a centralized IT organization, all IT decision-making and the IT budget are in one place, they are much easier to manage and require much less effort to organize. The CIO can take the lead in developing the governance processes and work directly with the CEO and executive team. The challenge for centralized IT organizations is to refrain from becoming a monarchy and to ensure that business units and operating groups have a voice in the process.
- **Decentralized.** Decentralized organizations most often reach the fragmented stage because each decentralized IT function has developed *its own* IT governance processes, but there are no formal processes *across* business units or between business units and corporate. IT investment decisions may be optimized at the business unit level, but they are not optimized across the enterprise. This often results in duplicated infrastructure and applications, and little sharing of systems or expertise, if any. The challenge is to develop an enterprisewide IT governance process that enables the organization to make tradeoffs.
- **Federated.** These are hybrid organizations that have both centralized and decentralized components. Most infrastructure and enterprisewide applications are centralized in a corporate IT organization and operated as a shared service with chargebacks, while business units retain control over BU-specific applications and development resources. This attempts to create the best of both worlds: centralized control for reduced costs, with applications development left with the business units where it can be more responsive. The challenge for federated IT organizations is to balance the needs of the business units for infrastructure investments and to conform to an enterprise architecture and standards.

Figure 2 IT Organizational Structures

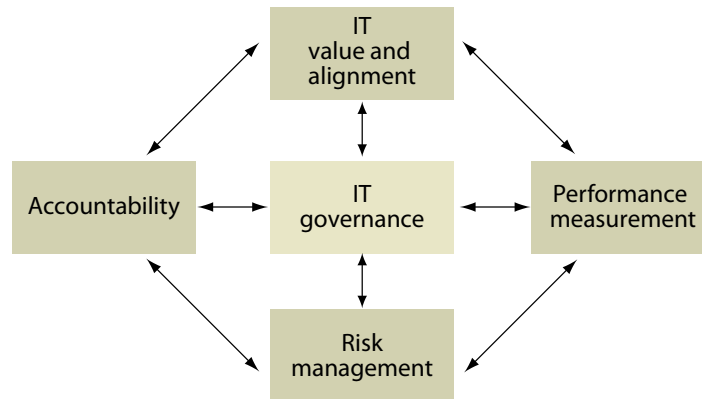
Project-based	All IT resources are centralized under a single reporting structure with centralized resource allocation (staffing). The organizational structure is built around resource pools. Line managers are replaced by resource managers.
Federated	IT takes on a hybrid structure. A centralized IT organization supports all infrastructure and enterprisewide applications, usually in a shared services environment. Individual business units maintain their own applications development organizations and budgets for BU-specific systems.
Decentralized	IT is decentralized by business unit, operating group, subsidiary, or geography. Each of these entities has its own CIO, IT organization, and IT budget. There is little or no attempt to coordinate across units or with corporate. Corporate IT supports the corporate HQ staff and perhaps some enterprisewide applications.
Centralized	IT is centralized under a single enterprise CIO. All IT systems and budgets reside at the corporate level.

Source: Forrester Research, Inc.

- **Project-based.** Project-based IT organizations are a relatively new phenomenon and take their lead from professional services firms. They are a form of centralized IT in that all IT resources are centrally located and report into a corporate CIO, but they differ mostly in the applications development area. Rather than the traditional applications development group, an organizational structure is built around resource pools, often called competence centers, consisting of like resources. Also the traditional line manager is replaced in favor of a resource manager or competence center manager who heads up each resource pool. This new role's performance is measured on resource utilization and the ability to loan out qualified staff in sufficient quantity as required by the project portfolio and pipeline. For project-based IT organizations to be effective, they need a strong governance mechanism in place to ensure that the right projects are selected and funded. The challenge, then, in project-based organizations is the process around the project selection, funding, and prioritization process.

The Four Objectives Of IT Governance

There are four objectives that drive IT governance: IT value and alignment, accountability, performance measurement, and risk management. Each of these objectives must be addressed as part of the IT governance process (see Figure 3).

Figure 3 The Four Dimensions Of IT Governance

Source: Forrester Research, Inc.

- IT value and alignment.** One of the primary goals of IT governance is to ensure alignment between the business units and IT. By creating the necessary structures and processes around IT investments, management can ensure that only those IT projects that are aligned with strategic business objectives are approved, funded, and prioritized. Furthermore, alignment also deals with balance between investments that run the current business, grow existing businesses, and have the potential to transform the business, while delivering IT value by managing projects that are on time, on budget, and deliver expected results. Delivering value to the business typically means things like growing revenues, improving customer satisfaction, increasing market share, reducing costs, and enabling new products and/or services.
- Risk management.** With more of an organization's value proposition built on IT, risks associated with IT are often the same as risks to the business. Therefore, managing IT risk is paramount. IT risks include security risks arising from hackers and denial of service attacks, privacy risks arising from identity thefts, recovery from disasters, resiliency of systems from outages, and the risks associated with project failures.
- Accountability.** At the end of the day, governance is about accountability. The Sarbanes-Oxley legislation is intended to hold senior executives accountable for the integrity and credibility of their financial information and controls. IT governance holds IT management accountable for the return on its investment in IT, as well as the credibility of IT's own information and controls.
- Performance measurement.** Accountability in IT governance requires that you keep score, typically by implementing a form of balanced scorecard. The IT Balanced Scorecard consists of four perspectives: IT Value, User, Operational Excellence, and Future Orientation. Two of these perspectives contain measures for the two key governance objectives: IT value and risk management. The IT value perspective contains specific measures for IT/business alignment and IT value, while the operational excellence perspective contains specific measures for managing IT risk.

EXISTING FRAMEWORKS

While there is no single, complete, off-the-shelf IT governance framework, there are a number of frameworks available that can serve as useful starting points for developing a governance model. As a result, most IT organizations today are “rolling their own” models, but borrowing heavily from existing frameworks. Most of the existing frameworks are complementary, with strengths in different areas, and so, a mix-and-match approach is often taken. Three of those frameworks are discussed in more depth below.

COBIT

Control Objectives for Information and related Technologies (COBIT) was developed in 1996 by the Information Systems Audit and Control Association (ISACA) and is now issued and maintained by the IT Governance Institute (ITGI) as a framework for providing control mechanisms over the information technology domain.⁴ Now in its third edition, COBIT has been extended to serve as an IT governance framework by providing maturity models, critical success factors, key goal indicators, and key performance indicators for the management of IT.

At the heart of COBIT are 34 high-level control objectives. These control objectives are grouped into four main domains: planning and organization, acquisition and implementation, delivery and support, and monitoring. Corresponding to each of the 34 control objectives are 318 detailed control objectives (see Figure 4).

- **Planning and organizing.** This domain covers a whole range of topics. Included are the strategy and tactics used by IT to achieve business objectives, strategy planning, strategy communication, strategy management, risk management, and resource management, which insures that the required technology infrastructure and human capital are in place.
- **Acquisition and implementation.** For IT to realize its strategy, it must identify, develop or acquire, and implement solutions to business processes. Additionally, it must manage the life cycle of existing systems through maintenance, enhancements, and retirements.
- **Delivery and support.** On its most basic level, IT delivers services to its customers (users). This domain concerns service and support issues including performance and security, and it also includes training.
- **Monitoring.** All IT processes need to be regularly assessed for their quality and compliance with control requirements. The monitoring domain addresses management’s oversight of the organization’s control processes.

Figure 4 COBIT Control Objectives

COBIT control objectives			
Planning and organizing	Acquisition and implementation	Delivery and support	Monitoring
Strategic planning Information architecture Technological direction IT organization and relationships Manage the IT investment Communicate aims and direction Manage human resources Ensure compliance Assess risks Manage projects Manage quality	Identify solutions Acquire and maintain application software Acquire and maintain technology architecture Develop and maintain IT procedures Install and accredit systems Manage changes	Define service levels Manage third-party services Manage performance and capacity Ensure systems security Identify and attribute costs Educate and train users Assist and advise IT customers Manage the configuration Manage problems and incidents Manage data Manage facilities Manage operations	Monitor the processes Assess internal control adequacy Obtain independent assurance Provide for independent audits

Source: Forrester Research, Inc.

More recently, COBIT added a set of action-oriented management guidelines to provide management direction for monitoring achievement of organizational goals, for monitoring performance within each IT process, and for benchmarking organizational achievement.

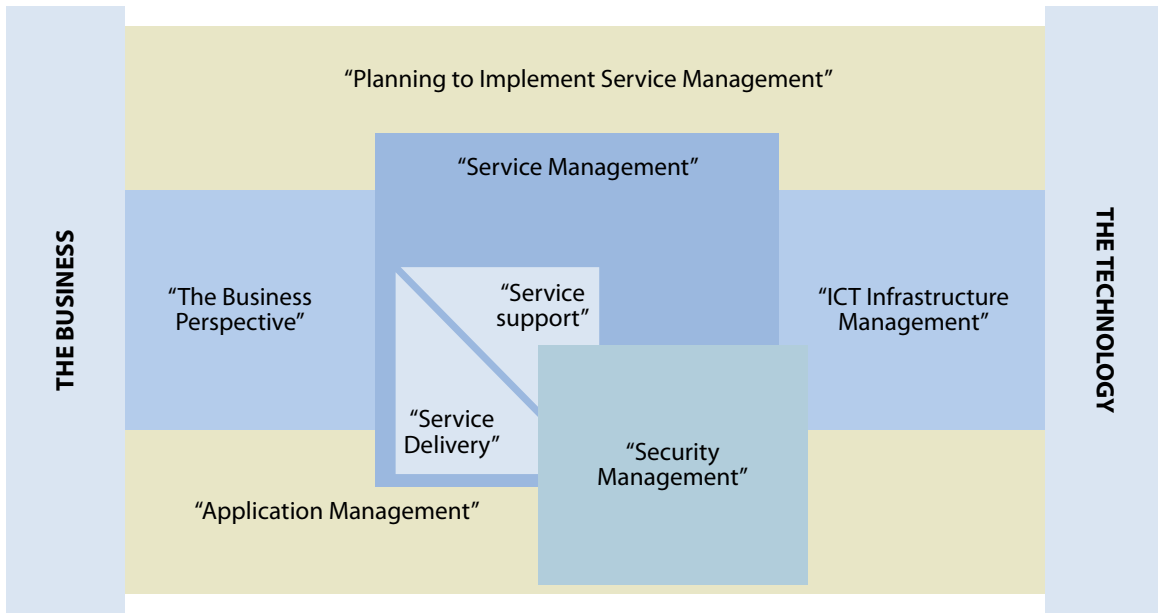
Overall, COBIT represents a comprehensive framework for implementing IT governance with a very strong auditing and controls perspective, which has increasing resonance in the era of Sarbanes-Oxley and other compliance-related regulations and legislation.

ITIL

The IT Infrastructure Library (ITIL), initially developed in the UK by the Office of Government Commerce (OGC), is gaining traction in the global IT community as a framework for IT governance.⁵ The library currently consists of eight books, including: “Software Asset Management,” “Service Support,” “Service Delivery,” “Security Management,” “Application Management,” “ICT

Infrastructure Management,” “The Business Perspective,” and “Planning to Implement Service Management” (see Figure 5). ITIL is focused on identifying best practices in regards to managing IT service levels and is particularly process-oriented.

- **“Planning to Implement Service Management.”** This book deals explicitly with the question of where to start with ITIL. It outlines the steps necessary to identify how the organization would benefit from ITIL. It helps identify current strengths and weaknesses and gives practical guidance on the evaluation of the current maturity levels of service management within the current organization.
- **“The Business Perspective.”** “The Business Perspective” is designed to familiarize business management with the architecture and components of information and communications technology (ICT) —infrastructure required to support the business processes. The book helps business leaders better understand the benefits of best practices in IT service management.
- **“Software Asset Management.”** This book encompasses the entire infrastructure and processes necessary for the effective management, control, and protection of the software assets within an organization, throughout all stages of their life cycle.
- **“Service Support.”** “Service Support” focuses on ensuring that the customer has access to appropriate services to support their business functions. It covers configuration management and other support management issues including incident, problem, change, and release management.
- **“Service Delivery.”** “Service Delivery” covers the service the business requires of IT to enable adequate support to the business users. This includes processes for service-level management, availability management, capacity management, financial management for IT services, and continuity management.
- **“Security Management.”** The security management book of ITIL looks at security from the service provider perspective, identifying the relationship between security management and the IT security officer, as well as outlining how it provides the level of security necessary for the entire organization. It further focuses on the process of implementing security requirements identified in the IT service level agreement.
- **“ICT Infrastructure Management.”** This covers all aspects of infrastructure management from identification of business requirements to acquiring, testing, installation, and deployment of infrastructure components. It includes the design and planning processes, deployment processes, operations processes, and technical support processes.

Figure 5 Eight ITIL Books

Source: ITIL

Source: Forrester Research, Inc.

- **“Application Management.”** “Application Management” addresses the complex subject of managing applications from initial business requirements through the application management lifecycle, up to and including retirement. A strong emphasis is placed on ensuring that IT projects and strategies are tightly aligned with those of the business throughout the applications life cycle. Once an application is approved and funded, it is tracked throughout its life cycle by the software asset management function of ITIL.

While COBIT takes the perspective of audit and control, ITIL takes the perspective of service management. The two frameworks are more complementary than competitive and components of both can be taken to build a governance framework.

ISO 17799

The International Organization for Standardization has developed the third major governance framework, ISO 17799, titled “Information Technology — Code of Practice for Information Security Management.”⁶ It was first released by the ISO in December 2000. However, it is based on British Standard 7799, which was finalized in 1999. The intent of the standard is to focus on security and aid an organization in the creation of an effective IT security plan.

The standard has the following high-level groupings: security policy, organizational security, asset classification and control, personnel security, physical and environmental security, communications

and operations management, access control, systems development and maintenance, business continuity management, and compliance. The standard is very thorough and covers a great deal of material in a concise manner.

ISO 17799's relatively narrow focus on security makes it unsuitable as the sole basis for an IT governance framework, but since risk management is a component of IT governance, there is relevance to ISO 17799, and parts of it can be adopted in building an overall IT governance framework.

CONSTRUCTING YOUR FRAMEWORK

The first three sections of this report laid the groundwork for developing an IT governance framework. There is not necessarily one right IT governance framework. Governance frameworks must work within the context of an organization's structure, culture, and strategy. Every IT governance framework must address three things: governance structures (the who of IT governance), governance processes (the how of IT governance), and governance communications to measure and communicate performance of the overall IT governance effort. Each of these is described in more detail below.

Governance Structures

Governance structures relate to the organizational mechanisms created around the IT investment process. They include reporting relationships, governance-specific positions, and committees either created especially for or repurposed to execute the governance processes. Examples of governance structures include the following:

- **Reporting relationships.** One of the more effective IT governance structures consists of the CIO reporting to the CEO. This ensures that IT is part of the executive team where most strategy discussions begin and end. Without this seat at the table, IT will almost always be limited to a support organization as opposed to an enabling organization.
- **Governance-specific positions.** Some large IT organizations are actually creating the position of IT governance officer reporting to the CIO. This sends a strong message that IT governance is important and it provides a continual focus on the issue. It prevents IT governance from becoming the flavor of the month by dedicating a resource and holding a senior manager accountable for IT governance initiatives.

A second position that plays an important role in IT governance is the IT relationship manager. The IT relationship manager acts as a go-between, communicating the implications of IT governance to the business units while articulating the needs of the business units back to IT. He is most successful when he can translate the benefits of IT governance into business terms and demonstrate that while at times it may be inconvenient, governance delivers value to the enterprise.

- **Committees.** The bulk of IT governance work is carried out by committees and for many organizations, multiple committees work at different levels to carry out IT governance processes. As mentioned earlier, sometimes these committees are already in existence and add IT governance responsibilities to their list of activities, while other times new committees are formed specifically to address IT governance issues. These committees include executive or senior management, IT investment, IT architecture and standards, and IT/business councils. The actual committees you use depend on organizational structures, culture, and other issues and not all organizations will employ all of these committees at the same time.

IT governance is a collaborative process, so IT governance committees should be as inclusive as possible. There must be a healthy mix of business unit membership, corporate membership, and IT membership.⁷

Governance Processes

The governance structures above are tasked with enforcing the governance processes articulated below. They include IT portfolio management, service-level agreements, chargeback mechanisms, and IT demand management.

- **IT portfolio management.** IT portfolio management is comprised of a number of subdisciplines, including IT asset management, application portfolio management, and project portfolio management. By rolling up all of these components, a complete and comprehensive view of the entire IT portfolio emerges, enabling better strategic decision-making.⁸

The IT portfolio is proactive management of the collection of projects, applications, systems, etc., and they are evaluated as a group against criteria like balance, flexibility, risk, and their ability to drive value for making future investment decisions.

- **Service-level agreements.** Service-level agreements (SLAs) list available services, alternative quality levels, and related costs provided by IT. SLAs are governance processes because they articulate what service(s) IT is providing to the user, at what service level, and at what cost. Users can negotiate with IT and trade service levels for cost. Once IT exposes service levels and costs in this way it often opens the door to competition from outside service providers (outsourcers), which typically results in market conditions and more efficient IT services. At the same time, SLAs often result in improved behavior from the business units. By exposing costs, the business units have a much better understanding of the implications of their requests for IT services. Ultimately, SLAs should help both IT and business units make better decisions about IT services.
- **Chargeback mechanisms.** Chargeback mechanisms can work in tandem with SLAs or by themselves. The objective is to chargeback the costs of shared services to the business units that

consume them. By IT having a better understanding of its costs, it can demonstrate the savings and efficiencies that result from shared services. At the same time, the business units can better rationalize their behavior with respect to their requirements for IT. With full cost transparency, better decisions can be made by both IT and business units with respect to the acquisition and deployment of IT assets.

- **Demand management.** Demands for IT resources come from all directions and in all forms. Some demand is routine, such as help desk requests and new employee provisioning, while other demand is strategic and complex, such as requests for new applications to support new business opportunities. Demand management forces all IT demand through a single point ,where it can be consolidated, prioritized, and fulfilled. Demand management works hand in hand with IT portfolio management to manage current and future IT investments.

Governance Communications

For IT governance to be effective, it has to be measured and communicated throughout the enterprise. Communicating about IT governance takes on a number of objectives. At the beginning, all employees need to be educated about what IT governance actually does, its importance, and how it's implemented across the enterprise. This communication needs to be continually reinforced.

Measurement is equally important, and a key piece of the communications strategy. The primary objective of IT governance is to optimize the investment in information technology through strong IT/business alignment, ensuring that these investments return value to the enterprise within an acceptable risk envelope.

- **IT Balanced Scorecard.** Once an IT governance model is developed for an organization, it needs to be implemented and then measured. The IT Balanced Scorecard has proven to be an effective tool with respect to IT governance, and consists of four perspectives: IT Value, User, Operational Excellence, and Future Orientation. Two of the Scorecard perspectives contain measures for the two key governance objectives: IT value and risk management. The IT value perspective contains specific measures for IT/business alignment and IT value, while the operational excellence perspective contains specific measures for managing IT risk.
- **IT portal.** Portals have become the premier method of choice for communicating company information. The IT organization should create an IT governance Web site. This site can then be used to communicate information about IT governance. It can also contain performance reports and information about project status, as well as serving as a repository for governance-related documents including architecture and standards documents, business case templates, and ROI models.

RECOMMENDATIONS

GOOD IT GOVERNANCE IS STRAIGHTFORWARD

Good IT governance isn't rocket science, but it requires discipline and commitment. Governance needs to adapt to the organizational structures, culture, and overall strategy of the company.

- **Executive buy-in is essential.** Once the decision is made to develop a framework for good IT governance, the first step is to get buy in from the board of directors and executive management, since IT governance is a subset of enterprise governance. Often the demand for an IT governance framework comes from the board or CEO.
- **Develop structures first.** It is important to develop the governance structures first. If the CIO is not at the executive level, consider doing this first. While it is not impossible to implement IT governance if the CIO is not a member of the executive team, it does make things more difficult. At a minimum, appoint an IT steering committee to review, approve, and prioritize IT investment, and an architecture committee to develop, communicate, and enforce enterprise architecture and IT standards.
- **Develop processes next.** Forrester strongly recommends adapting an IT portfolio management process for a comprehensive, enterprisewide picture of investments. Follow this with a demand management process. SLAs and chargeback mechanisms can come later.
- **Don't start from scratch.** Review the existing frameworks including COBIT, ITIL, and ISO 17799. Don't be afraid to borrow pieces from each of these when developing your own IT governance framework. If you are concerned about your risk management and compliance posture, lean heavily on COBIT. If service delivery is challenging, have a look at ITIL. If security is an issue, be sure to look at ISO 17799.
- **Communicate, communicate, communicate.** IT governance must be explained and continuously reinforced if it is to ever gain traction. Furthermore, it must be measured to determine what impact it is having. Forrester recommends that the balanced scorecard be adopted as the primary performance measurement and management methodology for IT governance.

ENDNOTES

- ¹ While surveys put planned budget increases at a lower level, Forrester predicts a 7% increase in US IT spending, as well as a 4% increase in Canada. See the November 19, 2004, Trends "North American IT Spending In 2005."
- ² In an effort to strengthen its IT governance, FedEx has established board oversight of IT. Additional information can be found at <http://ir.fedex.com/governance/board.cfm>.
- ³ The "Board Briefing on IT Governance" from the IT Governance Institute goes into much detail on the role of IT governance as part of enterprise governance.

- ⁴ The IT Governance Institute and COBIT can be found at <http://www.itgi.org>.
- ⁵ More information on ITIL can be found at <http://www.ogc.gov.uk/index.asp?id=2261>.
- ⁶ Information about ISO 17799 can be found at <http://www.iso17799software.com>.
- ⁷ A majority of companies now have an IT steering committee, but closer inspection reveals that not all of the committees are necessarily powerful and/or effective at what they do. There are a number of steps a CIO can take to ensure that the IT steering committee meets this test, as well as a number of pitfalls to avoid. See the July 9, 2003, IdeaByte “IT Governance: Steering Committee Do’s And Don’ts.”
- ⁸ IT asset management, applications portfolio management, and project portfolio management are explained as components of IT portfolio management. See the January 6, 2003, Planning Assumption “Maximizing IT Value: Portfolio Management Options For 2003.”

FORRESTER®

Helping Business Thrive On Technology Change

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617/613-6000
Fax: +1 617/613-5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia	Japan
Brazil	Korea
Canada	The Netherlands
France	Sweden
Germany	Switzerland
Hong Kong	United Kingdom
India	United States
Israel	

*For a complete list of worldwide locations,
visit www.forrester.com/about.*

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866/367-7378, +1 617/617-5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.