IT excellence starts with governance

Nick Robinson

Nick Robinson (nick.robinson@ey.com) is a manager in Ernst & Young's Technology & Security Risk Services Practice, Charlotte, North Carolina, USA.

Abstract

Purpose – *To explain how information technology (IT) governance enables an organization to achieve three vital objectives: regulatory and legal compliance, operational excellence, and optimal risk management.*

Design/methodology/approach – *Describes the role in IT governance of functions such as value creation (distilling company's mission and strategic direction into business needs for IT applications), value delivery (formal project management methodology and system development life cycle), value preservation (integrated control and risk management program), resource management, performance management (capability maturity model, balanced scorecard, Six Sigma), and oversight. Describes governance frameworks such as COBIT, ITIL, and ISO/IEC 17799: 2000. Offers advice on getting started.*

Findings – *When governance is effective, IT becomes a valued asset, inseparable from the business and regarded as an asset, not a cost.*

Originality/value – *Helps a compliance officer think about the connection between effective IT and compliance systems.*

Keywords *Communication technologies, Governance, Risk management*

Paper type *Viewpoint*

IT governance is emerging as the antidote to anemic IT performance, paving the way to more effective use of technology in supporting business needs. The pervasive nature of IT as a business enabler obscures some harsh realities about IT performance. Contrary to conventional wisdom, technology-driven increases in productivity have been meager relative to total expenditures. Lackluster IT performance is manifested in failed or aborted projects, missed deadlines, budget overruns, and poor returns on investment (ROI). Increasingly, these indications of low IT effectiveness are shining a spotlight on the need for IT governance as a vehicle for bolstering performance. Further fueling the emphasis on IT governance is the enactment of regulations such as the Sarbanes-Oxley Act, with its requirement for stronger controls over financial reporting to prevent a recurrence of recent high-profile corporate scandals.

Ask for a definition of IT governance and you will probably get a variety of answers. However, the central theme running through the responses is that the goal of IT governance is to create a control environment for desirable actions to drive the effective, efficient, and secure use of information technology. A control environment is shaped by the attitudes, abilities, awareness, and actions of the board and management regarding controls within the organization. It includes factors such as management's integrity, ethical values, philosophy, and operating style.

Note, too, that both corporate governance and IT governance are integral to enterprise risk management (ERM). An IT governance framework should not exist in isolation from either the

overarching corporate governance model or the ERM model – or, for that matter, from the company's compliance culture.

A three-legged stool

IT governance enables an organization to attain three vital objectives: regulatory and legal compliance, operational excellence, and optimal risk management.

Regulatory and legal compliance

The Sarbanes-Oxley Act, which implicitly mandates transparency, clear accountability, and rigorous internal controls, highlights the importance of both corporate and IT governance as the vital oversight apparatus for an organization. Other regulations, such as Basel II, with its focus on operational risk, demonstrate that this trend toward disclosure is growing.

Ironically, however, transparency can be a two-edged sword. It bolsters market confidence, but failures, whether due to operational or technical malfunction, become immediately apparent to users, with a direct impact on business operations. Thus, as regulators and shareholders continue to demand and mandate greater transparency, weaknesses in the IT infrastructure are becoming more visible.

Operational excellence

Senior IT management has grown increasingly frustrated with its inability to clearly and succinctly articulate ROI from IT expenditures. While the goal is to achieve operational excellence, the absence of clearly defined performance measures often leaves leadership ill-equipped to provide an accurate analysis of the state of IT.

In their book *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results* (Boston: Harvard Business School Publishing, 2004), Peter Weill of MIT's Sloan School of Management and Jeanne W. Ross of MIT's Center for Information Systems Research describe their study of 250 enterprises worldwide that have demonstrated superior governance. They conclude that an effective IT governance structure is the single most important predictor of whether an organization will derive value from IT. Furthermore, they establish that companies that have followed specific strategies and demonstrated above-average governance have had 20 percent higher profits than companies that have followed the same strategies but had poor governance. Other studies reinforce Weill's and Ross' findings.

Risk management and optimization

To survive and thrive in today's highly competitive business environment, companies need more adaptive and agile IT solutions, which inevitably translate into higher levels of technology and operational risk. An IT governance program defines the IT structure, measures, and monitoring framework needed to effectively identify and manage risk.

Achieving the objectives

To attain the objectives described above, an IT organization must ensure that business value is created and delivered in the most cost-effective and efficient manner (operational excellence), that risks are identified and controlled (risk management/optimization) and that the IT organization has a structure in place to assure effective oversight (regulatory and legal compliance). The following functions all play a critical role in this effort and are essential steps in creating and sustaining effective IT governance practices:

Value creation

To create IT value, the company's mission and strategic direction must be distilled into business needs for IT applications. This requires alignment of the company's business, operational, and IT strategies. Mechanisms should be in place to ensure that the respective planning functions cross-pollinate and remain synchronized, so that business needs are met on an ongoing basis. An IT investment and prioritization process should be in place,

facilitated by an IT strategy or steering committee, to provide a way to assess the cost/benefits of the IT investment.

Value delivery

A formal project management methodology and system development life cycle (SDLC) is needed to ensure that IT value is delivered to businesses on time, within budget, and at the required level of quality. A strong SDLC methodology, used in conjunction with a well crafted IT architecture, enables the delivery of IT services that are integrated, consolidated, and standardized. Operational effectiveness and efficiencies are maximized by the use of service-level agreements (SLA). Third-party management and sourcing decisions should be made in partnership with the business and IT, and a process should be in place to translate the necessary SLA and quality requirements into contractual obligations.

Value preservation

An integrated internal control and risk management program enables an organization to sustain the value that has been created. It also ensures compliance with Sarbanes-Oxley, which mandates the establishment of a control and risk management framework. Risk management should be a continuous process of impact analysis and risk identification and should include risk mitigation strategies – for example, disaster recovery and business continuity.

Resource management

Resource management ensures that the right IT capabilities for business needs are identified and deployed. It targets IT infrastructure management to assure implementation of an integrated, economical IT infrastructure. Resource management focuses on people in terms of their availability, training, competencies, and retention; and it does so through both in-house and outsourcing models. Project and infrastructure funds are allocated through an IT investment portfolio process based on a cost-benefit approach.

Performance management

The need to manage performance spans all of the preceding areas. Measures for strategy implementation, project completion, resource usage, service levels, process performance, and service delivery can be monitored and analyzed by the use of quality and continuous improvement methodologies such as:

- *The Capability Maturity Model.* An organizational model for achieving product and process improvement. It describes five evolutionary stages (levels) in which an organization manages its processes.
- *The Balanced Scorecard.* Enables organizations to clarify their vision and strategy and translate them into action. It provides feedback about both the internal business processes and external outcomes in order to continuously improve strategic performance and results. The balanced scorecard focuses specifically on four areas of the business: financial, customer, internal, and learning.
- *Six Sigma.* A measure of quality that strives for near perfection. The methodology incorporates data and statistical analysis into a project-based workflow that allows businesses to make intelligent decisions about where and how to incorporate improvements.

Oversight

IT governance is an inseparable element of good corporate governance and as such should instill a culture of integrity, accountability, and transparency. Effective oversight in support of these principles is achieved by ensuring clarity of roles and clearly defined responsibilities and by embedding effective decision-making organizational structures throughout the company.

Governance frameworks

Fortunately, companies can ease their venture into IT governance by leveraging various industry-standard frameworks. Many are well established and embrace sound practices. Most frameworks provide the requisite support materials in the form of roadmaps, guides, templates, and samples. While these are not turn-key methodologies that will magically embed IT governance into your organization, the frameworks provide a foundation for creating a governance structure.

Each governance framework has its own idiosyncrasies and strengths. While they tend to have been developed to serve specific aspects of IT governance, many share similar concepts, even if the terminology is somewhat different. Ongoing initiatives are underway to harmonize and integrate the leading frameworks to achieve greater compatibility. The three leading and most widely adopted frameworks are:

1. *COBIT*. Control Objectives for Information and related Technology was originally released as an IT process and control framework linking IT to business requirements. It has since morphed into the de facto IT governance standard. COBIT is an open standard for control over information technology and is independent of the software and hardware platform. It is maintained and refreshed on a four-year cycle by the IT Governance Institute.
2. *ITIL*. Information Technology Infrastructure Library (BS1500) is pegged as the de facto standard for service management and delivery. It defines IT quality as the level of alignment between IT services and actual business needs. ITIL meshes relatively well with the COBIT framework. Broadly, COBIT articulates what has to be done, whereas ITIL provides the practical steps to answer how it should be done and who should perform each task.
3. *ISO/IEC 17799: 2000*. The Code of Practice for Information Security Management is a widely accepted set of guidelines and controls for information security. The controls are either based on essential legislative requirements or considered best practices for implementing information security management.

Getting started

IT governance should not be approached in a haphazard manner. It demands careful thought about who makes decisions and how those decisions are made. Invariably, not all these decisions will be favorably received by the stakeholders, so communication is vital. Implementation plans and schedules need to be formalized, and all initiatives should have executive sponsorship and be supported by all levels of leadership within the organization.

For IT governance to be effective, two of its complementary facets need consideration. The first is some form of entrustment framework that encourages and cultivates responsibility by assigning decision rights and accountability to certain individuals or groups. The other facet is a framework that provides the rules and controls. At the apex of this framework are IT principles that encapsulate the essence of the firm's future direction and how IT should be used. In support of these principles are control mechanisms comprising organizational and decision-making structures, policies, standards, and procedures.

This naturally leads to the question: ''Where do we start?'' Company-specific variables make a boilerplate answer impossible. Factors such as the role of IT in the organization, the business's operating model, and management's risk appetite all will invariably mold the style and pattern of IT governance in a specific organization.

The initial stimulus that precipitated the need to change typically provides an indication of where to embark on an effort. If reducing high operating cost is the change driver, then concentrating effort on value delivery and performance management makes sense. Alternatively, if the company wants to increase its market share, there should be an emphasis on value creation. Other examples of change drivers include outsourcing, a drive to a service-based IT architecture, or an external event, such as new regulations or legislative changes.

Typically, an initiative will take the form of either an assessment (benchmark) project or an improvement project. Whichever approach is adopted, companies generally get better results from using established IT governance frameworks than from flying solo.

In an assessment project, an initial high-level review is conducted to evaluate the general status of IT governance within the organization and determine whether the primary elements of an IT governance framework are in place. A more detailed assessment will then unearth actual weaknesses and provide a basis for prioritizing remediation efforts.

In an improvement project, a needs assessment is performed to identify the relative severity of the weakness and the risks it poses, and to identify and isolate the areas affected (processes, mechanisms, organization structures). This is followed by a gap analysis of the current versus required state that will help to define the form and scale of the remediation effort. Once the remediation project has been implemented, measures are integrated into an IT balanced scorecard to ensure ongoing effectiveness.

We can think of governance as a sextant that guides companies through the galaxy of technological complexities and business challenges. It cultivates desirable behavioral patterns and provides the oversight mechanisms to ensure the sound use of IT, operational excellence, and legal and regulatory compliance. When governance is effective, IT becomes a valued asset, inseparable from the business and regarded as an investment, not a cost. In short, IT governance provides the essential bedrock for the effective acquisition and deployment of technology.