Gartner Research

Publication Date: 17 November 2009 ID Number: G00172463

IT Governance Must Be Driven by Corporate Governance

Julie Short, Michael Gerrard

IT governance is driven by good corporate governance. CIOs and other IT leaders need to understand these principles and how to obtain senior business participation in IT governance.

Key Findings

- Corporate governance is an important input for defining IT governance.
- IT governance must ensure that IT risks are effectively managed.
- IT governance requires senior business participation, especially at the board level.

Recommendations

- CIOs must understand the specific principles of corporate governance that drive IT governance.
- Use principles of corporate governance and the most appropriate resources to gain board and senior executive support and participation in IT governance.
- Use a variety of resources to ensure board-level involvement in IT governance.

ANALYSIS

Good corporate governance is vital for business viability. A collapse of trust in corporate governance and management over the past 10 years has led to increased regulation in the U.S. (for example, the Sarbanes-Oxley Act), and new regulatory initiatives in Europe and other developed countries, making good corporate governance mandatory. Professional investors are willing to pay a premium for companies with strong, effective corporate governance. However, IT management, which is considered to be the guardian of key IT corporate assets, often struggles to implement effective IT governance aligned to corporate governance goals.

What Is Corporate Governance, and How Does It Influence IT Governance?

Corporate governance is not new but has received heightened attention in the wake of corporate scandals, such as Enron, WorldCom, Tyco, Parmalat and others. With the recent financial crisis, corporate governance has again been reviewed and weaknesses noted. Effective implementation of risk management, board practices and the exercise of shareholder/stakeholder rights are under close scrutiny.

Corporate governance provides the structure for determining organizational goals, allocating the authority to achieve them and monitoring performance to ensure that those objectives are attained. Good corporate governance is also important in nonprofit and governmental organizations where foundations, sponsors, taxpayers or other stakeholders are equally concerned that their organization is governed appropriately.

Although several principles of corporate governance influence IT governance, there are two where this influence is substantial:

- **Disclosure and transparency —** This refers to the financial and operational information of the organization and foreseeable risk factors.
- **Responsibility of the board of directors —** This involves ensuring strategic guidance to the organization, effective monitoring and responsibility to shareholders/stakeholders.

Although the degree of liability varies from country to country, board members are expected to act in the best interest of shareholders/stakeholders (and may be legally bound to do so), to approve strategy, to oversee management, to make key decisions, and to approve the systems of risk oversight and internal control. Capital spending on IT assets may be as much as 50% of the total capital spending in some organizations.

However, when it comes to managing those assets, few boards understand how much their organizations rely on IT for continuing operations and information assets that reside in numerous applications in their infrastructure. Few realize how much of a role IT plays in enabling (or hindering) their business strategy. Few boards realize how many business decisions rely on the information contained in these assets. Even fewer have the fundamental knowledge needed to ensure that the appropriate oversight is in place. These issues, however, do not relieve them of responsibility to ensure that the company's IT assets are governed appropriately.

Although corporate governance has been formalized for a long time, the concept of IT governance is somewhat more recent. What is meant by IT governance? It is not simply the management of IT but refers to how organizations must ensure that IT assets deliver business value and whose performance is measured and risks are mitigated.

Until recently, there has not been a significant body of knowledge on the topic. The IT Governance Institute (ITGI), — an offshoot of the Information Systems Audit and Control Association (ISACA) — is a recognized leader in governance, control, security and assurance. It was formed in 1998. In 2009, the ITGI adopted the ISO/IEC 38500 IT governance standard, which is based on a pre-existing Australian standard and has been in place since April 2008. It represents an effort to provide guidance in defining IT governance as a component of corporate governance and is intended for all organizations, regardless of size or sector.

As with all governance, there is no one-size-fits-all solution. Effective IT governance must be a cohesive, integrated process aligned with the business, compatible with the management decision-making style and culture, and perceived by business management as providing value. Too often, IT governance has been left primarily to the CIO without engaging the board, which has responsibility to understand the inherent risks and strategic importance of IT. Boards must be more involved in IT governance to ensure that their organizations will be able to sustain operations and implement future strategies.

IT Governance: Demand- and Supply-Side

Gartner's IT Governance Demand/Supply Model (see "Defining IT Governance: The Gartner IT Governance Demand/Supply Model") clearly states that IT governance is a business goal, not just an IT goal. IT governance is defined as addressing two main areas: demand-side governance (deciding what IT should work on) and supply-side governance (deciding how IT should do what it does). Demand-side governance is a management investment decision-making and oversight process; therefore, it is primarily a business management responsibility, driven by the decision authority delegated under the corporate governance umbrella. Supply-side governance is primarily the CIO's responsibility and is the mechanism that ensures compliance with corporate policies, such as those addressing regulatory compliance, security and procurement.

In speaking with clients, Gartner sees the lines between the business and IT becoming more blurred. We see IT tasks being performed in the business, business taking on IT leadership roles and vice versa. However, when it comes to IT governance, we see that often this is erroneously delegated to the CIO due to several factors:

- A lack of business understanding regarding the role of the board in ensuring that IT assets and resources are managed and measured, and that IT risks are mitigated.
- A perception that anything IT needs should be handled by the CIO.
- Competing factions within IT, all wanting governance over their respective domains.

As a result, the term "governance" has become overused and misunderstood. IT leaders should understand that IT governance is effective when it is driven by corporate governance and defined as a cohesive process by using five steps: strategize, plan, implement, manage and monitor (see "Defining IT Governance: Roles and Relationships").

IT governance must integrate all IT governance structures by identifying the appropriate touchpoints, and using relevant inputs and outputs from other structures. Although supply-side governance involves significantly more CIO responsibility than demand governance, it is vital that supply-side IT governance include and address the corporate governance policies aimed at ensuring that the board meets its responsibilities to shareholders/stakeholders.

At the same time, the board is accountable for demand-side IT governance and must take the lead by providing direction for ensuring that the organization's resources are effectively managed and protected. The only way to do this is to ensure that all IT governance — whether demand- or supply-side — meets the principles defined in corporate governance.

Align Supply to Demand Using Principles of Corporate Governance

CIOs must ensure that they understand the principles of corporate governance, specifically disclosure and transparency, and the responsibilities of the board. Knowledge of these principles can help IT leaders gain the business involvement they need. They are widely accepted or even mandated by law in many countries. They are also well-understood by senior executives and are of great interest, because key executives (for example, the CEO, the CFO and board members) can be personally liable for breaches to these principles.

CIOs should create a bridge of understanding with senior executives, linking the principles and the responsibilities of management with the functions and processes of IT. A common understanding in this area can help both sides to better integrate business and IT management, thereby gaining more business participation in demand-side governance and driving the approach and policies of supply-side governance. It can lead to more clearly establishing IT governance as a component of corporate governance.

Disclosure and Transparency

This principle has two key aspects that impact IT governance. First, it provides for disclosure on material matters affecting the financial situation of the organization, issues affecting stakeholders, and — more importantly — foreseeable risk factors. Second, it provides for an independent annual audit that provides an external and objective assurance to the board regarding the financial situation of the organization. It further clarifies that these external auditors are accountable to the shareholder/stakeholders of the organization (see "Transparency Provides Opportunities and Threats in the 21st Century").

In today's environment, companies are heavily reliant on the reliability and accuracy of the IT systems (that is, the applications, information and infrastructure) containing their financial information. Using the principle of disclosure and transparency, IT governance has a duty to ensure that these components are available, reliable, and accurate.

It follows that, if these systems are poorly architected (from a technical or business standpoint), or if the infrastructure has reached its end of life, is complex or is impossible to recover for any reason, the impact on the principle of disclosure and transparency can be significant. Other examples include: if the IT assets are not adequately protected from security threats (internal or external) or if projects are not delivered on time, on budget or do not produce the anticipated business results.

Responsibility of the Board

The board's responsibility broadly encompasses the heart of corporate governance. A lack of board oversight of IT activities can put an organization in as much risk as a lack of underlying controls ensuring the quality of financial reporting. Board members and senior management go to great lengths to ensure that they pass external audits without considering the IT systems that store and report this information.

Most companies are spending increasingly significant amounts on IT assets. If those assets are not properly overseen, it follows that a lack of board involvement in the acquisition, management, and monitoring of those assets can negatively impact the effective governance of an organization. Board members need to understand the nature of the organization's reliance on IT as a first step in determining the appropriate governance arrangements.

In companies where the reliance on IT is more operational and tactical, but the organization could be adversely affected if IT systems are not available, boards need assurance that the organization is adequately protected against operational events, such as unplanned outages and security breaches (for example, viruses, hacking, etc.). They must also ensure that there are effective operational controls for the management of IT costs. If the role and reliance on IT is more strategic in nature (e.g., if the organization relies on technology as part of an effort to compete effectively or to differentiate itself), there may be a need for substantive board involvement.

Boards need assurance that the enterprise architecture (business information, solutions and technology) is aligned with the business strategy. The architecture should enable IT to respond quickly to new and changing business requirements in an efficient manner. More importantly, they need assurance that the enterprise architecture is positioned to ensure the ongoing and future success of the organization.

Projects involving IT are notorious because of high failure rates. Recent studies indicate that approximately 25% completely fail and an additional 40% are not delivered on time, on budget, or with full functionality and features. There is significant risk in projects, and large, strategic projects involve even greater risks. It is the board's responsibility to put in place governance that will ensure that risks are understood and mitigated.

What Can a CIO Do to Obtain the Involvement of the Board?

Many of Gartner's clients say they cannot get the attention and involvement of the board to participate in IT governance. CIOs need to employ strategies that are aimed at obtaining this involvement. In this case, some creative measures are required. Some ideas to obtain this involvement include:

- Increase the knowledge and awareness of the principles of corporate governance among the IT management team.
- Use available resources (such as enterprise architecture, security and compliance, infrastructure, and operations and project management teams) to ensure a common understanding of what is in place and where the likely risk candidates are. You will need to have this information on hand to deliver facts to the board.
- Create a coalition of supporters (e.g., corporate governance officers, chief internal auditors, enterprise risk officers or CISOs) to craft and send coordinated messages to the board.
- Use current relationships with senior business management as a means of sponsoring engagement with board members.

IT Is Part of the Business

The bottom line is that IT is an integral part of the business. Organizations should consider IT to be just as critical to the organization's success (or failure) as any other business unit. Business and IT leaders should regard IT governance as an opportunity to better integrate the two areas of business and IT and move toward a more cohesive model, providing a better understanding of the role of IT in the organization and enabling IT to contribute its share to meeting the principles of corporate governance.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner