



Exploring the Audit Committee's Role in IT Governance

KPMG LLP

IT Governance: a Critical Imperative

Information and IT are...

- ◆ Vital to the Financial Reporting Process
- ◆ Integral to Compliance
- ◆ Essential to the Business
- ◆ Increasingly Complex
- ◆ Becoming Even More Important...but May Lack Focus and Attention at the Board Level

Lack of IT Governance/Focus

- ◆ **Only 9% of audit committee members are “very satisfied” that their audit committee devotes sufficient agenda time to the oversight of IT risk** (ACI/NACD Annual Audit Committee Member Survey, 2007).
- ◆ **59% of organizations have either no process, or only an informal process, to measure the realization of IT investment benefits** (KPMG Global IT Project Management Survey, 2005).
- ◆ **84% of large North American companies experienced an IT security breach in the past year; 38% of breaches were internal, and 62% external** (Computer Associates International Survey, 2006).
- ◆ **40% of all IT spending brings no return to the organization** (2004 IBM survey of Fortune 1000 CIOs).

A Need for IT Governance

Examples of Critical Business Information

- ◆ Marketing and Sales
- ◆ Customer Information
- ◆ Employee Information
- ◆ Operations
- ◆ Quality Control
- ◆ Supply Chain, Procurement
- ◆ Project Management
- ◆ Service Order and Transaction Processing
- ◆ Customer Service and Care
- ◆ Financial Transactions
- ◆ Warehousing, Distribution, and Delivery
- ◆ Inventory Management
- ◆ Regulatory/Legal Compliance
- ◆ Strategic Planning, Budgeting

Focusing on Information Quality

- ◆ Accurate
- ◆ Complete
- ◆ Relevant
- ◆ Transparent
- ◆ Fresh/Current
- ◆ Availability
- ◆ Secure (protected from unwarranted access and modification)
- ◆ Satisfies legal/regulatory requirements
- ◆ Cost effective

Impediments to Information Quality

- ◆ **Manual Processes**
- ◆ **Complex IT Architecture**
- ◆ **Distributive Processing**
- ◆ **Lack of Standardization**
- ◆ **Poor System Integration**
- ◆ **Software Systems Fail to Test for Anomalies**

Examples of Information Reliability and Security Risks

- ◆ Information quality
- ◆ Privacy and security
- ◆ Outsourcing
- ◆ Business continuity/disaster planning

Who/What protects the company against these risks, and ensures that the information is accurate and secure?

Complexity of Critical IT Projects Poses Risks

- ◆ Adequacy of project management and related processes
- ◆ Do we really understand status of critical IT projects?
- ◆ Possible plans to deal with IT project delays and difficulties
- ◆ Risk of IT project failure
- ◆ Alternatives to successful project

IT Governance Oversight Challenges

- ◆ **“IT” is often a “foreign language,” lacking business context**
- ◆ **Fragmented IT governance (people, responsibilities, policies)**
- ◆ **Tone at the Top**

Alignment of Oversight Responsibilities for IT Governance - What Makes Sense?

- ◆ **Oversight of Financial Reporting-Related Information Risks**
- ◆ **Oversight of Other Information Reliability and Security Risks**
 - Poor information quality
 - Information privacy and security
 - Outsourcing
 - Business continuity/disaster planning
- ◆ **Oversight of Information Strategy and Investments**
 - IT project risks
 - Strategic alignment of IT investments
 - Prioritization of IT spending
 - Measurement of IT performance
 - Management of IT resources

Considerations for the Audit Committee

1. **Is management's IT governance process effective, with clearly identified and capable leaders?**
2. **Are the IT oversight responsibilities of the audit committee, board, and other standing committees clear? Does the board have adequate IT expertise?**
3. **If there is a language barrier, how can it be removed? Is there a need for audit committee/board education?**
4. **Are you satisfied that standing committees with IT oversight responsibilities effectively communicate and coordinate their oversight activities?**
5. **Does the audit committee devote sufficient agenda time to IT? Do the "right" senior managers brief the audit committee—as a regular agenda item—on information risks?**
6. **Is the audit committee obtaining independent assurance regarding the mitigation of significant information risks? Are audit plans focused on the major IT risks?**

Questions?
