Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges

Gary Hardy

Abstract

With Sarbanes–Oxley and other legislation, securing IT within a company has become law. This article takes a look at how compliance legislation can be used to get more support from the Board when it comes to security issues, and how information assets still need to be protected further.

1. Introduction

Controlling and securing information technology (IT) within an organization used to be considered a nicety, but today the stakes are much higher. With Sarbanes–Oxley (SOX) in the U.S. and other legislation enacted worldwide, effective governance over IT has become law for many companies.

Just one successful security breach, theft, error, hack or virus attack on a company’s IT can result in serious financial and reputation damage. As a result, regulators, investors, employees, customers and vendors are concerned about the safety and privacy of their organizations’ information and IT.

Although significant progress has been achieved, most businesses still have not established adequate control over IT. According to the 2005 survey, Information Risks: Whose Business Are They?, for which 200 IT professionals in 14 countries were polled by the IT Governance Institute (ITGI), fewer than one-quarter of the participating organizations reported that they review external risks and threats on a regular basis. This is worrying, given the extensive use of outsourcing and service providers and the globalization of businesses using IT.

Senior management and boards of directors should ensure that their organizations’ information assets are protected. IT governance should be a top concern on their agendas and be regularly addressed by senior executives in co-operation with their IT and IT security departments.

To provide effective oversight that will help keep their organization on track with its business strategy, boards of directors and other business executives need to understand their evolving roles in governance over IT. Basically, it is vital they apply to IT the same level of supervision that they give to all major assets.

Board and executive duties generally focus on cost-efficiency, revenue enhancement and building capabilities, all of which are integrated with information and the IT infrastructure. Because IT is such a driving force within an enterprise, and its solutions are becoming increasingly complex (e.g., outsourcing, third-party contracts, global networking), effective governance over IT is a critical factor of overall success.

In years past, IT was the sole domain of an IT department that operated separately from other business units. Boards and executives were kept in the loop only via occasional vague progress reports for ongoing projects and, thus, were often disappointed with outcomes beset by cost overruns, inefficient performance, fraud and dissatisfied users. Not surprisingly, IT and other departments pointed fingers of blame at each other. Large scale projects were abandoned after significant time, costs and manpower were expended. Now that legislation such as Sarbanes–Oxley in the U.S. and other regulations worldwide have been enacted, effective governance over IT is no longer just a smart thing to do. Executives have
to sign off on assurances, and they risk significant financial and legal repercussions if their organization is not adequately controlled and secured.

2. What is IT governance?

IT governance responsibilities are one aspect of a broad framework of enterprise governance, which is thoroughly discussed in the Principles of Corporate Governance issued by the Organisation for Economic Co-operation and Development (OECD). The document notes that the board’s responsibilities include reviewing and guiding corporate strategy, setting and monitoring management performance objectives, and ensuring the integrity of the enterprise’s systems.

The Bank for International Settlements (BIS) states that IT should be addressed like any other strategic agenda item of the board, and that for critical IT systems, governance should be effective, transparent and accountable.

Clearly, IT governance is the responsibility of the board of directors and executive management, and oversight responsibilities have changed and expanded greatly.

The overall objective for boards and executives driving IT governance should be to understand the issues and the strategic importance of IT so their enterprises can sustain operations and expand upon activities as they move into the future. IT governance activities should focus on ensuring whether expectations for IT are met, and that IT risks – and there will always be risks – are addressed.

This is all good information, but busy executives and board members need more specific guidance on how to achieve that vaunted goal of effective control. Advice to boards traditionally is focused on structure, composition, size and independence. Details on topics such as high-level IT risk management and practical aspects of governance over IT are harder to find. Despite the potential for huge losses, whether monetary or to an organization’s reputation and hard-earned good will, far too few boards provide thorough governance over IT.

The IT Governance Institute (ITGI), the non-profit, research-focused affiliate of the, non-profit Information Systems Audit and Control Association (ISACA), recognized this need and has developed an extensive library of materials – many available as free downloads from its web site (www.itgi.org).

In Board Briefing on IT governance, 2nd edition, boards and executives are encouraged to make sure processes are in place to:

- align IT strategy with the overall business strategy
- cascade IT strategy and goals throughout the enterprise
- ensure structure is in place to support strategies and goals
- provide strong, supportive messages about the importance of IT governance
- insist the organization adopt a globally recognized IT control framework (such as COBIT)
- use metrics to monitor and measure IT performance

In reality, IT governance oversight among board members is still lagging. After commissioning a survey of 335 CEOs, CIOs and other executives in 21 countries across all continents, ITGI found that while more than 91% of executives recognize that IT is vital to the success of their businesses, more than two-thirds of CEOs are not comfortable answering questions about governance and control over their IT processes.

On the other hand, the IT Governance Global Status Report also found a clear positive relationship between the effectiveness of IT governance measures and the frequency with which IT is discussed at the board level. Executives who said IT is always on the board agenda reported better measurement of IT performance, better management of IT and risks, better value and better alignment of IT with company strategy.

Based on the maturity model (see Box 1), it is clear that, fundamentally, IT governance pinpoints attention on two key issues – the value IT delivers to an organization, and the control and mitigation of IT-related risks. This leads to five focus areas of IT governance, which are all driven by stakeholder value: strategic alignment, value delivery, risk management, resource management (which overlays all of the areas), and performance measurement. The first two are outcomes, the last three are drivers.

All five domains should be regular items on the board agenda. Key facets for boards to consider about the domains are as follows.

Strategic alignment

Boards are encouraged to drive strategic alignment by ensuring that IT strategies are in harmony with business strategies; ensuring that IT deliverables are on-time, within budget, and possess appropriate functionality and benefits; balancing IT investments between systems that support the enterprise as is and those that help the business grow and compete in new arenas; and making decisions about the focus of IT resources, that is, directing resources to break into new markets, drive competitive strategies, improve customer satisfaction and/or assure customer retention.

Value delivery

Effective value delivery can be achieved only if the actual costs and ROI are managed. Boards should ensure IT is aligned to deliver value by ensuring infrastructures that enable the enterprise to grow by breaking into new markets, increasing overall revenue, improving customer satisfaction, assuring customer retention and driving competitive strategies.

Risk management

Risk management is driven by the board’s need to demonstrate good enterprise governance to shareholders, regulators, employees, vendors and customers. The board should manage risk by ascertaining that there is transparency about significant risks to the enterprise and clarifying risk-taking or risk-avoidance policies. The board should also insist that risk management be embedded in the operation of the enterprise to ensure quick reporting and response to the ever-changing risk challenges.

Resource management

In addressing resource management, boards should ensure that appropriate methods and adequate skills exist in the organization to manage IT projects, and benefits are real
Box 1. How good is your IT governance?
A key aspect of achieving effective IT governance and increased value is for the board to benchmark a company’s maturity and assess its current status against international standard guidelines, industry’s best practices and the enterprise’s strategy. Boards can rank maturity based on the following scale from the Board Briefing:

0 Nonexistent
There is no senior management oversight of IT-related activities to ensure that the enterprise’s IT goals add value to the organization and to ensure IT-related risks are appropriately managed.

1 Initial/ad hoc
The concept of IT governance does not exist formally and upper management is only involved when there are major problems or successes. Measurement of IT performance is typically limited to technical measures and only within the IT function.

2 Repeatable but intuitive
Regular governance practices, such as review meetings, performance reports and problem investigation, take place, but rely mostly on the initiative of the IT management team. Although there is realization that a more formal process of IT oversight is required, problems are identified and addressed on a project basis.

3 Defined process
Previous informal but successful practices have been institutionalized, and the techniques used are simple and unsophisticated. The board has issued guidance, which is the basis for specific procedures for management covering key governance activities, such as target setting, performance reviews, capability assessments, and project planning and funding.

4 Managed and measurable
The enterprise’s management team is working together to maximize value delivery and manage IT-related risks. Regular assessments of IT capabilities and projects have delivered real improvements to IT’s performance. Results have been communicated to management in the form of a balanced scorecard.

5 Optimized
IT governance’s best practices are followed and automated. The board feels it is in control of the IT strategy. The balanced scorecard focuses on the most important measures relevant to the enterprise’s overall business strategy. The value of IT to the enterprise can be measured and steps are taken on a timely basis to correct significant deviations or problems. The cost of IT is monitored effectively and the organization achieves optimal IT-related results through continuous assessment and improvements.

and achievable. Effective board governance of IT spending can result in significant cost savings and put the organization in the strong position of taking on new, beneficial initiatives.

Performance measurement
Performance measurement through use of an IT balanced scorecard is a highly effective tool for boards and management to achieve alignment. Board members should ensure that reporting via balanced scorecards addresses enterprise contribution, user orientation, operational excellence and future orientation.

Asking tough questions and insisting on thorough answers, demonstrated action and accountability are extremely effective ways for board members to address all domains of IT governance. This is a successful technique for boards to uncover and address issues before they become larger problems. Suggested questions that board can ask focus on three objectives:

To uncover IT issues
Are end users satisfied with IT service and deliverables?
How often and by how much do IT projects go over budget?
How much of the IT effort goes to fire fighting rather than business improvements?
Does IT support the enterprise in complying with regulations and service levels?

To learn how management addresses IT issues
Is there a current inventory of risks relevant to the enterprise?
What has been done to address these risks?
What are other similar organizations doing, and how does the enterprise measure in comparison?
What is industry’s best practice and how does the enterprise compare?
Is the enterprise taking reasonable precautions regarding risks?

To self-assess IT governance practices
Is IT a regular item on the board agenda and is it addressed in a structured manner?
Does the board have a clear view on the major IT investments from a risk and return perspective?
Is the board assured that suitable IT resources, infrastructures and skills are available to meet enterprise strategic objectives?
Does the board receive independent assurance on the achievement of IT objectives and containment of IT risks?

3. IT governance and compliance

Nothing has driven the current climate of intense high-level board attention to IT governance, control and security more powerfully than the Sarbanes-Oxley Act (SOX). Enacted in 2002 after a series of high-profile corporate scandals, SOX has focused high-beam scrutiny not only on enterprise finances, but also on the IT processes that underlie the financial systems of nearly all enterprises.
According to CIO magazine ("How to Dig Out From Under Sarbanes–Oxley," July 2005), “It wasn’t until companies conducted financial risk assessments in early 2004 that it dawned on them: The role IT systems play to ensure the accuracy of financial data is, in fact, critical.”

The Public Company Accounting Oversight Board (PCAOB) in the U.S., the private sector, non-profit corporation created by SOX to oversee the auditors of public companies to protect the interests of investors, concurs. Auditing Standard No. 2 from PCAOB reinforces the importance of IT in the arena of internal control: “The nature and characteristics of a company’s use of information technology in its information system affect the company’s internal control over financial reporting.”

In essence, SOX makes corporate executives explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting. In most organizations, IT is crucial to achieving this objective.

As SOX evolves, IT controls are becoming an even more important element in helping companies meet the stringent corporate governance regulations, since generating reliable reports is key to proving that a company is meeting the requirements of the Act.

The process of complying with SOX can also result in real benefits. Addressing IT issues regularly in the boardroom means that responsibility for compliance becomes shared among all of the necessary players, not just a few. When the CIO and CFO work together to comply with SOX requirements, they end up creating a mutually beneficial approach that synchronizes the internal control approach and the financial reporting process to the financial statements, ensures that IT controls are updated as necessary to correspond with changes in internal control or financial reporting processes, and enables IT participation in the company’s SOX programme management office.

These steps may not reduce the feeling at all levels of management that compliance is just plain hard. It must also be said that a 100% risk-free environment does not exist. SOX and other global legislation will never result in complete assurance of safety, privacy and control. However, building a strong governance model within IT that is designed to ensure accountability and responsiveness to business requirements can lead to more efficient and effective operations, such as:

- Improved enterprise and IT governance
- Increased understanding of IT among non-IT executives
- Better business decision making due to higher-quality, more timely information
- Project initiatives aligned with business requirements
- Compliance with other regulatory requirements, such as privacy
- Enhanced operations with an integrated approach to security, availability and processing integrity
- Optimized risk management
- More efficient prioritization of business and IT initiatives

Boards and executives now need to ensure that if their company is a qualifying US Securities and Exchange Commission (SEC)-registered organization, the company needs to document, evaluate, monitor and report on internal control over financial reporting and disclosure controls and procedures, which include IT controls. The first step in this process, according to IT Control Objectives for Sarbanes–Oxley (ITGI, 2004), is to assess the overall IT organization’s SOX financial reporting controls' status, potentially by asking the following types of questions:

1. Does the Sarbanes–Oxley steering committee understand the risks inherent in IT systems and their impact on compliance with SOX section 404?
2. Have business process owners defined their requirements for financial reporting control?
3. Has IT management implemented suitable IT controls to meet these business requirements?
4. Does the CIO have an advanced knowledge of the types of IT controls necessary to support reliable financial processing?
5. Are policies governing security and processing integrity established, documented and communicated to all members of the IT organization?
6. Are the roles and responsibilities for all those involved in processing financial IT systems related to section 404 documented and understood by all members of the department?
7. Do members of the IT department and all those involved in processing financial IT systems understand their roles, do they possess the requisite skills, are they supported with appropriate skill development and is there involvement by Certified Information Systems Auditors (CISAs)?
8. Is the IT department’s risk assessment process integrated with the company’s overall risk assessment process for financial reporting?
9. Does the IT department document, test, evaluate and remediate IT controls related to financial reporting on an annual basis?
10. Does the IT department have a formal process in place to identify and respond to IT control deficiencies?
11. Is the effectiveness of IT controls monitored and followed up on a regular basis?

Responses to these questions will help executives determine if the IT department and all those involved in processing financial IT systems are integrated with the overall SOX section 404 implementation plan, if the IT department has documented and evaluated IT controls, and if executive management – including the CIO – appreciates the impact that the IT department has on SOX section 404 compliance.

4. How does CobiT help?

SOX requires that organizations implement an appropriate internal control framework such as that from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control-Integrated Framework.

Although PCAOB has not endorsed a specific IT control framework, some auditors have found that Control Objectives for Information and related Technology (COBIT) aligns well with their SOX compliance efforts, according to Internal Auditor ("Sarbanes–Oxley: the IT Dimension," February 2004). The article also notes that the IT Control Objectives for Sarbanes–Oxley publication further clarifies CobiT’s relevance to SOX projects and reveals a high concentration of IT processes around COSO’s “control activities” and “information.
and communication” components. In addition, a survey of Corporate Executive Board members’ SOX compliance found that 67% incorporate COBIT-defined categories into their IT control environment and that others have developed categories that closely align with the COBIT framework.

Supporting this is a Financial Times special report on Understanding IT Governance (17 June 2005), which reported, “Putting an IT governance strategy in place involves rethinking some fairly central relationships—between IT and the board, between IT and the business units, and between the board and the business units. A clearly defined strategy is essential, either using a recognized standard, such as COBIT, ISO17799 or the Information Technology Infrastructure Library (ITIL), or a formal framework drawn up by the board in consultation with the CIO.”

Further, in “A Model for CIO Success,” published in the July 1st issue of CIO Canada, Graham J. McFarlane states that COBIT “is particularly valuable in that it not only describes processes in detail, but also outlines their control objectives and critical quality criteria. It also provides a guideline for self-assessing your organization’s level of maturity in executing each process … and provides a common vocabulary for an IT leadership team to discuss the business of IT.”

Effective IT governance can provide significant benefits to organizations. Instead of viewing compliance with SOX and other regulations worldwide as extra work and a greater expense, forward-thinking companies are achieving enhanced enterprise value as a result of their IT governance initiatives. Effective control and security of IT can be the foundation of improved competitive position, customer satisfaction, staff morale and productivity, reputation, sales and profitability.

5. Governance via COBIT

COBIT – or Control Objectives for Information and related Technology – issued by ITGI, has emerged as the leading globally recognized framework for achieving effective IT governance.

COBIT was first released 10 years ago. Through timely updates – the latest version COBIT 4.0 was released in November 2005 – and valuable related research and publications, the COBIT Framework has proved to help meet the multiple needs of management by bridging the gaps between business risks, control needs, value creation and technical issues.

COBIT provides a sound approach to implementing IT governance-related initiatives in a well-controlled environment. It identifies a set of 34 high-level control objectives grouped into four domains:

• plan and organize,
• acquire and implement,
• deliver and support,
• monitor and evaluate.

A business process owner can ensure that an adequate control system is in place for the IT environment by addressing, as required, those 34 objectives along with more than 200 detailed supporting control objectives.

To further strengthen the link between overall enterprise governance and IT governance, COBIT includes action-oriented and generic guidelines to provide direction for management regarding:

• getting an enterprise’s information and related processes under control,
• monitoring achievement of organizational goals,
• monitoring performance within each IT process,
• benchmarking organizational achievement.

Specifically, COBIT provides maturity models for assessing process capability so that management can map where the organization is positioned currently, where it is in relation to the best-in-class in its industry, where the organization sits with regard to international standards and where it wants to be. The latest release in November 2005, CobiT 4.0, consists of four sections:

• The executive overview
• The framework
• The core content (Control Objectives, Management Guidelines and Maturity Models)
• Appendices (various mappings and cross-references, more maturity model information, reference material, a project description and a glossary)

The core content is divided according to the 34 IT processes. Each process is covered in four sections of approximately one page each, combining to give a complete picture of how to control, manage and measure the process with process descriptions, inputs and outputs, key activities, and RACI charts showing who is responsible and accountable.

Additional COBIT-related publications such as COBIT QuickStart, COBIT Security Baseline, IT Governance Implementation Guide using COBIT and the COBIT mapping documents as well as relating educational programs will be updated early in 2006 to align with the new COBIT 4.0 content.

6. Creating value through IT governance and COBIT

Organizations are continuing to extend beyond their traditional physical boundaries at record rates and many have become true virtual enterprises. In addition to being compliant with SOX and other legislation, these businesses must be available globally 24 h a day, seven days a week, and they require their companies to focus on increasing the value of their IT, while reducing the resulting, ever-changing risks. Strong internal controls and executive accountability can actually filter throughout an organization and create a competitive advantage.

In its 2004 IT Governance Global Status Report, ITGI surveyed 335 CEOs and CIOs in 21 countries, and found that there is a positive relationship between the effectiveness of IT governance measures and the frequency with which IT is discussed
at the board level. Companies that say IT is always on the board agenda reported:

- better measurement of IT performance,
- better management of IT resources,
- better risk management,
- better delivery of business value through IT,
- better alignment of IT with the company strategy.

Within nearly all organizations, the demand for IT investment – both human and financial – far exceeds the resources available to deliver and maintain it. A process is needed to ensure that optimum investments are selected based on criteria free of political or personal bias.

International IT governance control frameworks, such as COBIT, help enterprises take full advantage of their information, thereby maximizing benefits, mitigating risks and capitalizing on business IT-related opportunities. Savvy companies look at effective governance and control over IT as a way to achieve the basic principles of IT value – on-time and within budget delivery of quality IT that achieves its promised benefits. Management can then use COBIT to translate this into increased competitive advantage, customer satisfaction, employee productivity and profitability, and reduced time for order/service fulfillment and customer wait time.

Mitigating IT risks and achieving IT value require a new brand of partnership among IT, business units, boards and executive management. To achieve effective control, board members should be involved in an IT strategy (or similar) committee, CEOs should provide organizational structures to support the IT strategy, CIOs should provide a bridge between IT and the business, all executives should become involved in IT steering committees. Further, all staff members should be made aware of the company’s goals and policies. Today, IT governance is everyone’s responsibility.

7. Case study – COBIT in action at Unisys

Unisys is a global leader in information and technology solutions. In 2004 it had revenue of US $5.8 billion and 36,400 employees. Based in Blue Bell, PA, USA, the company conducts business in more than 100 countries.

As a leading international IT services company, it is important for Unisys to have a standardized IT strategy to support global operations, align the IT infrastructure with the company’s overall business strategy and help comply with SOX. The company evaluated its options and adopted COBIT to provide an effective IT controls and IT governance framework. As a result of implementing COBIT, business processes within IT were improved and SOX-related controls were established.

The overall goal for COBIT was to provide a standardized framework across the entire Unisys IT organization. In addition, COBIT established the framework for SOX controls throughout 2003 and contributed to Unisys SOX certification in 2004. It also formed the basis of core vs. context analysis in 2004 that led to global sourcing activities in late 2004 and 2005.

The company has now evolved an IT governance process that is structured around ROI-based projects, a formalized project initiation process (PIP) and a CEO-led IT Governance Council (ITGC) consisting of the senior business unit executives.

In 2002 the company identified certain controls that needed to be audited. The basic concepts of those controls were explained during the audits and management reviews of the audits. Unisys IT began using COBIT as a framework to design a service-driven approach for internal customers. This implementation of COBIT helped define roles and responsibilities, and continues to help guide modelling of internal processes using Unisys 3D Visible Enterprise (3D-VE) tools. (Unisys 3D-VE is a methodology to see the cause and effect across an enterprise of contemplated infrastructure changes before actually committing resources to the changes.)

In the first two quarters of 2003, a Unisys corporate task team was organized to develop the approach and plan for compliance with SOX section 404. The SOX basic control framework for IT was developed by midyear, and formal and informal training programs were implemented over the next 9 months. The CIO’s staff attended instructor-led classes. Two different webcasts were created for employees, in addition to other specific classes.

In addition to being used for SOX-related controls, COBIT is also implemented by Unisys to help drive process standardization for the software development life cycle (SDLC), where the company has integrated the Rational Unified Process (RUP) and COBIT. Unisys has also utilized COBIT as a guideline for developing its approach for outsourcing work to third parties by identifying processes and tasks within the domains of COBIT that can be outsourced vs. those that are better off being retained internally by Unisys IT.

Companies need a strong governance model in place to approve, prioritize and manage IT investments on an ongoing basis. This is necessary to align IT investments with the business requirements needed to deliver IT value to the company. The process of IT governance must involve the business units at the highest level in a partnership with IT to ensure that effective strategic alignment is achieved. Unisys’ business process within IT has improved as a result of using COBIT for ongoing SOX compliance and other IT governance-related projects.

In relation to the goals of the company’s board of directors and the company’s strategic requirements, COBIT has a number of key attributes that Unisys IT deems important:

- communication – common terminology across IT to discuss policy, standards, process and controls
- quality – comprehensive view of the IT enterprise
- consistency – common approach to solve problems
- credibility – external standard against which to be measured
- maturity – ability to monitor and measure progress over time

As business and IT strategies are further integrated in the future, COBIT should help Unisys remain an agile enterprise with world-class efficiency and effectiveness.
Additional details about Unisys and other COBIT-related case studies are available at www.isaca.org/cobitcasestudies.

Gary Hardy is advisor to the IT Governance Institute (ITGI) and a member of the Information Systems Audit and Control Association. He is a recognized thought leader in IT governance and a lead member of the COBIT management team. Hardy has held director positions with Deloitte, Zergo, and Arthur Andersen, and is currently director of IT Winners, based in South Africa.