Overview

In one of the most controversial cybercrime cases in recent years, Gary McKinnon, a UK based systems administrator, was accused by the US government of hacking into dozens of US military and NASA computers between February 2001 and March 2002. Dozens of critical systems were rendered inoperable, US Naval Air Station files were altered and deleted, and an entire network of 2,000 US Army computers was brought down.
In another incident in 2008, a leading UK bank’s credit card website experienced a sudden surge in visitors. Unable to withstand the load, the site malfunctioned, leaving customers unable to access their accounts for days.

The common factor binding these two otherwise unrelated events is technology, and more specifically, its vulnerabilities. Today, technology forms the backbone of enterprises. Almost all business processes depend on IT in some way or the other. Gartner predicts that in 2010, worldwide IT spending will reach $3.4 trillion. But as the importance of IT increases, so do the associated risks. Chief Information Officer’s (CIO) therefore play a key role. Their ability to straddle both technology and business processes, and build IT while maximizing business benefits, has, in fact, transformed them into key strategic decision makers. However, their task is far from easy.

Another challenge confronting CIOs is that of mergers and acquisitions. Merging two companies with completely disparate processes and technology is an extremely complex process. More often than not, the emphasis is on business alignment rather than on technology integration. Legacy systems only heighten the challenge.

Then there is the ever-present concern over security. The more systems there are to manage, the more difficult it is to control access to applications, maintain lists of authorized users and shut down access to former employees. And those are just internal threats. Phishing, SQL injections, malware, spyware and other sophisticated external threats can also compromise valuable information, causing immense losses.

In response to these risks, governments and federal agencies across the globe have drafted standards and regulations like the Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), Basel II, the Federal Information Security Management Act (FISMA) and the Gramm-Leach-Bliley Act (GLBA). While these regulations help protect customers and shareholders, companies find it increasingly complex and costly to comply with the plethora of regulatory requirements.

Topics covered:

- Hurdles confronting the CIO
- COBIT to the rescue
- COBIT maturity assessment
- The relationship between COBIT and SOX
- Applying COBIT for effective governance

Hurdles confronting the CIO

Today’s IT infrastructures and systems along with the business operations they support are more complex than ever. Distributed computing has resulted in numerous desktop and laptop computers, servers, networks and other IT assets. Complicating matters further is the emergence of newer, more complex technologies such as wireless communication, virtualization and cloud computing. Managing this vast ocean of technology is nothing short of Herculean. Compounding the challenge is the growing size and complexity of organizations. Companies are now expanding their business operations to newer shores, which in turn, expands the scope of technology, as well as the supply and distribution chain. CIOs have to ensure that overall business strategy and objectives are integrated with technology. This can be difficult, given the fact that most business departments including IT, function in silos and define business strategy only in terms of how it affects them.

In response to these risks, governments and federal agencies across the globe have drafted standards and regulations like the Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), Basel II, the Federal Information Security Management Act (FISMA) and the Gramm-Leach-Bliley Act (GLBA). While these regulations help protect customers and shareholders, companies find it increasingly complex and costly to comply with the plethora of regulatory requirements.
COBIT to the rescue

Eliminating the challenges facing CIOs may not be the best solution simply because it prevents companies from fully leveraging the benefits of IT. The key is to control the challenges through effective IT governance. And that’s where COBIT plays a key role.

COBIT or the Control Objectives for Information and Related Technology is a set of best practices for IT management formulated in 1996 by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). The COBIT framework provides a set of internationally recognized guidelines and objectives to help CIOs align IT with business requirements, maximize business benefits, leverage IT resources responsibly and manage risks appropriately.

CIOs aren’t the only ones to benefit. Managers use COBIT to make better IT investments and decisions by defining a strategic IT plan, choosing and implementing the right technology, and monitoring its performance. IT users benefit from COBIT because of the assurance provided to them by COBIT’s defined controls, security, and process governance. Auditors benefit from COBIT by using it as a checklist to identify IT control issues and corroborate their audit findings.

COBIT has been revised several times since it was first released in 1996. The latest version is COBIT 4.1, although COBIT 5 has already been released as an exposure draft. For the purpose of this article, we will focus on COBIT 4.1.

COBIT 4.1 consists of 34 high level processes that cover 210 control objectives categorized in four domains - Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring and Evaluation.

The Planning and Organization domain covers aspects such as defining a strategic IT plan, choosing and implementing the right IT architecture, communicating management aims and directions, managing IT investments and resources, assessing and managing risks, and ensuring quality.

The Acquisition and Implementation domain focuses on acquiring and maintaining technology infrastructure, procuring IT resources, change management and the development of a maintenance plan to prolong the life of an IT system and its components.

The Delivery and Support domain focuses on the delivery aspects of the information technology. It covers areas such as defining and managing service levels, managing third party services, ensuring systems security, delivering continuous service, educating and training users, and managing data and configuration.

The Monitoring and Evaluation domain helps to assess if IT systems still meet their objectives, and if controls still meet regulatory requirements. It focuses on monitoring and evaluating IT processes and internal controls, ensuring regulatory compliance and providing IT governance.

Within the four domains, each of the 34 processes is described with corresponding control objectives. The controls help reduce risks, lower the incidence of errors, improve efficiency and achieve business objectives. The task of managers is to select the appropriate control objectives, choose how to implement them, decide on those controls that need to be implemented and accept the risk of those that are not.

COBIT maturity assessment

COBIT provides Maturity Models using which CIOs can rate their IT management processes, benchmark and target desired process maturity levels and encourage process improvement via gap analysis.

Based on how COBIT management processes are applied across the organization, there are six levels of maturity:

- **Level 0: Non-existent**
- **Level 1: Initial/ad hoc**
- **Level 2: Repeatable but Intuitive**
- **Level 3: Defined Processing**
- **Level 4: Managed and Measurable**
- **Level 5: Optimized**
By conducting a maturity assessment on a regular basis, companies can determine the status of their IT management processes. For instance, a rating of one indicates that processes are ad hoc and disorganized, while a rating of 5 indicates that best practices are being followed effectively.

**The relationship between COBIT and SOX**

Unlike most other regulations and standards, the Sarbanes-Oxley (SOX) Act does not clearly define its applicability to IT. Sections 302 and 404, the IT sections of SOX, don’t even mention technology or describe which controls must be used. They simply require that companies report on the adequacy of their internal control systems related to financial reporting. Noncompliance could result in significant penalties, not to mention a tarnished reputation. But without the appropriate guidance, how do companies know which controls to use?

Applying COBIT for effective governance

CIOs have a valuable aide in COBIT. It enables them to assess IT processes such as change management, comply with regulations efficiently, mitigate risks and manage controls. It also helps them ensure that third-party IT suppliers adhere to business policy, and that mergers and acquisitions are conducted smoothly.

The COBIT management guidelines are particularly useful to CIOs and CEOs because they provide useful tools to measure overall performance. Maturity Models can be used for benchmark comparison; Critical Success Factors (CSFs) define the most important actions for management to achieve control over IT processes; Key Goal Indicators (KGIs) help monitor achievement of IT goals; and Key Performance Indicators (KPIs) help monitor performance within each IT process.

While there is no single method of implementing COBIT, usually the first step is to identify business objectives and assess risks. COBIT is then used as a checklist to determine areas of risk that have been missed out, as well as high priority and low priority risks. Once the risks have been assessed and documented, COBIT can be used to apply the right controls.

Implementing COBIT throws up a host of challenges. However, proactive CIOs can turn to solution providers who will help them streamline IT and business processes, increase visibility into enterprise wide compliance, track and remedy issues, and improve the efficiency of reporting and documentation.