What is COBIT Security and when might you need to apply it?

One of the biggest challenges facing Administrators today is regulatory compliance. Several Acts such as the Gramm-Leach-Blighly Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) specifically address data security, so from a Security Administrator's point of view, it is fairly obvious what steps must be taken to be in compliance. Interestingly enough, the Sarbanes-Oxley Act (SOX), an Act that is probably causing Administrators the most headaches these days, says nothing about data security. One could argue however, that it is heavily implied. In fact, we have seen data security requirements being mandated by the Sarbanes-Oxley auditors. This actually makes a lot of sense since many of these auditors come from one of the fallen auditing firms, most of which ran a security practice. Knowing that ensuring the accuracy and integrity of a company's financial data takes more than sound accounting practices, these Sarbanes-Oxley auditing firms are requiring that data security processes and practices be addressed before signing off on the SOX audit.

So what is being suggested by the SOX auditing firms? In many cases, COBIT.

What is COBIT?

COBIT, which stands for Control Objectives for Information and related Technology has been developed by the Information Systems Audit and Control Foundation (ISACF) to address the need for management and control of information and information technology (IT). Their point is that technology is a vital part of business processes and, as such, management needs to have an appreciation for and a basic understanding of the risks and constraints to IT so they can make appropriate business decisions to determine what technology to implement and how to control its use. Since Sarbanes-Oxley is all about appropriate processes and controls, you can see why the SOX auditors are recommending companies implement COBIT.

However, COBIT is not the brain-child *of* a U.S.-based firm. Numerous companies and organizations contributed to the information found in COBIT and the ISACF itself is based in the U.K. COBIT is based on numerous sources ranging from ISO standards, to Codes of Conduct issued by the Council of Europe, to various qualification criteria such as ITSEC and ISO 9000, Industry and government best practices such as NIST as well as emerging industry-specific requirements.

What is IT Governance?

COBIT is touted as the model for "IT Governance", one of the buzz-words for SOX compliance. According to COBIT documentation, IT Governance is a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return when it comes to IT and its processes. COBIT looks at IT from the business perspective and places IT as part of the evaluation for meeting a

business objective with the goal to identify how IT can best contribute to the achievement of the business objective.

COBIT provides the process and structure that IT management can use to assess, manage and minimize risk across every aspect of an organization. The COBIT framework consists of four domains--Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. Each domain addresses a different aspect of the risk analysis and mitigation process IT must address. The domains are subsetted into 34 IT processes, which are further broken down into 318 detailed control objectives.

To give you an idea of the thorough nature of COBIT, let's take a look at the processes defined for each domain.

The Plan and Organize domain consists of the following processes:
- ? Define a strategic IT plan
- ? Define the information architecture
- ? Determine technological direction
- ? Define the IT organization and relationships
- ? Manage the IT investment
- ? Communicate management aims and direction
- ? Manage human resources
- ? Ensure compliance with external requirements
- ? Assess risks
- ? Manage projects
- ? Manage quality

The Acquisition and Implementation domain consists of the following processes:
- ? Identify automated solutions
- ? Acquire and maintain application software
- ? Acquire and maintain technology infrastructure
- ? Develop and maintain procedures
- ? Install and accredit systems
- ? Manage changes

The Delivery and Support domain consists of the following processes:
- ? Define and manage service levels
- ? Manage third-party services
- ? Manage performance and capacity
- ? Ensure continuous service
- ? Ensure systems security
- ? Identify and allocate costs
- ? Educate and train users
- ? Assist and advise customers
- ? Manage the configuration
- ? Manage problems and incidents
- ? Manage data

? Manage facilities
? Manage operations

The Monitoring domain consists of the following processes:
? Monitor the processes
? Assess internal control adequacy
? Obtain independent assurance
? Provide for independent audit

For each process in each domain, control objectives have been defined, making sure that no aspect can be ignored or forgotten.

Next month we will look at the sections that specifically address security.

****
****

What about Security?
While only one process is specifically devoted to security, control objectives that address security are scattered throughout the various processes in each domain. For example, under the Define the Information Architecture process in the Planning and Organization domain, there are the control objectives "Data Classification Scheme" and "Security Levels". The Educate and Train Users process in the Acquisition and Implementation domain includes the control process "Security Principles and Awareness Training". The Delivery and Support domain's Manage Third-Party Services' process includes the "Security Relationships" control objects and the Monitoring domain's Obtain Independent Assurance process contains several security-related control objectives. You can see that COBIT supports my recommendation that security needs to be addressed as a part of every business function.

Now let's go one step deeper and take a look at the individual control objectives for the Ensure Systems Security process defined in the Delivery and Support domain.

? Manage Security Measures – requires that security measures match up and are in sync with business requirements. It requires an IT security plan that is implemented and kept up-to-date.
? Identification, Authentication and Access – requires the implementation of the basic security principles of making people identify and prove who they are before accessing system resources as well as limiting access to specific system resources. Examples include a user profile and password or a digital certificate and private key.
? Security of Online Access to Data – requires that access to specific system resources (especially ones containing confidential or private data) only be allowed for users with a stated business need.
? User Account Management – requires good management of user accounts or, in the case of OS/400, user profiles. For example, "Old"

or unused profiles or profiles of individuals that have left the company should be removed from the system. This control point also raises the security issues that accompany third-party vendor access as well as security considerations for out-sourced work.

? Management Review of User Accounts – requires regular review of the capabilities given to each profile. For example, some of our clients have an annual review where employees' managers must approve of all of the menu options the employee has been given. Options no longer needed to perform their job function are removed. A similar review is held for users that have been given special authorities.

? User Control of User Accounts – requires that there be mechanisms in place to detect if a user account has been used by someone else or otherwise abused.

? Security Surveillance – requires auditing of security-related or relevant activities and that any improper actions be reported and acted upon in a timely fashion

? Data Classification – requires that all data is classified based on its sensitivity, privacy implications and confidentiality and that the owner of the data should be the one to determine who can access the data.

? Central identification and Access Rights Management – requires that access controls and user privileges be granted and managed centrally to ensure a consistent application of the enterprise's security policy

? Violation and Security Activity Reports – requires that the data gathered by the Security Surveillance control point requirements is reviewed, acted upon and knowledge of misuse of information is escalated appropriately to identify and resolve incidents quickly. Access to the logs keeping this information should be restricted to a "need to know" basis. In OS/400 terms that means access to the QAUDJRN audit journal should remain restricted.

? Incident Handling – requires the formation of a process and procedure for reporting security incidences.

? Reaccreditation – requires re-testing or certification of the implementation of your security policy to ensure it is up-to-date with actual function and configuration

? Counterparty Trust – requires control practices to ensure communications between entities providing electronic transactions are verifiable and that, before an exchange of information takes place, the other party is appropriately authenticated.

? Transaction Authorization – advocates the use of digital signatures to authenticate a user for electronic transactions

? Non-repudiation – requires that procedures be put in place and appropriate technology used so that neither party of an electronic transaction can deny that it actually occurred.

? Trusted Path – ensures that sensitive data or transactions only occur over a "trusted path." An example of a trusted path would be a VPN connection where both systems were authenticated using digital certificates.

- ? Protection of Security Functions – requires that security-related hardware and software be protected against tampering. An example would be to place all network routing and firewall equipment in a locked room or closet or to only authorize your security administrator to run software that helps you manage your security configuration. This control objective also includes a reminder that the security configuration of your systems and network should not be made public information to be viewed by the entire company. However, it also points out that *relying* on the design being secret (security by obscurity) is not appropriate.
- ? Cryptographic Key Management – If cryptography is used in the organization, this control objective requires appropriate management of all crypto keys as well as the need to manage the use of those keys including revocation lists when a key has been compromised.
- ? Malicious Software Preventions, Detection and Correction – requires policies and procedures to protect the enterprise from malicious software. The most common example is the need for virus scanning and detection. In OS/400 terms, this might include the setting of various system values to control what is restored onto the system and what checks OS/400 makes before allowing the object to be restored. It might also include the requirement to run the Check Object Integrity (CHKOBJITG) command on a regular basis.
- ? Firewall Architectures and Connections with Public Networks – requires appropriate use of firewalls – especially to protect internal networks
- ? Protection of Electronic Value – requires the protection of electronic data that has been stored on cards or other devices. An example would be a smart-card used for authentication to the network.

One criticism of COBIT is that it describes what needs to be done but only in broad generalities and it never describes how each of these control objects are to be accomplished or implemented. Providing the "hows" is not the intent of COBIT. COBIT exists to help you define your process for identifying and managing risk within the IT organization. Other standards exist that take up where COBIT leaves off. The "hows" will be the topic of a future column.

Summary

Unless you are a large enterprise, it is unlikely that you will be able to implement the entire COBIT process. In many shops, the rigorous process that a full-blown COBIT implementation produces could be considered over-kill and or could require more personnel to implement than is currently on the IT staff! Some control objectives are not applicable for all organizations. But for any company – large or small – COBIT is a great resource to help you determine the strategic areas of IT that you may be overlooking. I think you will find the Control Objectives documentation especially helpful as a place to start to develop a process to help you manage risk and address security as a business function. Whatever the size of the company, I do recommend that IT management follow the general principles of COBIT and establish a process to assess, manage and minimize risk throughout their IT organization.

For More Information
Go to the ISACA website at www.isaca.org for a comprehensive learning experience on COBIT. A tremendously informative document on COBIT and how it applies to Sarbanes-Oxley can be found at:
http://www.isaca.org/Template.cfm?Section=About_ISACA&Template=/ContentManagement/ContentDisplay.cfm&ContentID=9757

Carol Woodbury is co-founder of SkyView Partners, a firm specializing in security consulting and services as well as their recently released software product, SkyView Risk Assessor for OS/400. Carol has over 13 years in the security industry, 10 of those working for IBM's Enterprise Server Group as the AS/400 Security Architect and Chief Engineering Manager of Security Technology. Look for Carol's second book, Experts' Guide to OS/400 Security, to be released later this spring. Carol can be reached at carol.woodbury@skyviewpartners.com