



Implementing General IT Controls for Sarbanes-Oxley *Merging People, Processes and Technology*

About BMC Software

BMC Software is a leading provider of enterprise management solutions that empower companies to manage their IT infrastructure from a business perspective. Delivering Business Service Management, BMC Software solutions span enterprise systems, applications, databases and service management. Founded in 1980, BMC Software has offices worldwide and fiscal 2004 revenues of more than \$1.4 billion. For more information about BMC Software, visit www.bmc.com.

Implementing General IT Controls for Sarbanes-Oxley

Merging People, Processes and Technology

TABLE OF CONTENTS

Executive Summary	1
Section 1: Introduction	2
Section 2: The People Issues	3
Section 3: Increasing Knowledge, Awareness and Ownership	4
Section 4: Combining Processes and Technology	5
- Understand control objectives	5
Section 5: Use Technology to Help Meet General IT Control Objectives	6
Conclusion	12
Glossary	13

About the Author

Christopher Williams is the Marketing Manager for BMC Software's Identity Management Business Unit. His primary responsibilities include media and analyst relations, competitive and market analysis, product marketing and management. With over 23 years of experience in the IT industry, Williams has served in a variety of data management organizations with businesses in a number of different industries including textiles, financial, retail, defense contractors and software vendors. Throughout his career, Williams has been centered on managing various technical implementation and support teams, data center management, enterprise-wide project management, as well as infrastructure management. He also performed numerous tasks including implementing operational and security oriented solutions and strategies affecting all disciplines within the IT industry.

Glossary

COBIT

The IT Governance Institute (ITGI) has constructed an IT-focused control framework called Control Objectives for Information and related Technology (COBIT) that provides very specific IT governance guidelines.

General IT Controls

General IT controls span five critical IT process areas: security administration, application change management, data management and disaster recovery, operations and problem management, and asset management.

ITIL

IT Infrastructure Library (ITIL®), the industry framework for best practices in Service Management. ITIL is part of the foundation of the COBIT model.

PCAOB

The Public Company Accounting Oversight Board (PCAOB), established by Sarbox to oversee the audits of public companies, specifically mentions the importance of IT systems and IT general controls in its auditing guidelines dated March 9, 2004.

Sarbanes-Oxley Act of 2004 (Sarbox)

In accordance with Sarbanes-Oxley, executives must attest to the adequacy and effectiveness of their internal controls, including IT controls. Internal financial process controls and related IT controls will be externally audited, and a statement of control, including material weaknesses found during the audit, must now appear in annual reports filed with the Securities and Exchange Commission (SEC).

Section 404

This section of the Sarbanes-Oxley Act deals with the general controls that maintain the integrity of processing and reporting of financial data. According to Section 404, a company must attest to the adequacy and effectiveness of its internal controls for financial reporting.

Conclusion

Sarbanes-Oxley deadlines are here now, and organizations must meet and demonstrate compliance or face consequences that could include severe financial penalties and even criminal prosecution of executives. Yet, many organizations are unprepared.

Achieving and maintaining Sarbox compliance requires the successful orchestration of people, processes, and technology across the organization. The IT organization plays a pivotal role in this orchestration. Key to the successful performance of this role is the availability of underlying technology that permits the IT staff to achieve the control objectives specified in the COBIT framework.

With this technology in place, IT can impart to executives confidence that their attestation to compliance is valid and that they can back up their attestations with the necessary information to support even the most stringent audits.

BMC Software offers a wide variety of solutions that help organizations achieve and maintain compliance with Sarbanes-Oxley. For more information visit www.bmc.com/compliance.

Executive Summary

Prompted by corporate financial scandals of recent years, the Sarbanes-Oxley Act of 2002, "Sarbox" as it is commonly known, is one of the most significant revisions to U.S. federal securities laws. Deadlines for Sarbox compliance, and subsequent company auditing, are fast approaching. Publicly traded U.S.-based companies must now be prepared for addressing Sarbox requirements, including Sarbox-compliant IT control processes, which could alter the claims that corporations make to upcoming annual reports. Companies must ensure their financial processes comply with Sarbox legislation, and senior executives must attest to the adequacy and effectiveness of their internal control of these processes. Many companies, however, are not fully prepared for their audits. Without proper guidance, any employee could unwittingly violate Sarbox requirements, putting a company in jeopardy.

Achieving and maintaining compliance with the general IT controls specified in Section 404 of Sarbox involves far more than just establishing rigid control over various processes and access to information. It requires merging *people*, *processes* and *technology* into a unified, enterprise-wide compliance effort.

From a *people* perspective, compliance requires the philosophical adoption of the Sarbox legislation across the enterprise. This involves the indoctrination of ownership onto every individual who has access to records that affect the company's ability to attest to and validate that the data it provides is accurate—whether or not an individual's access has been deemed significant.

With respect to *processes*, compliance requires companies to establish processes and controls that ensure requirements are met and that readily demonstrate compliance. The interpretation of Sarbox is somewhat open, providing the flexibility to create processes that maintain compliance while still allowing efficient and profitable operations.

Finally, supporting *technology* is required to implement and enforce standard processes and to monitor and report on compliance.

It is important to note that Sarbox compliance involves continuous assessment and continuing education. Assessment helps ensure that compliance is maintained; education helps keep compliance firmly at the forefront of each employee's mind.

Introduction

Because most corporate financial processes are supported by information technology (IT) systems and the business processes related to those systems, the IT staff plays a primary role in Sarbox compliance. This paper focuses on compliance from the perspective of the IT organization, although it does review some of the Sarbox-related responsibilities pertaining to general IT controls for people in other functional areas of the business. It presents guidelines for ensuring the awareness and adoption of the Sarbox philosophy by IT.

This paper also discusses the appropriate IT control framework for implementing processes to help achieve Sarbox compliance with general IT controls, and the criteria for selecting software solutions to implement the framework.

Section 404 of Sarbox has the greatest relevance and impact for IT. This section deals with the general IT controls that maintain the integrity of processing and reporting of financial data. According to Section 404, a company must attest to the adequacy and effectiveness of its internal controls for financial reporting.

As shown in **Figure 1**, external auditors review current process and control documentation to meet the requirements of specific IT control objectives at three levels:

- > **Organization level:** At this level, the auditor reviews control objectives related to the overall IT organization and structure. Discovering lack of controls at this level may cause an auditor to dig deeper at the other levels.
- > **Entity level:** At this level, the auditor looks at the corporate organizational structure, and scopes the control requirements based on division of process and responsibilities within the business unit, division of process and responsibilities by geography, and assessment of third-party service provider processes and responsibilities.
- > **Process level:** At this level, the auditor evaluates process documentation that defines control objectives in three primary areas: *application integration controls*, *application and data owner controls*, and *general IT controls*.

This paper focuses on *general IT controls* because such controls can relieve a company from needing to prepare additional documentation and compensating controls for Section 404 compliance.

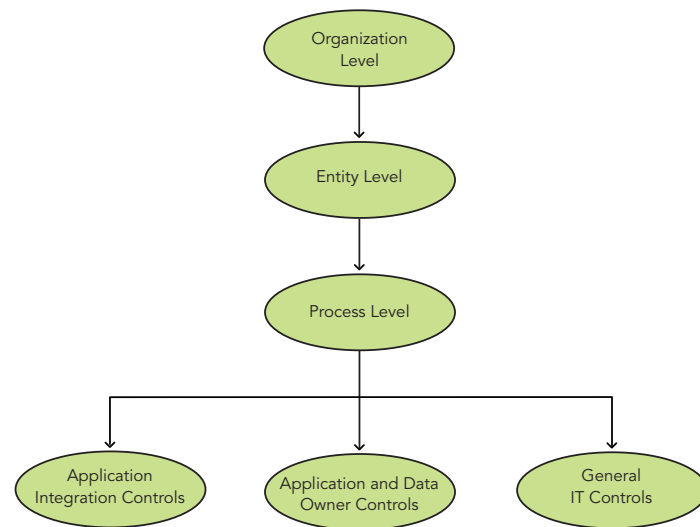


Figure 1. Levels of auditor review

Asset Management and Configuration	
COBIT CONTROL OBJECTIVES	SOFTWARE SOLUTION CRITERIA
DS9—Manage the Configuration	
Only authorized software is permitted for use by employees using company IT assets.	<ul style="list-style-type: none"> > Automatically discover software assets and manage standard configurations. > Compare discovery results to standard configuration. > Provide software license monitoring.
System infrastructure, including firewalls, routers, switches, network operating systems, servers, and other related devices, is properly configured to prevent unauthorized access.	<ul style="list-style-type: none"> > Provide complete configuration/asset database that tracks assets and their configuration, and standard configurations.
Application software and data storage systems are properly configured to provision access based on the individual's demonstrated need to view, add, change or delete data.	<ul style="list-style-type: none"> > Support the management of all aspects of provisioning user accounts, from the initial request for an access change until the requested change is executed and completed. > Provide mainframe storage provisioning.
IT management has established procedures across the organization to protect information systems and technology from computer viruses.	<ul style="list-style-type: none"> > Provide patch management capability that works in conjunction with virus detection system, managing patches and virus definitions, and forcing virus definition update based on standard configurations.
Security implication: Insufficient configuration controls can lead to security and availability exposures that may permit unauthorized access to systems and data.	<ul style="list-style-type: none"> > Permit a security manager to audit for inappropriate software usage by analyzing the application log. > Collect logs from security and network devices (such as firewalls, intrusion detection systems and routers) that can be used to compare actual performance with security and regulatory policy, enabling optimal tuning of these devices.

Table 6. COBIT Control Objectives: Asset Management and Configuration

Operations and Problem Management	
COBIT CONTROL OBJECTIVES	SOFTWARE SOLUTION CRITERIA
DS1—Define and Manage Service Levels	
Security implication: Roles and responsibilities are defined and used to ensure services are delivered as required.	> Provide data management and role management to ensure that the people responsible for tasks pertinent to the service management objectives are granted appropriate rights for that function.
DS10—Manage Problems and Incidents	
IT management has defined and implemented a problem management system to ensure that all operational events that are not part of the standard operation (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner.	> Support ITIL incident and problem management processes. > Help ensure that incidents are resolved according to SLAs. > Integrate with systems management solutions for automated response to systems level incidents.
Emergency program changes are approved, tested, documented and monitored.	> Ensure that emergency change is a standard type of change request. > Require mandatory approval to emergency changes that impact any Sarbox audited application.
Problem escalation procedures are defined and implemented to ensure that problems are resolved in a timely manner.	> Provide workflow that includes automatic escalation of incidents and problems according to terms of appropriate SLAs.
The problem management system provides for adequate audit trail facilities, which allow tracing from incident to communication underlying cause.	> Tightly integrate problem management processes with the incident management process. > Ensure that each incident and problem ticket creates a complete audit trail of steps taken, approvals and resolution.
A security incident response process exists to support timely response and investigation of unauthorized activities.	> Provide ability to identify security incident type, and manage appropriate automated resolution and approval workflow. > Collect and centralize security log data from heterogeneous sources, filter collected information against security policy, automatically trigger appropriate actions and alerts upon detecting suspicious activities, archive normalized log data for forensic review, and permit viewing and reporting from a dashboard.
DS13—Manage Operations	
Security implication: Addresses how an organization maintains reliable application systems in support of the business to initiate, record, process and report financial information.	> Create an environment that promotes consistency, reliability, and support for security, identity management, password management, security event management and policy/regulatory management by establishing a system of repeatable processes that does not allow deviation except by intention.

Table 5. COBIT Control Objectives: Operations and Problem Management

The People Issues

To address the “people-related issues” involves the philosophical adoption of the Sarbox regulation across the organization. Each individual in the IT organization who has access to information must understand that everything he or she does can affect the company’s ability to comply. The key to success is to get complete buy-in from all involved individuals to ensure those individuals understand the importance of delivering accurate financial information to stockholders.

In many cases, violations result from good intentions. In misguided attempts to do the right thing for the company, people might not always follow specific documentation of processes.

Example:

A manager is under deadline to report information to the chief executive officer. This manager is not authorized to access the needed information, however, and asks a colleague in IT to grant access privileges. Based on a high degree of personal trust in this manager, the IT person enables access just for the day. The manager’s problem is solved, but a greater problem for the company may have just been created. The IT person has violated process rules by going around standard identification management protocols, possibly compromising Sarbox compliance and exposing the company to the risk of severe penalties.

There are obstacles to philosophical adoption of Sarbox. A general lack of understanding of Sarbox requirements by employees is just one such obstacle. Employees may believe they fully understand the rules of compliance, but in actuality do not. Employees may believe Sarbox does not affect their jobs. They may believe that Sarbox is not within their scope of responsibility and do not comprehend how their jobs can influence compliance.

Because of this lack of knowledge and these misconceptions, there may not be complete buy-in at all levels of the company. This is especially true at lower levels. But even at lower levels, there are certain degrees of accountability, ownership, and responsibility that must be adopted.

A simple test to gauge employees’ familiarity with Sarbox and awareness of their roles in compliance is to ask four questions:

- > Have you read Sarbox?
- > Do you know how Sarbox impacts your job?
- > Do you know how to properly use your access to information with regard to Sarbox compliance?
- > Have you participated in company-sponsored education programs that define what Sarbox means to your organization and reporting?

Increasing Knowledge, Awareness and Ownership

Ignorance of Sarbox is one of the primary obstacles to achieving compliance. If people do not know what Sarbox is, they cannot comply with its requirements. Education is key to corporate compliance. Educating people on what Sarbox addresses and how the company is going to embrace it is fundamental and should be extended to all employees who access data. Furthermore, the organization must educate employees on their roles in maintaining compliance. Education is especially important for employees in the IT organization.

The company needs to initiate a continuing program to impart knowledge and increase the awareness of Sarbox across the enterprise. Only in this way can organizations bring about corporate change and increase the adoption of Sarbox philosophy. There are six essential parts of such a program:

- > **Ensure that employees understand the big picture.** Like all projects and initiatives, the initial phase of the education program should provide basic information to all involved parties. A fundamental difference between the Sarbox initiative and many other projects or initiatives is its broad scope.
- > **Effectively communicate the importance of the processes.** As with all issues in modern computing, the definition of process is essential to satisfying the control objectives needed to become Sarbox compliant. The organization must create and document processes, whether or not automation is involved. The organization must then provide education that articulates the processes, their constraints, and the ramifications of not following those processes.
- > **Demonstrate senior-level support.** Corporate-wide ownership is essential, even though:
 - The senior management team is ultimately culpable and must attest that compliance is being achieved by adding their signatures to the annual report.
 - The audit processes are restricted to a handful of internal employees and external auditors.
 - The creation and maintenance of automated services to execute processes may reside with a group of technical resources that involve only a small number of people.

It is imperative that top-level management takes an active role in the education and communication process to instill corporate-wide ownership of Sarbox, through such methods as written communications and the incorporation of Sarbox information into presentations, meetings, and goals.

- > **Empower employees.** Sarbanes-Oxley is the responsibility of everyone in the company. Subsequently, it is important to empower all employees. Empowerment can come in many forms. Organizations can empower a security administrator in the IT organization to deny access to anyone, regardless of corporate position, if that access breaches a policy such as segregation of duties, excessive rights, mutual rights, or exclusivity rules. In addition, the organization can establish an ombudsman to arbitrate access issues.
- > **Publish results.** Partial scores or promises to “do better next time” are not acceptable in the realm of Sarbox compliance—there is only compliance or non-compliance. Organizations should quickly make public their audit results. This provides immediate confirmation that the processes adopted by the organization are working. Moreover, it continues to foster strict adherence to control processes throughout the organization. Publishing compliance data can be used as a strong enforcement tool and can be used in education materials.
- > **Conduct a continuous campaign.** Sarbox compliance is not a one-time cure, so it is critical to keep the Sarbox initiative alive in the minds of all affected employees. Additionally, as companies evolve and processes are added or changed (such as rollout of a new help desk application), existing and new employees and business partners must be brought up-to-date on process changes that can affect Sarbox, and provided information about new processes and modifications. Moreover, senior-level management must be highly visible in this ongoing program to convey the organization’s continuing commitment.

Data Management	
COBIT CONTROL OBJECTIVES	SOFTWARE SOLUTION CRITERIA
DS11—Manage Data	
Security Implication: Include the controls and procedures used to support information integrity, including its completeness, accuracy, authorization and validity.	<ul style="list-style-type: none"> > Permit drill-down into the interaction of actual users with critical corporate data to determine what people actually did and what data was actually touched. > Provide a real-time-threat monitoring and alerting solution for critical security situations and configuration concerns.
Management has implemented a strategy for cyclical backup of data and programs.	<ul style="list-style-type: none"> > Determine if the organization has procedures in place to back up data and programs based on IT and user requirements. > Select a sample of data files and programs and determine if they are being backed up as required.
Procedures exist and are followed to periodically test the effectiveness of the restoration process and the quality of backup media.	<ul style="list-style-type: none"> > Inquire whether the retention and storage of messages, documents, programs and such, have been tested during the past year. > Obtain and review the results of testing activities.
Changes to data structures are authorized, made in accordance with design specifications and implemented in a timely manner.	<ul style="list-style-type: none"> > Obtain a sample of data structure changes and determine whether they adhere to the design specifications and were implemented in the timeframe required.

Table 4. COBIT Control Objectives: Data Management

Combining Processes and Technology

UNDERSTAND CONTROL OBJECTIVES

As previously stated, this paper focuses on general IT controls because robust general IT controls can reduce the need for a company to prepare additional documentation and compensating controls for Section 404 compliance.

An auditor will systematically check general IT controls by working through various control objectives detailed in a control framework. Companies must specify and use a recognized control framework to evaluate their controls.

The IT Governance Institute (ITGI) has constructed an IT focused control framework called Control Objectives for Information and Related Technology (COBIT) that provides very specific IT governance guidelines. IT Infrastructure Library (ITIL®), the industry framework for best practices in Service Management, is part of the foundation of the COBIT model. The ITGI also has published a subset of COBIT for Sarbox audit preparation called *IT Control Objectives for Sarbanes-Oxley (2004)*, which includes five application-specific controls and 12 general IT control objectives (each IT control objective consists of many individual general IT controls). Many companies are using this subset of COBIT to evaluate their IT controls for Sarbox compliance.

The 12 general IT control objectives proposed by ITGI for meeting Sarbanes-Oxley requirements are listed in **Table 1** on the next page. COBIT has been selected as the tool of choice for external auditors to use in IT audits for Sarbanes-Oxley. As a result, many companies have selected COBIT for their control framework.

Most, if not all, financial processes are supported by IT systems. Consequently, establishing the proper IT controls is paramount to achieving and maintaining Sarbox compliance. A company cannot pass an audit and demonstrate control of its financial reporting process without adequate management of the underlying IT systems.

The Public Company Accounting Oversight Board (PCAOB), which was established by Sarbox to oversee the audits of public companies, specifically mentions the importance of IT systems and general IT controls in its auditing guidelines dated March 9, 2004. According to guidance provided by Protiviti, a leading Sarbox consulting firm, "The independent accountant will have IT-related risks and controls in mind when evaluating the basis for management's assertions in the internal control report. The general IT controls are pervasive controls that impact the integrity of most, if not all, transactions, as well as most, if not all, of the internal financial reports from which the financial statements are derived. A weakness in general IT controls potentially could have an effect over significant transactions and accounts. If there are gaps in the general IT controls, it is possible that the external auditor could insist that those gaps be addressed before an overall opinion is reached on the effectiveness of the internal controls."

Application Change and Control Management	
COBIT CONTROL OBJECTIVES	SOFTWARE SOLUTION CRITERIA
AI2—Acquire or Develop Application Software	
Procedures exist to ensure that system software is installed and maintained in accordance with the organization's requirements.	> Ensure that software meets configuration requirements and meets software-licensing requirements.
Procedures exist to ensure that system software changes are controlled in line with the organization's change management procedures.	> Ensure that all software application change requests follow standard documented procedures and approval workflow, and create an auditable record of each change.
AI3—Acquire Technology Infrastructure	
IT management ensures that the setup and implementation of system software do not jeopardize the security of the data and programs being stored on the system.	> Ensure that each application change request is managed via standard process. > Help identify related financial applications, underlying systems, and databases affected by any software or infrastructure change.
Procedures exist and are followed to ensure that infrastructure systems—including network devices and software—are installed and maintained in accordance with the acquisition and maintenance framework.	> Ensure that each implementation or change request is managed via standard process. > Provide workflow that can enforce appropriate approval and release process. > Identify related financial applications, underlying systems, and databases affected by any infrastructure implementation or maintenance activity.
Procedures exist and are followed to ensure that infrastructure system changes are controlled in line with the organization's change management procedures.	> Provide a single consolidated change management system for request, assessment, planning, tasking, approval and implementation. > Automate the change process wherever possible. > Provide a complete audit trail for each completed change.
Where network connectivity is used, appropriate controls—including firewalls, intrusion detection and vulnerability assessments—exist and are used to prevent unauthorized access.	> Act as an "insider intrusion detection system," monitoring who touches what and detecting unauthorized access by trusted insiders. > Aggregate information from the insider intrusion detection system, firewall and antivirus logs, and present the consolidated information in a comprehensive dashboard that shows access compliance. > Provide the ability to enforce policy and deny repeated, unsuccessful attempts at access.
AI6—Manage Changes	
Requests for changes, system maintenance and supplier maintenance are standardized and are subject to formal change management procedures.	> Ensure that all change requests follow standard processes and system defined workflow.
Policies and procedures to manage emergency changes exist and are followed.	> Ensure that emergency change is a standard type of change request. > Require mandatory approval to emergency changes that impact any Sarbox-audited application.
Changes to systems and applications are performed in a timely manner and adhere to the company's overall change management standards.	> Automate change execution process wherever possible and log all change activities. > Provide standard workflow for different types of requests, and require risk assessment, planning and approval for all requests.
Changes to IT systems and applications are performed as designed and meet the expectations of users.	> Automate changes according to user specifications. > Ensure that standard change workflow includes indication of change success and can be integrated with help desk to monitor incidents related to recent changes.

Table 3. COBIT Control Objectives: Application Change and Control Management

Use Technology to Help Meet General IT Control Objectives

Technology plays an indispensable role in helping companies meet the COBIT control objectives, and software vendors are offering solutions that help support compliance. Because of the critical nature of Sarbox compliance, it is important for organizations to exercise great care in choosing among these software solutions. The COBIT control objectives for each of the 12 process areas are listed in **Table 1**. Criteria that organizations should look for in choosing software solutions to help them meet objectives are outlined in this paper (see **Tables 2 – 6** on pages 7 through 11).

It is important to note that security is one of the key factors in Sarbox compliance. There is a COBIT process area (DS5) dedicated to system security. In addition, security impacts several other process areas, and hence, the software solution criteria for those areas.

Other key factors, such as application change and control management, data management and disaster recovery, operations and problem management, and asset management are also covered. Controls in these five areas are critical to the integrity of the processes, systems, and applications that contribute to the organization's ability to produce accurate, reliable financial statements. The following tables, which appear on pages 7 through 11, include many of the key COBIT control objectives and the technology requirements to support those objectives.

ID	CORBIT Control Objective
AI2	Acquire or Develop Application Software
AI3	Acquire Technology Infrastructure
AI4	Develop and Maintain Policies and Procedures
AI5	Install and Test Application Software Technology Infrastructure
AI6	Manage Changes
DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS5	Ensure Systems Security
DS9	Manage the Configuration
DS10	Manage Problems and Incidents
DS11	Manage Data
DS13	Manage Operations

Table 1. General IT controls and corresponding COBIT process areas

Security Administration	
COBIT CONTROL OBJECTIVES	SOFTWARE SOLUTION CRITERIA
DS5—Ensure Systems Security	
Procedures exist and are followed to ensure that all users are authenticated to the system to support the validity of transactions.	<ul style="list-style-type: none"> > Streamline and automate the process of provisioning users to the system to improve the ability of the company to ensure that proper authentication is actually occurring. > The provisioning process should prevent controls from being circumvented and should prevent users from “borrowing” other users’ credentials to gain access to system resources.
Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms, such as regular password changes.	<ul style="list-style-type: none"> > Provide password management functionality that enables companies to implement and enforce strong password policies to improve the effectiveness of authentication mechanisms.
Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending, and closing user accounts.	<ul style="list-style-type: none"> > Provide core functionality that encompasses the management of all aspects of provisioning user accounts—from the initial request for access change until the requested change is executed and completed.
A formal approval process exists for granting access privileges to systems and data.	<ul style="list-style-type: none"> > Provide a workflow capability that enables the organization to formally define and enforce the process for handling requests and approvals. > The workflow capability must also enable the organization to manage and track the inevitable one-off requests that come through the system.
A control process exists and is followed to periodically review and confirm access rights.	<ul style="list-style-type: none"> > Map all accounts to a central definition of identity to facilitate viewing of all the access rights associated with a particular person or group of people. > Permit the use of role definitions to simplify the identity management process.
Where appropriate, controls exist to ensure that transactions cannot be denied by either party and that controls are implemented to provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions.	<ul style="list-style-type: none"> > Process transactions with specific conditions that prescribe the approved submission/execution/origin variables. > Record each transaction for audit activities.
Where network connectivity is used, appropriate controls—including firewalls, intrusion detection and vulnerability assessments—exist and are used to prevent unauthorized access.	<ul style="list-style-type: none"> > Act as an “insider intrusion detection system,” monitoring who touches what and detecting unauthorized access by trusted insiders. > Aggregate information from the insider intrusion detection system, firewall, and antivirus logs, and present the consolidated information in a comprehensive dashboard that shows access compliance. > Provide the ability to enforce policy and deny repeated, unsuccessful attempts at access.
The IT security plan and its related activities and priorities reflect results of recent security assessments.	<ul style="list-style-type: none"> > Permit security plans to be modified using the data within the tool environment, specifically the elements that refer to the granting of access and the monitoring of access (roles, rules, profiles, templates and policies all form the basic dynamics of a living security model that denotes the current characteristics of permissible and non-ordained actions and activities).
The IT security administrator monitors and logs security activity, and identified security violations are reported to senior management.	<ul style="list-style-type: none"> > Track security access violations, such as when accounts are modified out-of-process (an administrator creates or modifies an account directly on a system) or when suspicious password attempts are made (multiple unsuccessful attempts to access an account). > Monitor the security log for attempted breaches and generate alarm events according to escalation procedures. > Integrate with the help desk for automated response to security alarms.

Table 2. COBIT Control Objectives: Security Administration