



SOX 404 & IT CONTROLS

IT Control Recommendations
For
Small and Mid-size companies
by
Ike Ugochuku, CIA, CISA

INTRODUCTION

Small, medium, and large businesses today face similar challenges concerning assuring the public that their published financial results actually reflect their performance. The increasing reliance on technology for all business processes and transactions has led to greater technology expense and a need for a controlled technology structure to ensure that transactions are reliable and accurate. This gives senior management a greater assurance that the company's financial results actually represent the performance and that the organization is compliant with regulatory requirements.

Recently, the Committee of Sponsoring Organization (COSO) released a document "*Guidance for smaller public companies reporting on internal controls for financial reporting.*" The document is to assist smaller companies that desire better controls for their business. The question of how to translate these recommendations into practical application is covered by this document. This document gives practical advice concerning controls for IT operations.

Source

It is based on the author's years of experience working with large, mid-size, and small corporations. The author is an established technology risk audit professional experienced in analyzing IT and business processes, creating and implementing corrective recommendations to mitigate identified risks or gaps. He has been involved in the development and implementation of IT policies for several firms and has an experiential knowledge of truly effective policies that create a controlled IT environment.

Audience

This document is high level enough for business senior management who want to understand about IT processes. It is also suitable for IT management who want to understand about control requirements for IT processes. IT auditors and compliance officers will benefit from the information in this document.

OVERVIEW

The need for controls

It is increasingly important to have an IT department with proper internal controls built into its operations. Two major factors are causing senior management to take a closer look at the IT controls in their organizations.

- **Regulatory Compliance:** new laws like Sarbanes-Oxley (SOX) specify that select senior officers will attest to the state of the internal controls of the company and the reliability of the financial statement released. Since almost all company transactions involve use of a computer system, it is important that there are adequate systems controls in place to assure regulators that the attestation by management is reliable.
- **IT expenditure:** it is also important that IT expenditure is aligned with the company's business strategy. As the reliance on technology systems to perform and report on transactions increases, technology cost is one significant internal expense. It is important that this cost is aligned with business strategy. There should be a documented IT process that integrates business participation in the creation of an IT strategy plan.

The short-term approach to verify adequate internal controls is to test existing controls and recommend compensating or new controls for weak controls. A long term approach is to build controls into the IT planning processes. This can be achieved by using a standard IT framework like Control Objectives for Information and related Technology (COBIT) at the high level. But for implementation it may be necessary to hire expensive consultants to map the processes to the COBIT framework.

For small and mid-size companies with IT, a better, more cost effective way is to have a comprehensive information systems policy document (like this document) which can be used as a control guideline for assessing current operations and creating new processes. It also serves as a baseline that can be used by auditors to review if the IT department's operations are consistent with business objectives.

This document is based on the COBIT framework. It uses the 12 control objectives that are closely aligned with the US Public Accounting Oversight Board (PCAOB) general control guidelines for IT systems. It provides recommended controls that can be used to achieve these objectives.

SOX 404, PCAOB standards and the COBIT framework

The US Sarbanes Oxley Act of 2002 provides for new governance rules, regulations and standards for public companies. Section 404 of the act requires management officers to assess the

effectiveness of the internal controls that govern processes that affect financial reporting. There should be an annual control assessment report with attestation from senior management.

The US Public Accounting Oversight Board (PCAOB) was created by the SOX act. In order to protect the interest of investors, the board is to oversee the audit of public companies. The PCAOB auditing standard No.2 discusses the audit of internal controls that govern financial reporting. It states that since most financial transactions involve IT systems, the controls for IT operations should be examined. The standard identifies four key IT processes, namely, program development, program changes, computer operations, and access to programs and data.

The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI). Control Objectives for Information and related Technology provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes, and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

In its fourth edition, COBIT has 34 high level objectives that cover 215 control objectives categorized in four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

This document is based on *IT control objectives for Sarbanes-Oxley* a document by ISACA, which maps 12 of the COBIT control objectives to the four key IT processes identified by the PCAOB. The chapters discuss relevant policies and procedures that can be used to achieve the 12 objectives. The information provides a logical starting point for affected organizations.

COBIT Control Objective heading	PCAOB IT General Control Heading			
	Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire and develop application software	•	•	•	•
2. Acquire technology infrastructure	•	•	•	
3. Develop and maintain policies and procedures	•	•	•	•
4. Install and test application software and technology infrastructure	•	•	•	•
5. Manage changes		•		•
6. Define and manage service levels	•	•	•	•
7. Manage third-party services	•	•	•	•
8. Ensure systems security			•	•
9. Manage the configuration			•	•
10. Manage problems and incidents			•	
11. Manage data			•	•
12. Manage operations			•	•

DATA MANAGEMENT

Data management and control depend on what the data is used for and the classification of the data. Proper classification of data assists management in making decisions about data protection expenses.

Data ownership

The data owner should be a business person or user. A “business person” refers to a unit that has no direct management of the infrastructure that the data resides on. The user will determine who should have access rights to the data; authorize any changes to the data, determine appropriate backup and recovery times and be responsible for any cost related to maintenance of the data.

Data classification

Data should be classified to ensure that the right kind of security is implemented. The possible categories are the following:

1. **Restricted:** Data have a highly monitored distribution list. Where financially possible, data encryption should be enforced. Since encryption may be an expensive option for small size businesses, it may be useful to protect certain data with attorney-client privilege.
2. **Confidential:** Data are limited to only those defined as data owners. Data should be on an infrastructure that has a regular backup schedule.
3. **Internal:** Data are restricted to only employees. Data should have a regular backup schedule.
4. **Public:** Data that is already available to the public.

ENSURE SYSTEMS SECURITY

Access control

One of the most important internal controls an organization of any size should establish is access control — the doorway to all IT systems and corporate resources. Access controls specify how the business monitors its IT resources and how they should be used. The most commonly used access controls include user accounts, consisting of passwords and usernames; log in and resource access rights; and the establishment of privileged system accounts.

The User id

Because access controls are built around user accounts, the creation and management of user accounts is vital to an organization,. The purpose of user accounts is to grant employees access to specific network systems and resources.

The user should only have one user id and password, which should be used for access to all systems on the network. A central authentication system may be established for applications so that developers don't have to concern themselves with how to get security information from the operating system. There may be several operating systems in the organization.

The following controls should apply to user ids:

1. The user id should be related to personal information of the employee. This makes it easier for the employee to remember. It also makes it easy for the employee to be identified on the network.
2. The employee number should be used for uniqueness. Some small and mid-size companies may not have employee numbers, but where they have, a combination of employee number and initials can be used. This makes it difficult for unauthorized users to guess.
3. Three logon attempts should be allowed, after which the account is locked. It can only be unlocked after a formal request from the manager. The system should log the number of failed attempts for a user id, and this should be reviewed at least bi-annually. A report should be sent to responsible business managers of user ids with high failed attempts.
4. If the user id is not used for more than 90 days, it represents a security risk, so the user id should be disabled.

The password

Most small and mid-size companies may not assign employees a unique number, so user ids may be based on their names only. This makes it relatively easy to guess so it is important to have strong controls for the passwords.

The following controls should apply to passwords:

1. At least 6 characters (numbers and alphanumeric) should be required.
2. There should be at least one number required.
3. There should be at least one uppercase letter required.
4. The user should be required to change the password every 60 days.
5. The system should keep a history of 8 passwords.

These rules should be implemented as policy on the operating system. If a separate authentication system is used for some application, the rules should also be part of a system policy.

Login and resource rights

The username and password allow employees access to a company's network resources. Because of physical assets like printers and servers, or electronic assets like files and folders, it is important to define controls that govern resource access.

1. The user id and password give the user access to resources.
2. The user is responsible for all activity associated with the user id and password. The password should not be shared with anyone, written down on paper, or stored on a computer. If for IT support reasons, the user reveals the password to IT staff, the staff should set the system to prompt the user for a password change when the user next logs in.
3. Request for access to additional resources should come from the user's manager.
4. Making access rights administration easier, rather than given individual rights, users should be placed in groups and use groups to allocated resources.

Creation of a user account

When a new employee starts, the Human Resources department should send a request to IT. The request should contain the following:

1. Employee number if this is used in the company,
2. First name, last name, middle initial,
3. Approval from the employee manager that the network access is needed, (Since small and mid-size companies may have many manual processes, network access may not be needed.)
4. Employment period. (Since the employee may be contract staff, accounts should be created to expire after a specified period.)
5. Work schedule. (Since the employee may be a shift worker, the account should be set to be active for a given period during the day.)

Some small businesses have their network infrastructure hosted by an external vendor, so each account created comes with a cost. Senior management should weigh the benefits of better security of network access versus costs.

Account deletion

As soon as the employee contract is terminated, it is important that an account be disabled. This prevents the unauthorized account from being used to access resources.

Human resources should notify IT of the exact details of an employee's disengagement. Except in the case where there is a sudden termination, IT should be notified at least a week before the employee's final date.

Before being deleted, the account should be disabled for 30 days. Any exceptions to this should be submitted as a request from Human Resources.

Privileged or System account

Privileged system accounts are used by IT support staff to conduct system activities. When creating a privileged system account, organizations should identify the following in their IT procedures:

1. Business purpose should be defined.
2. Responsible owner should be defined (user id).
3. Business manager should approve the creation of the account.
4. The responsible owner should recertify account details every 6 months.
5. Use of the account should be documented and there should be an audit trail.
6. The technical use of the account should be briefly described.
7. If someone in the responsible IT group leaves or when there is a possibility of security breach, the password may be changed.

Entitlement review

When users are moved within the company or if a project has ended, the resources rights of a user may change. It is important to have a process where the access rights are reviewed by the resource owners.

All access rights to resources should be documented in a periodic report. The report should be prepared by the resource administrators or the information security officer. The Access report should show:

1. All the user ids that have accessed the resource within the period.
2. The names of the associated users
3. A list of resources that the users have accessed.
4. The access rights of that the users have to the resources.
5. Show the date of the last time that the user accessed the resource.

The resource owners should review the entitlement report every 6 months. The company data security officer should coordinate the review process and make sure that the resource owners sign the review.

Remote access

Remote access extends the boundaries of the network and allows users to access company resources from outside the office. Remote access should be through a remote server which can allow the creation of user profiles.

There should be at least two types of profiles. One, a normal user profile which will be used by a user that doesn't perform system administrative work. Two, an IT support user profile for users that perform system support work.

The request for remote access should come from the manager; it should specify the kind of access needed and specify the primary location where access would occur.

Connection

The following guidelines are recommended for securing a remote access connection:

1. The remote access connection should have encryption for all connections.
2. The remote access connection should have a time out for all connections.
3. The remote access connection should have a log for all connections.
4. User id should be different from the network id.
5. The password should change with every connection.

Small businesses that have their IT infrastructure hosted by an external vendor should ensure these controls exist in the vendor's operations. If they have their own IT infrastructure, cost consideration should not prevent the installation of a remote system with good controls.

Firewall and Intrusion detection systems

In many companies, firewalls serve as the main defense against intruders and act as a gateway for all inbound and outbound network connections. Intrusion detection software helps to keep track of all network activities. Internal auditors need to review that organizations implement the following protocols to enhance their firewall use:

1. All external IP connections should be through the firewall.
2. The firewall should be setup with a default "deny all" configuration.
3. All configuration changes should follow the normal change control process. Requests should be reviewed by the security staff and approved by senior management.
4. All system alarms should be logged and archived daily.

Vulnerability and Threat management

One of the main reasons data controls are established is to manage potential software and hardware risks. During the IT planning process, organizations should consider the following guidelines:

1. There should be a defined process to receive information from vendors about updates and security patches.

2. There should be a defined process to test and implement patches and updates. There should be a template test plan document. Implementation should follow the management process for change.
3. To verify system invulnerability, especially if an external website is available to the public, once a year an ethical hack should be conducted by an outside source.
4. Before being placed in production, applications should undergo an ethical hack

MANAGE OPERATIONS

Segregation of duty

For small and medium size companies, there are IT functions that should not be combined. Due to the size of the companies envisioned in the scope of this document, this could prove very difficult to enforce. The IT headcount should be proportionate to revenues generation and other financial factors. In situations where there is inadequate segregation of duties, the following recommendations are suggested and should serve as sufficient compensating controls:

1. There should be an audit trail of all operations.
2. Change should be as localized as possible.
3. Change access rights should be as specific as possible.
4. Developers should be separate from support staff. Where developers play a dual role of support, all changes should follow a change management process.
5. There should be regular independent review of the access logs.
6. There should be a maker-checker control on data entry operations.

Continuity of Business (COB)

Incorporating COB plans as part of the IT planning process helps organizations maintain the safety of all employees and ensure the continuity of business operations when emergencies occur that disrupt the flow of daily activities. Two entities are important to ensure the continuity of corporate processes: people and computer hardware.

People: Documentation of Jobs and process

COB plans should document employee roles during emergencies. For instance, job descriptions should outline what the employee is required to do when an emergency occurs, especially job descriptions for IT staff. Office processes, such as those involving the use of computer systems, also should be documented in the COB plan and should be reviewed and updated regularly, as well as tested periodically by an external auditor or other disinterested party.

In case of an emergency, the plan should show the critical people in the department or the organization, what hardware needs to be connected to the network and its location.

Computers: Architecture and design

First and foremost, the architecture and design of all computer systems should be documented. If a system needs to be rebuilt, this will assist IT staff. In addition, documentation should be part of the organization's change management process. This means that whenever changes are made to

the computer system, documentation should be reviewed and updated. This document change process should be part of the change control process.

The architecture and design document should show the objective, business requirement, testing, technical specifications, business process integration and implementation strategy

Alternate Hardware

There should be alternate hardware stored in a different location. A hot site is a location that has all the required IT hardware and software installed and running. Because it may be too expensive for small and mid-size companies, there is no recommendation for a dormant hot site. Excess capacity may be built into the network design so that the COB site can be used for some production traffic. Management would have to consider cost considerations and required recovery speed.

A cold site is a location where the company has access to IT hardware. For small or mid-size businesses, a lease contract with an external data center should be available. Requirements for alternate location would depend on overall business recovery strategy, available datacenters, and the number of employees at each location. At a minimum, mid-size companies should have an alternative cold site, while small companies should have a good backup strategy.

System Backup and recovery

There should be a backup schedule. This would depend on the amount of data in use and the recovery Service Level Agreement (SLA) with the business. The backup should be stored offsite periodically. This offsite storage should be updated daily if possible and weekly at a minimum.

To ensure data integrity and to confirm the expected time to recover the data, backup data should be periodically restored. This process should be documented and reviewed by the data owners.

MANAGE PROBLEMS AND INCIDENTS

Monitoring

IT should set up a monitoring system for infrastructure systems, like operating systems, network devices, and hardware. Applications should have monitoring built into the system. A documented risk assessment should be conducted on the system to determine the risk level. The risk level determines what kind of monitoring is setup for the system.

For high risk system or business critical systems, real time monitoring should be configured. A benchmark should be established for various performance counters of the system. These benchmarks are used for real-time monitoring of the performance of various system components. Systems are also monitored for significant events such as attempted violations of system security.

For less critical systems, a periodic monitoring system can be configured. A periodic report created by IT should be sent out to the system owners, showing performance and availability metrics of the system. The report contains items such as memory and CPU utilization, server uptime and average user response time.

The alert system should be composed of different systems so that there is a backup if one fails. There can be an email system alert or a pager or phone system. There should be at least 2 user ids to alert. One of them should be a generic user id, which can be monitored by a designated person.

Applications should have logging enabled, so that there is an audit trail of activities done on the system. Infrastructure systems like operating systems and network devices should also have activity logging turned on. So that unnecessary information isn't collected, analysis should be done to determine what relevant events should be logged. At a minimum, logging of the following events is recommended:

1. The failed logon attempts,
2. Activity of the functional accounts,
3. Locking of user accounts,
4. Configuration changes.

Where there are applications with no logging function, compensating controls should be used. But there should be an upgrade plan. Here are some suggested compensating controls:

1. Marker-checker for system changes. One individual makes a change and another verifies after that only the specified change was done.
2. A weekly comparison of system configurations.

Problem reporting

System issues can be reported by the users or by the system administrators. There should be a formal process to create a support ticket to track the problem. A helpdesk ticket system can be purchased to make it more efficient.

The following should be included:

1. Access specifications or profiles,
2. Ability to build policies into the system. (i.e., a request for a new employee id can only come from Human Resources),
3. Archiving of tickets,
4. Search feature.

Small and mid-size organizations may outsource their helpdesk. It is important that there is a good workflow link with the vendor's system. For instance, a request for creation of a network account for a new employee should go from Human Resources to the helpdesk. Or if an account is locked, the request to unlock the account should only come from the manager of the user.

MANAGE CHANGES

Change management is the process used to plan, schedule, apply, distribute, and track changes for all corporate activities. There should be a formal documented process for implementation of change.

To help identify problems that may not be seen during the development phase, many organizations establish a laboratory to conduct tests before system changes are implemented. A lab should be set up where all testing is done. Since the lab is not a secure environment, test data should be used and not production data. If possible, the lab should be on a separate network segment.

The staging area is a segment of the network set apart for tests to determine how proposed system changes would impact the production system. As much as possible, the staging environment should simulate the production. All changes to production should first be implemented in the staging. Specific users should be given access to the staging environment for User Acceptance Testing (UAT) testing. The staging environment should be secured and can not be on the same segment as production.

A process for communicating change should be developed. The IT department will develop a document specifying the description of the change, the impact analysis, the system documents that need to be updated, the responsible support engineer, the time for the change and the fallback procedure.

There should be a change committee which is comprised of at least one technology person and at least one person from the business. The committee will meet weekly to review all change requests. Once they have been approved, an announcement is made to the affected users.

If there is an emergency change, the following apply:

1. The technology manager should approve the change,
2. There should be proper communication to affected parties,
3. After the emergency, the change form should be filled and approved,
4. There should be a post-mortem report on the change that should be sent to the business and technology manager(s).

Fall back

If there is a problem with the change, there should be a back to reverse the change and go back to the previous state. If there is a need for a fall back, there should be a review in the change control meeting to discuss reasons.

APPLICATION DEVELOPMENT

There are several software development models that a company can take; each depends on the project and the business requirements. For consistency reasons, it is recommended that the company adopt one method. The model chosen should involve the business in the beginning and end stages of development and require proper documentation at all levels.

Software Development Life Cycle

Development of minor tools or major applications should follow a Software Development Life Cycle (SDLC) model. This ensures proper communication of changes and that the business is involved in the development process.

Whether for minor tools or for major applications, at a minimum, the following steps should be part of any kind of development:

1. Business requirements document,
2. Technical specifications,
3. Data flow and system diagrams,
4. Documented testing
5. Preparation of a standard operating procedure and user guide,
6. Implementation plan.

In small corporations where there may be only one IT person, because of competing demands, there may be the tendency to develop ad-hoc tools and software. One compensating control is to make sure that at the specified period after implementation, a document describing the tool or software is submitted to an executive officer. This way in case the IT staff leaves suddenly, the company has a documented knowledge of the application.

The programming code for all applications should be properly documented. The physical and electronic copy should be kept in a central location.

Pre-implementation review

During the various stages of the SDLC process, the business security officer should review the application for adequate controls. If possible, an auditor should be involved in all stages of development, but this is not always possible in small and mid-size companies where the IT auditors are probably less than 5.

Post implementation review

There should also be a post implementation review done by an independent source. An IT auditor from the audit department is recommended.

DEFINE AND MANAGE SERVICE LEVEL

A service level agreement (SLA) is a formal document that defines service expectations between the customer and the service provider. It serves as a means to evaluate if the service provider is meeting the needs and requirements of the client. This has been common practice when companies deal with external service providers, but this can also be used internally especially for support departments.

Internal SLA

For small businesses, an internal SLA may not be needed. However, even though it might change the informal culture, small businesses with IT departments of 20 or less should consider implementing an SLA within the business. Where an SLA doesn't exist, there should be a documented process for IT operations. The document should state details of the process. Information on the following items should be included in the document:

1. The expected delivery times to the business,
2. The expected result for the business.

The document should be developed with the business.

For mid-size companies, there should be an internal service level agreement between technology and other departments. The agreement should define the following items:

1. Expected service such as timeliness and accuracy of data,
2. Service thresholds for escalating a problem to higher management levels
3. The call tree for escalation.

The SLA should be signed by the data owners.

External SLA

There should be an SLA with the vendor. The agreement is similar to the internal SLA defined above. It should state the following:

1. Expected service such as timeliness and accuracy of data,
2. Service thresholds for escalation,
3. The call tree for escalation.

Monitoring SLA

There should be a periodic report that states whether service level expectations were met. This report should be reviewed and signed by the data owners.

The SLA should be for a period, for example, for 1 or 2 years. At the end of the period, the SLA should be reviewed and renewed or not.

ACQUISITION OF HARDWARE AND SOFTWARE

It is important that the IT acquisitions are related to business needs and that a proper IT strategy is defined for the year. There should be periodic capacity analysis to determine if the current IT infrastructure is enough to support current and future business needs.

IT strategy definition

For mid size companies, there should be an IT governance/steering committee consisting of business people and the technology manager. This committee reviews policies and defines IT strategy for the year.

At the end of the second quarter, the steering committee meets to develop a formal IT strategic plan for the next year. In small businesses, it should be developed by the IT manager, who should be part of the business strategy discussions for the year. Since this determines the budget for technology, the data owners should sign an approval of the IT strategic plan.

Capacity planning

Based upon current resource utilization, historical trends, and projected business needs, this is the annual forecasting of future hardware, software, and network resource requirements.

Every three months a review should be done by IT management of current resource utilization to detect notable trends. Showing performance and availability metrics of the network system, a periodic (preferably every quarter) report should be sent out. The report should show comparison with historic and expected figures. The report can contain items such as the memory and CPU utilization, server uptime and average user response. The steering committee should discuss this report and, based on expected business needs, decide if the current or projected resources are adequate. At the end of the second quarter of the year, the steering committee should meet to decide resource requirements for the coming year. This should be submitted to the company budget officer by the end of the third quarter.

Purchase justification

Each acquisition should have a business justification related to either defined IT strategy or capacity planning. Unplanned requests should be justified by showing evidence of related support issues or new project request(s) from the business.

Manage Vendor Products

There should be a formal assessment procedure before a vendor product is selected. As much as possible, the selection process should show evidence that several vendor products were considered.

The contract with the vendor should be handled by the legal department and it should state the product license agreement, permission to audit, updates and support. Depending on the size of the vendor and the classification of the data handled by the product, there should be provision for the following:

1. Audit the vendor IT department for controls,
2. Have an escrow service where a copy of the code is stored.

BUILDING IT CONTROLS TODAY FOR THE FUTURE

Establishing internal controls that are part of IT policies and procedures benefits organizations of all sizes in various ways:

1. It helps build a controlled and compliant IT department for the organization. (IT processes are not only compliant with management policy but also with regulatory policies which call for tighter IT controls.)
2. It helps lead to better IT service for the users. (Since the IT policy calls for the involvement of the business in the IT processes, the IT staff can obtain a better picture of the user needs and can design their processes accordingly.)

The internal controls described above and in part one of this article should be discussed early in the IT planning process and culminate in the implementation of solid IT policies and procedures that allow the organization to have a more secure IT environment.

IT policies and procedures also help executive managers know the role IT plays in the organization and how internal controls are implemented to meet corporate strategic goals. Once established, internal auditors can use these policies and procedure as guidelines to examine the effectiveness of IT operations and assess whether their activities are compliant with internal regulations.