Common IT Considerations

There are some IT considerations or elements that are common to any IT audit regardless of the specific audit subject. Click the links below to read more about each of these areas.

Standards

Policies

Procedures

Separation of Duties

Identity Access Management (IAM)

Change Management

Standards

A standard is a mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as the International Organization for Standardization (ISO). A standard mandates not only what must be done, but also the way an enterprise must comply with it. Enterprises meeting the requirements of standards may be certified as compliant. Standards can help implement policy, limit risk and support efficient business operations.

Many enterprises believe that the value of standards is the authority and perception of excellence that they provide. In lieu of formal certification, an enterprise may base its practices and operations on external standards such as an ISO standard. Alternatively, an enterprise may develop its own standards, such as requiring all staff to use the same product, operating system or desktop. Proper use of a standard facilitates support and maintenance, provides better cost control, and provides authority for the practices and procedures of the enterprise because a standard requires the implementation of certain practices.

Policies

A policy is a document that records a high-level principle or course of action that has been adopted. The intended purpose is to influence and guide both present and future decision-making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams. Additionally, policies need to describe the consequences of failing to comply, the means for handling exceptions, and the manner in which compliance will be checked and measured.

Policies must be developed and communicated. If not, the enterprise has no means of enforcing standards of behavior, which increases the risk that the behavior that occurs may be inappropriate. A lack of enforcement may also lead to circumvention of controls or increased liability because the enterprise recognizes the need for a policy but does not follow its own rules.

An IT auditor should understand that policies are a part of the audit scope and test the policies for compliance. IT controls should flow from the enterprise's policies, and an IT auditor should use policies as a benchmark for evaluating compliance. However, any policies that hinder the achievement of business objectives must be identified and reported for improvement. An IT auditor should also consider the extent to which the policies apply to third parties or outsourcers, the extent to which third parties or outsourcers comply with the policies, and whether the policies of the third parties or outsourcers are in conflict with the enterprise's policies.

Procedures

A procedure is a document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. A procedure is defined as a part of a process. Procedures are created to define the ways in which processes should be carried out. Procedures are invaluable as means of implementing the intent of policies because they specify the tasks that people perform. By describing actions in consistent and measurable ways, an enterprise can greatly increase the probability that an operation will be conducted according to good practice and that any abnormal operations will be detected.

Generally, procedures are more dynamic than their respective parent policies. Procedures must reflect the regular changes in business and aligned IT focus and environment. Therefore, frequent reviews and updates of procedures are essential if they are to be relevant. An IT auditor should review procedures to identify/evaluate and thereafter test controls over business and aligned IT processes. The controls embedded in procedures are evaluated to ensure they fulfill necessary control objectives while making processes as efficient and practical as possible. Where operational practices do not match documented procedures or where documented procedures do not exist, it is difficult for management and auditors to identify controls and ensure that they are in continuous operation.

Lack of procedures makes it difficult to carry out activities in a systematic manner and may result in undependable, inconsistent operations and elevated risk. Procedures should be published and used. It is common for procedures to be followed for only a short time, after which experienced staff begin to work from memory. This practice should be discouraged for any operations in which precision is important, such as shutdown procedures for power plants or industrial machinery, or complex monetary transactions. Quite often, procedures are embedded in information systems, which is an advisable practice to further integrate them within the enterprise.

Separation of Duties

An enterprise should have an organizational structure that provides an adequate separation of duties. An IT auditor should understand general organizational controls and be able to evaluate these controls in the enterprise. Where there is a strong emphasis on cooperative distributed processing or on end-user computing, IT functions may be organized somewhat differently from separate system and operation functions. An IT auditor should be able to review these organizational structures and assess the level of control they provide.

Separation of duties (SoD) is a basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for documenting the custody of assets. SoD avoids the possibility that a single person could be responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner during the normal course of carrying out business processes. SoD is an important means by which fraudulent and/or malicious acts can be discouraged and prevented. Duties that should be segregated include:

- Custody of assets
- Transaction authorization
- Recording transactions

If adequate SoD does not exist, the following can occur:

- Misappropriation of assets
- Misstated financial statements
- Inaccurate financial documentation (i.e., errors or irregularities)
- Undetected improper use of funds or modification of data
- Undetected unauthorized or erroneous changes or modification of data and programs

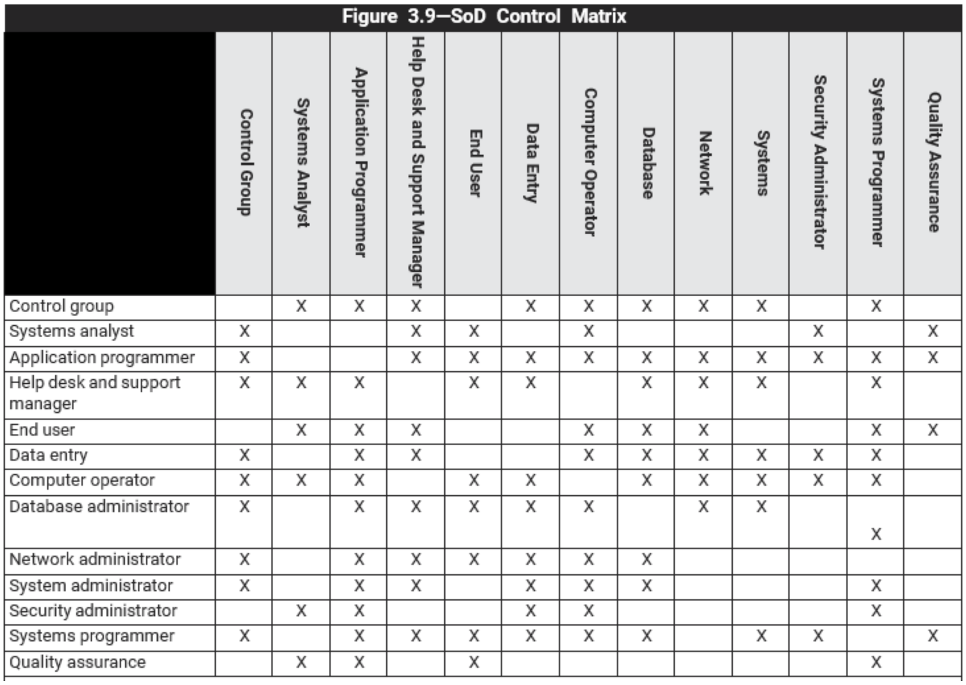
The IT and end-user departments should be organized to achieve adequate SoD.

Figure 3.9 shows an example of a guideline for the development of a SoD control matrix of job responsibilities that should not be combined.

The SoD control matrix (figure 3.9) is not an industry standard but a guideline indicating the positions that should be separated and those positions that require compensating controls when combined.

The matrix illustrates potential SoD issues and should not be viewed or used as an absolute; rather, it should be used to help identify potential conflicts so that proper questions may be asked to identify compensating controls.

Figure 3.9—SoD Control Matrix



	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database	Network	Systems	Security Administrator	Systems Programmer	Quality Assurance
Control group		X	X	X		X	X	X	X	X		X	
Systems analyst	X			X	X		X				X		X
Application programmer	X			X	X	X	X	X	X	X	X	X	X
Help desk and support manager	X	X	X		X	X		X	X	X		X	
End user		X	X	X			X	X	X			X	X
Data entry	X		X	X			X	X	X	X	X	X	
Computer operator	X	X	X		X	X		X	X	X	X	X	
Database administrator	X		X	X	X	X	X		X	X		X	
Network administrator	X		X	X	X	X	X	X					
System administrator	X		X	X		X	X	X				X	
Security administrator		X	X			X	X					X	
Systems programmer	X		X	X	X	X	X	X		X	X		X
Quality assurance		X	X		X							X	

Identity Access Management (IAM)

Identity access management encapsulates people, processes and products to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources. The goal of IAM is to provide appropriate access to enterprise resources.

Identity management is comprised of many components that provide a collective and common infrastructure, including directory services, authentication services (validating who the user is) and authorization services (ensuring the user has appropriate privileges to access systems based on a personalized profile). It also includes user management capabilities, such as user provisioning and deprovisioning.

Identification/authentication is a critical building block of IT security because it is needed for most types of access control and is necessary for establishing user accountability. User accountability requires the linking of activities on an IT system to specific individuals and therefore requires the system to identify users. For most systems, identification and authentication constitute the first line of defense by preventing unauthorized people (or unauthorized processes) from entering an IT system or accessing an information asset. If users are not properly identified and authenticated, an enterprise has a higher exposure to risk of unauthorized access.

Common identification and authorization vulnerabilities that may be exploited to gain unauthorized system access include:

- Weak authentication methods (e.g., no enforcement of password minimum length, complexity and change frequency)
- Use of simple or easily guessed passwords
- Potential for users to bypass the authentication mechanism
- Lack of confidentiality and integrity for the stored authentication information
- Lack of encryption for authentication and protection of information transmitted over a network
- Lack of user knowledge about the risk associated with sharing authentication elements (e.g., passwords and security tokens)

If an end user is asked about authentication, discussion usually turns to passwords. Passwords may be a familiar method of authentication, but they are not the only method, and their reliability has long been the subject of debate. Authentication of devices and users is performed to ensure that access to the enterprise resources is granted in accordance with the enterprise authentication policies.

Change Management

Change management is a holistic and proactive approach to managing the transition from a current to a desired organizational state, focusing specifically on the critical human, or soft, elements of change. Change management includes activities such as culture change (values, beliefs and attitudes), development of reward systems (measures and appropriate incentives), organizational design, stakeholder management, human resources policies and procedures, executive coaching, change leadership training, team building and communication planning and execution.

Change management in IT involves use of a defined and documented process to identify and apply, at the infrastructure and application levels, technology improvements that are beneficial to the enterprise and involve all levels of the enterprise impacted by the changes.

The primary concern is ensuring that changes to the environment do not introduce stability. Accordingly, an IT auditor should verify that the enterprise has an established methodology for prioritizing and approving system change requests and preventing unauthorized changes to programs.

An IT auditor should determine whether:

- Formal change management procedures are in place to handle in a standardized manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and underlying platforms.
- Requests for change are categorized, prioritized and authorized.
- There is an established process for handling emergency changes that do not follow the established change process.
- There is a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes.
- Approved changes are implemented as planned and document and user procedures are updated accordingly.

In addition to emergency changes, there are automated changes and blanket changes that the auditor should consider.

- Automated changes are processes that automatically generate software changes from one environment to another without human intervention.
- Blanket changes are a group of changes (e.g., router configuration changes, firewall rule updates) that are needed on a periodic basis.