

## **Module 5 - Introduction to Processes and Controls**

### Handout 4 - IT General Controls (Normative Model)

#### *IT General Controls*

Providing information to enable management's reporting to key stakeholders is a life cycle of collecting complete and accurate information and reporting it on a timely basis. As one might expect, this life cycle is highly dependent on information systems, such as applications, databases and other tools used to enhance the efficiency and effectiveness of data processing. The balance of this handout is dedicated to providing guidance on IT controls that are specifically designed to support financial reporting objectives. These controls are not intended to be an exhaustive list. However, they do provide a starting point as agencies determine which IT controls are necessary for their environment. Consideration should also be given to IT controls that may not be included below, but which an agency considers relevant nonetheless. The most relevant internal controls applicable to financial statement assertions can be defined to include activities that prevent or detect and correct a significant misstatement in the financial reporting or other required disclosures, including those over recording amounts into the general ledger and recording journal entries (standard, nonstandard and consolidation). The most relevant controls may be manual or automated, and preventive or detective in nature.

*As noted previously, this guidance is not intended to be authoritative. Professional judgment, as always, needs to be applied when determining the necessary controls that should be included in the compliance program, including some which may not be highlighted as most relevant controls in this document.*

**Note: The documentation noted below is from the IT Governance Institute (ITGI), IT Control Objectives For Sarbanes Oxley – “THE ROLE OF IT IN THE DESIGN AND IMPLEMENTATION OF INTERNAL CONTROL OVER FINANCIAL REPORTING (2<sup>ND</sup> EDITION)”.**

# Module 5 - Introduction to Processes and Controls

## Handout 4 - IT General Controls (Normative Model)

### Acquire and Maintain Application Software (AI2)

*Control Objective:* Controls provide reasonable assurance that application and system software is acquired or developed that effectively supports financial reporting requirements.

*Rationale:* The process of acquiring and maintaining software includes the design, acquisition/building and deployment of systems that support the achievement of business objectives. This process includes major changes to existing systems. This is where controls are designed and implemented to support initiating, recording, processing and reporting financial information and disclosure. Deficiencies in this area may have a significant impact on financial reporting and disclosure. For instance, without sufficient controls over application interfaces, financial information may not be complete or accurate.

IT General Controls supporting control objective:

<b>IT General Control (Bold controls are considered most relevant for EAGLE compliance)</b>	<b>Tests of Controls</b>	<b>COBIT References (4.0)</b>
<b>The organization has a system development life cycle (SDLC) methodology, which includes security and processing integrity requirements of the organization.</b>	Obtain a copy of the organization's SDLC methodology to determine that it addresses security and processing integrity requirements. Consider whether there are appropriate steps to determine if these requirements are considered throughout the development or acquisition life cycle, e.g., security and processing integrity are considered during the requirements phase.	PO8.3 AI2.3 AI2.4
The organization's SDLC policies and procedures consider the development and acquisition of new systems and major changes to existing systems.	Review the organization's SDLC methodology to determine if it considers both the development and acquisition of new systems and major changes to existing systems.	PO6.3 AI2 AI6.2
<b>The SDLC methodology includes requirements that information systems be designed to include application controls that support complete, accurate, authorized</b>	Review the SDLC methodology to determine if it addresses application controls. Consider whether there are appropriate steps so that application controls are	AI1 AI2.3 AC

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

<b>and valid transaction processing.</b>	considered throughout the development or acquisition life cycle, e.g., application controls should be included in the conceptual design and detail design phases.	
The organization has an acquisition and planning process that aligns with its overall strategic direction.	Review the SDLC methodology to determine if the organization's overall strategic direction is considered, e.g., an IT steering committee should review and approve projects so that a proposed project aligns with strategic business requirements and will utilize approved technologies.	PO4.3 AI3.1
<b>To maintain a reliable environment, IT management involves users in the design of applications, selection of packaged software and testing thereof.</b>	Review the SDLC methodology to determine if users are appropriately involved in the design of applications, selection of packaged software and testing.	AI1 AI2.1 AI2.2 AI7.2
Postimplementation reviews are performed to verify that controls are operating effectively.	Determine if postimplementation reviews are performed on new systems and significant changes reported.	AI7.12
<b>The organization acquires/develops application systems software in accordance with its acquisition, development and planning process.</b>	Select a sample of projects that resulted in new financial systems being implemented. Review the documentation and deliverables from these projects to determine if they have been completed in accordance with the acquisition, development and planning processes.	AI2

#### Acquire and Maintain Technology Infrastructure (AI3)

*Control Objective:* Controls provide reasonable assurance that technology infrastructure is acquired so that it provides the appropriate platforms to support financial reporting applications.

*Rationale:* The process of acquiring and maintaining technology infrastructure includes the design, acquisition/building and deployment of systems that support applications and

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

communications. Infrastructure components, including servers, networks and databases, are critical for secure and reliable information processing. Without an adequate infrastructure there is an increased risk that financial reporting applications will not be able to pass data between applications, financial reporting applications will not operate, and critical infrastructure failures will not be detected in a timely manner.

IT General Control	Tests of Controls	COBIT References (4.0)
Documented procedures exist and are followed so that infrastructure systems, including network devices and software, are acquired based on the requirements of the financial application they are intended to support.	Select a sample of technology infrastructure implementations. Review the documentation and deliverables from these projects to determine if infrastructure requirements were considered at the appropriate time during the acquisition process.	AI3

#### **Enable Operations (PO6, PO8, AI6, DS13)**

*Control Objective:* Controls provide reasonable assurance that policies and procedures that define required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.

*Rationale:* Policies and procedures include the SDLC methodology and the process for acquiring, developing and maintaining applications as well as required documentation. For some organizations, the policies and procedures include service level agreements, operational practices and training materials. Policies and procedures support an organization's commitment to perform business process activities in a consistent and objective manner.

IT General Control	Tests of Controls	COBIT References (4.0)
<b>The organization has policies and procedures regarding program development, program change, access to programs and data, and computer operations, which are periodically reviewed, updated and approved by management.</b>	Confirm that the organization has policies and procedures that are reviewed and updated regularly for changes in the business. When policies and procedures are changed, determine if management approves such changes.  Select a sample of projects and	PO6.1 PO6.3 PO8.1 PO8.2 PO8.3 AI6.1 D13.1

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

	determine that user reference and support manuals, systems documentation and operations documentation were prepared. Consider whether drafts of these manuals were incorporated in user acceptance testing. Determine whether any changes to proposed controls resulted in documentation updates.	
<b>The organization develops, maintains and operates its systems and applications in accordance with its supported, documented policies and procedures.</b>	Obtain the policies and procedures and determine if the organization manages its IT environment in accordance with them.	PO6.1 PO6.3 PO8.1 PO8.2 AI6.1 DS13.1

#### Install and Accredit Solutions and Changes (AI7)

*Control Objective:* Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and that associated controls operate as intended and support financial reporting requirements.

*Rationale:* Installation testing and validating relate to the migration of new systems into production. Before such systems are installed, appropriate testing and validation should be performed to determine if the systems are operating as designed. Without adequate testing, systems may not function as intended and may provide invalid information, which could result in unreliable financial information and reports.

<b>IT General Control</b>	<b>Tests of Controls</b>	<b>COBIT References (4.0)</b>
<b>A testing strategy is developed and followed for all significant changes in applications and infrastructure technology, which addresses unit, system, integration and user acceptance-level testing so that deployed systems operate as intended.</b>	Select a sample of systems development projects and significant system upgrades (including technology upgrades). Determine if a formal testing strategy was prepared and followed. Consider whether this strategy considered potential development and implementation risks and addressed all the necessary components to address these risks, e.g., if the completeness and accuracy of system interfaces are essential to the production of complete and accurate reporting, these	AI7.2 AI7.4 AI7.6 AI7.7

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

	interfaces were included in the testing strategy. (Note: Controls over the final move to production are addressed in <i>Manage Changes</i> )	
Load and stress testing is performed according to a test plan and established testing standards.	Select a sample of system development projects and system upgrades that are significant for financial reporting. Where capacity and performance were considered of potential concern, review the approach to load and stress testing. Consider whether a structured approach was taken to load and stress testing and the approach taken adequately modeled the anticipated volumes, including types of transactions being processed and the impact on performance of other services that would be running concurrently.	AI7.2
<b>Interfaces with other systems are tested to confirm that data transmissions are complete, accurate and valid.</b>	Select a sample of system development projects and system upgrades that are significant for financial reporting. Determine if interfaces with other systems were tested to confirm that data transmissions are complete, e.g., record totals are accurate and valid. Consider whether the extent of testing was sufficient and included recovery in the event of incomplete data transmissions.	AI7.5
<b>The conversion of data is tested between their origin and their destination to confirm that the data are complete, accurate and valid.</b>	Obtained a sample of system development projects and system upgrades that are significant for financial reporting. Determine if a conversion strategy documented. Consider whether it included strategies to “scrub” the data in the old system before the conversion, or to “run down” data in the old system before conversion. Review the conversion testing plan.	AI7.5

#### Manage Changes (AI6, AI7)

*Control Objective:* Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production.

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

*Rationale:* Managing changes addresses how an organization modifies system functionality to help the business meet its financial reporting objectives. Deficiencies in this area could significantly impact financial reporting. For instance, changes to the programs that allocate financial data to accounts require appropriate approvals and testing prior to the change so that proper classification and reporting integrity is maintained.

IT General Control	Tests of Controls	COBIT References (4.0)
<p><b>Requests for program changes, system changes and maintenance (including changes to system software) are standardized, logged, approved, documented and subject to formal change management procedures.</b></p>	<p>Determine that a documented change management process exists and is maintained to reflect the current process.</p> <p>Consider if change management procedures exist for all changes to the production environment, including program changes, system maintenance and infrastructure changes.</p> <p>Evaluate the process used to control and monitor change requests.</p> <p>Consider whether change requests are properly initiated, approved and tracked.</p> <p>Determine whether program change is performed in a segregated, controlled environment.</p> <p>Select a sample of changes made to applications/systems to determine whether they were adequately tested and approved before being placed into a production environment. Establish if the followed are included in the approval process: operations, security, IT infrastructure</p>	<p>AI6.1 AI6.2 AI6.4 AI6.5 AI7.3 AI7.8 AI7.9 AI7.10 AI7.11</p>

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

	<p>management and IT management.</p> <p>Evaluate procedures designed to determine that only authorized/approved changes are moved into production.</p> <p>Trace the sample of changes back to the change request log and supporting documentation.</p> <p>Confirm that these procedures address the timely implementation of patches to system software. Select a sample to determine compliance with the documented procedures.</p>	
<p><b>Emergency change requests are documented and subject to formal change management procedures.</b></p>	<p>Determine if a process exists to control and supervise emergency changes.</p> <p>Determine if an audit trail exists of all emergency activity and verify that it is independently reviewed.</p> <p>Determine that procedures require emergency changes to be supported by appropriate documentation.</p> <p>Establish that backout procedures developed for emergency changes.</p> <p>Evaluate procedures ensuring that all emergency changes are tested and subject to standard approval procedures after they have been made. Review a sample of changes that are recorded as “emergency” changes, and determine if they contain the needed approval and the needed access was terminated after a set period of time. Establish</p>	<p>AI6.3 AI7.10</p>

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

	that the sample of changes was well documented.	
<b>Controls are in place to restrict migration of programs to production by authorized individuals only.</b>	Evaluate the approvals required before a program is moved to production. Consider approvals from system owners, development staff and computer operations.  Confirm that there is appropriate segregation of duties between the staff responsible for moving a program into production and development staff. Obtain and test evidence to support this assertion.	AI7.8
IT management implements system software that does not jeopardize the security of the data and programs being stored on the system.	Determine that a risk assessment of the potential impact of changes to system software is performed. Review procedures to test changes to system software in a development environment before they are applied to production. Verify that backout procedures exist.	AI6.2 AI7.4 AI7.9

#### **Define and Manage Service Levels (DS1)**

*Control Objective:* Controls provide reasonable assurance that service levels are defined and managed in a manner that satisfies financial reporting system requirements and provides a common understanding of performance levels by which the quality of services will be measured.

*Rationale:* The process of defining and managing service levels addresses how an organization meets the functional and operational expectations of its users and, ultimately, the objectives of the business. Roles and responsibilities are defined and an accountability and measurement model is used to determine if services are delivered as required. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, if systems are poorly managed or system functionality is not delivered as required, financial information may not be processed as intended.

<b>IT General Control</b>	<b>Tests of Controls</b>	<b>COBIT References (4.0)</b>
Service levels are defined and	Obtain a sample of service level	DS1.2

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

<p>managed to support financial reporting system requirements.</p>	<p>agreements and review their content for clear definition of service descriptions and expectations of users.</p> <p>Discuss with members of the organization responsible for service level management and test evidence to determine whether service levels are actively managed.</p> <p>Obtain and test evidence that service levels are being actively managed in accordance with service level agreements.</p> <p>Discuss with users whether financial reporting systems are being supported and delivered in accordance with their expectations and service level agreements.</p>	<p>DS1.3 DS1.5 DS1.6</p>
<p>A framework is defined to establish appropriate performance indicators to manage service-level agreements, both internally and externally.</p>	<p>Obtain service-level performance reports and confirm that they include key performance indicators.</p> <p>Review the performance results, identify performance issues and assess how service-level managers are addressing these issues.</p>	<p>DS1.1 DS1.3</p>

#### Manage Third-party Services (DS2)

*Control Objective:* Controls provide reasonable assurance that third-party services are secure, accurate and available; support processing integrity; and are defined appropriately in performance contracts.

*Rationale:* Managing third-party services includes the use of outsourced service providers to support financial applications and related systems. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, insufficient controls over processing accuracy by a third-party service provider may result in inaccurate financial results.

## **Module 5 - Introduction to Processes and Controls**

### Handout 4 - IT General Controls (Normative Model)

<b>IT General Control</b>	<b>Tests of Controls</b>	<b>COBIT References (4.0)</b>
A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service-level performance criteria.	Determine if the management of third-party services has been assigned to appropriate individuals.	DS2.2
Selection of vendors for outsourced services is performed in accordance the organization's vendor management policy.	<p>Obtain the organization's vendor management policy and discuss with those responsible for third-party service management if they follow such standards.</p> <p>Obtain and test evidence that the selection of vendors for outsourced services is performed in accordance with the organization's vendor management policy.</p>	PO1.4 PO6.3 DS2
IT management determines that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service and a review of their financial viability.	<p>Obtain the criteria and business case used for selection of their-party service providers.</p> <p>Assess whether these criteria include a consideration of the third party's financial stability, skill and knowledge of the systems under management, and controls over security and processing integrity.</p>	DS2.3
Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.	Select a sample of third-party service contracts and determine if they include controls to support security and processing integrity in accordance with the company's policies and procedures.	DS2.3

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

<p>Procedures exist and are followed that include requirements that for third-party services a formal contract be defined and agreed to before work is initiated, including definition of internal control requirements and acceptance of the organization's policies and procedures.</p>	<p>Review a sample of contracts and determine whether:</p> <ul style="list-style-type: none"> <li>• There is definition of services to be performed</li> <li>• The responsibilities for the controls over financial reporting systems have been adequately defined.</li> <li>• The third party has accepted compliance with the organization's policies and procedures, e.g., security policies and procedures.</li> <li>• The contracts were reviewed and signed by appropriate parties before work commenced.</li> <li>• The controls over financial reporting systems and subsystems described in the contract agree with those required by the organization.</li> </ul> <p>Review gaps, if any, and consider further analysis to determine the impact on financial reporting.</p>	<p>DS2.3</p>
<p><b>A regular review of security and processing integrity is performed by third-party service providers (e.g., SAS 70, Canadian 5970, and ISA 402).</b></p>	<p>Inquire whether third-party service providers perform independent reviews of security and processing integrity, e.g., a service auditor report. Obtain a sample of the most recent review and determine if there are any control deficiencies that would impact financial reporting.</p>	<p>ME2.6</p>

#### Ensure System Security (DS5)

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

*Control Objective:* Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.

*Rationale:* Managing systems security includes both physical and logical controls that prevent unauthorized access. These controls typically support authorization, authentication, nonrepudiation, data classification and security monitoring. Deficiencies in this area could significantly impact financial reporting. For instance, insufficient controls over transaction authorization may result in inaccurate financial reporting.

IT General Control	Tests of Controls	COBIT References (4.0)
<p><b>An information security policy exists and has been approved by an appropriate level of executive management.</b></p>	<p>Obtain a copy of the organization's security policy and evaluate the effectiveness. Points to be taken into consideration include:</p> <ul style="list-style-type: none"> <li>• Is there an overall statement of the importance of security to the organization?</li> <li>• Have specific policy objectives been defined?</li> <li>• Have employee and contractor security responsibilities been addressed?</li> <li>• Has the policy been approved by an appropriate level of senior management to demonstrate management's commitment to security?</li> <li>• Is there a process to communicate the policy to all levels of management and employees?</li> </ul>	<p>PO6.3 PO6.5 PO5.2</p>
<p>A framework of security standards has been developed that supports the objectives of the security policy</p>	<p>Obtain a copy of the security standards. Determine whether the standards framework effectively meets the objectives of the security policy. Consider whether the</p>	<p>PO8.2 DS5.2</p>

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

	<p>following topics, which are often addressed by security standards, have been appropriately covered:</p> <ul style="list-style-type: none"> <li>• Security organization</li> <li>• Roles and responsibilities</li> <li>• Physical and environmental security</li> <li>• Operating system security</li> <li>• Network security</li> <li>• Application security</li> <li>• Database security</li> </ul> <p>Determine if there are processes in place to communicate and maintain these standards</p>	
An IT security plan exists that is aligned with overall IT strategic plans	Obtain a copy of security plans or strategies for financial reporting systems and subsystems and assess their adequacy in relation to the overall company plan.	DS5.2
The IT security plan is updated to reflect changes in the IT environment as well as security requirements of specific systems.	Confirm that the security plan reflects the unique security requirements of financial reporting systems and subsystems.	DS5.2
<b>Procedures exist and are followed to authenticate all users of the system (both internal and external) to support the existence of transactions.</b>	Assess the authentication mechanisms used to validate user credentials for financial reporting systems and subsystems and validate that user sessions time-out after the predetermined period of time. Validate that no shared user profiles (including administrative profiles) are used.	DS5.3 AC
<b>Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes)</b>	Review the security practices to confirm that authentication controls (passwords, IDs, two-factor, etc.) are used appropriately and are subject to common confidentiality requirements (IDs and passwords not shared, alphanumeric passwords used, etc.).	DS5.3 DS5.4
<b>Procedures exist and are followed</b>	Confirm that procedures for the	DS5.4

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

<p><b>relating to timely action for requesting, establishing, issuing, suspending and closing user account. (Include procedures for authenticating transactions originating outside the organization.)</b></p>	<p>registration, change and deletion of users from financial reporting systems and subsystems on a timely basis exist and are followed.</p> <p>Select a sample of new users and determine if management approved their access and the access granted agrees with the access privileges that were approved.</p> <p>Select a sample of terminated employees and determine if their access has been removed, and the removal was done in a timely manner.</p> <p>Select a sample of privileged and current users and review their access for appropriateness based upon their job functions.</p>	
<p><b>A control process exists and is followed to periodically review and confirm access rights.</b></p>	<p>Inquire whether access controls for financial reporting systems and subsystems are reviewed by management on a periodic basis.</p> <p>Assess the adequacy of how exceptions are reexamined, and if the follow-up occurs in a timely manner.</p>	DS5.4
<p>Where appropriate, controls exist so that neither party can deny transactions, and controls are implemented to provide nonrepudiation of origin or receipt, proof of submission, and receipt of transactions.</p>	<p>Determine how the organization established accountability for transaction initiation and approval.</p> <p>Test the use of accountability controls by observing a user attempting to enter an authorized transaction.</p> <p>Obtain a sample of transactions, and identify evidence of the</p>	DS11.6 AC

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

	accountability or origination of each.	
Appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access via public networks.	<p>Determine the sufficiency and appropriateness of perimeter security controls, including firewalls, and intrusion detection systems.</p> <p>Inquire whether management has performed an independent assessment of controls within the past year (e.g., ethical hacking, social engineering).</p> <p>Obtain a copy of this assessment and review the results, including the appropriateness of follow-up on identified weaknesses.</p> <p>Determine if antivirus systems are used to protect the integrity and security of financial reporting systems and subsystems.</p> <p>When appropriate, determine if encryption techniques are used to support the confidentiality of financial information sent from one system to another.</p>	DS5.10
<b>IT security administration monitors and logs security activity at the operating systems, application and database levels and identified security violations are reported to senior management.</b>	<p>Inquire whether a security office exists to monitor for security vulnerabilities at the application and database levels and related threat events.</p> <p>Asses the nature and extent of such events over the past year and discuss with management how they have responded with controls to prevent unauthorized access or manipulation of financial systems and subsystems.</p>	DS5.5

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

	Validate that attempts to gain unauthorized access to financial reporting systems and subsystems are logged and follow up on a timely basis.	
<b>Controls relating to appropriate segregation of duties over requesting and granting access to systems and data exist and are followed.</b>	Review the process to request and grant access to systems and data and confirm that the same person does not perform these functions.	DS5.3 DS5.4
Access to facilities is restricted to authorized personnel and requires appropriate identification and authentication.	<p>Obtain policies and procedures as they relate to facility security, key and card reader access, and determine if those procedures account for proper identification and authentication.</p> <p>Observe the in-and-out traffic to the organizations facilities to establish that proper access is controlled.</p> <p>Select a sample of users and determine if their access is appropriate based upon their job responsibilities.</p>	DS12.2 DS12.3

#### **Manage the Configuration (DS9)**

*Control Objective:* Controls provide reasonable assurance that IT components, as they relate to security and processing, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

*Rationale:* Configuration management includes procedures such that security and processing integrity controls are set up in the system and maintained through its life cycle. Insufficient configuration controls can lead to security exposures that may permit unauthorized access to systems and data and impact financial reporting. An additional potential risk is corruption to data integrity caused by poor control of the configuration when making system changes or by the introduction of unauthorized system components.

<b>IT General Control</b>	<b>Tests of Controls</b>	<b>COBIT References (4.0)</b>
Only authorized software is permitted for use by employees using company IT assets.	<p>Determine if procedures are in place to detect and prevent the use of unauthorized software. Obtain and review the company policy as it related to software use to see that it is clearly articulated.</p> <p>Consider reviewing a sample of applications and computer to determine if they are in conformance with organization policy.</p>	DS9.2
System infrastructure, including firewalls, routers, switches, network operating systems, servers and other related devices, is properly configured to prevent unauthorized access.	<p>Determine if the organization's policies require the documentation of the current configuration, as well as the security configuration, settings to be implemented.</p> <p>Review a sample of servers, firewalls, routers, etc., to consider if they have been configured in accordance with the organization's policy.</p>	DS5.3 DS5.4 DS5.10
<b>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.</b>	<p>Conduct an evaluation of the frequency and timeliness of management's review of configuration records.</p> <p>Assess whether management has documented the configuration management procedures.</p> <p>Review a sample of configuration</p>	DS5.4

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

	changes, additions or deletions, to consider if they have been properly approved based on a demonstrated need.	
IT management has established procedures across the organization to protect information systems and technology from computer viruses.	Review the organization's procedures to detect computer viruses.  Verify that the organization has installed and is issuing virus software on its networks and personal computers.	DS5.9
Periodic testing and assessment is performed to confirm that the software and network infrastructure is appropriately configured.	Review the software and network infrastructure to establish that it has been appropriately configured and maintained, according to the organization's documented process.	AI3.2 AI3.3

#### Manage Problems and Incidents (DS8, DS10)

*Control Objective:* Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution.

*Rationale:* The process of managing problems and incidents addresses how an organization identifies, documents and responds to events that fall outside of normal operations. Deficiencies in this area could significantly impact financial reporting.

<b>IT General Control</b>	<b>Tests of Controls</b>	<b>COBIT References (4.0)</b>
<b>IT management has defined and implemented an incident and problem management system such that data integrity and access control incidents are recorded, analyzed, resolved in a timely manner and reported to management.</b>	Determine if an incident management system exists and how it is being used. Review how management has documented how the system is to be used.  Review a sample of incident reports, to consider if the issues were addressed (recorded, analyzed and resolved) in a timely manner.	DS8
The problem management system	Determine if the organization's	DS10.2

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

provides for adequate audit trail facilities, which allow tracing from problem or incident to underlying cause.	procedures include audit trail facilities – tracking of the problems or incidents.  Review a sample of problems recorded on the problem management system to consider if a proper audit trail exists and is used.	
A security incident response process exists to support timely response and investigation of unauthorized activities.	Verify that unauthorized activities are responded to in a timely fashion, and there is a process to support proper disposition.	DS5.6 DS8.3 DS10.1 DS10.3

#### **Manage Data (DS11)**

*Control Objective:* Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.

*Rationale:* Managing data includes the controls and procedures used to support information integrity, including its completeness, accuracy, authorization and existence. Controls are designed to support initiating, recording, processing and reporting financial information. Deficiencies in this area could significantly impact financial reporting. For instance, without appropriate authorization controls over the initiation of transactions, resulting financial information may not be reliable.

<b>IT General Control</b>	<b>Tests of Controls</b>	<b>COBIT References (4.0)</b>
Policies and procedures exist for the distribution and retention of data and reporting output.	Review the policies and procedures for the distribution and retention of data and reporting output. Determine whether the policies and procedures are adequate for the protection of data and the timely distribution of the correct financial reports (including electronic reports) to appropriate personnel.  Obtain and test evidence that the controls over the protection of data and timely distribution of financial reports (including electronic	DS11.1 DS11.2 DS11.6

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

	reports) to appropriate personnel are operating effectively.	
Management protects sensitive information – logically and physically, in storage and during transmission – against unauthorized access or modification.	Review the results of security testing. Determine if there are adequate controls to protect sensitive information – logically and physically, in storage and during transmission – against unauthorized access or modification.	DS11.6
Retention periods and storage terms are defined for documents, data, programs, reports and messages (incoming and outgoing), as well as the data (keys, certificates) used for their encryption and authentication.	<p>Obtain the procedures dealing with distribution and retention of data.</p> <p>Confirm that the procedures define the retention periods and storage terms for documents, data, programs, reports and messages (incoming and outgoing), as well as the data (keys, certificates) used for their encryption and authentication.</p> <p>Confirm that the retention periods are in conformity with Sarbanes-Oxley Act.</p> <p>Confirm that the retention periods of previously archived material are in conformity with the Sarbanes-Oxley Act. Select a sample of archived material and test evidence that archived material is being archived in conformance with the requirements of the Sarbanes-Oxley Act.</p>	DS11.2
<b>Management has implemented a strategy for cyclical backup of data and programs.</b>	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.	DS11.5
<b>The restoration of information is</b>	Inquire whether the retention and	DS11.5

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

<p><b>periodically tested.</b></p>	<p>storage of messages, documents, programs, etc., have been tested during the past year.</p> <p>Obtain and review the results of testing activities.</p> <p>Establish whether any deficiencies were noted and whether they have been reexamined. Obtain the organization's access security policy and discuss with those responsible whether they follow such standards and guidelines dealing with sensitive backup data.</p>	
<p>Changes to data structures are authorized, made in accordance with design specifications and implemented in a timely manner.</p>	<p>Obtain a sample of data structure changes and determine whether they adhere to the design specifications and were implemented in the time frame required.</p>	<p>AI6</p>

#### Manage Operations (DS13)

*Control Objective:* Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing and error monitoring.

*Rationale:* Managing operations addresses how an organization maintains reliable application systems in support of the business to initiate, record, process and report financial information. Deficiencies in this area could significantly impact an entity's financial reporting. For instance, lapses in the continuity of application systems may prevent an organization from recording financial transactions and thereby undermine its integrity.

IT General Control	Tests of Controls	COBIT References (4.0)
<p><b>Management has established, documented and follows standard procedures for IT operations, including job scheduling and monitoring and responding to security and processing integrity</b></p>	<p>Determine if management has documented its procedures for IT operations, and operations are reviewed periodically for compliance.</p>	<p>DS13.1 DS13.2</p>

## Module 5 - Introduction to Processes and Controls

### Handout 4 - IT General Controls (Normative Model)

<p><b>events.</b></p>	<p>Review a sample of events to confirm that response procedures are operating effectively. When used, review the job scheduling process and the procedures in place to monitor job completeness.</p>	
<p>System event data are sufficiently retained to provide chronological information and logs to enable the review, examination and reconstruction of system and data processing.</p>	<p>Determine if sufficient chronological information is being recorded and stored in logs, and it is usable for reconstruction, if necessary. Obtain a sample of the log entries, to determine if they sufficiently allow for reconstruction.</p>	<p>DS13.3</p>
<p>System event data are designed to provide reasonable assurance as to the completeness and timeliness of system and data processing.</p>	<p>Inquire as to the type of information that is used by management to determine the completeness and timeliness of system and data processing.</p> <p>Review a sample of system processing event data to confirm the completeness and timeliness of processing.</p>	<p>DS11.1 SA13.3</p>