

IT General Controls Domain	COBIT Domain	Control Objective	Control Activity	Test Plan	Test of Controls Results
Program Development and Program Change	Acquire or develop application systems software	Controls provide reasonable assurance that application and system software is acquired or developed that effectively supports financial reporting requirements.	The organization's system development lifecycle methodology (SDLC) includes security, availability and processing integrity requirements for the organization.	Obtain a copy of the organization's SDLC methodology.  Review the methodology to determine that it addresses security, availability and processing integrity requirements.	
			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.	
			The SDLC methodology ensures that information systems are designed to include application controls that support complete, accurate, authorized, and valid transaction processing.	Review the methodology to determine if it addresses application controls.  Consider whether there are appropriate steps to ensure that application controls are considered throughout the development or acquisition life cycle, e.g., application controls should be included in the conceptual design and detailed design phases.	
			The organization has an acquisition and planning process that aligns with its overall strategic direction.	Review the SDLC methodology to ensure that the organization's overall strategic direction is considered, e.g., an IT steering committee must review and approve projects to ensure that a proposed project aligns with strategic business requirements and that it will utilize approved technologies.	
			IT management ensures that users are appropriately involved in the design of applications, selection of packaged software and the testing thereof, to ensure a reliable environment.	Review the SDLC to determine if users are appropriately involved in the design of applications, selection of packaged software and testing.	
			Post-implementation reviews are performed to verify controls are operating effectively.	Determine if post-implementation reviews are performed on new systems and significant changes reported.	
			The organization acquires/develops systems software in accordance with its acquisition, development and planning process.	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 process.	
			Program Development and Program Change	Acquire Technology Infrastructure	Controls provide reasonable assurance that technology infrastructure is acquired so that it provides the appropriate platforms to support financial reporting applications.
Program Development and Program Change	Develop and Maintain Policies and Procedures	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.	The organization's SDLC methodology and associated policies and procedures are regularly reviewed, updated and approved by management.	Confirm that the organization's policies and procedures are regularly reviewed and updated as changes in the environment dictate.  When policies and procedures are changed, determine if management approves such changes.  Select a sample of projects and determine that user reference and support manuals and systems documentation and operations documentation were prepared.	
			The organization ensures that its systems and applications are developed in accordance with its supported, documented policies and procedures.	Review a sample of application documentation (including user documented policies and manuals) to determine if they comply with the policies and procedures that have been documented by the organization.	
Program Development and Program Change	Install and Test Application Software and Technology Infrastructure	Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and associated controls operate as intended and support financial reporting requirements.	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 to help ensure that deployed systems operate as intended.	Select a sample of system 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 were essential to the production of complete and accurate reporting, these interfaces were included in the testing strategy.	

IT General Controls Domain	COBIT Domain	Control Objective	Control Activity	Test Plan	Test of Controls Results
			Load and stress testing is performed according to a test plan and established testing standards.	<p>Select a sample of system development projects and significant systems upgrades that are significant for financial reporting.</p> <p>Where it was considered that capacity and performance were of potential concern, review the approach to load and stress testing.</p> <p>Consider whether a structured approach was taken to load and stress testing and that 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.</p>	
			Interfaces with other systems are tested to confirm that data transmissions are complete, accurate and valid.	<p>Select a sample of system development projects and significant systems upgrades that are significant for financial reporting.</p> <p>Determine if interfaces with other systems were tested to confirm that data transmissions are complete, e.g., record totals are accurate and valid.</p> <p>Consider whether the extent of testing was sufficient and included recovery in the event of incomplete data transmissions.</p>	
			The conversion of data is tested between its origin and its destination to confirm that it is complete, accurate, and valid.	<p>Obtain a sample of system development projects and significant system upgrades that are significant for financial reporting.</p> <p>Determine if a conversion strategy was documented.</p> <p>Consider whether it included strategies to "scrub" the data in the old system before conversion or to "run down" data in the old system before conversion.</p> <p>Review the conversion testing plan.</p> <p>Consider whether the following were considered: data transformations, input of data not available in the old system, edits, completeness controls and timing of conversions.</p> <p>Determine if the conversion was included in acceptance testing and was approved by user management.</p>	
<b>Program Development and Program Change</b>	<b>Manage Changes</b>	Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production.	Requests for program changes, system changes and maintenance (including changes to system software) are standardized, documented and subject to formal change management procedures.	<p>Determine that a documented change management process exists and is maintained to reflect the current change 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 (non-production), 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.</p> <p>Establish if the following are included in the approval process: operations, security, IT infrastructure management and IT management.</p> <p>Evaluate procedures designed to ensure only authorized/ approved changes are moved into production.</p> <p>Trace the sample of changes back to the change request log and</p>	

IT General Controls Domain	COBIT Domain	Control Objective	Control Activity	Test Plan	Test of Controls Results
			Emergency change requests are documented and subject to formal change management procedures.	<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 that it is independently reviewed.</p> <p>Determine that procedures require that emergency changes be supported by appropriate documentation.</p> <p>Establish that backout procedures are 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.</p> <p>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.</p> <p>Establish that the sample of changes was well documented.</p>	
			Controls are in place to restrict migration of programs to production only by authorized individuals.	<p>Evaluate the approvals required before a program is moved to production.</p> <p>Consider approvals from system owners, development staff and computer operations.</p> <p>Confirm that there is appropriate segregation of duties between the staff responsible for moving a program into production and development staff.</p>	
			IT management ensures that the setup and implementation of system software do not jeopardize the security of the data and programs being stored on the system.	<p><u>Obtain and test evidence to support this assertion.</u></p> <p>Determine that a risk assessment of the potential impact of changes to system software is performed.</p> <p>Review procedures to test changes to system software in a development environment before they are applied to production.</p> <p>Verify that backout procedures exist.</p>	
<b>Computer Operations and Access to Programs and Data</b>	<b>Define and Manage Service Level</b>	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 with which the quality of services will be measured.	Service levels are defined and managed to support financial reporting system requirements.	<p>Obtain a sample of service level system agreements and review their content requirements. 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>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 this issues.</p>	
<b>Computer Operations and Access to Programs and Data</b>	<b>Manage Third Party Services</b>	Controls provide reasonable assurance that third-party services are secure, accurate and available, support processing integrity and defined appropriately in performance contracts.	A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.	<p>Determine if the management of the third-party services has been assigned to appropriate individuals.</p> <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>	

IT General Controls Domain	COBIT Domain	Control Objective	Control Activity	Test Plan	Test of Controls Results
			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 third-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, availability and processing integrity.</p>	
			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, availability and processing integrity in accordance with the company's policies and procedures.	
			Procedures exist and are followed to ensure that a formal contract is defined and agreed for all third-party services before work is initiated, including definition of internal control requirements and acceptance of the organization's policies and procedures.	<p>Review a sample of contracts and determine whether:</p> <ul style="list-style-type: none"> <li>• There is a 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>	
			A regular review of security, availability and processing integrity is performed for service level agreements and related contracts with third-party service providers.	<p>Inquire whether third-party service providers perform independent reviews of security, availability and processing integrity, e.g., service auditor report.</p> <p>Obtain a sample of the most recent review and determine if there are any control deficiencies that would impact financial reporting.</p>	
<b>Computer Operations and Access to Programs and Data</b>	<b>Ensure Systems Security</b>	Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.	An information security policy exists and has been approved by an appropriate level of executive management.	<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>	
			A framework of security standards has been developed that supports the objectives of the security policy.	<p>Obtain a copy of the security standards. Consider whether the 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>• Asset classification and control</li> <li>• Personnel security</li> <li>• Software security policy</li> <li>• Physical and environmental security</li> <li>• Workstation security</li> <li>• Computing environment management</li> <li>• Network environment management</li> <li>• System access control</li> <li>• Disaster recovery</li> <li>• Compliance</li> <li>• System development and maintenance</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.	
			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.	
			Procedures exist and are followed to authenticate all users to the system to support the validity of transactions.	Assess the authentication mechanisms used to validate user credentials for financial reporting systems and validate that user sessions time-out after a predetermined period of time.	

IT General Controls Domain	COBIT Domain	Control Objective	Control Activity	Test Plan	Test of Controls Results
			Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes).	Review 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.).	
			Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending and closing user accounts.	<p>Confirm that procedures exist for the registration, change and deletion of users from financial reporting systems and subsystems on a timely basis and the procedures are followed.</p> <p>Validate that attempts to gain unauthorized access to financial reporting systems and subsystems are logged and are followed up on a timely basis.</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 was done in a timely manner.</p> <p>Select a sample of current users and review their access for appropriateness based upon their job functions.</p>	
			A control process exists and is followed to periodically review and confirm access rights.	<p>Inquire whether access controls are reviewed for financial reporting systems and subsystems on a periodic basis by management.</p> <p>Assess the adequacy of how exceptions are reexamined, and if the follow-up occurs in a timely manner.</p>	
			Where appropriate, controls exist to ensure 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>Determine how the organization establishes accountability for transaction initiation and approval.</p> <p>Test the use of accountability controls by observing a user attempting to enter an unauthorized transaction.</p>	
			Where network connectivity is used, appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access.	<p>Obtain a sample of transactions, and identify evidence of the accountability or origination of each.</p> <p>Determine the sufficiency and appropriateness of perimeter security 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>	
			IT security administration monitors and logs security activity, and identified security violations are reported to senior management.	<p>Inquire whether a security office exists to monitor for security vulnerabilities and related threat events.</p> <p>Assess 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>	
			Controls relating to appropriate segregation of duties over requesting and granting access to systems and data exist and are followed.	Review the process to request and grant access to systems and data and confirm that the same person does not perform these functions.	
			Access to facilities is restricted to authorized personnel and requires appropriate identification and authentication.	<p>Obtain policies and procedures as they 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 organization's 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>	

IT General Controls Domain	COBIT Domain	Control Objective	Control Activity	Test Plan	Test of Controls Results
Computer Operations and Access to Programs and Data	Manage the Configuration	Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.	Only authorized software is permitted for use by employees using company IT assets.	Determine if procedures are in place to detect and prevent the use of unauthorized software.  Obtain and review the company policy as it relates to software use to see that this is clearly articulated.  Consider reviewing a sample of applications and computers to determine if they are in conformance with organization policy.	
			System infrastructure, including firewalls, routers, switches, network operating systems, servers and other related devices, is properly configured to prevent unauthorized access.	Determine if the organization's policies require the documentation is properly of the current configuration, as well as the security configuration settings to be implemented.  Review a sample of servers, firewalls, routers, etc., to consider if they have been configured in accordance with the organization's policy.	
			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.	Conduct an evaluation of the frequency and timeliness of management's review of configuration records. Assess whether management has documented the configuration management procedures.  Review a sample of configuration 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 using virus software on its networks and personal computers.	
			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.	
			Computer Operations and Access to Programs and Data	Manage Problems and Incidents	Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution.
The problem management system provides for adequate audit trail facilities, which allow tracing from incident to underlying cause.	Determine if the organization's procedures include audit trail facilities—tracking of the 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 all unauthorized activities are responded to in a timely fashion, and there is a process to support proper disposition.				
Computer Operations and Access to Programs and Data	Manage Data	Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.	Policies and procedures exist for the handling, distribution and retention of data and reporting output.	Review the policies and procedures for the handling, 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 all the correct financial reports (including electronic reports) to appropriate personnel.  Obtain and test evidence that the controls over the protection of data and the timely distribution of financial reports (including electronic 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, both logically and physically, in storage and during transmission against unauthorized access or modification.	
			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.	Obtain the procedures dealing with distribution and retention of data.  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.	
				Confirm that the retention periods are in conformity with the Sarbanes-Oxley Act.	

IT General Controls Domain	COBIT Domain	Control Objective	Control Activity	Test Plan	Test of Controls Results
			Management has implemented a strategy for cyclical backup of data and programs.	Determine if the organization has procedures in place to back up data and programs based on IT and user requirements.	
				Select a sample of data files and programs and determine if they are being backed up as required.	
			Procedures exist and are followed to periodically test the effectiveness of the restoration process and the quality of backup media.	Inquire whether the retention and storage of messages, documents programs, etc., have been tested media. during the past year.	
				Obtain and review the results of testing activities. 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.	
			Changes to data structures are authorized, made in accordance with design specifications and implemented in a timely manner.	Obtain a sample of data structure changes and determine whether they adhere to the design specifications and were implemented in the time frame required.	
<b>Computer Operations and Access to Programs and Data</b>	<b>Manage Operations</b>	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, error monitoring and system availability.	Management has established and documented standard procedures for IT operations, documented including scheduling, managing, monitoring and responding to security, availability and processing integrity events.	Determine if management has documented its procedures for IT operations, and operations are reviewed periodically to ensure processing integrity events. compliance.	
				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.	
			System event data are sufficiently retained to provide chronological information and logs to enable the review, examination and reconstruction of system and data processing.	Determine if sufficient chronological information is being recorded and stored in logs, and it is useable for reconstruction, if necessary.	
				Obtain a sample of the log entries, to determine if they sufficiently allow for reconstruction.	
			System event data are designed to provide reasonable assurance as to the completeness and timeliness of system and data processing.	Inquire as to the type of information that is used by management to verify the completeness and timeliness of system and data processing.	
				Review a sample of system processing event data to confirm the completeness and timeliness of processing.	
			End-user computing policies and procedures concerning security, availability and processing integrity exist and are followed.	Obtain a copy of the end-user computing policies and procedures and confirm that they address security, availability and processing integrity controls.	
				Select a sample of users and inquire whether they are aware of this policy and if they are in compliance with it.	
			End-user computing, including spreadsheets and other user-developed programs, are documented and regularly reviewed for processing integrity, including their ability to sort, summarize and report accurately.	Inquire as to management's knowledge of end-user programs in use across the company.	
				Inquire as to the frequency and approaches followed to review enduser programs for processing integrity, and review a sample of these to confirm effectiveness.	
				Review user-developed systems and test their ability to sort, summarize and report in accordance with management intentions.	
			User-developed systems and data are regularly backed up and stored in a secure area.	Inquire how end-user systems are backed up and where they are stored.	
			User-developed systems, such as spreadsheets and other end-user programs, are secured from unauthorized use.	Review the security used to protect unauthorized access to user-developed systems.	
				Consider observing a user attempting to gain unauthorized access to userdeveloped systems.	
				Inquire how management is able to detect unauthorized access and what follow-up procedures are performed to assess the impact of such access.	
			Access to user-developed systems is restricted to a limited number of users.	Select a sample of user-developed systems and determine who has access and if the access is appropriate.	

IT General Controls Domain	COBIT Domain	Control Objective	Control Activity	Test Plan	Test of Controls Results
			Inputs, processing and outputs from user-developed systems are independently verified for completeness and accuracy.	Inquire how management verifies the accuracy and completeness of information processed and reported from user-developed systems.  Inquire who reviews and approves outputs from user-developed systems prior to their submission for further processing or final reporting.  Consider re-performing or reviewing the logic used in user-developed systems and conclude on its ability to process completely and accurately.	