

General IT Controls Audit Program

Purpose / Scope

Perform a General Controls review of Information Technology (IT). The reviews will include all IT related policies, procedures, data security administration, data center operations, system development / maintenance, the IT Disaster / Recovery plan and its relation to the corporate Business Continuity plan.

Audit steps	Date	Initials	W/P Ref.
IT General Controls			
Planning			
Determine if committees review, approve, and report to the board on: Short and long term information systems plans IT operating standards Data security policies and procedures Resource allocation (major hardware/software acquisition and project priorities) Status of major projects IT budgets and current operating cost			
Policies, Standards, and Procedures			
Determine whether the board of directors has reviewed and approved IT's policies.			
Examine how IT management has defined standards and adopted a methodology governing the process of developing, acquiring, implementing, and maintaining information systems and related technology. Determine if IT management has adequate standards and procedures for: Systems development Program change control Data Center operations Data Base administration DASD management Performance monitoring Capacity planning Network administration Information security Contingency planning/disaster recovery			
Assess compliance with these policies and procedures.			
Data Security Administration and Accountability			
Verify the names associated with the DSA function. Determine that the DSA is prohibited from routine operating duties in the computer facility. (this person should not have system operating duties and should be sufficiently independent from the computer operation to ensure that he/she cannot create, delete, or suppress passwords in order to cover improper activities.)			

<p>Security Policy</p> <p>Review the data security policy.</p> <p>Determine if the security procedures cover: Physical protection of the facility. Designation and duties of the security officer(s). Authorized data and program access levels. Requirements for password creation and change procedures. Requirements for access via terminals, modems or computer system (LAN) connection. Monitoring and follow-up of security violations.</p> <p>Determine whether procedures are in place to update the security policy. Ensure updates to the policy and procedures are distributed to and reviewed by management.</p> <p>Determine if an education program has been implemented to promote user awareness about security policies and procedures.</p>			
<p>Data and Program Security</p> <p>Determine how access levels are granted. Whether all access is restricted unless specifically authorized. If the password file is controlled (e.g., encryption). How security violations are detected and reported.</p> <p>Determine that password security is in effect on all applications.</p> <p>Assess the adequacy of controls over: Development and test programs. Identify whether levels of access are periodically reviewed. Assess whether passwords, user IDs are adequately controlled for: Changing on a regular basis Suppressing passwords on a terminal.</p> <p>Determine that passwords are removed as soon as an individual's employment is terminated to ensure that a terminated employee cannot gain access to the computer files through an outside terminal.</p>			
<p>Security Controls</p> <p>Obtain copies of the security access and control files for the operating system. Obtain a list of data altering utilities, user exits, user interface programs, and privileged commands. Using these documents, determine:</p> <p>Whether the data security administration function is independent of systems and programming. If all programmers have unique user IDs and passwords. If system access levels are consistent with job functions. If all changes to the system security software are approved by the system security administrator. If security software provides an adequate audit trail to identify the programmer, the programs or utilities used, the files or programs accessed and the nature of the access. The adequacy of segregation of duties for application programming, systems programming, computer operation, and system security functions. If physical or logical separation between the production and test environments is maintained. The adequacy of controls over dial-up access.</p>			

IT Servicing			
Provider			
Obtain a list of services performed by the data processing center. Determine if written contracts are in effect for all customers. Review a copy of the contract(s) used.			
Receiver			
If receives major support from one or more outside servicers: List the name(s) and location(s) of the servicer(s). Prepare a listing of the services outside vendors provide. Assess the adequacy of the procedure for monitoring the financial condition of its servicer(s) and whether the procedure is sufficient to project the continued viability of contracted services.			
Insurance			
Review the adequacy of insurance coverage (if applicable) for: Employee fidelity (blanket-bond) IT equipment and facilities Loss resulting from business interruptions Determine whether the board of directors has approved requirements for related insurance coverage. Examine the business-interruption coverage limits.			
Contingency Planning			
Determine if IT has a documented disaster recovery plan. Verify that the IT disaster recovery plan supports the goals and priorities found in the corporate business continuity plan. Review the IT disaster recovery plan to determine if it: Clearly identifies the management individuals who have authority to declare a disaster. Clearly defines responsibilities for designated teams or staff members. Explains actions to be taken in specific emergency situations. Allows for remote storage of emergency procedures manuals. Defines the conditions under which the backup site would be used. Has procedures in place for notifying the backup site. Has procedures for notifying employees. Establishes processing priorities to be followed. Provides for reserve supplies. Determine if all critical resources are covered by the plan. Determine if a copy of the IT contingency plan is stored off-site. Determine if the backup site: Has the ability to process the required volume. Provides sufficient processing time for the anticipated workload based on emergency priorities. Allows the subsidiary to use the facility until it achieves a full recovery from any interruption. Determine if there is physical security at the recovery site. Determine what agreements, commitments, or projections have been made with and by hardware vendors regarding the period of time required to replace hardware. Verify that vendors has been identified. Determine if: Duplicates of the operating system are available on and off site.			

<p>Duplicates of the production programs are available on and off site (including both source and executable versions).</p> <p>Determine if all master files and transaction files are backed up adequately to facilitate recovery.</p> <p>Determine if the IT disaster recovery plan is tested at least annually, including critical applications and services</p> <p>Determine if the tests include: Setting goals in advance. Realistic conditions and activity volumes. Use of actual backup system and data files from off-site storage. Participation and review by internal audit. A post-test analysis report and review process that includes a comparison of test results to the original goals. Development of a corrective action plan for all problems encountered. Determine if several user departments have been involved in testing at the same time to uncover potential conflicts.</p>			
SYSTEMS DEVELOPMENT AND PROGRAMMING			
Project Management and Control			
<p>Determine whether there is a written plan for future changes to current hardware, software, or the addition of new applications.</p> <p>Obtain a copy of the plan and note major items.</p>			
Standards			
<p>Determine whether policies and procedures are adequate for: Application systems / program development Operating system maintenance Program change control Testing Program and system documentation Implementation</p>			
Application Systems Development			
<p>Obtain a list of all application systems currently in use or under development. Indicate if the applications were purchased or developed in-house.</p> <p>Determine whether: All required documentation is present and sufficiently detailed to evidence complete compliance with established standards. The structure of the System Development Life Cycle (SDLC) planning includes all appropriate phases and whether they were completed as prescribed by the plan. The audit trails, exception reports and system security designs are adequate. User manuals are adequate. The board, senior management, applicable committees, computer operations, user departments, and audit were involved in all phases of the development process.</p> <p>For purchased software: Determine whether new releases are tested before installation. Determine if the most recent release is being used.</p> <p>Application Program Development Review selected documentation for at least one in-house developed program. Trace the program's development from the initial request through the post implementation review process.</p>			

<p>Determine: If all required documentation is present and sufficiently detailed to evidence compliance with established programming procedures. Whether the program meets the objectives of the original request, based on test results and user feedback. For program requests, determine: Whether program request procedures were followed. If a user department was affected, whether there was appropriate consultation between users and the IT department. Whether appropriate documentation and training was provided to users and computer operators.</p>			
<p>Operating System Maintenance</p>			
<p>Obtain and review the operating system installation plan, the system generation report, the system log, and other system related activity reports. Review changes made to the operating system and supporting system software to determine compliance with procedures.</p> <p>Determine if: The overall supervision by management over system programmer activities is adequate. Controls over the following are adequate: New system installation Implementation of new releases In-house enhancements Emergency fixes and other temporary modifications Documentation of changes System testing Management or supervisory approvals.</p>			
<p>Program Maintenance</p>			
<p>Review program changes to determine compliance with procedures and the adequacy of internal control.</p> <p>Determine: If the program change control procedures provide adequate guidelines to control the function. If change standards and procedures are adhered to. If documentation is complete. The adequacy of involvement of users, audit, and IT management in the request and approval processes.</p> <p>For emergency program fixes and other temporary changes, determine if: Prescribed procedures are followed. Documentation is sufficiently detailed to explain the nature of the emergency change, the immediate action taken to address the problem, and subsequent actions to permanently correct the problem.</p>			

Testing			
Determine whether procedures require that: The scope of testing includes all functions, programs, and interface systems. All test discrepancies are adequately documented and resolved. Users participate in the actual testing phase All test plans and results are documented and retained			
Documentation			
Determine if: Overall systems and program documentation adheres to standards. Documentation is complete and current.			
Implementation			
Review documentation generated from the implementation process and determine if: Controls ensure complete integrity of programs between the test and the production environments. System level implementations are subject to the same controls as application level activity.			
Vendor Software/Support			
Obtain and review copies of all vendor and consultant contracts, available financial statements and escrow agreements. Ensure software purchase and selection procedures require: Clear definition of user requirements Clear definition of system requirements (equipment, interface, etc.) Cost/benefit analysis. Software support (in-house or vendor provided) Financial condition of vendor. Escrow agreements. User documentation and training.			