

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

**Objective:**

IT General Controls (ITGC) address the overall operation and activities of the IT function and its management and governance. The ITGC audit will identify and assess general controls throughout the organization’s IT infrastructure. The auditor(s) will inquire, observe, and gather evidence to obtain an understanding of the IT control environment. COBIT provides the general framework for the assessment and is augmented as necessary with applicable regulations, legislation, standards, policies, agreements, and related guidance.

Reference:

Section	Procedures	Workpaper #	Date	Auditor and Comments
<b>A</b>	<b>General</b>			
A.1	Review prior assessments, audit reports, findings, and recommendations of IT activities for two years to include: <ul style="list-style-type: none"> <li>• External audit reports</li> <li>• Internal audit reports</li> <li>• Regulatory agency reports</li> <li>• Consulting reports</li> </ul> Assess appropriateness of corrective actions has taken. Document the action taken for each recommendation and determine whether any prior year's comments should be carried forward to the current year's comments.			
A.2	Identify the technology platforms in use and the applications processed on each platform. Platform information for includes: <ul style="list-style-type: none"> <li>• Equipment manufacturer and model</li> <li>• Quantity</li> </ul> Software applications information includes: <ul style="list-style-type: none"> <li>• Application vendor and name</li> <li>• Version / Release</li> </ul>			
A.3	Review Board of Directors and Committee agenda and minutes from the past year for content relevant to IT. Establish and document follow-up plans as appropriate.			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
A.4	Review Business & IT Strategic Planning Initiatives. Establish and document follow-up plans as appropriate.			
A.5	Review status of IT initiatives underway (changes in business operations or IT infrastructure, outsourcing initiatives, web strategies, etc.) and note those impacting risks and controls.			
A.6	Review the status of outsourced IT services and respective vendor(s) and adjust audit procedures as appropriate to address issues affected by outsourcing.			
A.7	Review the list of trading partners / business associates with whom the organization shares or exchanges electronic information, and assess arrangements for information security and compliance across organizational boundaries.			
A.8	Review example business associate contract / chain of trust agreements			
A.9	Assess the roles and related risks for key personnel responsible for the exchange of data / information with external entities.			
A.10	Review the job descriptions for IT positions including Security and Privacy Officers. Assess their appropriateness for the roles identified, how well they address separation of duties, and other considerations.			
A.11	Assess the general state of training provided to IT staff and the related policies, procedures, and plans, schedules, and training records. (See also Security Training in the Security and Application Systems Sections.)			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
A.12	Assess the management, maintenance, planning, and appropriateness of Documented Policies, Procedures, Standards, and Guidelines including, but not limited to: <ul style="list-style-type: none"> <li>a. General IT and IS Policies and Procedures</li> <li>b. All Security Policies including HIPAA, HITECH. State and other Security Requirements, etc.</li> <li>c. All Privacy Policies including HIPAA, HITECH. State and other Privacy Requirements, etc.</li> <li>d. Policies and Procedures for Release of Information</li> <li>e. Employee Termination Process</li> <li>f. Personnel Practices – e.g., clearance policies and procedures (background check, etc.), visitor and maintenance personnel control, disciplinary policies</li> <li>g. Vendor Policies and Procedures</li> <li>h. Change management policies and procedures</li> </ul>			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
<b>B</b>	<b>IT Organization and Operations</b>			
B.1	Obtain the current IT Organization Chart(s) and assess segregation of duties for key functions (i.e.: system analysis, development, programming, testing, operations, quality...).			
B.2	Review the current IT organization chart(s) and assess segregation of duties for key functions (i.e.: system analysis, development, programming, testing, operations, quality...).			
B.3	Review business process flows / diagrams for IT-related activities and assess IT process controls as identified.			
B.4	Through discussion with IT personnel, evaluate the segregation of critical processing functions.			
B.5	Ensure the IT function is a support group within the organization and does not initiate or authorize transactions.			
B.6	Determine whether an IT steering committee or an equivalent committee provides effective IT governance within the organization.			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
<b>C</b>	<b>Data Center (Environment and Physical Access)</b>			
	Note: The physical environment reviewed will consider the size and complexity of the organization and its operations, and the types of technology in use or coming into use by the organization and its affiliates, partners, and related groups. Consider also the areas where technology is used and whether the locations present risks due to people and activities and/or natural or man-made threats.			
C.1	Evaluate the data center location(s) and the host building(s). Ensure combustible materials are not stored on floors above or below the data center. If combustible materials are stored above, evaluate the fire suppression system, i.e. sprinkler system will result in water damage to floors below.			
C.2	Tour the data center(s). Document the measures taken to control physical access to such areas as the data center, computer room, telecommunications, wiring closets, network access points... <ul style="list-style-type: none"> <li>• Identify all doors into the data center and ensure each adequately restricts access.</li> <li>• Ensure all visitors, including vendors, are required to sign-in upon entry, as escorted as appropriate, and visitor records are retained.</li> </ul>			
C.3	Identify and observe the techniques in place (surveillance cameras, security guards, electronic card keys, etc.) used to restrict data center access.			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
C.4	<p>Determine whether the following environmental controls are in place and operational:</p> <ul style="list-style-type: none"> <li>a. Fire suppression equipment (e.g., halon system or dry line water suppression and extinguishers)</li> <li>b. Uninterruptible power supply (UPS)</li> <li>c. Emergency Power (e.g., generators)</li> <li>d. Temperature and humidity controllers – including backup HAV</li> <li>e. Emergency power cut-off switches</li> <li>f. Smoke and water detectors</li> <li>g. Emergency lighting</li> </ul>			
C.5	Ensure the above are regularly tested and maintenance contracts are in force.			
C.6	Identify the equipment cooling system(s). If water-cooled, assess the protection for leakage and whether a backup water chiller exists.			
C.7	Assess the routine maintenance of system equipment to ensure its performance as expected and to monitor fragile or unstable systems.			
C.8	Identify the location(s) of consoles for system and network operation and maintenance, and assess the use and control of remote consoles.			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
<b>D</b>	<b>Access or Security Controls</b>			
	<b>Physical Access</b>			
D.1	Ensure physical access to computer room(s) is limited to operators and appropriate supervisors. <ul style="list-style-type: none"> <li>a. Locked computer labs that require coded ID cards or keys for entry</li> <li>b. Manual key locks on the computer</li> <li>c. Restricted access to program libraries, and logs of all program access</li> </ul>			
D.2	Assess the completeness and appropriateness of Facility Security Standards for authentication, personnel, access, etc.			
	<b>Electronic Access</b>			
D.3	Assess the data security policies and their enforcement for all individuals with opportunities to access data. Assess whether the policies address data ownership, privacy, access requirements, encryption, media, communications, passwords...			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
D.4	<p>Determine how system resources (i.e., batch, on-line transactions, datasets, and sensitive utilities) are protected across all platforms, media, and transmissions. Identify all applications that provide their own security mechanisms. Ensure appropriate capabilities are implemented to include:</p> <ul style="list-style-type: none"> <li>• Unique user IDs assigned to all users</li> <li>• Unattended devices automatically logged off after a specified period of inactivity.</li> <li>• Users are forced to change passwords within a specified timeframe.</li> <li>• Old passwords cannot be reused.</li> <li>• Passwords are properly masked on the system.</li> </ul>			
D.5	Review and assess the description of user authentication mechanisms—secure ID, biometric, CHAP/PAP, etc.			
D.6	Identify and review the use of automated authorization and authentication mechanisms, profile templates, etc.			
D.7	Assess the connectivity of remote, dial-up, wireless, mobile, and other systems that provide access to sensitive data and the specific security techniques in place for remote or mobile access and user authentication.			
D.8	Review the procedures to authorize and revoke system access. Ensure proper authorization is obtained prior to granting user access to the system resources. Evaluate the procedures established to remove user IDs and passwords from the system when an employee leaves and to adjust access privileges as user roles and responsibilities change.			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
D.9	Select a sample of users in the system's security package and ensure system access is appropriate and properly authorized.			
D.10	Select a sample of sensitive data elements and ensure appropriate access management.			
D.11	Identify all users with privileged access authorities and assess the procedures for monitoring all activities of privileged users.			
D.12	Review documentation for intrusion protection / detection and IT infrastructure management / monitoring systems. (internal and external network infrastructure)			
D.13	Review descriptions of logging and auditing systems and assess their appropriateness.			
D.14	Assess the logging of security related information and the identification and management of security incidents or violations. Review sample logs and reporting for incident assessment and remediation.			
D.15	Review the documentation for the Incident Response Team and Incident Response Process related to protected information loss, theft, disclosure, security breach, notification procedures, etc.			
D.16	Review the incident response tracking mechanism and records of security incidents, and assess the timeliness and appropriateness of response, recovery, notification, follow-up review, corrective procedures, etc.			
D.17	Assess the information security training provided to IT staff and the related policies, procedures, and plans, schedules, and training records.			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
D.18	Assess the information security training provided to non-IT staff and the related policies, procedures, and plans, schedules, and training records.			
D.19	Assess the results of the most recent security penetration testing and the methods used.			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
<b>E</b>	<b>Systems Development and Documentation Controls</b>			
E.1	Obtain an understanding of the systems development, maintenance, and change management processes.			
E.2	Assess the written procedures (in the overall policies and procedures manual) outlining the steps followed to modify IT systems. Ensure these steps include <ul style="list-style-type: none"> <li>d. proper approval to implement program changes;</li> <li>e. appropriate documentation describing the nature and logic of proposed changes;</li> <li>f. proper methodology for testing, debugging, and approving all changes on a test system before implementing the changes in production systems; and</li> <li>g. a log is maintained of all system enhancements and modifications.</li> </ul>			
E.3	Assess the training for security of online applications, the appropriateness for applicable personnel, and the extent to which it is integrated with the building, maintenance, testing, implementation, and use of online systems processing sensitive and protected information.			
E.4	Assess the methodology for approving and developing new application systems. Ensure the methodology applies to all types of systems.			
E.5	Assess the Systems Development Life Cycle as performed by IT personnel. Consider the following: <ul style="list-style-type: none"> <li>a. User participation and sign-off</li> <li>b. Acceptance Testing</li> <li>c. Proper review and approval at the completion of key stages in the development process and documentation requirements</li> </ul>			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
E.6	Select a sample of systems in the development life cycle process and review the development documentation to assess compliance with the SDLC methodology.			
E.7	<p>Review the IT change management processes and procedures to ensure critical functions are performed:</p> <ul style="list-style-type: none"> <li>a. All changes to programs, files, and devices require written authorization before they are implemented.</li> <li>b. All changes go through a single control point.</li> <li>c. Only specified personnel are authorized to approve and apply changes.</li> <li>d. Users accept the change, via sign-off, prior to implementation of any change in production.</li> <li>e. Documentation of all changes clearly identifies the trail from initiation through every step including post change acceptance.</li> <li>f. Processes are in place to ensure agreement on priority of change requests.</li> <li>g. Changes are implemented into the production environment by personnel not responsible for making the changes (segregation of duties).</li> <li>h. Procedures are in place for emergency changes.</li> </ul>			
E.8	Select a sample of recent program changes and review the change documentation for compliance with application program change procedures.			
E.9	Assess the procedures in place to routinely test for unauthorized or undocumented program changes (e.g. by comparison of the working program to the approved code).			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
E.10	Evaluate the separation of the test environment from production systems and data, and ensure changes are thoroughly tested and approved prior to moving the changed code into the production environment.			
E.11	Review the application program change turnover procedures performed by the independent group responsible for implementing the application changes into the production environment.			
E.12	Assess the emergency change procedures and whether emergency changes are migrated through segregated libraries to enable management review and approval of the change.			
E.13	Select a sample of emergency program changes and assess compliance with established procedures.			
E.14	Assess the procedures for making routine rate changes (e.g., tax rates) to application programs or tables.			
E.15	Assess whether programming standards include naming conventions and coding conventions.			
E.16	Identify the software package (i.e., CA-Librarian) on the processing system to provide security over production libraries for source programs, JCL, and other files.			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
<b>F</b>	<b>Hardware and System Software Controls</b>			
F.1	Identify the functions / individuals responsible for hardware and system software controls built into IT equipment by the manufacturer which may include: <ul style="list-style-type: none"> <li>a. Self-diagnosis</li> <li>b. Regular maintenance</li> <li>c. Echo check</li> <li>d. Duplicate process check</li> <li>e. Parity check</li> </ul>			
F.2	Assess the processes to identify and address errors that may occur in operating systems and system software. <ul style="list-style-type: none"> <li>a. Logic occurs before the operational stage</li> <li>b. Coding detected during the program's testing (debugging) stage</li> <li>c. Modification can occur at any time, even while processing. If not handled properly, program modifications can produce unexpected operations and invalid output and data                             <ul style="list-style-type: none"> <li>o Make inquiry of any unauthorized program modifications (which is the most ominous type of software error)</li> <li>o Assess completeness of records kept of all modifications and records for any post modification debugging</li> </ul> </li> </ul>			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
<b>G</b>	<b>Computer Operations (Job Scheduling)</b>			
G.1	Determine through inquiry the process for scheduling production batch processing. Ensure user authorization of all changes to the production schedule. Select a sample of changes and review them for compliance to the scheduling procedures.			
G.2	If an automatic scheduler is not used, determine how production processing is controlled.			
G.3	Determine how the computer operator ensures production processing properly completes.			
G.4	Identify the various output media in use and assess the processes for distribution of production-processing output to users. Ensure sensitive data is properly controlled.			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
<b>H</b>	<b>Backup/Recovery</b>			
H.1	Review the Business Continuity Plan and Disaster Recovery Plan and ensure the systems and communications backup and recovery procedures are appropriately integrated in the plan.			
H.2	Ensure system and incremental backups are performed on a regular basis. Assess the frequency of backups and determine through inquiry and review of documentation whether all files and programs are backed up properly. Ensure on-line transaction journals are backed up to provide recovery of transactions that update the databases.			
H.3	Review the description of backup and archiving system(s)			
H.4	Assess the procedures to ensure backup copies of system, programs, and data files are rotated to a secure offsite storage location on a scheduled basis. Assess the procedures for verifying the inventory of the backup data.			
H.5	Identify the media and processes involved in backup and recovery and assess their effectiveness. If a tape management system (TMS) is part of the processing system and provides an inventory of tapes by location, observe that tapes maintained offsite are properly segregated on the TMS.			
H.6	Review the results of system recovery testing to ensure a successful test was performed and documented within the prior twelve months.			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
<b>I</b>	<b>Business Continuity Planning and Disaster Recovery</b>			
I.1	Review the business continuity and resumption plans. Through discussions with management and review of the business continuity and resumption plans, determine whether the plans are current and include the necessary key components.			
I.2	Review the documentation of the results of the most recent test of the business resumption plan determine the dates of prior plans. Document the frequency and success of the tests. If the plan has not been tested, inquire as to the plans for testing.			
I.3	Assess IT management's plans for and roles in assuring business continuity and the recovery of IT resources. Determine if the plan includes recovery of IT at a vendor site and review the service agreement.			
I.4	Evaluate the disaster recovery plan for the IT division. Ensure application recovery is based on risk (applications critical to the organization are recovered first).			
I.5	Evaluate the recovery service vendor agreement(s) to ensure they provide for adequate infrastructure to recover the organization's IT resources and operations. Ensure telecommunications are included and covered during testing.			
I.6	Review the results of recovery testing of IT operations at the vendor site(s). Ensure tests were successfully completed and results documented.			

## Information Technology General Controls Review (ITGC) Audit Program

2012 Internal Audit Work Plan  
Project:

Prepared by:  
Date Prepared:  
Reviewed by:

Section	Procedures	Workpaper #	Date	Auditor and Comments
<b>J</b>	<b>Telecommunications</b>			
J.1	Review technical configurations, charts, schematics, network diagrams (internal and external network infrastructure).			
J.2	Review documentation regarding approved remote communication channels, mechanisms, protocols, and standards (i.e., extranet, VPN, SSH, FTP, Wi-Fi, etc.)			
J.3	Review procedures for setting up, siting, and managing networked work stations and portable and mobile devices. Assess the security of procedures for monitoring, adding, removing, and configuring all devices on the network.			
J.4	Review description of messaging architecture, authentication, encryption methods, auditing/logging.			
J.5	Determine whether telecommunications provide a reliable and secure environment. Consider load balancing devices, redundant systems, and alternate procedures for the continuation of telecommunication operations.			
J.6	Determine if EDI (Electronic Data Interchange) is utilized. If so, evaluate security and authenticity of interchange.			