



Information Technology General Controls (ITGCs) 101

Presented by – Sugako Amasaki (Principal Auditor)
University of California, San Francisco
December 3, 2015

Webinar Agenda

- Introduction
- Why are IT General Controls Important?
- Types of Controls
- IT General Controls Review - Audit Process
- IT General Controls Review - Overview and Examples
 - Access to Programs and Data
 - Program Changes and Development
 - Computer Operations
- Q&A

Why are IT General Controls Important?

- IT systems support many of the University's business processes, such as these below:
 - Finance
 - Purchasing
 - Research
 - Patient care
 - Inventory
 - Payroll

We cannot rely on IT systems or data therein
without effective IT General Controls

Why are IT General Controls Important?

Financial Objectives, such as:

- Completeness
- Accuracy
- Validity
- Authorization

Operational & IT Objectives, such as:

- Confidentiality
- Integrity
- Availability
- Effectiveness and Efficiently

Ineffective ITGCs = No achievement of
business objectives

Types of Controls

How are controls implemented?

- Automated Controls
- Manual Controls
- Partially Automated Controls

What are controls for?

- Preventive Controls
- Detective Controls
- Corrective Controls

IT General Controls Review - Audit Process

1. Understand and identify the IT Environment and systems to be reviewed
2. Perform interviews, walkthroughs, and documentation reviews to gain an understanding on processes
3. Assess appropriateness of existing control environment (control design)
4. Validate existing controls to assess control operating effectiveness

IT General Controls Review - Overview

Access to Program and Data

IT General Controls

Access to
Program and
Data

Program Changes

Program
Development

Computer
Operations

- **Risk:** Unauthorized access to program and data may result in improper changes to data or destruction of data.
- **Objectives:** Access to program and data is properly restricted to authorized individuals only.

IT General Controls Review - Overview

Access to Programs and Data

- **Access to programs and data components to be considered:**

- Policies and procedures
- User access provisioning and de-provisioning
- Periodic access reviews
- Password requirements
- Privileged user accounts
- Physical access
- Appropriateness of access/segregation of duties
- Encryption
- System authentication
- Audit logs
- Network security

IT General Controls Review - Example

Access to Programs and Data

Area	Existing Control Design	How to Test/Validate
User access provisioning	A formal process for granting or modifying system access (based on appropriate level of approval) is in place.	Review an evidence of approval
User access de-provisioning	A formal process for disabling access for users that are transferred or separated is in place.	Compare existing user accounts with a list of users that are transferred or separated
Periodic access reviews	Periodic access reviews of users, administrators, and third-party vendors are performed.	Review an evidence of periodic reviews
Password requirements	Unique (to individual) and strong passwords are used.	Assess password rules enforced
Privileged user accounts	Accounts having privileged system access rights (e.g. servers, databases, applications, and infrastructure) are limited to authorized personnel.	Review accounts with privileged access rights
Physical access	Only authorized personnel are allowed to access secured areas and computer facilities.	Walkthrough of areas (e.g. data center, backup storage etc.)

IT General Controls Review - Overview

Program Changes and Development

IT General Controls

Access to
Program and
Data

Program Changes

Program
Development

Computer
Operations

- **Risk:** Inappropriate changes to systems or programs may result in inaccurate data.
- **Objectives:** All changes to existing systems are properly authorized, tested, approved, implemented and documented.

- **Risk:** Inappropriate system or program development or implementation may result in inaccurate data.
- **Objectives:** New systems/applications being developed or implemented are properly authorized, tested, approved, implemented and documented.

IT General Controls Review - Overview

Program Changes and Development

- **Program changes and development components to be considered:**

- Change management procedures and system development methodology
- Authorization, development, implementation, testing, approval, and documentation
- Migration to the production environment (Separation of Duties (SOD))
- Configuration changes
- Emergency changes
- Data migration and version controls
- Post change/implementation testing and reviews

IT General Controls Review - Example

Program Changes and Development

Area	Existing Control Design	How to Test/Validate
Change management controls	A formal process for proper change management is in place.	Review/assess change management procedures and validate that procedures are followed
Change documentation	All changes made to systems (e.g. servers, databases, applications, batch jobs and infrastructure) are documented and tracked.	Review change logs
Testing	Appropriate level of testing is performed.	Review an evidence of test plans and results
Approval	Appropriate approval prior to migration to production is required.	Review an evidence of approval
Migration	Access to migrate changes into production is appropriately restricted.	Verify that a separation of duties (SOD) between developers and operators (= making changes) exists

IT General Controls Review - Overview

Computer Operations

IT General Controls

Access to
Program and
Data

Program Changes

Program
Development

Computer
Operations

- **Risk:** Systems or programs may not be available for users or may not be processing accurately.
- **Objectives:** Systems and programs are available and processing accurately.

IT General Controls Review - Overview

Computer Operations

- Computer operations components to be considered:

- Batch job processing
- Monitoring of jobs (success/failure)
- Backup and recovery procedures
- Incident handling and problem management
- Changes to the batch job schedules
- Environmental controls
- Disaster Recovery Plan (DRP) and Business Continuity Plan (DRP)
- Patch management

IT General Controls Review - Example

Computer Operations

Area	Existing Control Design	How to Test/Validate
Batch job processing	Batch jobs are appropriately scheduled, processed, monitored, and tracked.	Review/assess procedures for batch job processing and monitoring and validate that procedures are followed
Monitoring of jobs	Failed jobs are followed-up and documented (including successful resolutions and explanations)	Validate that failed jobs are followed-up and documented
Backup and recovery	Backups for critical data and programs are available in the event of an emergency.	Review/assess procedures for backup and recovery and validate that procedures are followed
Problem/issue management	A formal process for problem/issue handling is in place in order to ensure timely identification, escalation , resolution and documentation of problem.	Review/assess procedures for problem/issue management and validate that procedures are followed

Conclusion/Q&A

