A Sunera How To: Information Technology General Controls Review

June 3, 2015

SUNERA®

Speakers

Sharon Gallo, Manager, CISA - sgallo@sunera.com

- More than 7 years of work experience providing audit and advisory services to large multinational and smaller Fortune 1000 clients in various industries.
- **Expertise:** Information Technology General Controls (ITGC) testing and remediation, SSAE 16 reports, application control testing, entity level testing, vendor assessments, and Software Development Lifecycle (SDLC) projects.
- Prior to Sunera, she was a Senior within Ernst & Young's Information Technology Risk & Assurance practice.

Cliff Stephens, Director - cstephens@sunera.com

- **Expertise:** Data analytics and CCM initiatives, implementing analytics tools, and leading teams on process improvement advisory, ITGC testing and remediation, application controls, and internal audit engagements.
- Prior to joining Sunera, he was a Senior Manager at Home Depot and was responsible for creating and leading the Internal Audit Data Analytics team.
- Built data analytics capabilities by implementing ACL Analytics Exchange, Tableau, SQL Server/Reporting Services, and Teratraining.

Agenda

- **Introductions**
  - Speakers
  - What is Sunera?
- **Background**
  - Overview of standard ITGCs
  - Audit Frameworks
- **How to perform an ITGC standard review**
- **Practice Exercises**
  - Access to Programs and Data
  - Program Development and Change Management
  - Computer Operations
- **Questions**

What is Sunera?

Sunera is a business and technology risk management consulting firm dedicated to reducing technology risk, designing cost-saving solutions, and protecting our clients' customers and reputations.

With a decade-long track record of delivering successful projects, we have the experience and expertise to solve even the most complex technical challenges.

Core Services

Data Privacy | Internal Audit | Information Security

IT Audit | Enterprise Risk Management | Data Analytics

Technology Training | SOX Compliance | PCI

National Reach

Atlanta
Boston
Calgary
Charlotte
Chicago
Dallas
Denver
Houston

Los Angeles
Miami
New York
Phoenix
Raleigh
San Francisco
Tampa
Toronto
Vancouver

Background

Information Technology General Controls (ITGCs)

Why are ITGCs important?

- **Information Technology General Controls (ITGCs)** can be defined as internal controls that assure the secure, stable, and reliable performance of computer hardware, software and IT personnel connected to financial systems.

- ITGCs affect the ability to rely on application controls and IT dependent manual controls.

- Without effective ITGCs, reliance cannot be placed on any application controls or IT dependent manual controls unless additional procedures are performed (e.g., benchmarking). Even these additional procedures limit the ability to rely upon more than one application control at a time.

- ITGCs are an integral part of many different operational and regulatory (federal and state) audits, including:
  - IT operational reviews
  - HIPAA assessments
  - SSAE16 assessments
  - PCI reviews/audits
  - SOX assessments

ITGC Areas of Focus

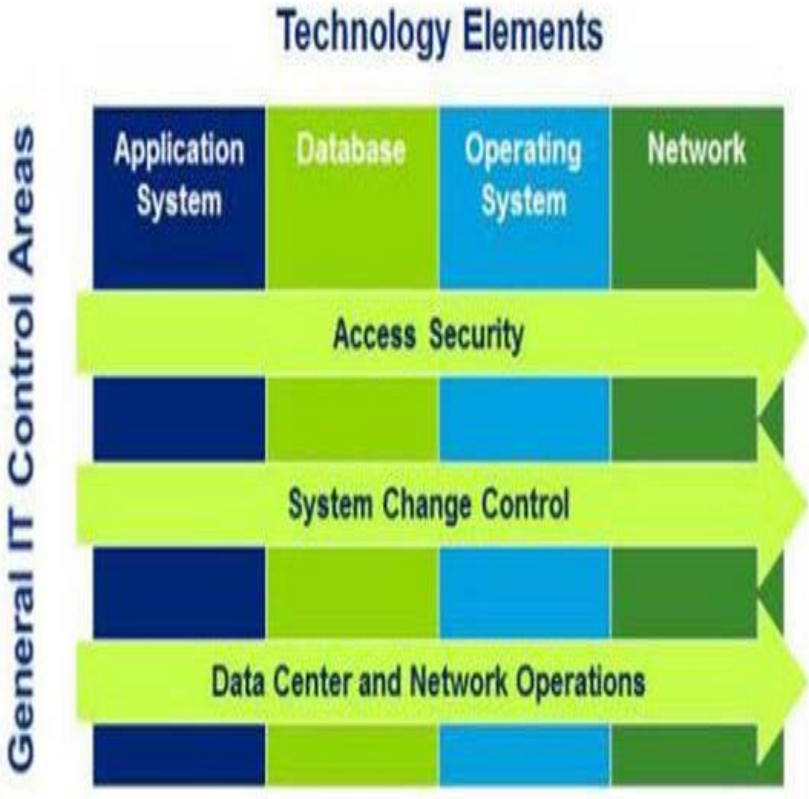
The following areas are typically addressed as part of ITGC:

- **Access to Programs and Data**
  - Controls that prevent inappropriate and unauthorized use of the system across all layers of systems, operating system, database and application.
    - Security Policy, Password, Unique IDs, Authorized Administrators, Users Access Provisioning, Users Access Reviews, Physical Security, Firewall, Monitoring (i.e. invalid logins, audit trails)
- **Program Changes**
  - Controls may involve required authorization of change requests, review of the changes, approvals, documentation, testing and assessment of changes on other IT components and implementation protocols.
    - Change Management Process for Regular and Emergency Changes (i.e. infrastructure and software changes for all layers: O/S, database, application)
- **Program Development**
  - Controls over development methodology, including system design and implementation, that outline specific phases, documentation requirements, change management, approvals and checkpoints to control the development or maintenance of the project.
  - Controls over the effective acquisition, implementation and maintenance of system software, database management, telecommunications software, security software, and utilities.
    - Software Development Life Cycle (SDLC)
- **Computer Operations**
  - Controls over the effective job configuration and scheduling, data center operations, data backup and data recovery procedures.
    - Backups, Restorations, Job Scheduling

ITGC Approach Across all Layers

ITGCs should be applied across all layers of the identified in-scope systems, including:

- **Application System**
  - Typically the system used by front-end users to perform specific tasks (i.e., PeopleSoft).
- **Database**
  - Collects and stores data supporting the application. Typically restricted to back-end users.
- **Operating System**
  - Supports the entire organization and serves as a back-bone to all systems (i.e., Windows).
- **Network**
  - A group of two or more computer systems linked together that allows the exchange of data.



Key Terms

- SOX – **Sarbanes-Oxley Act of 2002**. U.S. federal legislation that establishes new or enhanced requirements for financial reporting for all U.S. public company boards, management, and public accounting firms.
- PCAOB – **Public Company Accounting Oversight Board**. A private-sector, non-profit corporation created by the Sarbanes-Oxley Act, to oversee the auditors of public companies.
- COBIT – **Control Objectives for Information and Related Technology**. A comprehensive framework for management of the governance of risk and control of IT, comprising 5 domains, 37 IT processes and 210 control objectives. COBIT includes controls that address all aspects of IT governance, but only those significant to financial reporting have been used to develop this document.
- COSO – **Committee of Sponsoring Organizations of the Treadway Commission**. A private-sector initiative, formed in 1985 to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence. COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.
- ISACA – **Information Systems Audit and Control Association**. International professional organization for information governance, control, security and audit professionals. Its auditing and control standards are followed by practitioners worldwide.

COSO vs. COBIT

The most common framework used to evaluate ITGCs is the COBIT framework

COSO vs. COBIT

COSO

- Established to provide a generic framework for evaluating internal controls.
- SEC's suggested Internal Controls Framework for Sarbanes Oxley.
- Addresses application controls and general IT controls at a high level.
- Does not dictate requirements for control objectives and related controls activity.

COBIT

- Established by ISACA to be used for the IT component of documenting and testing internal controls.
- Comprehensive framework for managing risk and control for IT.
- More detailed and IT specific.
- Not a comprehensive Internal Controls framework.

How COBIT is used for evaluating ITGCs:

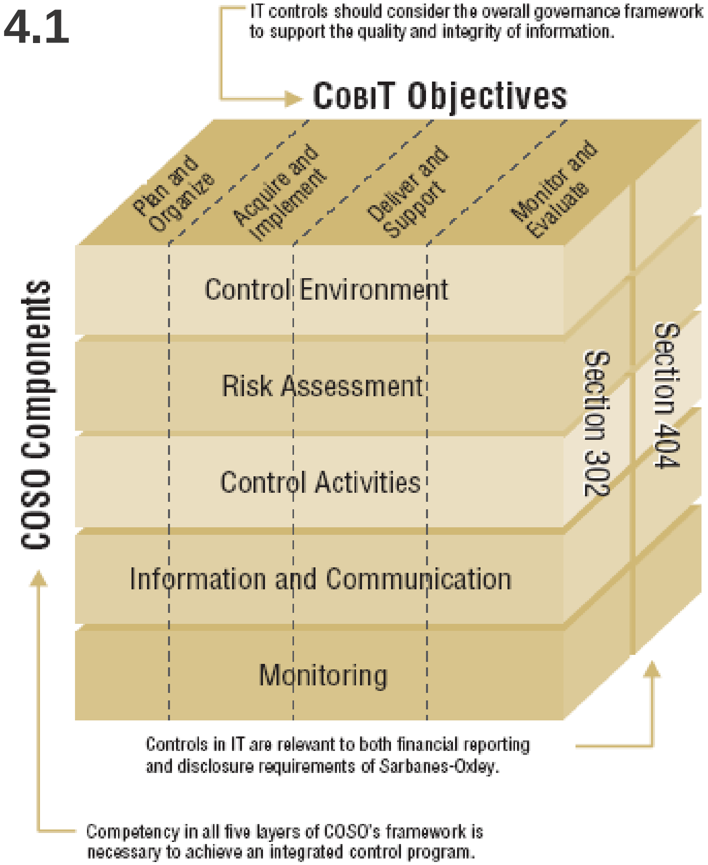
- Since ITGCs affect the entire organization, COBIT is mapped to COSO.
- 15 COBIT IT processes are identified as being relevant for the IT component of internal controls. However, companies may add or remove other COBIT processes based on the specific situation.

COBIT 4.1 Mapped to COSO

The Control Objectives for Information and related Technology (COBIT) defines an IT governance framework.

- **Control Environment –** The control environment sets the tone of an organization, influencing the control consciousness of its people.
- **Risk Assessment** – Every entity faces a variety of risks from external and internal sources that must be identified and analyzed at both the entity and the activity level.
- **Control Activities** – These policies and procedures help ensure management directives are carried out (e.g., preventive, detective, and mitigating controls).
- **Information and Communication** – Pertinent information must be identified, captured, and communicated in a manner and timeframe that supports all other control components.
- **Monitoring** – The monitoring process assesses the quality of the system's performance over time by reviewing the output generated by control activities and conducting special evaluations.

COBIT 4.1



IT controls should consider the overall governance framework to support the quality and integrity of information.
COBIT Objectives
Plan and Organize
Acquire and Implement
Deliver and Support
Monitor and Evaluate
COSO Components
Control Environment
Risk Assessment
Control Activities
Information and Communication
Monitoring
Section 302
Section 404
Controls in IT are relevant to both financial reporting and disclosure requirements of Sarbanes-Oxley.
Competency in all five layers of COSO's framework is necessary to achieve an integrated control program.

ITGC Framework

COBIT 5 Overview

- The focus of COBIT 5 is on processes, that are split into governance and management areas. These two areas contain a total of **5 domains**:

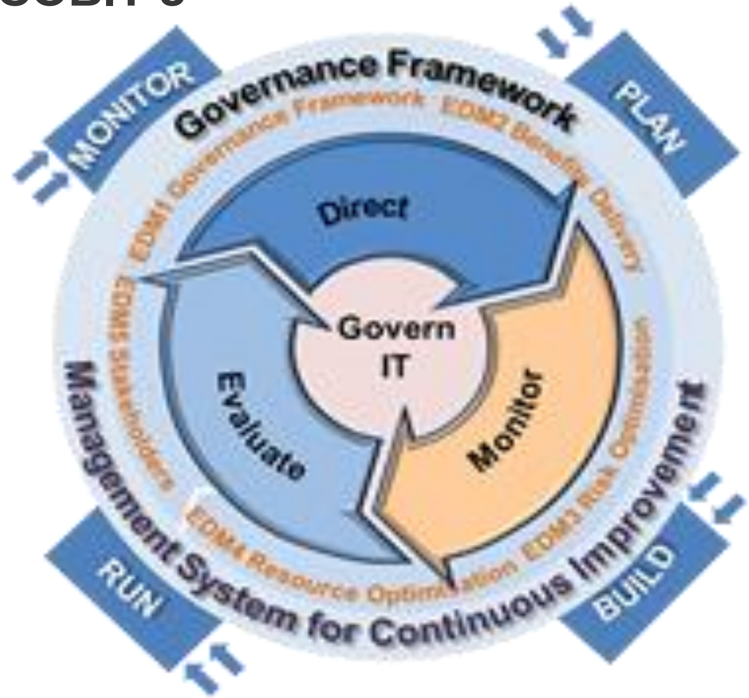
Governance of Enterprise IT

- **Evaluate, Direct and Monitor (EDM)** – Provides direction to information security and monitoring the outcome

Management of Enterprise IT

- **Align, Plan and Organize (APO)** – Provides direction to solution delivery (BAI) and service delivery (DSS),
- **Build, Acquire and Implement (BAI)** – Provides the solutions and passes them to be turned into services,
- **Deliver, Service and Support (DSS)** – Receives the solutions and makes them usable for end users, and
- **Monitor, Evaluate and Assess (MEA)** – Monitors all processes to ensure that the direction provided is followed.

COBIT 5



Across these 5 domains, COBIT has identified **37 IT processes** that are generally used by an organization as well as specific practices.

Mapping PCAOB AS 5 to COBIT 5

Processes to Identify Relevant ITGC controls

- COBIT 5 processes mapped to PCAOB Auditing Standard No. 5
- Identifies ITGCs that have a direct impact on the audit of the effectiveness of internal controls over financial reporting (SOX section 404) which can be used as a baseline for non-public organizations.

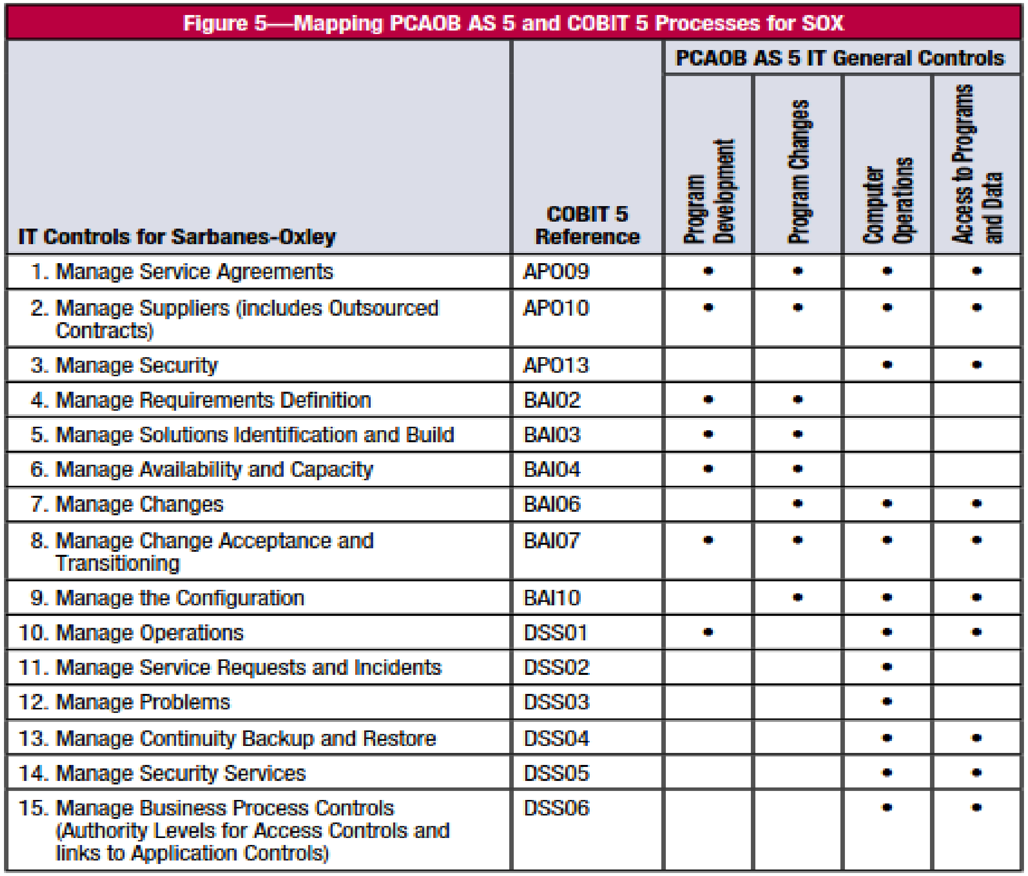


Figure 5—Mapping PCAOB AS 5 and COBIT 5 Processes for SOX

IT Controls for Sarbanes-Oxley	COBIT 5 Reference	PCAOB AS 5 IT General Controls			
		Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Manage Service Agreements	APO09	•	•	•	•
2. Manage Suppliers (includes Outsourced Contracts)	APO10	•	•	•	•
3. Manage Security	APO13			•	•
4. Manage Requirements Definition	BAI02	•	•		
5. Manage Solutions Identification and Build	BAI03	•	•		
6. Manage Availability and Capacity	BAI04	•	•		
7. Manage Changes	BAI06		•	•	•
8. Manage Change Acceptance and Transitioning	BAI07	•	•	•	•
9. Manage the Configuration	BAI10		•	•	•
10. Manage Operations	DSS01	•		•	•
11. Manage Service Requests and Incidents	DSS02			•	
12. Manage Problems	DSS03			•	
13. Manage Continuity Backup and Restore	DSS04			•	•
14. Manage Security Services	DSS05			•	•
15. Manage Business Process Controls (Authority Levels for Access Controls and links to Application Controls)	DSS06			•	•

How to Perform an ITGC Standard Review

Our Approach for ITGC Testing

Phase I Activities - IT Risk Assessment and Scoping

- **IT Risk Assessment**
  - Review and evaluate existing IT risk assessment documentation, if any.
  - Perform discovery sessions with key IT process/system owners to evaluate the current IT environment.
  - Evaluate any scheduled or pending IT projects that may impact the control environment.
  - Identify any relevant prior year audit feedback.
  - Perform IT risk assessment and map risks to ITGC framework (i.e., COBIT 5 objectives).
- **Application Scoping**
  - Identify the population of IT systems that are material (in-scope) for your particular audit through the IT risk assessment activities and documentation reviews.
  - Create/update an in-scope systems matrix that contains all in-scope systems attributes (software version, OS layers, database layers, authentication mechanism, etc.).
- **ITGC Control Catalog**
  - Identify relevant ITGC controls according to the IT environment and relevant to your type of audit.
  - Asses the control frequency and level of risk.
  - Design test procedures.

ITGC Catalog Overview

An ITGC Catalog gives an organization and the auditors an overview of key controls. The catalog typically lists the Control Number, Control Objective, Frequency, Risks, and Control Description, and may also include prior noted deficiencies and whether or not the control is manual/automated and preventive/detective.

COBIT 5 Process Name	COBIT 5 Process Details	COBIT 5 Practice Details	Risk	Expected Control Description	Control Category	Key / Non-Key	Preventative / Detective Controls	Frequency
05 Manage Security Services	Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges and perform security monitoring.	Ensure that all users have information access rights in accordance with their business requirements and coordinate with business units that manage their own access rights within business processes.	Unauthorized access to resources, programs or data may result in fraud, theft, loss of data or unauthorized transactions in financial systems.	Management periodically reviews user access rights to critical systems including administrator, super user and other privileged account access at all levels of the system (application, database and operating system).	Access to Programs and Data	Key	Detective	Semi-annual

Our Approach for ITGC Testing

Phase II Activities – Gather Audit Evidence

- Document Request List ("DRL")
  - Identify evidence required for your audit and prepare a DRL.
  - Send the DRL to functional area managers to request evidence (such as IT Managers and Human Resource Manager).
  - **Observe IT generate computer-generated reports, where possible. Capture input parameters.**
  - Obtain evidence and ensure that source data is accurate, complete and directly generated from the system, where possible.
- Population and Sample Selection
  - Define your population.
  - Select samples that are representative of the population, according to the control's risk and frequency.
  - Reference AICPA AU Section 350 Audit Sampling guide.

Document Request List

A DRL is a list prepared by the auditor for items that will be required from the process and/or data owner prior to the commencement of fieldwork. This documentation is what is necessary for the testing of ITGC controls. The DRL may include items such as policies/procedures, system documentation, user access lists, audit logs and configurations.

Request Type	Control Ref#	Key Control Activity	System	Requested Items
Population	DSS 05.02b	A standard password policy has been defined and critical applications and supporting platforms are configured according to the corporate standard.	Windows Active Directory	For each AD production domain, please run the following script: Script 4 will extract the domain Password Policy, Screensaver Policy, and Audit Policy. 1. Download and save "Script 4" from the link listed to the right (i.e. cell F17) to the desktop of the production server where the domain controller is installed. 2. Extract the "Windows Server - Domain Policies Script" to the desktop. 3. Double click the "Windows Server - Domain Policies Script" file. 4. Wait for the DOS command prompt windows to close. 5. Provide a copy of the output files (i.e. WinDomainPolicies.vbs)
Population			Dynamics - App	Screenshot of password configuration settings for the corresponding system or configuration to show that the server relies on Active Directory for authentication (typically shown by LDAP, web server or windows authentication settings).
Population			HighJump - App	

Sample Selection

Samples are selected based on:

- **Frequency of Control:** Determined by the assumed population of control occurrences per year and risk level.

Frequency	Population Size (typical)	Sample Size (typical)
Annual	1	1
Quarterly	4	2
Monthly	12	2 to 5
Weekly	52	5 to 10
Daily	250	20 to 40
Multiple Times per Day	250+	25 to 45

- **Inherent Risk:** The measure of auditor's assessment that the control will not operate as intended (control failure).
  - ○ High
  - ○ Medium
  - ○ Low

Sample Selection (continued)

Statistical Sample Selection – Ensures that each member of the population has an equal chance of being selected.

- **Random –** Each item chosen from a population by a method involving an unpredictable component. The sample is such that selected so that every possible sample has an equal chance of being selected from the population.
- **Computer –** Software (such as ACL) is used to automate or simplify the audit process

Non-Statistical Sample Section – The auditor may employ some bias when selecting the sample.

- **Haphazard –** The auditor selects a sample from a population without following a structured technique, however avoiding any conscious bias or predictability.
- **Judgmental –** The auditor intentionally places a bias on the sample (e.g., all sampling units over a certain value, all for a specific type of exception, all negatives, all new users, etc.) selected from a population

- **Note:** Population - the entire set of data from which a sample is selected and about which the IT Auditor wishes to draw conclusions.

Our Approach for ITGC Testing

Phase III Activities – Perform testing procedures

- **Testing**
  - Prepare detailed test procedures for the key ITGC's.
  - **Perform the tests of design and evaluate the operating effectiveness of each ITGC.**
  - Document test results and highlight any exceptions.
  - Confirm exceptions with stakeholders.
  - Provide IT Management and stakeholders feedback for future remediation of identified exceptions.
- **Remediation Testing**
  - Perform remediation testing.
  - Communicate results to all stakeholders.

Testing Methods

Methods for testing ITGCs:

Testing Method	Definition
Inquiry	The auditor inquires (in writing or verbally) of the responsible individual as to what procedures are in place to address the control being tested. This is typically the first step in each test.
Inspection	The auditor inspects the evidence provided to ensure that it is accurate.
Corroborative Inquiry	The auditor inquires with one individual and corroborates the inquiry separately with another individual.
System Query	The auditor tests that automated controls within an IT application are operating as expected. Examples of these kinds of controls may be: - That a predefined exception will be identified appropriately by the system (this exception may be associated with completeness and/or accuracy of input, processing and output of the application) - That logical access configuration within the application are set in a way that establishes segregation of duties and otherwise provides for the authorization of transactions.

Test of Design vs. Test of Effectiveness

Test of Design - Determines whether the controls, *if operating properly*, can effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements.

- Procedures the auditor performs to test and evaluate design effectiveness include inquiry, observation, and inspection of relevant documentation. The procedures the auditor performs to test and evaluate design effectiveness might also provide evidence that can be used to test the effectiveness of the control. Was the control designed appropriately?

Test of Effectiveness – Involves evaluating whether internal control is operating as designed.

- Procedures the auditor performs to test and evaluate test of operating effectiveness include inquiry, observation, and inspection of relevant documentation. Was the control consistently performed? Was the control performed by a person who had the necessary authority and qualifications to perform the control effectively?

Testing Methods (continued)

Methods for testing ITGCs:

Testing Method	Definition
Observation	The auditor observes the responsible individual performing a procedure.
Re-Performance	The auditor independently performs the steps as previously performed by a client or as detailed in a procedure.
Knowledge Assessment	The auditor combines inquiry, inspection and re-performance techniques to test the individuals’ knowledge of a subject or competency to perform a control.

The Language Auditors Speak

Audit Term	Test Step	Test Results
Inquiry	Inquire of the IT Operations Manager to gain an understanding of how user ID's are assigned to new users within each critical application.	Inquired with the IT Operations Manager, Joe Smith, on January 18, 2015, and noted that PeopleSoft and Active Directory user IDs are administered by the IT Department. It is noted that new users are assigned a unique ID based on the standard protocol of first initial and last name.
Inspection	Obtain and inspect the "Backup and Restore Policy" to determine if the policy clearly defines procedures in place for restoring and testing backups for critical systems.	Obtained and inspected the "Backup and Restore Policy" from the company's intranet on May 11, 2015, and noted that page 1 of the policy details the procedures for restoration testing as follows: "A structured test of the restore process will be performed to verify the quality and reliability of all backup tapes. All test details including the scope of the test, procedures and results will be documented in the ticketing system to maintain a record of the testing history."

Note: Inquiry alone is never sufficient to provide a level of certainty that a control is operating effectively. It should always be used in conjunction with one or more of the other procedures. As a result, the inquiry step will only have a conclusion if an exception was noted during the inquiry.

The Language Auditors Speak

(continued)

Audit Term	Test Step	Test Results
Corroboration	Corroborate the inquiry of the IT Operations Manager with the Database Administrator.	Corroborated the inquiry of the IT Operations Manager, Joe Smith, with the Database Administrator, Angelina Jolie, on January 19, 2015, and noted that user IDs are administered by the IT Department. It was noted that new users are assigned a unique ID based on the standard protocol of first initial and last name.
System Query	Perform a system query to obtain the security configuration for Windows Active Directory and inspect that the configuration is properly configured to require a password with a minimum of 8 characters that is complex (1 upper case, 1 lower case and a special symbol) and that is set to expire after 90 days.	IA observed the Windows Active Directory administrator, Jim Carey, perform a system query to obtain the security configuration on February 10, 2015. IA inspected the password configurations and noted that the system was properly configured to require a password with a minimum of 8 characters that is complex (1 upper case, 1 lower case and a special symbol) and that is set to expire after 90 days.

Note: Corroboration is useful only if the other party does not have prior knowledge of the question being asked.

The Language Auditors Speak (continued)

Audit Term	Test Step	Test Results
Observation	Observe the Support Services Supervisor create a work order in the ticketing system. Perform a system query to obtain the audit history log from the system to determine if the work order created by the Supervisor is appropriately tracked in the system.	IA observed as the Support Services Supervisor, Donald Trump, performed work order #8937 in the Remedy ticketing system on January 12, 2015 and noted that all modifications made by Donald to work order #8937 were captured by Remedy ticketing system.
Re-Performance	Execute a system query to obtain a list of inventory items acquired during the 2015 fiscal year. Judgmentally select a sample of 15 items. Re-perform the calculation of the average cost of the items to determine that the average cost of parts is properly calculated by the PeopleSoft system.	The Inventory Manager, John Smith, executed a system query to obtain a list of items acquired during the 2015 fiscal year on January 20, 2015. IA Judgmentally selected a sample of 15 items and re-performed the calculation of the average cost of parts on January 21, 2015 and noted the following...

Notes:

Observation - During observation, evidence must be retained that support the control being observed. Observation is a weaker form of assurance than the other procedures and should be performed in conjunction with other procedures where possible.

Re-Performance - Not typically performed as part of ITGC testing.

Documenting the Test Procedures

The procedures performed and associated results found during testing must be documented. Test procedures should be clearly documented and understandable to allow any 3rd party to re-perform the testing of the control.

Example

- **Control Description: DSS 05.04a –** Unique identities are required for system access. Group or shared logins are disabled. Users are uniquely authenticated to the system to support the validity of transactions and system administrators do not use generic standard system accounts (e.g., root, sa) to login to critical systems. Vendor supplied default and generic passwords are removed or changed.

- **Test Procedures:**
  1. Inquire of IT Management to gain understanding of how users are uniquely authenticated to systems and whether vendor supplied default and generic passwords are removed or changed.
  2. Obtain a complete list of user IDs from the manager of each key application and platform and inspect the entire population of user IDs to determine that unique IDs are used.
  3. For system components that utilize vendor supplied default and generic accounts, obtain evidence to verify that default accounts and passwords have been changed.

Documenting the Test Results

All test results should end with a conclusion (except inquiry).

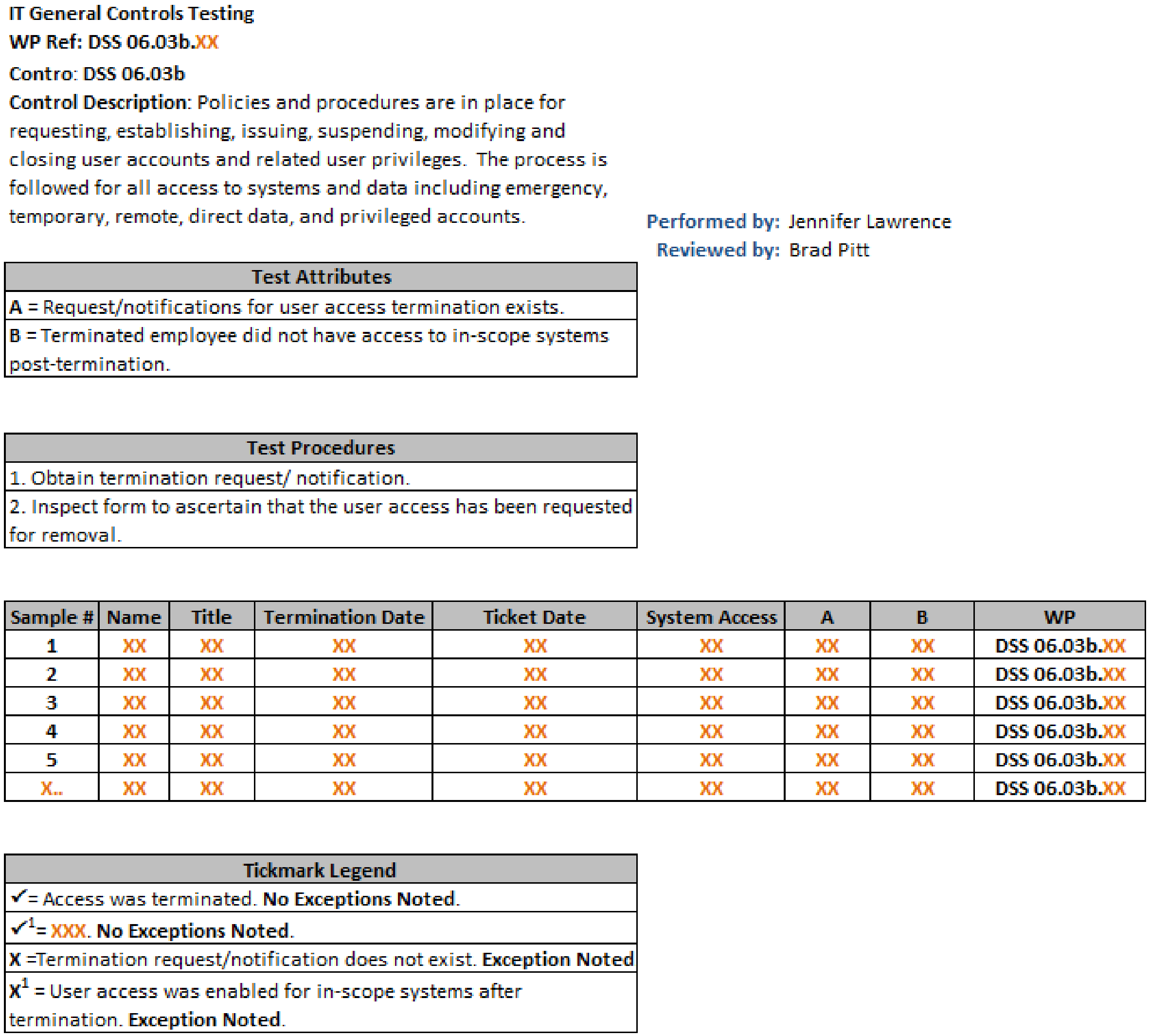
- Exception noted.
- No exception noted.

Example

- **Control Description: DSS 04.07a –** Procedures are in place to ensure that systems are backed up according to the backup operating procedures.
- **Test Results:**
  1. Inquired with the Disaster Recovery Manager, Lucy Lu, on March 1, 2015, and noted that for Windows AD servers, daily differential backups are performed Monday through Thursday, and a full backup is performed on Friday. It is noted that the weekly rotational backup tapes are stored at the company's co-located site (Iron Mountain) for a period of 5 weeks. The only IT staff members with keys to the safe are the IT Operations Manager, Janice Houston, and the Manager of Business Systems & Development, Roger Wallace.
  2. Obtained and inspected the Backup and Restore policy from the Disaster Recovery Manager, Lucy Lu, on March 2, 2015, and noted the following:
     - Differential Backups are performed for all Windows AD Servers on a daily basis. **No exception noted.**
     - Weekly rotational backup tapes are stored in the backup tape drive at the company's co-located site (Iron Mountain) for a period of 5 weeks. **No exception noted.**
  3. Inspected the Backup and Restore policy on March 2, 2015, and noted that the CTO, Bill Johnson, reviewed and updated the policy on January 20, 2015. **No exception noted.**

Test Workpapers

Example



IT General Controls Testing

WP Ref: DSS 06.03b.XX

Contro: **DSS 06.03b**

Control Description: Policies and procedures are in place for requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges. The process is followed for all access to systems and data including emergency, temporary, remote, direct data, and privileged accounts.

Performed by: Jennifer Lawrence
Reviewed by: Brad Pitt

Test Attributes
A = Request/notifications for user access termination exists.
B = Terminated employee did not have access to in-scope systems post-termination.

Test Procedures
1. Obtain termination request/ notification.
2. Inspect form to ascertain that the user access has been requested for removal.

Sample #	Name	Title	Termination Date	Ticket Date	System Access	A	B	WP
1	XX	XX	XX	XX	XX	XX	XX	DSS 06.03b.XX
2	XX	XX	XX	XX	XX	XX	XX	DSS 06.03b.XX
3	XX	XX	XX	XX	XX	XX	XX	DSS 06.03b.XX
4	XX	XX	XX	XX	XX	XX	XX	DSS 06.03b.XX
5	XX	XX	XX	XX	XX	XX	XX	DSS 06.03b.XX
X..	XX	XX	XX	XX	XX	XX	XX	DSS 06.03b.XX

Tickmark Legend
✓= Access was terminated. **No Exceptions Noted**.
$\checkmark^{1}$= XXX. **No Exceptions Noted**.
X =Termination request/notification does not exist. **Exception Noted**
X^{1} = User access was enabled for in-scope systems after termination. **Exception Noted**.

Practice Exercise #1

Access to Programs and Data

Practice Exercise #1

Access to Programs and Data

Control Description:

Only authorized individuals have Administrator access to PeopleSoft on the application level.

For the control description above, answer the following questions:

1. What pieces of evidence should be obtained?
2. How do you determine the sample size?
3. What testing steps are necessary to test this control?

Practice Exercise #1

Access to Programs and Data

Control Description : Only authorized individuals have Administrator access to Peoplesoft on the application level.

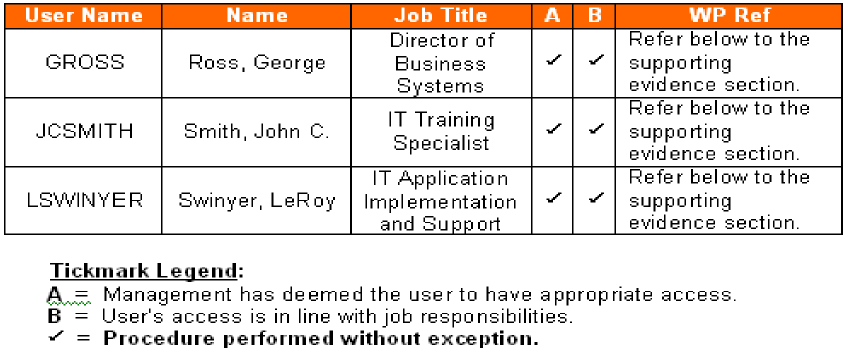
- **Sample Size:** The sample size for a system access control is the entire population of user accounts.
- **Testing Steps:**
  1. Inquire with IT to gain an understanding of how the security is configured in the PeopleSoft application.
  2. Observe IT generate a system query to obtain the list of PeopleSoft users.
  3. Compare the list of administrators to the IT organization chart or active employee listing to determine if user access is in line with job responsibilities.
  4. Inquire with IT Management to determine if the individuals with administrator access are appropriate.
- **Supporting Evidence:**
  1. User Access List.
  2. If available, a copy of the IT organization chart and/or HR reports (active employees, new hires, terminations from beginning of audit period to present).
  - ○ If available, system documentation.

Practice Exercise #1

Access to Programs and Data

Documenting the Test Results:

1. Internal Audit (IA) inquired with the IT Application Implementation and Support Manager, Janet Jackson, on March 2, 2015, and noted that only users with the ‘Super User’ role had administrator access within the PeopleSoft application.
2. IA observed Janet Jackson execute a system query to generate the list of the PeopleSoft users on March 2, 2015. IA filtered the user list in Microsoft Excel by the ‘Super User’ role.
3. IA obtained the job titles for the users with administrator access from the Director of Human Resources, Johnny Depp, on March 3, 2015, to determine if the users’ access were in line with job responsibilities, and noted the results in the table below. Further, no developers had been granted administrator level access. **No exception noted**.
4. Inquired with Janet Jackson, on March 4, 2015 and corroborated the inquiry with Ellie Goldberg, Director of IT Applications and noted that all users with administrator access were appropriate. **No exception noted.**



User Name	Name	Job Title	A	B	WP Ref
GROSS	Ross, George	Director of Business Systems	✓	✓	Refer below to the supporting evidence section.
JCSMITH	Smith, John C.	IT Training Specialist	✓	✓	Refer below to the supporting evidence section.
LSWINYER	Swinyer, LeRoy	IT Application Implementation and Support	✓	✓	Refer below to the supporting evidence section.

Tickmark Legend:
A = Management has deemed the user to have appropriate access.
B = User's access is in line with job responsibilities.
✓ = **Procedure performed without exception.**

Practice Exercise #2

Program Development & Change Management

Practice Exercise #2

Program Development & Change Management

Control Description:

Requests for normal changes to application systems, data structures, or any other information systems software or devices running in the production environment, are documented in a change management request form and authorized by the designated approver, where applicable, either through a work order or change request form.

For the control description above answer the following questions:

1. What pieces of evidence should be obtained?
2. How do you determine the sample size?
3. What testing steps are necessary to test this control?

Practice Exercise #2

Program Development & Change Management

Control Description : Requests for normal changes to application systems, data structures, or any other information systems software or devices running in the production environment, are documented in a change management request form and authorized by the designated approver, where applicable, either through a work order or change request form.

- **Sample Size:** The sample size for a program development/change control is based on the entire population of changes, frequency and level of risk.
- **Testing Steps:**
  1. Inquire with IT to gain an understanding of the Change Management process and how changes are approved. Obtain the formal Change Management policy/procedure, if available.
  2. Observe IT execute a system query to obtain a listing of changes promoted to the production environment at all layers.
  3. Select a sample of changes and obtain supporting documentation.
  4. Inspect the forms for appropriate approval.
- **Supporting Evidence:**
  1. Change Management policy/procedure, if available.
  2. Change Approval Matrix.
  3. Computer-generated listing of OS, application, database changes.
  4. Sample support documentation (i.e., work order, change request form, approvals).

Practice Exercise #2

Program Development & Change Management

Documenting the Test Results:

1. IA inquired with the Application Manager, Kim Kardashian, on July 1, 2015, and noted that change forms require approval by a documented list of authorized approvers contained within the Change Management Policy. IA obtained the Change Management Policy from Kim and noted that it was reviewed January 4, 2015.
2. Observed Kim execute a system query to generate a list of the changes migrated to the PeopleSoft production (OS, application and databases) between January 1, 2015, and July 1, 2015.
3. IA noted a total of 25 changes and selected a sample of 7 changes (based on a weekly frequency and medium to high risk level) and obtained the supporting documentation for each sample.
4. IA inspected the supporting documentation for each change sampled; compared against the authorized approver list within the change management policy to verify that each change had evidence of approval by an authorized individual. **No exception noted**.

Practice Exercise #3

Computer Operations

Practice Exercise #3

Computer Operations

Control Description: Automated data retention tools have been implemented to manage the backup and retention data plan and schedule. Backup logs are reviewed daily and documented in the Backup Log check sheet.

For the control description above, answer the following questions:

1. What pieces of evidence should be obtained?
2. How do you determine the sample size?
3. What testing steps are necessary to test this control?

Practice Exercise #3

Computer Operations

Control Description: Automated data retention tools have been implemented to manage the backup and retention data plan and schedule. Backup logs are reviewed daily and documented in the Backup Log check sheet.

- **Sample Size:** The sample size for computer operations control is based on the entire population of changes, frequency and level of risk.
- **Testing Steps:**
  1. Obtain backup schedule (for in-scope applications) from the automated tool from the backup administrator.
  2. Randomly select a sample of days.
  3. From sample, obtain history file and determine that jobs were run according to policy.
  4. Obtain backup log check sheet and determine that jobs were run according to backup schedule.
  5. If jobs were not run according to policy, determine that they were investigated and resolved.
- **Supporting Evidence:**
  1. Computer Operations policy/procedure, if available.
  2. Backup schedule from backup tool for in-scope servers.
  3. History files for backup jobs.
  4. Backup log check sheet.

Practice Exercise #3

Computer Operations

Documenting the Test Results:

1. IA inquired with IT Operations Manager, TJ Mix, on November 3, 2015, and noted that backups are performed on a daily basis and backup logs are reviewed daily and documented in the Backup Log check sheet. IA corroborated this inquiry with IT Operations Supervisor, DJ Mix A Lot and confirmed TJ's statement. IA also obtained the Computer Operations Policy which also stated the same process and backup schedule.
2. IA randomly selected a sample of 30 days across the year (based on a daily frequency and medium risk level).
3. IA obtained the history file for the selected samples to determine if the jobs ran according to policy and noted that backup did not run on February 2, 2015 however it ran successfully the next day. **No exception noted.**
4. IA also obtained the backup log check sheet to determine if the logs were reviewed daily and documented in the Backup Log check sheet. The jobs were reviewed on the selected dates, except on February 2, 2015 (as noted in procedure 3), however the job ran successfully the next day. **No exception noted.**
5. Refer to test results #3 and 4. **No exception noted**.

Pop Quiz!

1. Which of the following would ***not*** be in scope in a general computer control review?
   a. Change Management
   b. Operating System Security
   c. The Financial Statement Close Process
   d. Physical Security
2. Access to systems and data should be assigned on a need-to-know basis – True or False?
3. Inquiry alone is a suitable way to test a control – True or False?
4. The appropriate sample size required to test a general computer control is always:
   a. 1
   b. 30
   c. The entire population
   d. None of the above
5. The programmer who developed a new piece of code is the most appropriate individual to migrate that new code into the production environment – True or False?

Pop Quiz! (Answers)

1. Which of the following would ***not*** be in scope in a general computer control review?
   a. Change Management
   b. Operating System Security
   c. The Financial Statement Close Process
   d. Physical Security
2. Access to systems and data should be assigned on a need-to-know basis – ***True*** or False?
3. Inquiry alone is a suitable way to test a control – True or ***False***?
4. The appropriate sample size required to test a general computer control is always:
   a. 1
   b. 30
   c. The entire population
   d. None of the above
5. The programmer who developed a new piece of code is the most appropriate individual to migrate that new code into the production environment – True or ***False***?

Questions