IT Audit – Auditing IT General Controls
Agenda

- Introduction
- IT Audit
- IT General Controls Overview
  - Access to Programs and Data
  - Program Change & Development
  - Computer Operations
- Lessons Learned from Regulatory Reviews
- Questions, Closing Remarks, and Wrap-up
IT Audit
ITGC Workflow

Understand the IT environment

Identify in-scope systems

Review existing documents

Conduct interviews

Document processes

Review process flows

Identify and communicate Gaps

Finalize ITGC flows and risks

Test controls and evaluate deficiencies
IT General Controls
Overview
Risk: Unauthorized access to data may result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions or inaccurate recording of transactions.

Objective: Adequate controls for access to programs and data have been established to restrict access to properly authorized individuals.
Access to Programs and Data Overview

We consider the following access to programs and data components:

- Policies and procedures
- User access add/move/termination requests
- Password requirements
- Privileged users
- Physical access
- Periodic access reviews
- Appropriateness of access/segregation of duties
IT General Controls

Risk: Unauthorized changes to systems or programs may result in incomplete or inaccurate data.

Objectives: Adequate controls for program changes have been established to help ensure that changes to existing systems/applications are authorized, tested, approved, properly implemented and documented. Adequate controls for program development have been established to help ensure that new systems/applications which are developed or acquired are authorized, tested, approved, properly implemented and documented.
Program Change & Development Overview

We consider the following program change and development components:

- Change and new development methodology
- Design, authorization, development, testing, and approval
- Migration to the production environment (SOD)
- Configuration changes
- Emergency changes
- Data migration
- Post-installation reviews (typically a secondary control)
Risk: Systems or programs are inaccurately processing data and/or processing inaccurate data.

Objective: Adequate controls for computer operations have been established to ensure that system/application processing is appropriately authorized and scheduled and deviations from scheduled processing are identified and resolved.
Computer Operations Overview

We consider the following computer operations components:

- Job processing and monitoring
- Backup and recovery procedures*
- Incident and problem management

* Disaster Recovery plans are typically not in-scope. Companies need to show that they have adequate controls in place to backup their systems and data, and recover data for financially relevant systems.
Lessons Learned from Regulatory Reviews

- Completeness and Accuracy of user listings/reports
- Change Management Testing
- Re-performance Approach
Questions, Closing Remarks, and Wrap-up
Thank you!

Paul Torres, Director
ptorres@kpmg.com
Phone: 480 459 3632

Kati Stojak, Manager
kstojak@kpmg.com
Phone: 480 459 3520

www.kpmg.com
The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2014 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in the U.S.A.

The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International.