Agenda

• Understanding the IT Environment
• What are IT Application Controls?
  • The use of System Generated Reports in Controls
  • Completeness and Accuracy
• GITC Areas
  • Access to Programs and Data
  • Program Change
  • Program Development
  • Computer Operations
• Assessing Outsourced Systems
  • SOC reports
  • Other 3rd party reports
Understanding the IT Environment
Layers of Technology Overview

- Application
- Database
- Operating System
- Internal Network
- Perimeter Network
Understanding the use of Data

- **Initial capture of information and data-flow.**
  - Understand the Process!

- **What are the application controls used within these processes?**
  - Key calculations
  - System access (enter → approve)
  - Use of data in reports (i.e., edit/exception reports)
  - Interfaces between systems

- **Data Flow, Application controls and reports drive the in-scope applications**
  - For Internal Control over Financial Reporting, only systems involved in financial reporting are part of scope.
  - Other types of audits may lead to different scoping decisions.
Application Controls
Examples of Application Controls

System Access Controls:
- Access to modify loan data (i.e., loan amount, interest rate, term, etc.) is restricted to loan operations personnel.
- The GL application is configured so that the user who enters a journal entry cannot release the transaction.

System Configuration/Account Mapping:
- Revenue is recognized once an invoice is created and the sales order has shipped.
- An invoice is matched to the receipt record and the original PO and can only proceed if all three match within a 5% difference.

Interface Control:
- Sales transactions from the previous day are interfaced into the general ledger application via a nightly batch job.

Edit/Exception Reports:
- The system is configured to identify each customer transaction which does not process.
Reports: Completeness and Accuracy

*Do you know where the data is from—and that it is correct?*

**System Generated Reports:**

- Confirm that a key manual control is “dependent” on identified report.
- Identify each report(s) used as part of your audit objective (e.g. control over financial reporting) and define each report by name, version, etc.
- Identify financially significant fields on the report (i.e., the customer address may not be relevant when reviewing open AR).
- Determine how the report is generated using a report writer (e.g., Business Objects, Cognos, etc.).
- Identify the data sources as well as the data flow.
  - Data may be sourced from different systems, databases, data warehouses. (GITCs should be in place over each data source).
  - If data flows through various systems each interface and application may need to be scoped-in for the audit.
Completeness and Accuracy (continued)

**Potential Completeness Test Steps:**
- Reconcile to a GL account
- Inspect the query used to generate the report
- Inspect the report configuration
- Reconcile to 3rd party records over which completeness assurance is obtained.

**Potential Accuracy Test Steps:**
- Select data from the system that should be included on the report and confirm the information is correctly listed
- For edit/exception reports, determine each scenario that generates an exception to be listed on the report. Complete a sample test case for each scenario and determine that it is correctly listed on the report.
GITCs

Logical and Physical Access (APD)
- Policies
- Authentication (User IDs and Passwords)
- New Users
- Terminations
- Super User & Administrative Access
- Physical Access
- Periodic Access Monitoring

Change Management (PC)
- Policies
- Change Authorization
- Change Testing
- Change Approval
- Implementation/Migration to Production
- access segregation
- Monitoring
GITCs (continued)

Program Development (SDLC)
- SDLC
- Project Authorization
- Project Execution
- Testing
- Issues Management
- Go-Live Approval

Computer Operations (CO)
- Job Processing
- Backup/Replication
- Restoration
- Incident Management
GITC and Application Control Linking

Applications & Tools

<table>
<thead>
<tr>
<th>APD</th>
<th>CO</th>
<th>PC</th>
<th>SDLC</th>
</tr>
</thead>
</table>

GITCs

Testing at App/Database/OS Levels

Symbol definitions:
- **R** – Risk
- **Manual control**
- **IT dependent manual control**

Term definitions:
- GITC – IT General Control
- ITAC – IT Application Control
- APD – Access to Programs and Data
- CO – Computer Operations
- PC – Program Changes
- SDLC – Software Development Lifecycle

© 2020 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affliated with KPMG International, a Swiss entity. All rights reserved.
Impact of GITC Issues on Application Controls

Applications & Tools

<table>
<thead>
<tr>
<th>APD</th>
<th>CO</th>
<th>PC</th>
<th>SDLC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GITCs

<table>
<thead>
<tr>
<th>R</th>
<th>IT application control</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>App 1</td>
</tr>
<tr>
<td>R</td>
<td>App 2</td>
</tr>
<tr>
<td>R</td>
<td>App 3</td>
</tr>
</tbody>
</table>

Testing at App/Database/OS Levels

<table>
<thead>
<tr>
<th>APD</th>
<th>PC issue</th>
<th>Testing at App/Database/OS Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Symbol definitions:
- R - Risk
- IT application control
- Manual control
- Applicable testing area
- Non-applicable testing area
- IT dependent manual control
- Control issue or gap noted

Term definitions:
- GITC - IT General Control
- ITAC - IT Application Control
- APD - Access to Programs and Data
- CO - Computer Operations
- PC - Program Changes
- SDLC - Software Development Lifecycle

© 2020 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.
Assessing Outsourced Systems
What to Consider When Assessing Outsourced Systems

• Not a check the box activity!!
• How is the outsourced system used to support processes relevant to the audit (business processes as well as IT)?
• What is the support model for the outsourced system?
  • Fully “Cloud” – Software-as-a-Service
  • Just a platform – Platform-as-a-Service
  • Just the infrastructure – Infrastructure-as-a-Service
  • Just the physical hosting - Physical Hosting
• How much or what type of assurance is required?
  • Part of Internal Control over Financial Reporting: SOC1 Type II.
  • Security & Availability: SOC2 Type II
Further considerations

• Evaluation of controls in a SOC report should follow the same general process as if the controls were completed internally
• Items to review
  • Type 1 (Design Only) versus Type 2 (Test of Operating Effectiveness)
  • Report Dates
  • Report Opinion
  • CEUCs (Complimentary End User Control Considerations)
  • Control Evaluation including Deficiency Evaluation
  • Sub-service organizations
• What if there is no SOC1 or SOC2 report? Alternatives exist such as:
  • Certifications (e.g. ISO-27000, HITRUST, PCI-DSS)
  • Agreed-upon-procedures report
  • ???
  • Consider the circumstances for each situation (e.g. scope of certification, reporting available, testing performed) and the intended use of the report.
  • For SOX/ICOFR alternatives to a SOC report may be difficult to rely on.
Common Pitfalls

• SOC reports that do not cover (all of) the system you use;
• Scope of controls in the SOC report do not match the scope expected/needed.
• Year-over-year changes in the SOC report.
• CUEC’s that are not addressed.
• SOC reports with exceptions that are not properly addressed by the service provider management or the service auditor.
• Sub-service organizations that are not included in the scope.
• Qualified opinions
• Not expecting any challenges because the vendor is [insert name of large IT vendor here]…
Thank you
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia

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 on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 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.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.