Effectively Assessing IT General Controls

Tommie Singleton
UAB

AGENDA

• Introduction
• Five Categories of ITGC
  – Control Environment/ELC
  – Change Management
  – Logical Access Controls
  – Backup/Recovery
  – Third-Party Providers
• What the Results Mean

INTRODUCTION

• PCAOB/AS5-ICFR
• AICPA/Risk-Based Standards
• IIA/GAIT, GTAG
• ISACA/COBIT, ITAF

<table>
<thead>
<tr>
<th>ISACA</th>
<th>ITAF</th>
<th>3630/ITGC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to ITGC</td>
<td>Information Resource Planning</td>
<td>IT Service Delivery</td>
</tr>
<tr>
<td>IT Human Resources</td>
<td>Physical/Environment Control</td>
<td>Outsourcing/3rd Party IT</td>
</tr>
<tr>
<td>InfoSec Management</td>
<td>Information Systems Operations</td>
<td>BCP/DRP</td>
</tr>
<tr>
<td>Database Mgmt &amp; Control</td>
<td>Identification &amp; Authentication</td>
<td>Systems Software Support</td>
</tr>
<tr>
<td>Hardware Support</td>
<td>Network Management &amp; Controls</td>
<td>SDLC</td>
</tr>
<tr>
<td>Enterprise Portals</td>
<td>O/S Management &amp; Controls</td>
<td></td>
</tr>
</tbody>
</table>

4/7/2011
ITGC: Control Environment
• OBJECTIVE:
  – Ensure that the data processing that takes place in systems and IT occurs in a controlled environment, supporting data integrity and security.
• Loosely equivalent to COSO’s control environment & COBIT’s PO domain
• a.k.a. Entity-level controls

ITGC: Control Environment
• ISSUES:
  – Data processing accuracy, timeliness, integrity, and security depend on it
  – Financial reporting systems depend on it
  – “umbrella” of applications and automated controls
  – Application controls affected by it

ITGC: Control Environment
• MEASURES:
  – IT risks that have substantive inherent risks
  – Controls that mitigate those IR
  – Compared to generally accepted benchmarks (could be a set of best practices)
  – Two factors of likelihood/probability and impact/magnitude

ITGC: Control Environment
• ILLUSTRATIONS:
  – IT Strategy
  – IT Governance (e.g., ITGI)
  – Computer Operations (e.g., ITIL)
  – IT Investment & Capital Budgeting, including IT portfolio (e.g., ROI)
  – Alignment of IT with business goals, objectives
  – Managing IT Projects (e.g., PM principles)
  – Managing IT Human Resources
  – IT Risk Assessment
  – IT Policies & Procedures
ITGC: Change Management

• OBJECTIVE:
  - Structure and processes for software and hardware acquisitions, development, and implementation that ensure that they are appropriately managed to provide assurance that automated business processes, application controls and automated controls adequately support business goals and objectives, especially financial reporting.
  - Equivalent to COBIT’s A16 process

• ISSUES:
  - Data processing accuracy, timeliness, integrity, and security depend on it
  - Financial reporting systems depend on it
  - Can affect applications and automated controls
  - Applies to commercial and proprietary IT
  - Initiation, authorization, development or purchase, testing, deployment of IT: effectively managing changes to IT

• MEASURES:
  - IT risks that have substantive inherent risks (e.g., programming)
  - Controls that mitigate those IR
  - Compared to generally accepted benchmarks (could be a set of best practices)
  - Two factors of likelihood/probability and impact/magnitude

• ILLUSTRATIONS:
  - P&P (i.e., a formal process)
  - Application Development (e.g., SDLC)
  - Configuration Management (e.g., ITIL, ISACA’s G37, COBIT’s DS9)
  - Software Management (e.g., updates)
  - O/S Management
  - Network Management
  - Hardware/Infrastructure Management
ITGC: Logical Access Control

- **OBJECTIVE:**
  - Restricted access control to data and programs to prevent unauthorized access or changes, including prevention of unintentional errors and fraud.
  - Becoming more and more critical, high IR
  - Can also be used to implement logical SoD

- **ISSUES:**
  - Protecting programs from unauthorized changes or malicious activities
  - Protecting data from unauthorized changes or malicious activities
  - To implement effective logical SoD
  - Includes employees and external malicious intruders
  - Back door and front door (i.e., lots of ways to exploit access)

- **MEASURES:**
  - Password policy (best practices)
  - SoD (restricted access)
  - Access controls at all levels (e.g., no defaults, no open access)

- **ILLUSTRATIONS:**
  - P&P (i.e., a formal process)
  - InfoSec
  - DBA access controls
  - O/S access controls
  - Application access controls
  - Network access controls
  - Software library access controls
ITGC: Backup/Recovery

• OBJECTIVE:
  – To ensure the entity can recover computer operations from a failure or pandemic event in a timely manner with integrity and accuracy.
  – Scope can vary significantly b/w internal audit and external audit

• ISSUES:
  – Able to restore data after a system failure and loss of data, timely and accurately
  – Able to restore data after a natural disaster, timely and accurately
  – Able to restore business operations after a pandemic system failure
  – Able to restore business operations after a natural disaster

• MEASURES:
  – Data backups (best practices: offsite, regular, etc.)
  – BCP (best practices)
  – DRP (best practices)

• ILLUSTRATIONS:
  – Backup (e.g., best practices)
  – Testing of restoring backup of data
  – Testing of restoring business operations after a pandemic event
  – Testing of BCP and DRP
  – Make sure it is IN SCOPE!
ITGC: 3rd-Party Providers

• OBJECTIVE:
  – To ensure reliable vendors are being used to provide IT services which operate at a high level of assurance and operational effectiveness.
  – Focus here is providers associated with IT, not providers in general

• ISSUES:
  – Vendors who are competent and reliable to provide quality services
  – Vendor systems that have adequate controls for relevant areas
  – Does the vendor have independent verification of adequate controls?

• MEASURES:
  – Reliability of vendor (reputation, tenure, etc.: e.g., is the Geek Squad a reliable vendor for network support?)
  – Competency of vendor (experience, credentials, reputation)
  – Adequacy of controls in vendor’s services (SSAE #16/SOC-1 report, or SOC-2/SOC-3 report, etc.)

• ILLUSTRATIONS:
  – Network support
  – Help desk
  – Application development
  – Communication lines
  – eCommerce
  – Data center
  – Cloud computing
  – SaaS
  – IaaS
RESULTS

• Downstream controls may mitigate the deficiency
• Consider manual and IT-dependent controls where control objectives overlap

RESULTS

• Linking residual risks (RMM) to specific financial systems, transaction cycles, material account balances, or other audit objectives (GAIT & RBA)
  – That is, make sure it is in scope
• Group or aggregated related controls for best analysis (GAIT)
  – That is, make sure to consider all weaknesses and deficiencies

ASSESSMENT PRINCIPLES

1. To assess ITGC deficiencies, it is necessary to understand the reliance chain between the financial statements and the ITGC key controls that have failed.

2. For there to be a material weakness, two tests have to be met, (a) likelihood and (b) impact (i.e., the potential misstatement of the financial statements).

3. Because an ITGC deficiency does not directly affect the financial statements, the assessment is similarly not direct. The assessment is in stages or steps, and the likelihood and impact tests are applied across a combination of the steps.

4. All ITGC deficiencies that relate to the same ITGC control objective should be assessed as a group.

5. All ITGC control objectives that are not achieved and relate to the same key automated controls, key reports, or other critical functionality should be assessed as a group.

6. The principle of aggregation requires that control deficiencies of all types — including manual and automated control deficiencies relating to the same significant account or disclosure — be considered as a group.

CONCLUSION

• Deficiencies in ITGC can INDIRECTLY lead to RMM
• ITGC deficiencies can lead directly or indirectly to operational failures
• Application controls can only be appropriately tested and relied upon if ITGC as a whole is reliable
• ITGC MATTERS!!
Effectively Assessing IT General Controls

Tommie Singleton, Ph.D., CPA, CISA, CITP
tsingleton@uab.edu