IT Auditing For Non-IT Auditors

2022 Atlanta Chapter of IIA Government and Non-For-Profit Conference

Yolanda Lockett, CIA, CISA
Marietta, GA

January 21, 2022
INTRODUCTION:

- In today’s environment, Information Technology (IT) is a critical part of every program or process. Government, like many enterprises, is extremely dependent on technology to accomplish the objectives of its agencies and programs.
- This reliance on technological data and systems must be a major concern for all audit professionals.
- As a result, all audits should address technological risks and include a review of the adequacy of controls in the technological environment in order to assure effectiveness and efficiency in government programs and processes and to provide the highest level of value and accuracy.
POLLING QUESTION

Most of the programs or functions within my agency or department are dependent upon some type of technology.

_____ True
_____ False
_____ I don’t know
WHAT WE WANT TO ACCOMPLISH:

Basic Understanding of IT Audits

- **Comparison**
  - Process Comparison
  - Objective Comparison
- **Types of IT Controls**
- **Examples of IT Audits**
- **IT General Controls Audit Components**
- **Common IT Audit Findings**
WHAT IS AN IT AUDIT?

- An IT Audit is a Performance Audit.
- Evaluation of an organization's information technology infrastructure policies and operations.
- Ensure information technology processes are in compliance with IT-specific policies and standards.
- Assessment of the controls to:
  - ensure data integrity is aligned with the business's overall goals.
  - protect corporate assets.
  - ensure overall business and financial controls that depend on the systems.
- Ensure information technology dependent controls and processes are working properly.
# COMPARISON

<table>
<thead>
<tr>
<th>Audit Process</th>
<th>Business Performance Audit</th>
<th>IT Performance Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Planning Phase</td>
<td>Organizational Chart and job descriptions</td>
<td>Organizational Chart and job descriptions</td>
</tr>
<tr>
<td></td>
<td>Performance Measures and Key Performance Indicators</td>
<td>IT Strategic Plan and Standards</td>
</tr>
<tr>
<td></td>
<td>Review of policies and procedures</td>
<td>Review of policies, standards, and procedures</td>
</tr>
<tr>
<td></td>
<td>Interview staff to verify to gain an understanding of the business process.</td>
<td>Interview staff to verify that policies and procedures are being followed.</td>
</tr>
<tr>
<td></td>
<td>Applications, Systems, and Tools</td>
<td>IT Topology Diagram and Assets</td>
</tr>
<tr>
<td>2) Fieldwork Phase</td>
<td>Assess whether controls reduce risks</td>
<td>Assess whether controls reduce risks</td>
</tr>
<tr>
<td></td>
<td>Compliance test business controls</td>
<td>Tests compliance with policies and procedures</td>
</tr>
<tr>
<td></td>
<td>Tests performance measures and KPIs</td>
<td>Verify implementation of standards and policies</td>
</tr>
<tr>
<td></td>
<td>Tests operating effectiveness of controls</td>
<td>Tests operating effectiveness of controls</td>
</tr>
</tbody>
</table>
# COMPARISON

## AUDIT OBJECTIVES

<table>
<thead>
<tr>
<th>Financial/Performance</th>
<th>IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completeness</td>
<td>Integrity</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Reliability</td>
</tr>
<tr>
<td>Validity</td>
<td>Security</td>
</tr>
<tr>
<td>Authorization</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Rights &amp; Obligation</td>
<td>Availability</td>
</tr>
<tr>
<td>Presentation &amp; Disclosure</td>
<td>Scalability</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Effectiveness</td>
</tr>
<tr>
<td>Effectiveness</td>
<td>Efficiency</td>
</tr>
</tbody>
</table>
## TYPES OF IT CONTROLS

<table>
<thead>
<tr>
<th>Control Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Preventive Controls</td>
<td>Data-entry edits&lt;br&gt;Access Controls&lt;br&gt;Antivirus software&lt;br&gt;Firewalls&lt;br&gt;Intrusion prevention tools</td>
</tr>
<tr>
<td>2) Detective Controls</td>
<td>Data-entry edits&lt;br&gt;Alerts to identify unauthorized or fraudulent transactions&lt;br&gt;Monitoring and Review of accounts</td>
</tr>
<tr>
<td>3) Corrective Controls</td>
<td>Correcting data entry errors&lt;br&gt;Incident recovery</td>
</tr>
</tbody>
</table>
EXAMPLES OF IT AUDITS

- IT General Controls
- Change Management
- IT Security
  - Physical Security
  - Access Controls
- Computer Operations
- Asset Management
- Disaster Recovery/Business Continuity
- Application Controls
IT GENERAL CONTROLS
AUDIT COMPONENTS
IT GENERAL CONTROLS AUDIT COMPONENTS (continued)
IT GENERAL CONTROLS AUDIT COMPONENTS (continued)

SECURITY

Physical Access

- 1. Perimeter Defense
- 2. - 3. Gated Key-Card Access to Property with 24/7/365 Security Staff
- 3. The reception area
- 4. Escorted Area
- 5. Data Centre Room
- 6. Data Center Cabinet
- 7. Private Access Door to Each KeyBlock
- 8. Key-Card Access to Each Rack
- 9. Discrete Vendor Access to Racks
- 10. Video Camera Surveillance Throughout Property
- 11. Located on Secure Peninsula
- 12. Multi-Factor ID for Building Access
- 13. 24/7/365 Armed Security in Building

Logical Access

- Physical Security
- Perimeter and Network Security
- Secure Endpoints
- Application Security
- Data Security
- (Proactive) Policy Management
- (Reactive) Monitoring + Response
POLLING QUESTION

Who is responsible for application access controls?

_____ Business Management

_____ IT

_____ Both
IT GENERAL CONTROLS AUDIT COMPONENTS (continued)

PROGRAM CHANGE MANAGEMENT

Change Management Process

1. Request for Change
2. Impact Analysis
3. Approve / Deny
4. Implement Change
5. Review / Reporting
IT GENERAL CONTROLS AUDIT COMPONENTS (continued)

SYSTEM DEVELOPMENT/IMPLEMENTATION

System Development Life Cycle

- Planning
- Analysis
- Design
- Development
- Testing
- Implementation
- Maintenance

15
POLLING QUESTION

Who should authorize changes to applications or systems?

_____A. Business Management
_____B. IT Management
_____C. Project Leader
_____D. Steering Committee Chairperson
• Batch job processing
• Monitoring of jobs (success/failure)
• Changes to the batch job schedules
OTHER COMPUTER OPERATIONS CONSIDERATIONS:

- Backup and recovery procedures
- Incident handling and problem management
- Disaster Recovery Plan (DRP) and Business Continuity Plan (DRP)
- Patch management
POLLING QUESTION

We obtain an annual independent service organizations’ control report (SOC) for every program or business process we have outsourced to a vendor.

_____ True
_____ False
_____ I don’t know
COMMON IT AUDIT FINDINGS

Physical Security:

- **Access is not limited to authorized personnel.**
- **Environmental and monitoring systems:**
  - The lack of uninterruptable power supplies (UPS) and a backup generator.
  - No independent air conditioning.
  - The lack of fire suppression.
  - No or inadequate monitoring of data center environment.
Logical Access:

- No formal procedures for setting up new user setup.
- Users with access where they have no business need.
- Users who no longer need access are not deactivated timely.
Change Management:

- Changes that have been implemented without any documented authorization or approval.
- Developers or persons who have the ability make changes who also have access to the production environment.
- No testing environment or testing environment that does not sufficiently mirror the production environment.
COMMON IT AUDIT FINDINGS (continued)

Computer Operations:

- Program management are not involved in backup and recovery procedures.
- No testing of the disaster recovery plan occurs.
- Segregation of duties are not used in job processing.
IT Policies and Procedures:

- **No formal or incomplete policies and procedures in the following areas:**
  - Physical security of IT assets.
  - Agency access to computer information and hardware.
  - Installation and use of software.
  - Personal use of computer hardware and software.
  - Mobile device management.
  - Password configuration and maintenance.
References

(Links to Presentation Images and Other Resources of Information)

- IT General Controls Audit Components: https://cplusglobal.wordpress.com/2015/04/23/it-general-controls-review/
- Program Change Management: https://www.smartsheet.com/8-elements-effective-change-management-process
- Computer Operations: https://byjus.com/govt-exams/computer-components/
Questions & Comments

Contact
Yolanda Lockett, CIA, CISA
locketty1@yahoo.com
Phone (850) 879-5647