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

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

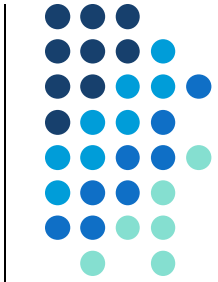
COMPARISON

AUDIT OBJECTIVES	
Financial/Performance	**IT**
Completeness	Integrity
Accuracy	Reliability
Validity	Security
Authorization	Confidentiality
Rights & Obligation	Availability
Presentation & Disclosure	Scalability
Efficiency	Effectiveness
Effectiveness	Efficiency

TYPES OF IT CONTROLS

Control Type	Examples
1) Preventive Controls	Data-entry edits
	Access Controls
	Antivirus software
	Firewalls
	Intrusion prevention tools
2) Detective Controls	Data-entry edits
	Alerts to identify unauthorized or fraudulent transactions
	Monitoring and Review of accounts
3) Corrective Controls	Correcting data entry errors
	Incident recovery

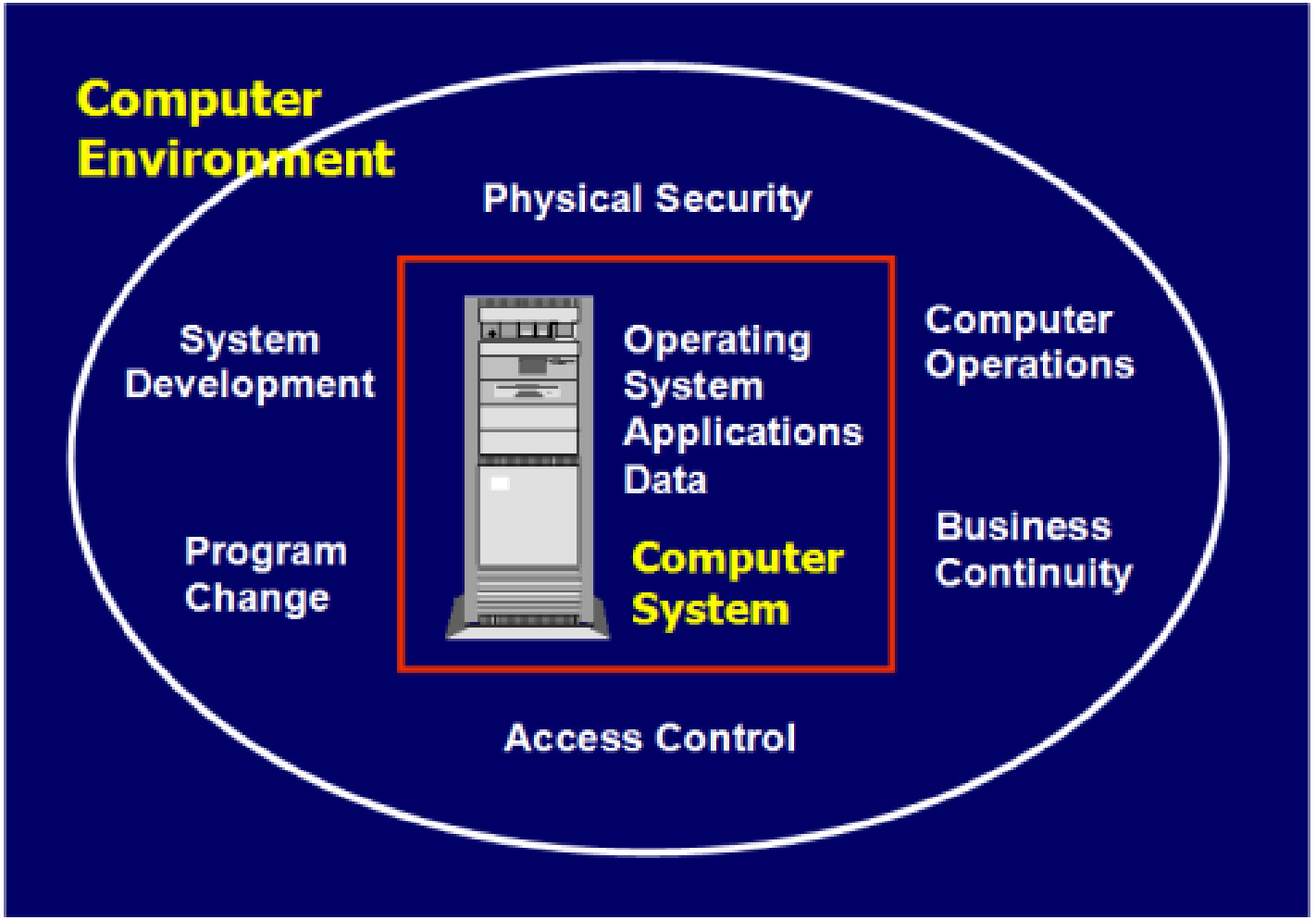
EXAMPLES OF IT AUDITS



- 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

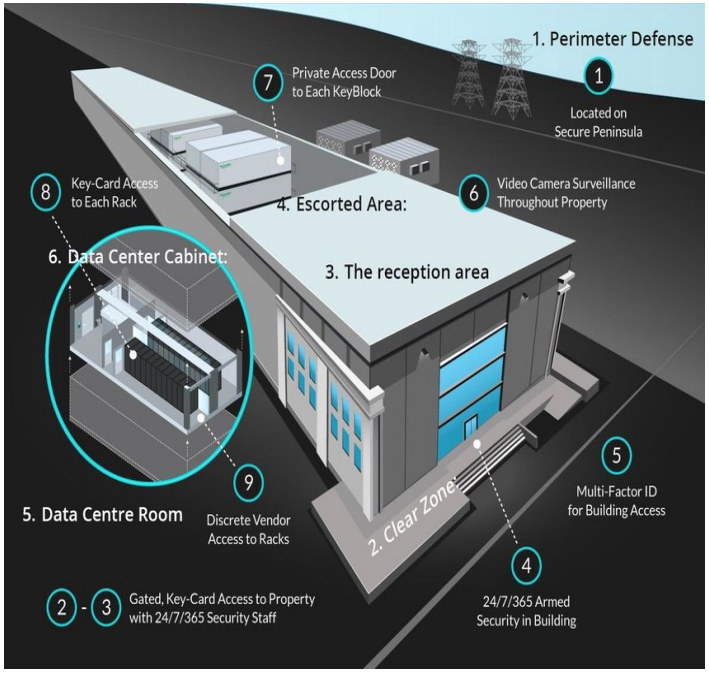
IT GENERAL CONTROLS AUDIT COMPONENTS *(continued)*



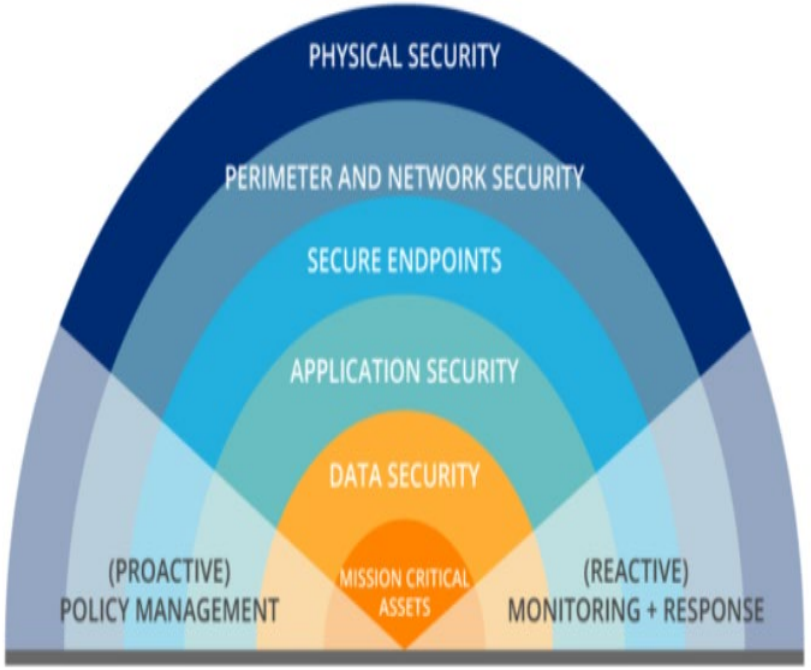
IT GENERAL CONTROLS AUDIT COMPONENTS *(continued)*

SECURITY

Physical Access



Logical Access



POLLING QUESTION

Who is responsible for application access controls?

_____ **Business Management**

_____ **IT**

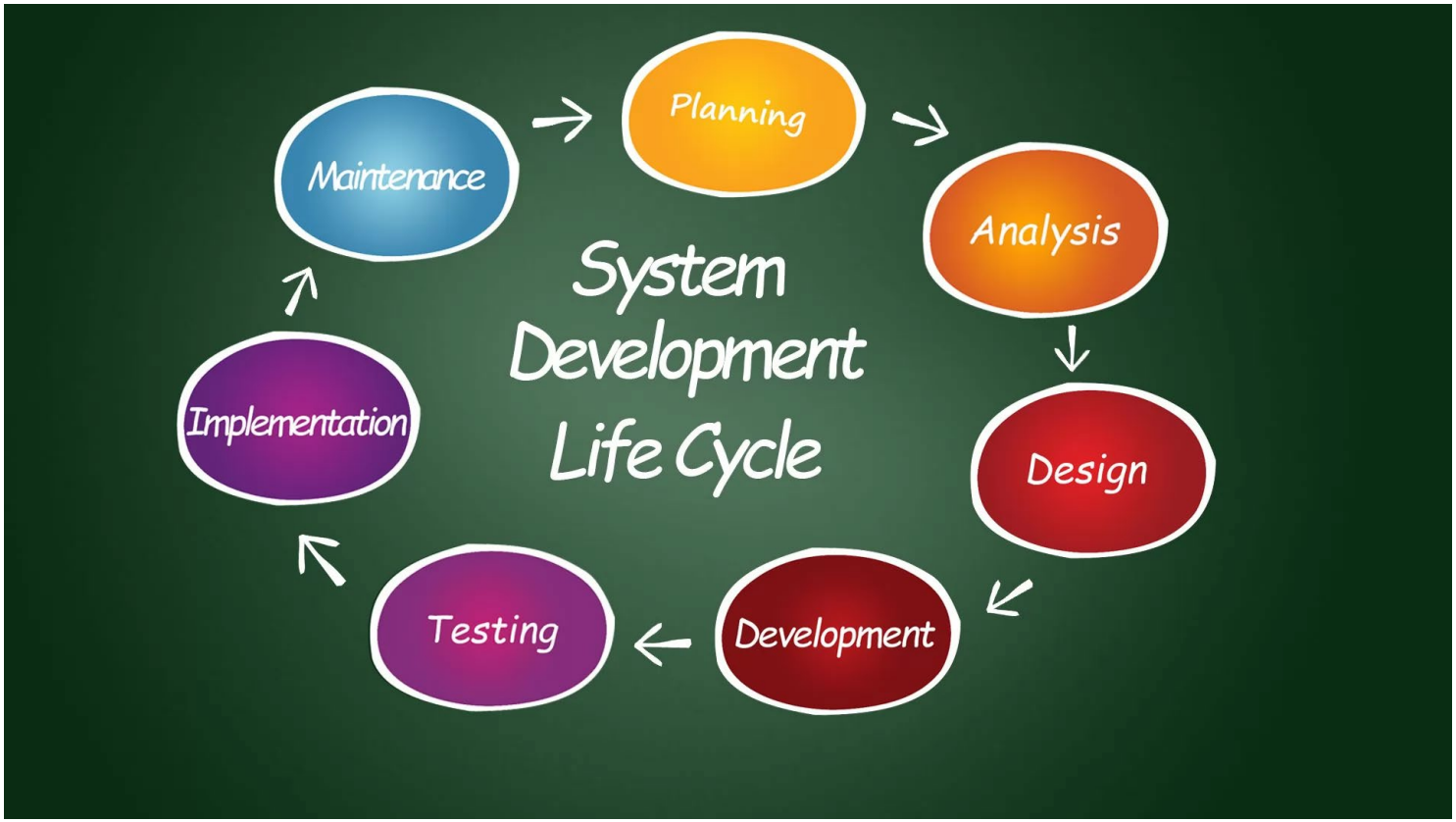
_____ **Both**

IT GENERAL CONTROLS AUDIT COMPONENTS *(continued)*

PROGRAM CHANGE MANAGEMENT

IT GENERAL CONTROLS AUDIT COMPONENTS *(continued)*

SYSTEM DEVELOPMENT/IMPLEMENTATION



POLLING QUESTION

Who should authorize changes to applications or systems?

_____A. Business Management

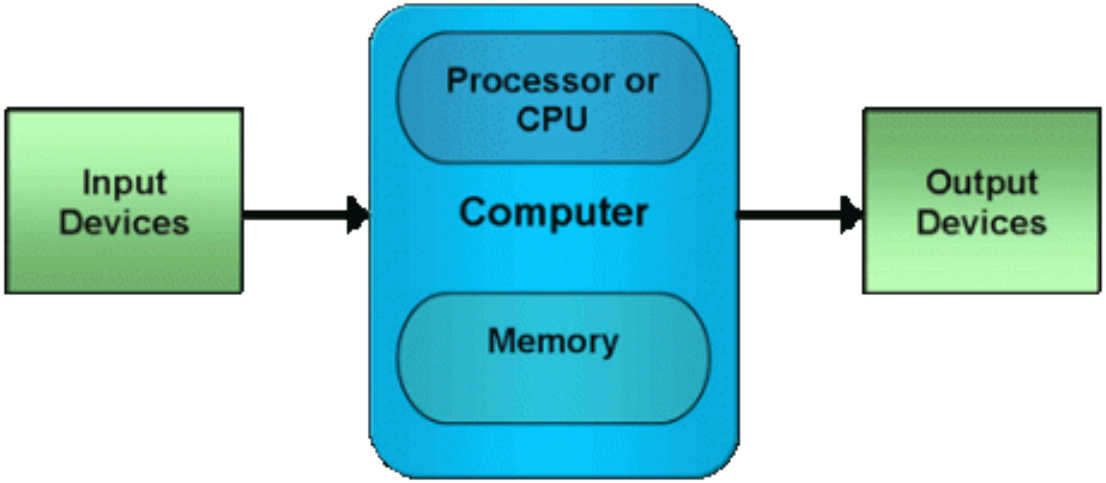
_____B. IT Management

_____C. Project Leader

_____D. Steering Committee Chairperson

IT GENERAL CONTROLS AUDIT COMPONENTS *(continued)*

COMPUTER OPERATIONS



- Batch job processing
- Monitoring of jobs (success/failure)
- Changes to the batch job schedules

IT GENERAL CONTROLS AUDIT COMPONENTS *(continued)*

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.

COMMON IT AUDIT FINDINGS*(continued)*

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.**

COMMON IT AUDIT FINDINGS*(continued)*

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.**

COMMON IT AUDIT FINDINGS *(continued)*

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/
- Physical Security of Data Center Operations: https://www.researchgate.net/figure/show-layers-and-its-features-of-the-physical-security-layers-Keystone-NAP-2017_fig7_328769165
- Levels of Security: https://www.business2community.com/cybersecurity/organizations-operating-in-the-digital-world-need-multiple-layers-of-defense-02086925
- Program Change Management: https://www.smartsheet.com/8-elements-effective-change-management-process
- Computer Operations: https://byjus.com/govt-exams/computer-components/
- Business Continuity: https://powersolution.com/it-support-solutions-and-services-provider-in-new-jersey/backup-recovery-and-intelligent-business-continuity-services-new-jersey/

Questions & Comments

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