IT Web Application Audit Principles

Presented by:

James Ritchie, CISA, CISSP….

Welcome!

An IT audit is the process of collecting and evaluating evidence of an organization's information systems, practices, and operations.

The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives.

A control is developed to mitigate a known risk to a level acceptable by Senior Management.

The concept of attaining a secure computing environment (ie, an ideal state free from risk or danger) by mitigating the vulnerabilities associated with computer use.

ISACA®
Trust in, and value from, information systems
Greater Hartford Chapter

Risks Types

- Strategic
- Compliance
- Market
- Operational
- Environmental
- Reputational
- Market

ISACA®
Trust in, and value from, information systems
Greater Hartford Chapter

Application Risks

- Unauthorized and/or erroneous transactions
- Processing inefficiencies due to incomplete data entry
- Access control violations
- Data entry errors undetected
- Breach of system integrity and loss of critical data
- Non-compliance with federal and state laws regarding computer and data communications use
- Destruction of critical information by unauthorized users
- Impairment of the Organization’s reputation

Security Domains

- Access Control Systems and Methodology
- Telecommunications and Network Security
- Business Continuity Planning and Disaster Recovery Planning
- Security Management Practices
- Security Architecture and Models
- Law, Investigation, and Ethics
- Application and Systems Development Security
- Cryptography
- Computer Operations Security
- Physical Security

CoBIT Domains

- ➢ Plan and Organize
  - ✓ PO 8 – Manage Quality
- ➢ Acquire and Implement
  - ✓ AI 2 - Acquire and Maintain Application Software
  - ✓ AI 6 - Manage Changes
  - ✓ AI 7 - Install and Accredit Solutions and Changes
- ➢ Deliver and Support
  - ✓ DS 5 - Ensure Systems Security
- ➢ Monitor and Evaluate
  - ✓ ME 2 - Monitor and Evaluate Internal Control

ISACA®

Trust in, and value from, information systems

Greater Hartford Chapter

Internal Controls 101

- ➢ Primary Objectives of Internal Controls
  - ✓ Accurate Financial Information
  - ✓ Compliance with Policies and Procedures
  - ✓ Safeguarding Assets
  - ✓ Efficient Use of Resources
  - ✓ Accomplishment of Business Objectives and Goals

ISACA®
Trust in, and value from, information systems
Greater Hartford Chapter

Point of View

- Security Perspective
  - ✓ Security requirements early in SDLC process.
  - ✓ Ensure legal, regulatory, contractual, and internal compliance requirements.
  - ✓ Follows industry best practices.
  - ✓ Testing during development, QA, pre and post production.
- Audit Perspective
  - ✓ Compliance to legal, regulatory, contractual, and internal compliance requirements.
  - ✓ Appropriate evidence is documented.
  - ✓ Business objectives and goals are maintained.
  - ✓ Each audit point is reached during the SDLC phases.