ISACA®

Trust in, and value from, information systems

Trinidad & Tobago Chapter

TRAINING WEEK COURSE OUTLINE

May 9-13 2016

RADISSON HOTEL TRINIDAD

Port of Spain, Trinidad, W.I.

FACILITATOR'S BIOGRAPHY

John Tannahill, CA, CISM, CGEIT, CRISC is a management consultant specializing in information security and audit services. His current focus is on information security management and control in large information systems environments and networks. His specific areas of technical expertise include UNIX and Windows operating system security, network security, and Oracle and Microsoft SQL Server security. John is a frequent speaker in Canada, Europe and the US on the subject of information security and audit.

He is a member of the Toronto ISACA Chapter and has spoken at many ISACA Conferences and Chapter Events including ISACA Training Weeks; North America CACS; EuroCACS; Asia- Pacific CACS; International and Network and Information Security Conferences.

John is the 2008 Recipient of the **ISACA John Kuyer Best Speaker/ Best Conference Contributor** Award.

Prior speaking engagements include:

- ISACA Chapter seminars (e.g. Toronto, Washington, Trinidad & Tobago)
- ISACA Training Weeks (2001- present)
- ISACA NACACS, EuroCACS, Asia-Pacific CACS Conferences
- ISACA Information Security Management Conferences
- ISACA International Conferences
- CSI Annual Computer Security Conference (2009)
- Presented many in-house 1-day – 5-day seminars

CYBERSECURITY RISK, CONTROL AND AUDIT: 3 DAYS (SEMINAR)

SESSION OBJECTIVES

This session will focus on the risk and control issues related to cyber security and emerging information security and technology, including key controls and how to audit them.

Session will use specific IT technologies as examples of control mappings including network components, operating systems and TCP/IP Services.

- Understand cyber security risk and control issues
- Understand emerging risk areas
- Understand NIST Cyber Security Framework and Mapping to Key Security & Control Frameworks
- Understand relationship of NIST Cyber Security Framework to COBIT 5 Goals Cascade
- Understand mapping of NIST Cyber Security Framework to COBIT 5 Processes
- Understand Critical Security Controls and related audit objectives and steps

AREAS OF COVERAGE:

DAY 1: CYBERSECURITY CONCEPTS; EMERGING THREATS & RISKS

Understanding Cyber Security:

- Key concepts and relationship to business organizations
- Cyber Warfare / Terrorism / Hacktivism / Crime / Espionage

Understanding Emerging Threats and Risks:

- Overview of Threat Landscape
- Advanced Persistent Threats (APT)
- Understanding Malware: e.g. Stuxnet;
- Botnets; Command and Control
- Distributed Denial of Service Attacks (DDoS)
- Key Attack Vectors including Social Engineering; Phishing; Watering Holes

DAY 2: KEY CYBERSECURITY CONTROLS

- **Cyber Security Governance**
- **Risk Management**
- **Key Cyber Security Controls**
- **Key Control Requirements:**
  - Network Segmentation / Isolation
  - Security Configuration
  - Patch Management
  - Privilege Management
  - Anti-Malware Defense and Application Whitelisting
  - Data Loss Prevention
  - Incident Management
  - Security Awareness
- **Security and Audit Tools & Techniques**
  - Questions auditors should ask in relation to IT infrastructure and corporate information protection
  - Useful reference material

DAY 3: CONDUCTING A CYBER SECURITY ASSESSMENT

Cyber Security Frameworks

- Key cyber security concepts and relationship to business organizations
- Cyber Security overview including industry threat trends and techniques using examples
- Cyber Security Governance controls and processes to manage Cyber Risk
- Cyber Risk considerations when performing technology platform, application and business audits
- NIST Cyber Security Framework & Functions, Categories, etc.
- Mapping of NIST Framework Control Categories to relevant COBIT5 processes
- Mapping of NIST Framework Control Categories and Sub-Categories to Critical Security Controls, ISO/IEC 2700-2013, etc.
- Top 4 Mitigation Strategies
- Critical Security Controls and Related Audit Objectives & Steps
- Discussion of current Cybersecurity Self-Assessment Tools

RISK-BASED IT INFRASTRUCTURE SECURITY & CONTROL ASSESSMENTS: 2 DAYS (SEMINAR)

Key information security governance controls, including a risk-based approach to design, operation and assessment of security and controls are critical to ensuring that an organization's information assets are adequately protected to prevent compromise.

SESSION OBJECTIVES:

This session will discuss a risk-based approach to assessment of security and control in the following areas:

- Configuration Management Controls
- Security Configuration Standards
- Build Processes
- Patch and Change Management Processes
- Security Event Monitoring
- Vulnerability Assessment & Management
- Security Compliance Processes

AREAS OF COVERAGE:

1. IT INFRASTRUCTURE RISK & CONTROL

- Information Security Governance
- Security Policy and Standards Framework
- Mapping IT Infrastructure to Application Systems and Business Processes
- Security Architecture & Design
- Risk Assessment Processes
- Building a Risk Profile
- Threat and Vulnerability Management
- Security Compliance Processes
- Key Security Metrics

2. SECURITY STANDARDS & BASELINES

- Key Baselines & Security Configuration Standards
- Best Practice Analysis

3. SECURITY COMPLIANCE PROCESS AND CONTROL ASSESSMENT

- Assessment Methodologies & Approaches
- Key Assessment Tools
- Results Reporting & Management

The approach to building risk profiles, key controls and assessment methodologies will be discussed and applied to the following technology environments:

1. VIRTUALIZATION SECURITY

- VMware ESXi; vSphere and Hyper-V
- Risk Profile and Key Risks
- Key Security Controls
- Key Security Compliance Assessment Tools

2. OPERATING SYSTEM SECURITY

- Windows Server 2008/2012, Unix and Linux
- Risk Profile and Key Risks
- Key Security Controls
- Key Security Compliance Assessment Tools

3. DATABASE SECURITY

- Oracle, SQL Server and DB2-LUW
- Risk Profile and Key Risks
- Key Security Controls
- Key Security Compliance Assessment Tools

4. NETWORK SECURITY

- Network Perimeter, Firewalls, Core Switches and Routers, NGFW
- Risk Profile and Key Risks
- Key Security Controls
- Key Security Compliance Assessment Tools