

Course 759: Information Security Risk Assessments (2 days Lecture Only or 4 days w/Hands-On Workshops)

Course Description...

Managing Security risks within Information Technology (IT) Systems is a continuing challenge. IT Systems are no longer isolated, they are interconnected within, between and beyond organizations. This course is designed to increase security awareness by taking a structured look at identifying risks and ranking the risks based on operational requirements. Through the use of lecture, demonstrations, and (optionally) Hands-On workshops, risks analysis and assessment will be performed. NOTE: This course utilizes NIST 800-53 and 800-39, as well as other public government, military and industry documents and practices for guidance.

Who should attend...

The lecture-only version of this course is recommended for anyone with system-administrator level privileges on organization computer systems, including: Managers, Security Officers, System Administrators, Programmers, Developers, Database Administrators (DBA), Information owners, Power-Users. The Hands-on workshops supplement the lecture material with real-world examination of security using either Windows or UNIX running enterprise applications, and are recommended for those who require hands-on experience with their choice of operating system. (students will select *either* Windows or UNIX for workshops)

Prerequisites...

- A need to understand security risk assessments
- Operating System Management Experience is recommended

Course Outline...

Chapter 1: Elements of Information Technology Risk Assessment

What is Security Management

Security Overview & Controls

Laws, Executive Orders, Directives, Polices, Standards and Regulations

Federal Information Security Management Act (FISMA)

NIST Special Publication 800-53 & 800-39

DoD Security Technical Implementation Guides (STIGS)

Health Insurance Portability and Accountability Act (HIPPA)

Payment Card Industry (PCI) Compliance

Additional Guidance Documents and Directives



Chapter 2: Building an effective Information Security Program

What is *Adequate Security*

Security Requirements and Specifications

Principles and Practices

Testing and Evaluation

Life-cycle management

Certification & Accreditation (C&A) Process

Pro-active vs Re-active measures

Chapter 3: Gathering Necessary Information

Security Control Organization and Structure

The Organization-Wide Perspective

Classifying Security Controls: Management, Operational, Technical

Identification of Information and Information Systems

Security functionality and security assurance

Chapter 4: Analyze Information and Assign Risk Rating

Classify and Rank Sensitive Data, Systems and Applications

Assess Threat and Vulnerabilities

Evaluate Control Effectiveness

Identifying Responsibility

Analyze trusts between organizations

Chapter 5: Threats and Vulnerabilities

How do I know what threats/vulnerabilities are present

Identifying individual threats and vulnerabilities

Operating System Threats

Application Threats

Networking Threats

User/Administrator Threats

Auditing Tools and Testing techniques

Non-technical Threats

Threats beyond our control

Chapter 6: Managing and Mitigating Risk

How can risk be managed and mitigated

Categorize and Documenting Risk

Implement Risk Security Controls

Assessing Mitigated Risk

Authorize System Operation

Accepting Risk

Desired/Required level of assurance

Defining/Understanding consequence management



Chapter 7: Case Study: Performing a Risk Assessment

How to perform a Technical Risk Assessment

Scenario based assessment of a newly designed system. Risk Assessment will be performed by teams of students and results will be presented to the classroom during the last 45 minutes of the course

Additional/Custom Topics are available, and hands-on labs can be customized for specific environments - please contact your ROI representative to discuss course tailoring!!!