

## ESSENTIAL ELEMENTS OF INFORMATION SECURITY



**Audience:** (Non IT Professionals)      **Duration:** 2.5 days

**Cost:** \$1,250 PER PERSON (EARLY REGISTRATION)

\$1,500 PER PERSON (LATE REGISTRATION)

### Overview

This course is designed for mid-, junior-, and senior level managers and executives, both Government and Industry, interested in learning more about the growing impacts of Information Systems security in our workplace. This course will cover general IT administrative/regulatory security policy, ethics, and FISMA compliance, guidelines and practices. Drawing upon current standard practice methodologies and experienced experts in both federal government and private industry, this course will broaden one's general knowledge of IS security, and also address critical topics that are essential in today's security conscious environment.

This course is divided into the following four parts:

- ◆ Introduction to Security and Objectives
- ◆ Security Management and Practices
- ◆ Business Continuity and Physical Security Planning
- ◆ Law Investigation and Ethics

### PART I: Introduction to Security and Objectives

Part 1 introduces IS security concepts by discussing:

- ◆ The history of and the need for security
- ◆ The Systems Development Life Cycle (SDLC)
- ◆ Differences between threats and attacks
- ◆ Security Ethics

Upon completion of Part I, an understanding of an organization's potential security vulnerabilities and security options will be realized.

### **COURSE OBJECTIVES:**

- ◆ To compare and contrast the mechanisms and procedures used by management to influence behavior, use, and content of an information system.
- ◆ To propose best practices which utilize the means and methods of disguising information through cryptography in order to protect confidentiality and integrity.
- ◆ To evaluate the impact of high level procedures, structures and standards used in defining, designing, and implementing information systems and technology.
- ◆ To analyze structures, transmission methods, transport formats and security measures that enable confidentiality, integrity and availability in business communications.
- ◆ To assess best practices used in establishing controls, within business applications, that supports the security strategy of the enterprise.

### **MODULES:**

- ◆ Overview of Objectives
- ◆ Introduction to Information Security
- ◆ The Security Function Within an Organization's Structure
- ◆ Security Considerations Within an Organization
- ◆ Introduction to Risk Management and Analysis
- ◆ Introduction to System Development Life Cycle (SDLC)
- ◆ Security Certifications

### **PART II: Security Management and Practices**

Part II introduces the Analysis phase of the System Development Life Cycle by outlining:

- ◆ Risk identification and assessment
- ◆ Risk management, control, and mitigation

Upon completion of Part II, an understanding of factors to consider and steps to take in analyzing a security system project will be realized.

### **COURSE OBJECTIVES:**

- ◆ To evaluate the role of business and technical risk analysis within the context of Information Security.
- ◆ To identify and analyze prevalent threats and vulnerabilities facing businesses today.
- ◆ To identify and analyze business and technical threats to an organization. To analyze and evaluate Information Security methods used to address business threats and vulnerabilities.
- ◆ To identify and evaluate the controls necessary to address business and technical threats.

### **MODULES:**

#### **Overview of Objectives**

- ◆ Risk Management & Discussion Points
- ◆ Risk Assessment
- ◆ Risk Identification
- ◆ Risk Control Strategies and Mitigation Selection
- ◆ Risk Categories of Control
- ◆ Risk Assessment in Real Life

### **PART III: Business Continuity and Physical Security Planning**

Part III introduces the Design phase of the System Development Life Cycle by addressing:

- ◆ IS security policies and procedures
- ◆ IS security design models
- ◆ Incident response and disaster recovery
- ◆ The Business Continuity Plan

- ◆ Physical security
- ◆ Testing and Training

Upon completion of Part III, an understanding of standard security practices in designing a security system will be realized.

### **COURSE OBJECTIVES:**

- ◆ To analyze and evaluate the interrelationship between risk management objectives and the application of effective business and IT controls.
- ◆ To identify, define and evaluate key business and IT processes, requirements and performance metrics used by management to monitor and control risk.
- ◆ To identify, analyze and evaluate organizational, administrative, network, and application-specific controls and risk mitigation strategies to meet business and technical objectives.
- ◆ To demonstrate knowledge of the management of business and IT controls assessment projects.
- ◆ To transform high-level business and technical objectives into quantifiable and measurable controls and mechanisms which enforce data and process integrity, availability and confidentiality.

### **MODULES:**

- ◆ Overview of Objectives
- ◆ Information Security Policy, Standards, and Procedures
- ◆ System design, Security Blueprint, and Security Models
- ◆ Security Education, Training, and Awareness
- ◆ Continuity Strategy and Planning
- ◆ Incident Response, Reaction, and Recovery
- ◆ Disaster Recovery and Business Continuity
- ◆ Firewalls
- ◆ Introduction to Intrusion Detection Systems
- ◆ Physical Security Parts I & II
- ◆ Wireless Insecurity
- ◆ Wireless Networking

## **PART IV: Law Investigation and Ethics**

### **COURSE OBJECTIVES:**

- ◆ To assess associated security risks of various frameworks, policies, and structures of enterprise information assets.
- ◆ To evaluate physical, procedural, and environmental risks associated with a business information technology infrastructure.
- ◆ To recommend procedures and best practices required to preserve business in the face of major disruptions to normal operations.
- ◆ To propose best practices for the protection and control of information technology resources.
- ◆ To evaluate ethical investigative measures and techniques used to identify and retain evidence of security incidents within the constraints of general computer crime legislation and regulations.

### **MODULES:**

- ◆ Overview of Objectives
- ◆ Current Issues in Information Security
- ◆ Laws & Ethics in Information Security
- ◆ Discussion on types of computer crime
- ◆ The legal system - Law
- ◆ Criminal and civil law
- ◆ Ethics
- ◆ Administrative/Regulatory law
- ◆ Protecting intellectual property
- ◆ Information privacy laws
- ◆ Handling computer evidence
- ◆ Computer crime investigation
- ◆ Liability
- ◆ Course Summary and Wrap-up

## ESSENTIAL ELEMENTS OF INFORMATION SECURITY

### Course Requirements

Each part of this course is divided into modules. To satisfy requirements, the following must be completed:

- ◆ All course lectures
- ◆ Corresponding reading assignments
- ◆ Assessment Tests

During each lecture, class exercises will be assigned. Exercises will generally be case oriented and will be assigned individually and by group dependent upon the subject matter topic. Although these exercises will not be graded, the completion of all assignments will be valuable in applying security concepts in your current or future security professional careers.