INSTRUCTOR ALTON

# Information Security Management Fundamentals for Non-Techies

Instructor: Alton Hardin

## Course Curriculum

### Section 1: Course Introduction

- Welcome to the Course!
- Why Learn Information Security Management from Me?
- What This Course Is & What It Isn't
- Course Curriculum Overview
- Course-Taking Interface Tips & Tricks
- Download Course Lecture PDFs and the Udemy Ratings System
- Student Activity: Introduce Yourself

### Section 2: Getting Started in Information Security

- The Many Areas of Information Security
- The State of Cybersecurity in 2023
- The Most Valuable Beginner IT Security Certifications for 2023

### Section 3: Information Security Principles

- Section Introduction
- The CIA Triad
- Authentication, Authorization, and Accounting (AAA)
- Defense in Depth
- Least Privilege
- Non-Repudiation
- Implicit Deny
- Legal and Regulatory Issues
- Information Security Governance
- Authentication Basics
- Identify Proofing
- General Password Rules
- **Quiz 1: Information Security Principles Quiz**

INSTRUCTOR ALTON

## Section 4: Risk Management

- Section Introduction
- Introduction to Risk Management
- Risk Management Process
- Exploring Risks and Threats
- Quantitative Risk Analysis
- Attack Surface Analysis
- Student Activity: Qualitative Risk Assessment
- **Quiz 2: Risk Management Quiz**

## Section 5: Asset Management

- Section Introduction
- Identifying & Classifying Assets
- Understanding the Asset Lifecycle
- Data Retention
- Understanding Data States
- **Quiz 3: Asset Management Quiz**

## Section 6: Access Control

- Section Introduction
- Access Control
- Physical and Logical Access Controls
- Access Control Models
- Attribute-Based Access Controls (ABAC)
- Student Activity: Analyzing Your Organization's Access Control
- **Quiz 4: Access Control Quiz**

## Section 7: IT Auditing

- Section Introduction
- Introduction to IT Audits
- Role of IT Audits
- Benefits of IT Audits
- Risk of Not Performing IT Audits
- IT Audit Process and Phases
- Audit and Control Objectives
- Gathering Evidence
- Documenting and Reporting
- IT Audit Frameworks
- Student Activity: Auditing Your Home Network
- **Quiz 4: IT Auditing Quiz**

INSTRUCTOR ALTON

## Section 8: Security Malware Threats

- Section Introduction
- Buffer Overflows
- Viruses & Polymorphic Viruses
- Worms
- Trojan Horses
- Logic Bombs
- Spyware and Adware
- Ransomware
- Rootkits
- Zero Day Attacks
- Protecting Against Malware
- Case Study: WannaCry Ransomware Attack
- Student Activity: WannaCry Case Study Analysis
- **Quiz 5: Security Malware Threats Quiz**

## Section 9: Additional Threats & Vulnerabilities

- Section Introduction
- Social Engineering
- Social Engineering Phone Impersonation Scenarios
- Social Engineering Phone Call Example #1
- Social Engineering Phone Call Example #2
- Social Engineering Phone Call Example #3
- Social Engineering Phone Impersonation Scenarios Discussion
- Email Spam, Spoofing, Phishing and Pharming
- Protocol Spoofing
- Common Attack Methods
- Student Activity:  Phishing Awareness Campaign
- **Quiz 6: Additional Threats & Vulnerabilities Quiz**

## Section 10: Network Segmentation & Isolation

- Section Introduction
- Intro to Network Segmentation & Isolation
- Demilitarized Zone (DMZ)
- Basic Network Zones
- Virtual LANs (VLANs)
- Routers
- Network Address Translation (NAT)
- Access Control Lists (ACLs)
- **Quiz 7: Network Isolation Quiz**

INSTRUCTOR ALTON

## Section 11: Network Security

- Section Introduction
- Virtual Private Networks
- Firewalls
- Web Proxy Servers
- Honeypots
- Intrusion Detection & Prevention Systems
- Student Activity: Network Security
- **Quiz 8: Network Security Quiz**

## Section 12: Wireless Networking Security

- Section Introduction
- Wireless Encryption Standards
- Wireless Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)
- Wi-Fi Protected Access 3 (WPA3)
- WPA Enterprise vs. Personal Mode
- Wireless Vulnerabilities & Security Measures
- Common Wireless Security Threats
- Case Study: TJX Companies Inc. (TJX) WEP Exploit Data Breach
- Student Activity: TJX Case Study Analysis
- **Quiz 9: Wireless Networking Security Quiz**

## Section 13: Security Assessment & Testing

- Section Introduction
- Open-Source Intelligence (OSINT)
- Vulnerability Assessments
- Penetration Testing
- Exploit Frameworks
- Interview with a Professional Ethical hacker Blog Article
- Security Assessments
- **Quiz 10: Security Assessments and Testing Section Quiz**

INSTRUCTOR ALTON

## Section 14: Security Assessment Tools

- Section Introduction
- WireShark Network Sniffing
- Nmap Zenmap Network Scanner
- Tenable Nessus Vulnerability Scanner
- Ethical Hacking for Beginners (YouTube Series)
- Case Study: Equifax Web App Vulnerability
- Student Activity: Equifax Case Study Analysis

## Section 15: Hardening Client Systems & Servers

- Section Introduction
- Hardening End-User Systems
- Hardening Servers
- Patch and Change Management
- Separation of Services
- **Quiz 11: Hardening Systems Qui**

## Section 16: Introduction to Cryptography

- Section Introduction
- Introduction to Cryptography
- Symmetric Encryption
- Asymmetric Encryption
- Hashing Algorithms
- Digital Certificates and Certificate Authorities
- Email Encryption Use Cases
- Windows Encrypted File System Use Case
- Revisiting VPN
- Software versus Hardware-Based Encryption
- Student Activity: Exploring Hashing
- **Quiz 12: Introduction to Cryptography Quiz**

## Section 17: Incident Response, Disaster Recovery and Business Continuity

- Section Introduction
- Understanding Incidents and Disasters
- Incident Response
- Disaster Recovery and Business Continuity
- Case Study: British Airways IT Failure
- Student Activity: British Airways Case Study Analysis
- **Quiz 13: Incident Response, DRP and BCP Quiz**

INSTRUCTOR ALTON

## Section 18: Application Development Security

- Section Introduction
- Importance of IT Security in Application Development
- Software Development Lifecycle (SDLC)
- Static and Dynamic Testing
- Authorization to Operate (ATO)
- **Quiz 14: Application Development Security Quiz**

## Section 19: Introduction to Zero Trust

- Section Introduction
- What is Zero Trust?
- Tenets of Zero Trust
- Why Do We Need Zero Trust?
- Digital Transformation & Zero Trust
- The NIST Zero Trust Architectural (ZTA) Model
- The State of Zero Trust
- Student Activity: Your Organization & Zero Trust
- Quiz 15: Zero Trust Quiz

## Section 20: Personnel Policies

- Section Introduction
- Acceptable Use
- Code of Ethics
- Mandatory Vacations
- Separation of Duties
- Job Rotation
- Education and Training
- Student Activity: Acceptable Use Policy
- **Quiz 15: Personnel Policies Quiz**

## Section 21: Conclusion

- Congratulations!
- How to Download Your Udemy Course Certificate of Completion
- Your Bonus Lecture