GAQM®
Global Association for Quality Management

Certified Information Security Professional (CISP)™

Course Outline

www.gaqm.org

What Modules are covered?

Module 1 - Introduction to Information Security

1) More Than Just Computer Security
2) Employee Mind-Set toward Controls
3) Roles and Responsibilities
4) Director, Design and Strategy
5) Common Threats
6) Policies and Procedures
7) Risk Management
8) Typical Information Protection Program

Module 2 - Threats to Information Security

1) What Is Information Security?
2) Common Threats
3) Errors and Omissions
4) Fraud and Theft
5) Malicious Hackers
6) Malicious Code
7) Denial-of-Service Attacks
8) Social Engineering
9) Common Types of Social Engineering

Module 3 - The Structure of an Information Security Program

1) Enterprisewide Security Program
2) Business Unit Responsibilities
3) Creation and Implementation of Policies and Standards
4) Compliance with Policies and Standards
5) Information Security Awareness Program
6) Frequency
7) Media
8) Information Security Program Infrastructure
9) Information Security Steering Committee
10) Assignment of Information Security Responsibilities
11) Senior Management
12) Information Security Management
13) Business Unit Managers
14) First Line Supervisors
15) Employees
16) Third Parties

Module 4 - Information Security Policies

1) Policy Is the Cornerstone
2) Why Implement an Information Security Policy
3) Corporate Policies
4) Organizationwide (Tier 1) Policies
5) Employment
6) Standards of Conduct
7) Conflict of Interest
8) Performance Management
9) Employee Discipline
10) Information Security
11) Corporate Communications
12) Workplace Security
13) Business Continuity Plans (BCPs)
14) Procurement and Contracts
15) Records Management
16) Asset Classification
17) Organizationwide Policy Document
18) Legal Requirements
19) Duty of Loyalty
20) Duty of Care
21) Federal Sentencing Guidelines for Criminal Convictions
22) The Economic Espionage Act of 1996
23) The Foreign Corrupt Practices Act (FCPA)
24) Sarbanes–Oxley (SOX) Act
25) Health Insurance Portability and Accountability Act (HIPAA)
26) Gramm–Leach–Bliley Act (GLBA)
27) Business Requirements
28) Policy
29) Standards
30) Procedures
31) Guidelines
32) Policy Key Elements
33) Policy Format
34) Global (Tier 1) Policy
35) Topic
36) Scope
37) Responsibilities
38) Compliance or Consequences
39) Sample Information Security Global Policies
40) Topic-Specific (Tier 2) Policy
41) Thesis Statement
42) Relevance
43) Responsibilities
44) Compliance

Module 5 - Asset Classification

1) Introduction
2) Overview
3) Why Classify Information?
4) What Is Information Classification?
5) Where to Begin?
6) Information Classification Category Examples
7) Example 1
8) Example 2
9) Example 3
10) Example 4
11) Resist the Urge to Add Categories
12) What Constitutes Confidential Information
13) Copyright
14) Employee Responsibilities
15) Owner
16) Information Owner
17) Custodian
18) User
19) Classification Examples
20) Classification: Example 1
21) Classification: Example 2
22) Classification: Example 3
23) Classification: Example 4
24) Declassification or Reclassification of Information
25) Records Management Policy
26) Sample Records Management Policy
27) Information Handling Standards Matrix
28) Printed Material
29) Electronically Stored Information
30) Electronically Transmitted Information
31) Record Management Retention Schedule
32) Information Classification Methodology
33) Authorization for Access
34) Owner
35) Custodian
36) User

Module 6 - Access Control

1) Business Requirements for Access Control
2) Access Control Policy
3) User Access Management
4) Account Authorization
5) Access Privilege Management
6) Account Authentication Management
7) System and Network Access Control
8) Network Access and Security Components
9) System Standards
10) Remote Access
11) Operating System Access Controls
12) Operating Systems Standards
13) Change Control Management
14) Monitoring System Access
15) Event Logging
16) Monitoring Standards
17) Intrusion Detection Systems
18) Cryptography
19) Definitions
20) Public Key and Private Key
21) Block Mode, Cipher Block, and Stream Ciphers
22) Cryptanalysis
23) Sample Access Control Policy

Module 7 - Physical Security

1) Data Center Requirements
2) Physical Access Controls
3) Assets to be Protected
4) Potential Threats
5) Attitude toward Risk
6) Sample Controls
7) Fire Prevention and Detection
8) Fire Prevention
9) Fire Detection
10) Fire Fighting
11) Verified Disposal of Documents
12) Collection of Documents
13) Document Destruction Options
14) Choosing Services
15) Agreements
16) Duress Alarms
17) Intrusion Detection Systems
18) Purpose
19) Planning
20) Elements
21) Procedures
22) Sample Physical Security Policy

(End of Page)