Certified Information Security Professional (CISP)

Introduction

The Certified Information Security Professional (CISP) certification program is exclusively designed for professionals who want to develop their careers in the Information Security domain. The CISP certification validates the technical knowledge and expertise to effectively design, execute, and manage the overall security posture of an organization. Not to miss the fact that the CISP certification has also become a prerequisite for many careers in the information security field. Therefore, earning the CISP certification not only boosts the candidate's career but also proves their expertise and helps them in achieving higher packages.

Course Highlights

This course teaches you about core aspects such as:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Course Outline

Module 1 - Introduction to Information Security	1.2 More Than Just Computer Security 1.2.1 Employee Mind-Set toward Controls 1.3 Roles and Responsibilities 1.3.1 Director, Design and Strategy 1.4 Common Threats 1.5 Policies and Procedures 1.6 Risk Management 1.7 Typical Information Protection Program
Module 2 - Threats to Information Security	2.1 What Is Information Security? 2.2 Common Threats 2.2.1 Errors and Omissions 2.2.2 Fraud and Theft 2.2.3 Malicious Hackers 2.2.4 Malicious Code 2.2.5 Denial-of-Service Attacks 2.2.6 Social Engineering 2.2.7 Common Types of Social Engineering
Module 3 - The Structure of an Information Security Program	3.1.1 Enterprisewide Security Program 3.2 Business Unit Responsibilities 3.2.1 Creation and Implementation of Policies and Standards 3.2.2 Compliance with Policies and Standards 3.3 Information Security Awareness Program 3.3.1 Frequency 3.3.2 Media

	3.4 Information Security Program Infrastructure 3.4.1 Information Security Steering Committee 3.4.2 Assignment of Information Security Responsibilities 3.4.2.1 Senior Management 3.4.2.2 Information Security Management 3.4.2.3 Business Unit Managers 3.4.2.4 First-Line Supervisors 3.4.2.5 Employees 3.4.2.6 Third Parties
Module 4 - Information Security Policies	4.1 Policy Is the Cornerstone 4.2 Why Implement an Information Security Policy 4.3 Corporate Policies 4.4 Organizationwide (Tier 1) Policies 4.4.1 Employment 4.4.2 Standards of Conduct 4.4.3 Conflict of Interest 4.4.4 Performance Management 4.4.5 Employee Discipline 4.4.6 Information Security 4.4.7 Corporate Communications 4.4.8 Workplace Security 4.4.9 Business Continuity Plans (BCPs) 4.4.10 Procurement and Contracts 4.4.11 Records Management 4.4.12 Asset Classification 4.5 Organizationwide Policy Document 4.6 Legal Requirements 4.6.1 Duty of Loyalty 4.6.2 Duty of Care 4.6.3 Federal Sentencing Guidelines for Criminal Convictions 4.6.4 The Economic Espionage Act of 1996 4.6.5 The Foreign Corrupt Practices Act (FCPA) 4.6.5 Sarbanes–Oxley (SOX) Act 4.6.6 Health Insurance Portability and Accountability Act (HIPAA) 4.6.7 Gramm–Leach–Bliley Act (GLBA) 4.7 Business Requirements 4.8 Policy 4.8.1 Standards 4.8.2 Procedures 4.8.3 Guidelines 4.9 Policy Key Elements 4.10 Policy Format 4.10.1 Global (Tier 1) Policy 4.10.1.1 Topic 4.10.1.2 Scope 4.10.1.3 Responsibilities 4.10.1.4 Compliance or Consequences 4.10.1.5 Sample Information Security Global Policies 4.10.2 Topic-Specific (Tier 2) Policy 4.10.2.1 Thesis Statement 4.10.2.2 Relevance 4.10.2.3 Responsibilities 4.10.2.4 Compliance 4.10.2.5 Supplementary Information 4.10.3 Application-Specific (Tier 3) Policy
Module 5 - Asset Classification	5.1 Introduction 5.2 Overview 5.3 Why Classify Information? 5.4 What Is Information Classification? 5.5 Where to Begin? 5.6 Information Classification Category Examples 5.6.1 Example 1 5.6.2 Example 2

	5.6.3 Example 3 5.6.4 Example 4 5.7 Resist the Urge to Add Categories 5.8 What Constitutes Confidential Information 5.8.1 Copyright 5.9 Employee Responsibilities 5.9.1 Owner 5.9.1.1 Information Owner 5.9.2 Custodian 5.9.3 User 5.10 Classification Examples 5.10.1 Classification: Example 1 5.10.2 Classification: Example 2 5.10.3 Classification: Example 3 5.10.4 Classification: Example 4 5.11 Declassification or Reclassification of Information 5.12 Records Management Policy 5.12.1 Sample Records Management Policy 5.13 Information Handling Standards Matrix 5.13.1 Printed Material 5.13.2 Electronically Stored Information 5.13.3 Electronically Transmitted Information 5.13.4 Record Management Retention Schedule 5.14 Information Classification Methodology 5.15 Authorization for Access 5.15.1 Owner 5.15.2 Custodian 5.15.3 User
Module 6 - Access Control	6.1 Business Requirements for Access Control 6.1.1 Access Control Policy 6.2 User Access Management 6.2.1 Account Authorization 6.2.2 Access Privilege Management 6.2.3 Account Authentication Management 6.3 System and Network Access Control 6.3.1 Network Access and Security Components 6.3.2 System Standards 6.3.3 Remote Access 6.4 Operating System Access Controls 6.4.1 Operating Systems Standards 6.4.2 Change Control Management 6.5 Monitoring System Access 6.5.1 Event Logging 6.5.2 Monitoring Standards 6.5.3 Intrusion Detection Systems 6.6 Cryptography 6.6.1 Definitions 6.6.2 Public Key and Private Key 6.6.3 Block Mode, Cipher Block, and Stream Ciphers 6.6.4 Cryptanalysis 6.7 Sample Access Control Policy
Module 7 - Physical Security	7.1 Data Center Requirements 7.2 Physical Access Controls 7.2.1 Assets to be Protected 7.2.2 Potential Threats 7.2.3 Attitude toward Risk 7.2.4 Sample Controls 7.3 Fire Prevention and Detection 7.3.1 Fire Prevention 7.3.2 Fire Detection 7.3.3 Fire Fighting 7.4 Verified Disposal of Documents 7.4.1 Collection of Documents 7.4.2 Document Destruction Options

	7.4.3 Choosing Services 7.5 Agreements 7.5.1 Duress Alarms 7.6 Intrusion Detection Systems 7.6.1 Purpose 7.6.2 Planning 7.6.3 Elements 7.6.4 Procedures 7.7 Sample Physical Security Policy

Prerequisites

The Certified Information Security Professional (CISP)™ Certification has no pre-requisites.

Target Audience

- IT consultants
- Managers
- Security policy
- Privacy officers
- Information Security Officers
- Network Administrators
- Security Device Administrators
- Security engineers

Duration

30 to 35 Hours