C)ISSM™

mile2®
Cyber Security Training & Consulting

Certified Information Systems Security Manager

COURSE OVERVIEW

4 Days 32 CPE Credits $2,500

The Certified Information Systems Security Manager certification course is was designed to teach towards and certify a information systems professional's high standard of excellence in following areas:

1. Information Security Governance
2. Information Risk Management and Compliance
3. Information Security Program Development and Management
4. Information Security Incident Management

While we provide thorough training in these 4 critical areas of information systems security management, most who take the C)ISSM have professional experience in all four of these areas. A gap of experience in some of these fields can be bridged by achieving our C)ISSM: Certified Information Systems Security Manager Certification available at mile2.com.

C)ISSM TRACK

Professional Roles:
IT Auditor
IT Consultant
Security Consultant
Chief Information Officer

Prerequisites:
C)ISSO: Certified Information Systems Security Officer
Or equivalent experience and knowledge

C)ISSM Exam:
- 2 Hours
- 100 Questions
- $400 USD
- Purchase on mile2.com

UPON COMPLETION

Students will:

- Have an in-depth knowledge of Information Security Risk, Security, Compliance & Incident Management
- Have knowledge to manage today's most difficult information systems security challenges
- Be ready to sit for the C)ISSM Exam

EXAM INFORMATION

The Certified Information Systems Security Manager exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is $400 USD and must be purchased from the store on mile2.com.

COURSE CONTENT

Module 1 - Introduction
Module 2 - Information Security Governance
Module 3 - Information Risk Management and Compliance
Module 4 - Information Security Program Development and Management
Module 5 - Information Security Incident Management

gsTM GENERAL SECURITY ptTM PENETRATION TESTING wsTM WIRELESS SECURITY scTM SECURE CODING vbpTM VIRTUALIZATION BEST PRACTICES cfTM COMPUTER FORENSICS drTM DISASTER RECOVERY iasTM INFORMATION ASSURANCE SERVICES

mile2™ SECURITY TRAINING PARTNER

DETAILED MODULE DESCRIPTION

Module 1 – Introduction

Welcome
Agenda
CISM
CISM Exam Review Course Overview
CISM Qualifications
The Learning Environment
Daily Format
Domain Structure
Course Structure
Logistics

Module 2 – Information Security Governance

Course Agenda
Examination Content
Chapter 1 Learning Objectives
The First Question
Information Security Governance Overview
Selling the Importance of Information Security
The First Priority for the CISM
Business Goals and Objectives
Outcomes of Information Security Governance
Benefits of Information Security Governance
Performance and Governance
Information Security Strategy
Developing Information Security Strategy
Elements of a Strategy
Objectives of Security Strategy
The Goal of Information Security
Defining Security Objectives
Business Linkages
Business Case Development
The Information Security Program
Security Program Priorities
Security versus Business
Security Program Objectives
What is Security?
Security Integration
Security Program
Architecture
Information Security Frameworks
Using an Information Security Framework
The Desired State of Security
The Maturity of the Security Program Using CMM
Using the Balanced Scorecard
The ISO27001:2013 Framework
Examples of Other Security Frameworks
Examples of Other Security Frameworks
Constraints and Considerations for a Security Program
Elements of Risk and Security
Risk Management
Information Security Concepts
Security Program Elements
Third Party Agreements
Roles and Responsibilities of Senior Management
Senior Management Commitment
Steering Committee
CISO Chief Information Security Officer Responsibilities
Business Manager Responsibilities
IT Staff Responsibilities
Centralized versus Decentralized Security
Evaluating the Security Program
Audit and Assurance of Security
Evaluating the Security Program
Effective Security Metrics
Key Performance Indicators (KPIs)
End to End Security
Correlation Tools
Reporting and Compliance
Regulations and Standards
Effect of Regulations
Reporting and Analysis
Ethics
Ethical Standards
Ethical Responsibility
Practice Question

Module 3 – Information Risk Management and Compliance

Exam Relevance
Information Asset Classification
Roles and Responsibilities
Roles and Responsibilities
Information Classification Considerations
Regulations and Legislation
Asset Valuation
Valuation Process
Information Protection
Information Asset Protection
Definition of Risk
Why is Risk Important
Risk Management Definition
Risk Management Objective

Risk Management Overview
Defining the Risk Environment
Threats to Information and Information Systems
Threat Analysis
Aggregate Risk
Cascading Risk
Identification of Vulnerabilities
The Effect of Risk
Impact
Risk Management Process
Risk Assessment Methodology
Annualized Loss Expectancy (ALE)
Qualitative Risk Assessment
Data Gathering Techniques
Results of Risk Assessment
Alignment of Risk Assessment and BIA
Risk Treatment
Risk Mitigation and Controls
Control Recommendations
Cost Benefit Analysis of Controls
Risk Mitigation Schematic
Control Types and Categories
Security Control Baselines
On-going Risk Assessment
Measuring Control Effectiveness
Building Risk Management In (Agenda)
Risk Related to Change Control
Controlling Risk in Change Control
Risk Management During SDLC
On-going Risk Management Monitoring and Analysis
Audit and Risk Management
Risk in Business Process Re-Engineering
Risk in Project Management
Risk During Employment Process
New Employee Initiation
Risk During Employment
Risk at Termination of Employment
Risks During Procurement
Reporting to Management
Documentation
Training and Awareness
Training and Awareness
Training for End Users
Practice Question
Practice Question 2

Module 4 – Information Security Program Development and Management

Course Agenda
Exam Relevance
Definition
Security Strategy and Program Relationship
Information Security Management
Importance of Security Management
Definition
Effective Security Management
Reasons for Security Program Failure
Program Objectives
Security Program Development
Outcomes of Information Security Program Development
Governance of the Security Program
Role of the Information Security Manager (Agenda)
Strategy
Policy
Creating Effective Policy
Awareness
Implementation
Monitoring
Compliance
Developing an Information Security Road Map
Defining Security Program Objectives
Inventory of Information Systems
Challenges in Developing an Information Security Program
Elements of a Security Program Road Map
Security Programs and Projects
Security Program and Project Development
Security Project Planning
Selection of Controls
Common Control Practices
Security Program Elements (Agenda)
Policies
Acceptable Use Policy
Standards
Procedures
Guidelines
Technology
Personnel Security
Training and Skills Matrix
Organizational Structure
Outsourced Security Providers
Third-party Service Providers
Facilities
Facilities Security
Environmental Security
Information Security Concepts (Agenda)
Access Control
Identification
Authentication
Authorization
Accounting / Auditability
Criticality

Sensitivity
Trust Models
Technology-based Security Technologies
Security in Technical Components
Operations Security
Technologies – Access Control Lists
Filtering and Content Management
Technologies - SPAM
Technologies – Databases and DBMS
Encryption
Technologies - Cryptography
Technologies – Encryption cont.
Technologies – Hashing Algorithms
Technology – Communications OSI Model
Technology – Communications TCP/IP
Technologies – Operating Systems
Technology - Firewalls
Emerging Technologies
Intrusion Detection Policies and Processes
Intrusion Detection Systems
IDS / IPS
Password Cracking
Vulnerability Assessments
Penetration Testing
Third Party Security Reviews
Integration into Life Cycle Processes
Security in External Agreements
Security Program Implementation
Phased Approach
Challenges During Implementation
Evaluating the Security Program
Measuring Information Security Risk and Loss
Measuring Effectiveness of Technical Security Program
Measuring Effectiveness of Security Management
Security Project Management
Review of Security Compliance
Practice Question

Module 5 - Information Security Incident Management

Learning Objectives
Definition
Goals of Incident Management and Response
What is an Incident - Intentional
What is an Incident - Unintentional
History of Incidents
Developing Response and Recovery Plans
Incident Management and Response
Importance of Incident Management and Response
Incident Response Functions
Incident Response Manager Responsibilities
Requirements for Incident Response Managers
Senior Management Involvement
The Desired State
Strategic Alignment of Incident Response
Detailed Plan of Action for Incident Management
Prepare
Protect
Detect
Triage
Response
Elements of an Incident Response Plan
Crisis Communications
Challenges in Developing an Incident Management Plan
Personnel
Team Member Skills
Security Concepts and Technologies
Organizing, Training and Equipping the Response Staff
Value Delivery
Performance Measurement
Reviewing the Current State of Incident Response Capability
Audits
Gap Analysis – Basis for an Incident Response Plan
When an Incident Occurs
During an Incident
Containment Strategies
The Battle Box
Evidence Identification and Preservation
Post Event Reviews
Disaster Recovery Planning (DRP) and Business Recovery Processes
Development of BCP and DRP
Plan Development
Recovery Strategies
Recovery Strategies
Basis for Recovery Strategy Selections
Disaster Recovery Sites
Recovery of Communications
Notification Requirements
Response Teams
Insurance
Testing Response and Recovery Plans
Types of Tests
Test Results
Plan Maintenance Activities
BCP and DRP Training
Practice Questions