CISM – Certified Information Security Manager (ISACA)

Days: 5

Prerequisites: In addition to professional experience, a prospective client should have an understanding of the following environments:

- Knowledge of Information Security Practices

Audience: Security Professionals

Description: Demonstrate your information security management expertise. The uniquely management-focused CISM promotes international security practices and recognizes the individual who manage designs, and oversees and assesses an enterprise's information security. The course is updated to keep pace with rapid changes in the management, design, oversight, and assessment of information security.

OUTLINE:

CHAPTER 1: INFORMATION SECURITY GOVERNANCE

SECTION 1: OVERVIEW

- Domain Definition
- Task and Knowledge Statements

SECTION 2: CONTENT

- Introduction
- Information Security Governance Overview
- Effective Information Security Governance
- Roles and Responsibilities
- Risk Management Roles and Responsibilities
- Governance of Third-party Relationships
- Information Security Governance Metrics
- Information Security Strategy Overview
- Information Security Strategy Objectives
- Determining the Current State of Security
- Information Security Strategy Development
- Strategy Resources
- Strategy Constraints
- Action Plan to Implement Strategy
- Information Security Program Objectives
- Case Study

CHAPTER 2: INFORMATION RISK MANAGEMENT

SECTION 1: OVERVIEW

- Domain Definition
- Task and Knowledge Statements

SECTION 2: CONTENT

- Introduction
- Risk Management Overview
- Risk Management Strategy
- Effective Information Risk Management
- Information Risk Management Concepts
- Implementing Risk Management
- Risk Assessment and Analysis Methodologies
- Risk Assessment
- Information Asset Classification
- Operational Risk Management
- Third-party Service Providers
- Risk Management Integration with Life Cycle Processes
- Security Control Baselines
- Risk Monitoring and Communication
- Training and Awareness
- Documentation
- Case Study

CISM – Certified Information Security Manager (ISACA)

CHAPTER 3: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT

SECTION 1: OVERVIEW

- Domain Definition
- Task and Knowledge Statements

SECTION 2: CONTENT

- Introduction
- Information Security Program Management Overview
- Information Security Program Objective
- Information Security Program Concepts
- Scope and Charter of an Information Security Program
- The Information Security Management Framework
- Information Security Framework Components
- Defining an Information Security Program Roadmap
- Information Security Infrastructure and Architecture
- Architecture Implementation
- Security Program Management and Administrative Activities
- Security Program Services and Operational Activities
- Controls and Countermeasures
- Security Program Metrics and Monitoring
- Common Information Security Program Challenges
- Case Study

CHAPTER 4: INFORMATION SECURITY INCIDENT MANAGEMENT

SECTION 1: OVERVIEW

- Domain Definition
- Task and Knowledge Statements

SECTION 2: CONTENT

- Introduction
- Incident Management Overview
- Incident Response Procedures
- Incident Management Organization
- Incident Management Resources
- Incident Management Objectives
- Incident Management Metrics and Indicators
- Defining Incident Management Procedures
- Current State of Incident Response Capability
- Developing an Incident Response Plan
- Business Continuity and Disaster Recovery Procedures
- Testing Incident Response and Business Continuity/Disaster Recovery Plans
- Executing Response and Recovery Plans
- Postincident Activities and Investigation
- Case Study

CISM – Certified Information Security Manager (ISACA)

GENERAL INFORMATION

- Requirements for Certification
- Description of the Exam
- Registration for the CISM Exam
- CISM Program Accreditation Renewed Under ISO/IEC 10724:2012
- Preparing for the CISM Exam

- Types of Exam Questions
- Administration of the Exam
- Sitting for the Exam
- Budgeting Time
- Rules and Procedures
- Grading the CISM Exam and Receiving Results