C)ISRM: Information Systems Risk Manager

Course ID #: 7000-786-ZZ-Z

Hours: 28

Course Content

Course Description:

In this course, you will first learn to assess a system, then implement risk controls. Finally, you will be able to monitor and maintain risk procedures. With this training, you will be able to identify risks associated with specific industries. After course completion, you will be able to design, implement, monitor and maintain risk-based, efficient and effective IS controls.

Course Objectives:

Upon successful completion of this course, students will be prepared to:

- Pass the C)ISRM exam

Prerequisites:

C)SP

Target Audience:

- IS Security Officers
- Privacy Officers
- Health IS Managers
- Risk Mangers
- Info Security Managers
- Government Employees

Topics:

Lesson 1: The Big Picture

- About the C)ISRM Exam
- Exam Relevance
- About the C)ISRM Exam
- Section Overview
- Overview of Risk Management
- Risk and Opportunity Management
- Responsibility vs. Accountability
- Risk Management
- Roles and Responsibilities
- Relevance of Risk Management Frameworks, Standards and Practices
- Frameworks
- Standards
- Practices
- Relevance of Risk Governance
- Overview of Risk Governance
- Objectives of Risk Governance
- Foundation of Risk Governance
- Risk Appetite and Risk Tolerance
- Risk Awareness and Communication
- Key Concepts of
- Risk Governance
- Risk Culture

C)ISRM: Information Systems Risk Manager

Course ID #: 7000-786-ZZ-Z

Hours: 28

Lesson 2: Risk Identification Assessment and Evaluation

- Task Statements
- Knowledge Statements
- The Process
- Describing the Business Impact of IT Risk
- IT Risk in the Risk Hierarchy
- IT Risk Categories
- High Level Process Phases
- Definition of Risk Scenario
- Risk Scenario Development
- Risk Registry & Risk Profile
- Risk Scenario Components
- Risk Scenario Development Enablers
- Systemic, Contagious or Obscure Risk
- Generic IT Risk Scenarios
- Definitions and Examples of Risk Factors
- Risk Factors— External Environment
- Risk Factors— Risk Management Capability
- Risk Factors— IT Capability
- Risk Factors— IT Related Business Capabilities
- Methods for Analyzing IT Risk
- Likelihood and Impact
- Risk Analysis Output
- Risk Analysis Methods
- Risk Analysis Methods—Quantitative
- Risk Analysis Methods—Qualitative
- Risk Analysis Methods—for HIGH impact risk types
- Risk Analysis Methods
- Risk Analysis Methods—Business Impact Analysis (BIA)
- Methods for Assessing IT Risk
- Identifying and Assessing IT Risk
- Adverse Impact of Risk Event
- Business Impacts From IT Risk
- Business Related IT Risk Types
- IT Project-Related Risk
- Risk Components—Inherent Risk
- Risk Components—Residual Risk
- Risk Components—Control Risk
- Risk Components—Detection Risk
- Business Risk and Threats
- Addressed By IT Resources
- Identifying and Assessing IT Risk
- Methods For Describing
- IT Risk In Business Terms

Lesson 3: Risk Response

- Task Statements
- Knowledge Statements
- Risk Response Objectives
- The Risk Response Process
- Risk Response Options
- Risk Response Parameters
- Risk Tolerance and Risk Response Options
- Risk Response Prioritization Options
- Risk Mitigation Control Types
- Risk Response Prioritization Factors
- Risk Response Tracking, Integration and Implementation
- Process Phases
- Phase 1—Articulate Risk
- Phase 2—Manage Risk
- Phase 3—React To Risk Events

Lesson 4: Risk Monitoring

- Task Statements
- Knowledge Statements
- Essentials
- Risk Indicators
- Risk Indicator Selection Criteria
- Key Risk Indicators
- Risk Monitoring
- Risk Indicator Types and Parameters
- Risk Indicator Considerations
- Criteria for KRI Selection
- Benefits of Selecting Right KRIs
- Disadvantages of Wrong KRIs
- Changing KRIs
- Gathering KRI Data
- Steps to Data Gathering
- Gathering Requirements
- Data Access
- Data Preparation

- Data Validating Considerations
- Data Analysis
- Reporting and Corrective Actions
- Optimizing KRIs
- Use of Maturity Level Assessment
- Assessing Risk Maturity Levels
- Risk Management Capability Maturity Levels
- Changing Threat Levels
- Monitoring Changes in Threat Levels
- Measuring Changes in Threat Levels
- Responding to Changes in Threat Levels
- Threat Level Review
- Changes in Asset Value
- Maintain Asset Inventory
- Risk Reporting
- Reporting Content
- Effective Reports
- Report Recommendations
- Possible Risk Report Recipients

Lesson 5: IS Control Design and Implementation

- Task Statements
- Knowledge Statements
- C)ISRM Involvement
- Control Definition
- Control Categories
- Control Types and Effects
- Control Methods
- Control Design Considerations
- Control Strength
- Control Strength
- Control Costs and Benefits
- Potential Loss Measures
- Total Cost of Ownership For Controls
- Role of the C)ISRM in SDLC
- The SDLC Process
- The Systems
- Development Life Cycle (SDLC)
- 'Meets and Continues to Meet'
- SDLC
- SDLC Phases
- Addressing Risk Within the SDLC
- Business Risk versus Project Risk
- Understanding Project Risk
- Addressing Business Risk
- Understanding Business and Risk Requirements
- Understand Business Risk
- High Level SDLC Phases
- Project Initiation
- Phase 1 – Project Initiation
  - Task 1—Feasibility Study
  - Feasibility Study Components
  - Determining Feasibility
  - Outcomes of the Feasibility Study
  - Task 2—Define Requirement
  - Requirement Progression
  - Business Information Requirements (COBIT)
  - Requirements Success Factors
  - Task 3—Acquire Software "Options"
  - Software Selection Criteria
  - Software Acquisition
  - Software Acquisition Process
  - Leading Principles for Design and Implementation
  - C)ISRM Responsibilities
  - Key System Design Activities:
- Phase 2 - Project Design and Development
  - System Testing
  - Test Plans
  - Project Testing
  - Types of Tests
  - UAT Requirements
  - Certification and Accreditation
  - Project Status Reports
- Phase 3 - Project Testing
  - Testing Techniques
  - Verification and Validation
- Phase 4 - Project Implementation
  - Project Implementation
  - Implementation Phases
  - End User Training Plans & Techniques
  - Training Strategy
  - Data Migration/Conversion Considerations
  - Risks During Data Migration
  - Data Conversion Steps
  - Implementation Rollback

- Data Conversion Project Key Considerations
- Changeover Techniques
- Post-Implementation Review
- Performing Post-Implementation Review
- Measurements of Critical Success Factors
- Closing a Project
- Project Management and Controlling
- Project Management Tools and Techniques
- Project Management Elements
- Project Management Practices
- PERT chart and critical path
- PERT Attribute

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535