C)ISRM™ CERTIFIED INFORMATION SYSTEMS RISK MANAGER

mile2® CYBER SECURITY CERTIFICATIONS

CertifiedInformation Systems Risk Manager

KEY DATA

Course Name: Certified Information Systems Risk Manager

Duration: 3days

Language: English

Format:

Instructor-led
Live Virtual Training

Prerequisites:

- A minimum of 1 year of Information Systems

Student Materials:

- Student Workbook
- Student Reference Manual
- Key Security Concepts & Definitions Book

Certification Exam:

- Mile2 C)ISRM
- Covers ISACA CRISC®

CPEs: 24

WHO SHOULD ATTEND?

- Information System Security Officers
- Risk Managers
- Information Systems Owners
- Info Security Control Assessors
- System Managers
- State & Local Government Risk Managers

COURSE OVERVIEW

The vendor neutral Certified Information Systems Risk Manager certification is designed for IT and IS professionals who are involved with risk identification, assessment& evaluation, risk response, risk monitoring, IS control design & implementation as well as IS control monitoring & maintenance.

The Certified Information Systems Risk Manager training will enable professionals to elevate their understanding in identifying and evaluating entity-specific risk but also aid them in assessing risks associated to enterprise business objectives by equipping the practitioner to design, implement, monitor and maintain risk-based, efficient and effective IS controls.

The Certified Information Systems Risk Manager covers 5 critical subjects; Risk Identification Assessment and Evaluation, Risk Response, Risk Monitoring, IS Control Design and Implementation and IS Control Monitoring & Maintenance.

IS Management Electives

C)ISSM™

ISCAP™

C)ISRM™*

All Combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide*)
  *in all technical classes
- Exam Prep Questions
- Exam

C)ISRM™ CERTIFIED INFORMATION SYSTEMS RISK MANAGER

mile2® CYBER SECURITY CERTIFICATIONS

ACCREDITATIONS

COMMITTEE ON NATIONAL SECURITY SYSTEMS — CNSS — SYSTEMS SECURITY FOR THE 21st CENTURY

NICCS™ NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

DEPARTMENT OF JUSTICE — FEDERAL BUREAU OF INVESTIGATION — FIDELITY BRAVERY INTEGRITY

mile2 is **ACCREDITED** by the **NSA CNSS 4011-4016**
Is **MAPPED** to NIST/Homeland Security NICCS's Cyber Security Workforce Framework
is **APPROVED** on the **FBI Cyber Security Certification Requirement list (Tier 1-3)**

UPON COMPLETION

Upon completion, **Certified Information Systems Risk Manager** students will be prepared to pass the CISRM exam. In addition, the candidate will be competent to implement risk management best practices and Federal standards. Students will enjoy an in-depth course that is continuously updated to maintain and incorporate the ever-changing security and risk environment.

EXAM INFORMATION

The **Certified Information Systems Risk 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 Mile2.com.

macs Assessment & Certification System

COURSE CONTENT

I. **The Big Picture**
II. **Domain 1 Risk Identification Assessment and Evaluation**
III. **Domain 2 - Risk Response**
IV. **Domain 3 - Risk Monitoring**
V. **Domain 4 - IS Control Design and Implementation**

C)ISRM™ CERTIFIED INFORMATION SYSTEMS RISK MANAGER

mile2® CYBER SECURITY CERTIFICATIONS

DETAILED MODULE DESCRIPTION

C)ISRM Part 1: The Big Picture

About the C)ISRM Exam
Exam Relevance
About the C)ISRM Exam
Section Overview
Part 1 Learning Objectives
Section Topics
Overview of Risk Management
Risk
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
Case Study
Practice Question 1
Practice Question 2
Practice Question 3
Practice Question 4
Practice Question 5
Acronym Review
Definition Review

C)ISRM Part II - Domain 1 Risk Identification Assessment and Evaluation

Section Overview
Exam Relevance
Domain 1 Learning Objectives
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
Risk Scenarios
Definition of Risk Scenario
Purpose of Risk Scenarios
Event Types
Risk Scenario Development
Risk Registry & Risk Profile
Risk Scenario Development
Risk Scenario Components
Risk Scenario Development
Risk Scenario Development Enablers
Systemic, Contagious or Obscure Risk
Generic IT Risk Scenarios
Definition of Risk Factor
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
Definitions
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
Case Study
Acronym Review
Definition Review
Domain 1 – Exercises

C)ISRM Part II Domain 2 - Risk Response

Section Overview
Exam Relevance
Domain 2 Learning Objectives
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
Sample Case Study
Domain 2 – Exercise 1

C)ISRM Part II - Domain 3 - Risk Monitoring

Course Agenda
Exam Relevance
Learning Objectives
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
Periodic Reporting
Reporting Topics
Risk Reporting Techniques
Sample Case Study
Practice Question 1
Practice Question 2
Practice Question 3
Practice Question 4
Acronym Review
Definition Review
Domain 3 – Exercises

C)ISRM Part II Domain 4 - IS Control Design and Implementation

Section Overview
Exam Relevance
Domain 4 Learning Objectives
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

Outcomes of the Feasibility Study
Task 1—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:
Steps to Perform Phase 2
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

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
Phase 1 Tasks
Task 1—Feasibility Study
Feasibility Study Components
Determining Feasibility
Implementation Phases
Phase 4 - Project Implementation
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
Sample Case Study
Practice Question 1
Practice Question 2
Practice Question 3
Practice Question 4
Practice Question 5