CISM Certification Training

About DevOpsSchool

DevOpsSchool is a unit of "Cotocus PVT ltd" and a leading platform which helps IT organizations and professionals to learn all the emerging technologies and trend which helps them to learn and embrace all the skills, intelligence, innovation and transformation which requires to achieve the end result, quickly and efficiently. We provide over 40 specialized programs on DevOps, Cloud, Containers, Security, AI, ML and on big data that are focused on industry requirement and each curriculum is developed and delivered by leading experts in each domain and aligned with the industry standards.

About Course

CISM (Certified Information Security Manager) is a key certification for information security professionals who manage, design, oversee, and assess enterprise information security. This CISM certification course, closely aligned with ISACA's best practices, helps you learn about IT security systems.

You will acquire the requisite skills to design, deploy, and manage security architecture for your organization with this CISM certification training from Simplilearn. This course is aligned with ISACA best practices. Today, enterprises and government agencies increasingly expect their IT professionals to hold a CISM certification.

Co-coordinator – Akanksha Kumari

Call/WhatsApp: - +91 1800 889 7977

Mail Address: -

contact@DevOpsSchool.com

Secondary contact – Patrick

Call/WhatsApp: - +91 7004 215 841

Mail Address: -contact@DevOpsSchool.com

Duration	45 Hours
Mode	Online (Instructor-led, live & Interactive)
Projects (Real time scenario based)	1

FEATURES	DEVOPSSCHOOL	OTHERS
Faculty Profile Check	✔	✖
Lifetime Technical Support	✔	✖
Lifetime LMS access	✔	✖
Top 25 Tools	✔	✖
Interviews Kit	✔	✖
Training Notes	✔	✖
Step by Step Web Based Tutorials	✔	✖
Training Slides	✔	✖
Training + Additional Videos	✔	✖

AGENDA OF THE CISM CERTIFICATION TRAINING

Domain 01: Information Security Governance

- Lesson 1: Information Security Governance Overview
- Information Security Governance Overview Part 1
- Information Security Governance Overview Part 2
- Information Security Governance Overview Part 3
- Information Security Governance Overview Part 4
- Information Security Governance Overview Part 5
- Importance of Information Security Governance Part 1
- Importance of Information Security Governance Part 2
- Outcomes of Information Security Governance Part 1
- Outcomes of Information Security Governance Part 2
- Outcomes of Information Security Governance Part 3
- Outcomes of Information Security Governance Part 4
- Outcomes of Information Security Governance Part 5
- Outcomes of Information Security Governance Part 6
- Lesson 2: Effective Information Security Governance
- Business Goals and Objectives Part 1
- Business Goals and Objectives Part 2
- Roles and Responsibilities of Senior Management Part 1
- Roles and Responsibilities of Senior Management Part 2
- Domain Tasks Part 1
- Domain Tasks Part 2
- Business Model for Information Security Part 1
- Business Model for Information Security Part 2
- Business Model for Information Security Part 3
- Business Model for Information Security Part 4
- Dynamic Interconnections Part 1
- Dynamic Interconnections Part 2
- Dynamic Interconnections Part 3
- Dynamic Interconnections Part 4
- Lesson 3: Information Security Concepts and Technologies
- Information Security Concepts and Technologies Part 1
- Information Security Concepts and Technologies Part 2
- Information Security Concepts and Technologies Part 3
- Technologies Part 1
- Technologies Part 2

- Lesson 4: Information Security Manager
- Responsibilities
- Senior Management Commitment Part 1
- Senior Management Commitment Part 2
- Obtaining Senior Management Commitment Part 1
- Obtaining Senior Management Commitment Part 2
- Establishing Reporting and Communication Channels Part 1
- Establishing Reporting and Communication Channels Part 2
- Lesson 5: Scope and Charter of Information Security Governance
- Assurance Process Integration and Convergence
- Convergence
- Governance and Third-Party Relationships
- Lesson 6: Information Security Governance Metrics
- Metrics
- Effective Security Metrics Part 1
- Effective Security Metrics Part 2
- Effective Security Metrics Part 3
- Effective Security Metrics Part 4
- Security Implementation Metrics
- Strategic Alignment Part 1
- Strategic Alignment Part 20
- Risk Management
- Value Delivery
- Resource Management Part 1
- Resource Management Part 2
- Performance Measurement
- Assurance Process Integration/Convergence
- Lesson 7: Information Security Strategy Overview
- Another View of Strategy
- Lesson 8: Creating Information Security Strategy
- Information Security Strategy
- Common Pitfalls Part 1
- Common Pitfalls Part 2
- Objectives of the Information Security Strategy
- What is the Goal?
- Defining Objectives
- Business Linkages
- Business Case Development Part 1
- Business Case Development Part 2

- Business Case Development Part 3
- Business Case Objectives
- The Desired State
- COBIT
- COBIT Controls
- COBIT Framework
- Capability Maturity Model
- Balanced Scorecard
- Architectural Approaches
- ISO/IEC 27001 and 27002
- Risk Objectives Part 1
- Risk Objectives Part 2
- Lesson 9: Determining Current State Of Security
- Current Risk Part 1
- Current Risk Part 2
- BIA01:11
- Lesson 10: Information Security Strategy Development
- The Roadmap
- Elements of a Strategy
- Strategy Resources and Constraints
- Lesson 11: Strategy Resources
- Policies and Standards
- Definitions05:48
- Enterprise Information Security Architectures
- Controls
- Countermeasures
- Technologies
- Personnel
- Organizational Structure
- Employee Roles and Responsibilities
- Skills
- Audits
- Compliance Enforcement
- Threat Assessment
- Vulnerability Assessment
- Risk Assessment
- Insurance
- Business Impact Assessment
- Outsourced Security Providers

- Lesson 12: Strategy Constraints
- Legal and Regulatory Requirements
- Physical Constraints
- The Security Strategy
- Lesson 13: Action Plan to Implement Strategy
- Gap Analysis Part 1
- Gap Analysis Part 2
- Gap Analysis Part 3
- Policy Development Part 1
- Policy Development Part 2
- Standards Development
- Training and Awareness0
- Action Plan Metrics
- General Metric Considerations Part 13
- General Metric Considerations Part 2
- General Metric Considerations Part 3
- General Metric Considerations Part 4
- CMM4 Statements
- Objectives for CMM4
- Section Review

Knowledge Check

- Knowledge Check 1

Domain 02: Information Risk Management and Compliance

- Lesson 1: Risk Management Overview
- Risk Management Overview
- Types of Risk Analysis
- The Importance of Risk Management
- Risk Management Outcomes
- Risk Management Strategy
- Lesson 2: Good Information Security Risk Management
- Context and Purpose
- Scope and Charter
- Assets
- Other Risk Management Goals
- Roles and Responsibilities
- Lesson 3: Information Security Risk Management Concepts
- Technologies
- Lesson 4: Implementing Risk Management
- The Risk Management Framework
- The External Environment
- The Internal Environment
- The Risk Management Context
- Gap Analysis
- Other Organizational Support
- Lesson 5: Risk Assessment
- NIST Risk Assessment Methodology
- Aggregated or Cascading Risk
- Other Risk Assessment Approaches
- Identification of Risks
- Threats
- Vulnerabilities Part 1
- Vulnerabilities Part 2
- Risks
- Analysis of Relevant Risks
- Risk Analysis
- Semi-Quantitative Analysis
- Quantitative Analysis Example04:14
- Evaluation of Risks
- Risk Treatment Options
- Impact
- Lesson 6: Controls Countermeasures
- Controls
- Residual Risk

- Information Resource Valuation
- Methods of Valuing Assets
- Information Asset Classification
- Determining Classification
- Impact Part 1
- Impact Part 2
- Lesson 7: Recovery Time Objectives
- Recovery Point Objectives
- Service Delivery Objectives
- Third-Party Service Providers
- Working with Lifecycle Processes
- IT System Development
- Project Management Part 1
- Project Management Part 2
- Lesson 8: Risk Monitoring and Communication
- Risk Monitoring and Communication
- Other Communications01:25
- Section Review

Knowledge Check

- Knowledge Check 2

Domain 03: Information Security Program Development and Management

- Introduction
- Lesson 1: Development of Information Security Program
- Importance of the Program
- Outcomes of Security Program Development
- Effective Information Security Program Development
- Lesson 2: Information Security Program Objectives
- Cross-Organizational Responsibilities
- Program Objectives Part 1
- Program Objectives Part 2
- Defining Objectives Part 1
- Defining Objectives Part 2
- Lesson 3: Information Security Program Development Concepts Part 1
- Information Security Program Development Concepts Part 2
- Technology Resources
- Information Security Manager
- Lesson 4: Scope and Charter of Information Security Program Development
- Assurance Function Integration
- Challenges in Developing Information Security Program
- Pitfalls
- Objectives of the Security Program
- Program Goals
- The Steps of the Security Program
- Defining the Roadmap Part 1
- Defining the Roadmap Part 2
- Elements of the Roadmap Part 1
- Elements of the Roadmap Part 2
- Elements of the Roadmap Part 3
- Elements of the Roadmap Part 4
- Elements of the Roadmap Part 5
- Gap Analysis00:44
- Lesson 5: Information Security Management Framework
- Security Management Framework
- COBIT 5
- ISO/IEC 27001
- Lesson 6: Information Security Framework Components
- Operational Components Part 1
- Operational Components Part 2
- Management Components
- Administrative Components
- Educational and Informational Components
- Lesson 7: Information Security Program Resources
- Resources
- Documentation

- Enterprise Architecture Part 1
- Enterprise Architecture Part 2
- Enterprise Architecture Part 3
- Controls as Strategy Implementation Resources Part 1
- Controls as Strategy Implementation Resources Part 2
- Controls as Strategy Implementation Resources Part 3
- Controls as Strategy Implementation Resources Part 4
- Common Control Practices
- Countermeasures
- Technologies Part 1
- Technologies Part 2
- Technologies Part 3
- Technologies Part 4
- Personnel Part 1
- Personnel Part 2
- Security Awareness
- Awareness Topics
- Formal Audits
- Compliance Enforcement
- Project Risk Analysis
- Other Actions
- Other Organizational Support
- Program Budgeting Part 1
- Program Budgeting Part 2
- Lesson 8: Implementing an Information Security Program
- Policy Compliance
- Standards Compliance
- Training and Education
- ISACA Control Objectives
- Third-party Service Providers Part 1
- Third-party Service Providers Part 2
- Integration into Lifecycle Processes
- Monitoring and Communication
- Documentation01:33
- The Plan of Action Part 1
- The Plan of Action Part 2
- Lesson 9: Information Infrastructure and Architecture
- Managing Complexity Part 1
- Managing Complexity Part 2
- Objectives of Information Security Architectures Part 1
- Objectives of Information Security Architectures Part 2
- Physical and Environmental Controls
- Lesson 10: Information Security Program
- Information Security Program Deployment Metrics
- Metrics
- Strategic Alignment
- Risk Management
- Value Delivery

- Resource Management
- Assurance Process Integration
- Performance Measurement
- Security Baselines
- Lesson 11: Security Program Services and Operational Activities
- IS Liaison Responsibilities Part 1
- IS Liaison Responsibilities Part 2
- Cross-Organizational Responsibilities
- Security Reviews and Audits Part 1
- Security Reviews and Audits Part 2
- Management of Security Technology
- Due Diligence Part 1
- Due Diligence Part 2
- Compliance Monitoring and Enforcement Part 1
- Compliance Monitoring and Enforcement Part 2
- Assessment of Risk and Impact Part 1
- Assessment of Risk and Impact Part
- Outsourcing and Service Providers
- Cloud Computing Part 1
- Cloud Computing Part 2
- Cloud Computing Part 3
- Integration with IT Processes00:42
- Section Review

Knowledge Check

- Knowledge Check 3

Domain 04: Information Security Incident Management

- Lesson 1: Incident Management Overview Part 1
- Incident Management Overview Part 2
- Incident Management Overview Part 3
- Types of Events Part 1
- Types of Events Part 2
- Goals of Incident Management Part 1
- Goals of Incident Management Part 2
- Goals of Incident Management Part 3
- Lesson 2: Incident Response Procedures Part 1
- Incident Response Procedures Part 2
- Importance of Incident Management
- Outcomes of Incident Management
- Incident Management
- Concepts Part 1
- Concepts Part 2
- Concepts Part 3
- Incident Management Systems Part 1
- Incident Management Systems Part 2
- Lesson 3: Incident Management Organization
- Responsibilities Part 1
- Responsibilities Part 2
- Responsibilities Part 3
- Senior Management Commitment
- Lesson 4: Incident Management Resources
- Policies and Standards
- Incident Response Technology Concepts
- Personnel
- Roles and Responsibilities (eNotes)
- Skills
- Awareness and Education
- Audits02:49
- Lesson 5: Incident Management Objectives
- Defining Objectives
- The Desired State
- Strategic Alignment
- Other Concerns
- Lesson 6: Incident Management Metrics and Indicators
- Implementation of the Security Program Management
- Management Metrics and Monitoring Part 1

- Management Metrics and Monitoring Part 2
- Other Security Monitoring Efforts
- Lesson 7: Current State of Incident Response Capability
- Threats
- Vulnerabilities
- Lesson 8: Developing an Incident Response Plan
- Elements of an Incident Response Plan
- Gap Analysis
- BIA Part 1
- BIA Part 2
- Escalation Process for Effective IM
- Help Desk Processes for Identifying Security Incidents
- Incident Management and Response Teams
- Organizing, Training, and Equipping the Response Staff
- Incident Notification Process
- Challenges in making an Incident Management Plan
- Lesson 9: BCP/DRP
- Goals of Recovery Operations Part 1
- Goals of Recovery Operations Part 2
- Choosing a Site Selection Part 1
- Choosing a Site Selection Part 2
- Implementing the Strategy
- Incident Management Response Teams
- Network Service High-availability
- Storage High-availability
- Risk Transference
- Other Response Recovery Plan Options
- Lesson 10: Testing Response and Recovery Plans
- Periodic Testing
- Analyzing Test Results Part 1
- Analyzing Test Results Part 2
- Measuring the Test Results
- Lesson 11: Executing the Plan
- Updating the Plan01:15
- Intrusion Detection Policies
- Who to Notify about an Incident
- Recovery Operations
- Other Recovery Operations
- Forensic Investigation
- Hacker / Penetration Methodology
- Section Review01:15
- Sequence 05

Thank you!

Connect with us for more info

Call/WhatsApp: - +91 968 682 9970

Mail: contact@DevOpsSchool.com

www.DevOpsSchool.com