



CISM Training Certification



Table of Contents

1. About the Program

2. Key Training Features

3. Training Options

4. Why CISM?

5. What will you learn?

Career Option
6. with Salary Compensation

7. Target Audience

8. Prerequisites

9. Course Detail









10. Course Curriculum

About the Program

Wissenhive's CISM Certification helps pupils in adequating the understanding and knowledge of the IT Security Techniques by covering end-to-end aspects of governance and security. CISM can evaluate and reconstruct the current state of information security successfully and assist with the effective solution in managing and governing the IT security professionals team.

PMP Certification Course is professionally designed for experts who are willing to acquire the requisite skills for designing, deploying, and managing security architecture for the organization. CISM certified are globally recognized professionals in IT security as it validates the experience and learning of pupils required for creating a robust data security program.

Key Training Features

-  Ask Questions Real-Time and Interact with the Trainer Live
-  Learner assistance and support - 24x7x365
-  Flexible classes
-  High-quality content created by industry experts
-  Professionally designed Student Training Material
-  High-Quality Audio-Video Lectures
-  Lifetime Training Access
-  Assessments



Training Options

- Self-paced Training
- Live Virtual Classes
- One on One Training

Why CISM?

- Higher Paying Opportunities
- Gain Knowledge and Credibility
- Stand Out Among the Ordinary
- Knowledge of CISM Best Practices
- Better Career Growth & Job Opportunities
- Better ROI with Flexibility
- Sharpen your IT Skillset



What will you learn?

- Learn ensuring the security and safety of enterprise IT
- Set strategic IT Security goals and security incident management
- Managing risk factors
- Designing Security Architecture
- Maintaining operational eminence by effectively utilizing the security frameworks, tools, and processes
- Abide by the laws and regulations of IT Security
- Information Security Governance

Career Option with Salary Compensation

Internal Auditor

- Minimum - \$45,000
- Avg Salary - \$59,000
- Maximum - \$80,000

Project Manager

- Minimum - \$57,000
- Avg Salary - \$89,000
- Maximum - \$128,000

Cybersecurity professional

- Minimum - \$66,000
- Avg Salary - \$97,000
- Maximum - \$138,000

Internal Auditing Manager

- Minimum - \$71,000
- Avg Salary - \$101,000
- Maximum - \$128,000

Information Security Officer

- Minimum - \$59,000
- Avg Salary - \$92,000
- Maximum - \$136,000

Target Audience

- Security Consultants
- Security Managers
- IT Directors
- IT Managers
- Information security managers
- IT consultants
- Security Auditors
- Security Architects
- Security system engineers
- CISOs
- Risk officers

Prerequisites

There are prerequisites for the CISM certification course; Wissenhive recommends at least having one of the following:

- A completed application must be submitted from the date of initially passing the examination within 5 years
- Experience must be verified independently with employers
- This experience must have been gained within five years of passing the examination or within the 10 years preceding the application date for CISM certification.
- 3 years of the 5 years of work experience
- Work experience must be gained in 3 of the 4 CISM domains.



Course Details

Wissenhive's CISM Certification course will allow individuals to enhance their skills and gain advanced knowledge.

- In-depth understanding, designing, and defining a security architecture for the IT operations in the organization
- Work knowledge development of the 4 prescribed domains by ISACA.
- Demonstrating a deep knowledge of the relationship between broader business objectives/goals and information security programs.
- Alignment of business goals with IT security and safety of the organization
- Focusing on the integrity of enterprise systems and IT compliance to establish a secured IT framework of the enterprise
- Become experienced in the management and development of an information security program and generating value for the organization.
- Gaining relevant skills and knowledge to clear the CISM exam by ISACA.



Course Curriculum:

1. Detailed introduction of CISM

2. Information Security Governance
 - Information Security Governance Overview
 - Importance of Information Security Governance
 - Outcomes of Information Security Governance
 - Effective Information Security Governance
 - Business Goals and Objectives
 - Roles and Responsibilities of Senior Management
 - Domain Tasks
 - Business Model for Information Security
 - Dynamic Interconnections
 - Information Security Concepts and Technologies
 - Technologies
 - Information Security Manager
 - Senior Management Commitment
 - Obtaining Senior Management
 - Establishing Reporting and Communication
 - Scope and Charter of Information Security Governance
 - Assurance Process Integration and Convergence
 - Convergence
 - Governance and Third-Party Relationships
 - Information Security Governance Metrics
 - Metrics
 - Effective Security Metrics
 - Security Implementation Metrics
 - Strategic Alignment
 - Risk Management
 - Value Delivery
 - Resource Management
 - Performance Measurement



Course Curriculum:

2. Information Security Governance

- Assurance Process Integration/Convergence
- Information Security Strategy
- Creating Information Security Strategy
- Information Security Strategy
- Common Pitfalls
- Objectives of the Information Security Strategy
- What is the Goal?
- Defining Objectives
- Business Case Development
- The Desired State
- COBIT
- Capability Maturity Model
- Balanced Scorecard
- Architectural Approaches
- Risk Objectives
- Determining Current State Of Security
- Current Risk
- Information Security Strategy Development
- The Roadmap
- Elements of a Strategy
- Strategy Resources and Constraints
- Policies and Standards
- Enterprise Information Security Architectures
- Controls
- Countermeasures
- Technologies
- Personnel
- Organizational Structure
- Employee Roles and Responsibilities
- Compliance Enforcement

Course Curriculum:

2. Information Security Governance

- Threat, Vulnerability, and Risk Assessment
- Business Impact Assessment
- Outsourced Security Providers
- Strategy Constraints
- Physical Constraints
- Legal and Regulatory Requirements
- The Security Strategy
- Action Plan to Implement Strategy
- Gap Analysis
- Policy and Standards Development
- Training and Awareness
- Action Plan Metrics
- General Metric Considerations

Course Curriculum:

3. Risk Management

- Risk Management Overview
- The Importance of Risk Management
- Risk Management Outcomes
- Types of Risk Analysis
- Risk Management Strategy
- Good Information Security Risk Management
- Context and Purpose
- Other Risk Management Goals
- Assets
- Scope and Charter
- Roles and Responsibilities
- Information Security Risk Management Concepts
- Implementing Risk Management
- The Risk Management Framework
- The External and Internal Environment
- The Risk Management Context
- Gap Analysis
- Other Organizational Support
- Risk Analysis and Assessment
- NIST Risk Assessment Methodology
- Aggregated or Cascading Risk
- Other Risk Assessment Approaches
- Identification of Risks
- Threats
- Analysis of Relevant Risks and Risk Analysis
- Controls Countermeasures
- Recovery Time Objectives
- Recovery Point and Service Delivery Objectives
- Third-Party Service Providers
- Working with Lifecycle Processes

Course Curriculum:

3. Risk Management

- IT System Development
- Risk Monitoring and Communication

4. Information Security Program Development

- Development of Information Security Program
- Outcomes of Security Program Development
- Information Security Program Objectives
- Cross Organizational Responsibilities
- Program and Defining Objectives
- Information Security Program Development Concepts
- Technology Resources
- Information Security Manager
- Scope and Charter of Information Security Program Development
- Information Security Management Framework
- Information Security Framework Components
- Information Security Program Resources
- Information Infrastructure and Architecture
- Information Security Program
- Security Program Services and Operational Activities

Course Curriculum:

5. Information Security Incident Management

- Incident Management Overview
- Types of Events
- Goals of Incident Management
- Incident Response Procedures
- Importance and Outcomes of Incident Management
- Incident Management Systems
- Incident Management Organization
- Incident Management Resources
- Incident Management Objectives
- Incident Management Metrics and Indicators
- Current State of Incident Response Capability
- Developing an Incident Response Plan
- BCP/DRP
- Testing Response and Recovery Plans
- Executing the Plan
- Information Security Incident Management
- IT Governance
- Information Risk Management
- Security Program Management and Development
- Incident Management and Response

Contact us

DREAM BIG IT SOLUTION INDIA PVT LTD

Noida

B-115, B Block, Sector 2,
Noida, Uttar Pradesh-201301

If you have any further questions or would like to chat with us, give us a call

IND +91 9368569359 **US** +1 (908)-(952)-(2400)



<https://www.facebook.com/Wissenhive>



<https://www.linkedin.com/company/wissenhive/>



<https://www.instagram.com/wissenhive/>



<https://twitter.com/HiveWissen>



<https://in.pinterest.com/wissenhive/>



<https://www.youtube.com/channel/UCEalUuf4czgsl9F0PTs0lDg>

