

# Certified Information Security Manager (CISM®) Certification

## Who Should Attend

The intended audience for this course is information security and IT professionals, such as network administrators and engineers, IT managers, and IT auditors, and other individuals who want to learn more about information security, who are interested in learning in-depth information about information security management, who are looking for career advancement in IT security, or who are interested in earning the CISM certification.

## Duration

- 5 Day(s)

## Prerequisites

To ensure your success, we recommend that students taking this course should have professional experience in information security in at least one of the following areas:

- Information security governance
- Information risk management
- Information security program development
- Information security program management
- Incident management and response

## Hardware Requirements

This course is designed so that it can be run without computer hardware or software for students. If the instructor wants to use the overheads provided on the course CD-ROM, the following hardware will be required.

- A Pentium® III with 500 MHz (or better), or Macintosh® Intel-based or PowerPC G4 (or better) processor.
- At least 512 MB of RAM.
- A monitor capable of 1024 x 768 screen resolution and 32-bit color display.
- A projection system to display the overheads to the students.

## Software Requirements

Each computer requires the following software:

- Microsoft® Windows Vista®, Windows® XP (Professional or Home Edition), Windows 2000, or Apple® Mac OS® X 10.4 (or higher).

# Certified Information Security Manager (CISM<sup>®</sup>) Certification

## Course Objectives

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

- Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.
- Identify and manage information security risks to achieve business objectives. create a program to implement the information security strategy.
- Implement an information security program.
- Oversee and direct information security activities to execute the information security program.
- Plan, develop, and manage capabilities to detect, respond to, and recover from information security incidents.

## Topics

<p><b>Lesson 1</b></p>	<p><b>Information Security Governance</b></p> <ul style="list-style-type: none"> <li>• Topic 1A: Develop an Information Security Strategy</li> <li>• Topic 1B: Align Information Security Strategy with Corporate Governance</li> <li>• Topic 1C: Identify Legal and Regulatory Requirements</li> <li>• Topic 1D: Justify Investment in Information Security</li> <li>• Topic 1E: Identify Drivers Affecting the Organization</li> <li>• Topic 1F: Obtain Senior Management Commitment to Information Security</li> <li>• Topic 1G: Define Roles and Responsibilities for Information Security</li> <li>• Topic 1H: Establish Reporting and Communication Channels</li> </ul>
<p><b>Lesson 2</b></p>	<p><b>Information Risk Management</b></p> <ul style="list-style-type: none"> <li>• Topic 2A: Implement an Information Risk Assessment Process</li> <li>• Topic 2B: Determine Information Asset Classification and Ownership</li> <li>• Topic 2C: Conduct Ongoing Threat and Vulnerability Evaluations</li> <li>• Topic 2D: Conduct Periodic BIAs</li> <li>• Topic 2E: Identify and Evaluate Risk Mitigation Strategies</li> <li>• Topic 2F: Integrate Risk Management into Business Life Cycle Processes</li> <li>• Topic 2G: Report Changes in Information Risk</li> </ul>

# Certified Information Security Manager (CISM<sup>®</sup>) Certification

<p><b>Lesson 3</b></p>	<p><b>Information Security Program Development</b></p> <ul style="list-style-type: none"> <li>• Topic 3A: Develop Plans to Implement an Information Security Strategy</li> <li>• Topic 3B: Security Technologies and Controls</li> <li>• Topic 3C: Specify Information Security Program Activities</li> <li>• Topic 3D: Coordinate Information Security Programs with Business Assurance Functions</li> <li>• Topic 3E: Identify Resources Needed for Information Security Program Implementation</li> <li>• Topic 3F: Develop Information Security Architectures</li> <li>• Topic 3G: Develop Information Security Policies</li> <li>• Topic 3H: Develop Information Security Awareness, Training, and Education Programs</li> <li>• Topic 3I : Develop Supporting Documentation for Information Security Policies</li> </ul>
<p><b>Lesson 4</b></p>	<p><b>Information Security Program Implementation</b></p> <ul style="list-style-type: none"> <li>• Topic 4A: Integrate Information Security Requirements into Organizational Processes</li> <li>• Topic 4B: Integrate Information Security Controls into Contracts</li> <li>• Topic 4C: Create Information Security Program Evaluation Metrics</li> </ul>
<p><b>Lesson 5</b></p>	<p><b>Information Security Program Management</b></p> <ul style="list-style-type: none"> <li>• Topic 5A: Manage Information Security Program Resources</li> <li>• Topic 5B: Enforce Policy and Standards Compliance</li> <li>• Topic 5C: Enforce Contractual Information Security Controls</li> <li>• Topic 5D: Enforce Information Security During Systems Development</li> <li>• Topic 5E: Maintain Information Security Within an Organization</li> <li>• Topic 5F: Provide Information Security Advice and Guidance</li> <li>• Topic 5G: Provide Information Security Awareness and Training</li> <li>• Topic 5H: Analyze the Effectiveness of Information Security Controls</li> <li>• Topic 5I : Resolve Noncompliance Issues</li> </ul>

# Certified Information Security Manager (CISM®) Certification

<b>Lesson 6</b>	<b>Incident Management and Response</b> <ul style="list-style-type: none"><li>• Topic 6A: Develop an Information Security Incident Response Plan</li><li>• Topic 6B: Establish an Escalation Process</li><li>• Topic 6C: Develop a Communication Process</li><li>• Topic 6D: Integrate an IRP</li><li>• Topic 6E: Develop IRTs</li><li>• Topic 6F: Test an IRP</li><li>• Topic 6G: Manage Responses to Information Security Incidents</li><li>• Topic 6H: Perform an Information Security Incident Investigation</li><li>• Topic 6I : Conduct Post-Incident Reviews</li></ul>
-----------------	---