4350 Executive Drive, Suite 100
San Diego, CA 92121
San Diego (858) 546-1400

Certified Information Security Manager (CISM)

Getting CISM certified shows you have arrived.
The knowledge that comes with it shows how you got there.

Length: 5 days

Summary: This blended-learning course employs outcome-based (Lecture | Lab | Review)™ delivery that focuses on preparing you with the real-world skills required to pass the certification exams (and to hit the ground running in your career). The CISM certification is for the individual who manages, designs, oversees and/or assesses an enterprise's information security (IS).

Each training day is segmented into Lecture, Lab, and Review components that cater to a student's multiple learning styles (auditory, visual, and kinesthetic-tactual).

*Note that significant changes may be made to the schedule on a daily basis to ensure that the goals of the course are met.

Course Content

Information Security Governance

- Information security concepts.
- The relationship between information security and business operations techniques used to secure senior management commitment and support of information security management.
- Methods of integrating information security governance into the overall enterprise governance framework.
- Practices associated with an overall policy directive that captures senior management.
- Level direction and expectations for information security in laying the foundation for information security management within an organization.
- An information security steering group function.
- Information security management roles, responsibilities and organizational structure.
- Areas of governance (for example, risk management, data classification management, network security, system access).
- Centralized and decentralized approaches to coordinating information security.
- Legal and regulatory issues associated with Internet businesses, global transmissions and transborder data flows (for example, privacy, tax laws and tariffs, data import/export restrictions, restrictions on cryptography, warranties, patents, copyrights, trade secrets, national security).
- Common insurance policies and imposed conditions (for example, crime or fidelity insurance, business interruptions).
- The requirements for the content and retention of business records and compliance.

4350 Executive Drive, Suite 100
San Diego, CA 92121
San Diego (858) 546-1400

- The process for linking policies to enterprise business objectives.
- The function and content of essential elements of an information security program (for example, policy statements, procedures and guidelines).
- Techniques for developing an information security process improvement model for sustainable and repeatable information security policies and procedures.
- Information security process improvement and its relationship to traditional process management.
- Information security process improvement and its relationship to security architecture development and modeling.
- Information security process improvement and its relationship to security infrastructure.
- Generally accepted international standards for information security management and related process improvement models.
- The key components of cost benefit analysis and enterprise transformation/migration plans (for example, architectural alignment, organizational positioning, change management, benchmarking, market/competitive analysis).
- Methodology for business case development and computing enterprise value proposition.

Risk Management

- Information resources used in support of business processes.
- Information resource valuation methodologies.
- Information classification.
- The principles of development of baselines and their relationship to risk-based assessments of control requirements.
- Life-cycle-based risk management principles and practices.
- Threats, vulnerabilities and exposures associated with confidentiality, integrity and availability of information resources.
- Quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events.
- Use of gap analysis to assess generally accepted standards of good practice for information security management against current state.
- Recovery time objectives (RTO) for information resources and how to determine RTO.
- RTO and how it relates to business continuity and contingency planning objectives and processes.
- Risk mitigation strategies used in defining security requirements for information resources supporting business applications.
- Cost benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable levels.
- Managing and reporting status of identified risks.

Information Security Program Management

- Methods to develop an implementation plan that meets security requirements identified in risk analyses.
- Project management methods and techniques.
- The components of an information security governance framework for integrating security principles, practices, management and awareness into all aspects and all levels of the enterprise.
- Security baselines and configuration management in the design and management of business applications and the infrastructure.
- Information security architectures: (for example, single sign-on, rules-based as

4350 Executive Drive, Suite 100
San Diego, CA 92121
San Diego (858) 546-1400

opposed to list-based system access control for systems, limited points of systems administration).
- Information security technologies (for example, cryptographic techniques and digital signatures, to enable management to select appropriate controls).
- Security procedures and guidelines for business processes and infrastructure activities. The systems development life cycle methodologies (for example, traditional SDLC, prototyping).
- Planning, conducting, reporting and follow-up of security testing.
- Certifying and accrediting the compliance of business applications and infrastructure to the enterprise's information security governance framework.
- Types, benefits and costs of physical, administrative and technical controls.
- Planning, designing, developing, testing and implementing information security requirements into an enterprise's business processes.
- Security metrics design, development and implementation.
- Acquisition management methods and techniques (for example, evaluation of vendor service level agreements, preparation of contracts).

Information Security Management

- How to interpret information security policies into operational use.
- Information security administration process and procedures.
- Methods for managing the implementation of the enterprise's information security program through third parties including trading partners and security services providers.
- Continuous monitoring of security activities in the enterprise's infrastructure and business applications.
- Methods used to manage success/failure in information security investments through data collection and periodic review of key performance indicators.
- Change and configuration management activities.
- Information security management due diligence activities and reviews of the infrastructure.
- Liaison activities with internal/external assurance providers performing information security reviews.
- Due diligence activities, reviews and related standards for managing and controlling access to information resources.
- External vulnerability reporting sources, which provide information that may require changes to the information security in applications and infrastructure.
- Events affecting security baselines that may require risk reassessments and changes to information security requirements in security plans, test plans and performance.
- Information security problem management practices.
- Information security manager facilitative roles as change agents, educators and consultants.
- The ways in which culture and cultural differences affect the behavior of staff.
- The activities that can change culture and behavior of staff.
- Methods and techniques for security awareness training and education.

Response Management

- The components of an incident response capability.
- Information security emergency management practices (for example, production change control activities, development of computer emergency response team).
- Disaster recovery planning and business recovery processes.
- Disaster recovery testing for infrastructure and critical business applications.

4350 Executive Drive, Suite 100
San Diego, CA 92121
San Diego (858) 546-1400

- Escalation processes for effective security management.
- Intrusion detection policies and processes.
- Help desk processes for identifying security incidents reported by users and distinguishing them from other issues dealt with the help desks.
- The notification process in managing security incidents and recovery: (for example, automated notice and recovery mechanisms for example in response to virus alerts in a real-time fashion).
- The requirements for collecting and presenting evidence; rules for evidence, admissibility of evidence, quality and completeness of evidence.
- Post-incident reviews and follow-up procedures.