ISACA CISM Bootcamp

Course Summary

Description

The CISM Bootcamp is an intensive, cram-style course that will cover some of the more challenging topics from the CISM job practice. Drill through sample exam items, ask your most pressing questions and get the answers to build your confidence as you prepare for exam day.

Topics

- Information Security Governance
- Risk Management
- Information Security Program Management
- Information Security Management

Audience

This course is designed for CISM Exam Candidates and information security managers with 3-5 years of experience.

Prerequisites

There are no prerequisites for this course.

Duration

Four or five days

ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

ISACA CISM Bootcamp

Course Outline

I. Information Security Governance

A. Information security concepts.
B. The relationship between information security and business operations techniques used to secure senior management commitment and support of information security management.
C. Methods of integrating information security governance into the overall enterprise governance framework.
D. Practices associated with an overall policy directive that captures senior management.
E. Level direction and expectations for information security in laying the foundation for information security management within an organization.
F. An information security steering group function.
G. Information security management roles, responsibilities and organizational structure.
H. Areas of governance (for example, risk management, data classification management, network security, system access).
I. Centralized and decentralized approaches to coordinating information security.
J. 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).
K. Common insurance policies and imposed conditions (for example, crime or fidelity insurance, business interruptions).
L. The requirements for the content and retention of business records and compliance.
M. The process for linking policies to enterprise business objectives.
N. The function and content of essential elements of an information security program (for example, policy statements, procedures and guidelines).
O. Techniques for developing an information security process improvement model for sustainable and repeatable information security policies and procedures.
P. Information security process improvement and its relationship to traditional process management.
Q. Information security process improvement and its relationship to security architecture development and modeling.
R. Information security process improvement and its relationship to security infrastructure.
S. Generally accepted international standards for information security management and related process improvement models.
T. The key components of cost benefit analysis and enterprise transformation/migration plans (for example, architectural alignment, organizational positioning, change management, benchmarking, market/competitive analysis).
U. Methodology for business case development and computing enterprise value proposition.

II. Risk Management

A. Information resources used in support of business processes.
B. Information resource valuation methodologies.
C. Information classification.
D. The principles of development of baselines and their relationship to risk-based assessments of control requirements.
E. Life-cycle-based risk management principles and practices.

ISACA CISM Bootcamp

Course Outline (cont'd)

F. Threats, vulnerabilities and exposures associated with confidentiality, integrity and availability of information resources.
G. Quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events.
H. Use of gap analysis to assess generally accepted standards of good practice for information security management against current state.
I. Recovery time objectives (RTO) for information resources and how to determine RTO.
J. RTO and how it relates to business continuity and contingency planning objectives and processes.
K. Risk mitigation strategies used in defining security requirements for information resources supporting business applications.
L. Cost benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable levels.
M. Managing and reporting status of identified risks.

III. Information Security Program Management

A. Methods to develop an implementation plan that meets security requirements identified in risk analyses.
B. Project management methods and techniques.
C. 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.
D. Security baselines and configuration management in the design and management of business applications and the infrastructure.
E. Information security architectures: (for example, single sign-on, rules-based as opposed to list-based system access control for systems, limited points of systems administration).
F. Information security technologies (for example, cryptographic techniques and digital signatures, to enable management to select appropriate controls).
G. Security procedures and guidelines for business processes and infrastructure activities. The systems development life cycle methodologies (for example, traditional SDLC, prototyping).
H. Planning, conducting, reporting and follow-up of security testing.
I. Certifying and accrediting the compliance of business applications and infrastructure to the enterprise's information security governance framework.
J. Types, benefits and costs of physical, administrative and technical controls.
K. Planning, designing, developing, testing and implementing information security requirements into an enterprise's business processes.
L. Security metrics design, development and implementation.
M. Acquisition management methods and techniques (for example, evaluation of vendor service level agreements, preparation of contracts).

IV. Information Security Management

A. How to interpret information security policies into operational use.
B. Information security administration process and procedures.
C. Methods for managing the implementation of the enterprise's information security program through third parties including trading partners and security services providers.

ISACA CISM Bootcamp

Course Outline (cont'd)

D. Continuous monitoring of security activities in the enterprise's infrastructure and business applications.
E. Methods used to manage success/failure in information security investments through data collection and periodic review of key performance indicators.
F. Change and configuration management activities.
G. Information security management due diligence activities and reviews of the infrastructure.
H. Liaison activities with internal/external assurance providers performing information security reviews.
I. Due diligence activities, reviews and related standards for managing and controlling access to information resources.
J. External vulnerability reporting sources, which provide information that may require changes to the information security in applications and infrastructure.
K. Events affecting security baselines that may require risk reassessments and changes to information security requirements in security plans, test plans and performance.
L. Information security problem management practices.
M. Information security manager facilitative roles as change agents, educators and consultants.
N. The ways in which culture and cultural differences affect the behavior of staff.
O. The activities that can change culture and behavior of staff.
P. Methods and techniques for security awareness training and education.

Q. Response Management
R. The components of an incident response capability.
S. Information security emergency management practices (for example, production change control activities, development of computer emergency response team).
T. Disaster recovery planning and business recovery processes.
U. Disaster recovery testing for infrastructure and critical business applications.
V. Escalation processes for effective security management.
W. Intrusion detection policies and processes.
X. Help desk processes for identifying security incidents reported by users and distinguishing them from other issues dealt with the help desks.
Y. 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).
Z. The requirements for collecting and presenting evidence; rules for evidence, admissibility of evidence, quality and completeness of evidence.
AA. Post-incident reviews and follow-up procedures