INFOSEC Skills
LIVE BOOT CAMPS

# Get live, expert instruction from anywhere.

# ISACA CISM Boot Camp

Infosec's Certified Information Security Manager (CISM) Boot Camp is a five-day training focused on preparing you for the ISACA CISM exam. You'll leave with the knowledge and domain expertise needed to pass the CISM exam the first time you take it.

## Course description

This CISM Boot Camp is designed for experienced information security managers and other professionals who manage, design, oversee or assess an enterprise's information security.

The training prepares you for the CISM examination by testing your knowledge and your ability to apply it to real-world scenarios. You will gain in-depth knowledge of security governance, risk management, security program development and management, and security incident management. The boot camp has been updated to align with the new CISM job practice areas and is designed to fully prepare you to pass the challenging CISM exam.

## Who should attend

- Information security managers
- Information security consultants
- Chief information officers
- Chief information security officers
- Anyone interested in learning information security management skills and getting certified

## Boot camp at a glance

### What you'll learn

- ✓ Information security governance
- ✓ Security metrics and measuring effectiveness
- ✓ Managing acquisitions, implementations, incidents and more!

### Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

### Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 5-day boot camp
- ✓ 90-day extended access to all boot camp materials

### The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

**Start training immediately**

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

**Learn by doing in the cyber range**

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

**Get unlimited custom practice exams**

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

**700+ IT and security courses**

Earn CPEs and build new skills with 100s of additional training courses.

# What's included

- Five days of live, expert CISM instruction
- Exam Pass Guarantee
- Exam voucher
- Unlimited practice exam attempts
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- 12-month subscription to the ISACA Official Question, Answer & Explanation (QAE) Database
- Pre-study learning path
- Knowledge Transfer Guarantee

### Prerequisites

To become a CISM, you must submit verified evidence of a minimum of five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice analysis areas. The work experience must be gained within the ten-year period preceding the application date for certification or within five years from the date of originally passing the exam.

## CISM objectives

The CISM certification promotes international practices and validates your knowledge and experience around effective security management and consulting. The four CISM domains include:

- Security governance: To effectively address the challenges of protecting an organization's assets, senior management must define the desired outcomes of the information security program.
- Risk management: Asset classification and valuation is an essential part of an effective risk management program — the greater the value, the greater the impact, the greater the risk.
- Information security program development and management: The purpose of this area is to implement management's governance strategy — the "due diligence" and "due care" of protecting the corporation's assets.
- Information security incident management: This area focuses on effectively managing unexpected (and expected) events, which may or may not be disruptive, and can be summed up in five words: identify, protect, detect, respond and recover.

## ISACA Accredited Training Organization (ATO)

Infosec is one of just two ISACA-accredited Elite+ Partners in the world. When you enroll in an Infosec CISM Boot Camp, you can rest assured you are receiving the most effective and up-to-date certification prep available, including official ISACA training materials and instruction that has been independently assessed to meet ISACA's quality standards.

## What you'll learn

- Information security governance
- The role of an information security steering group
- Legal and regulatory issues associated with internet businesses, global transmissions and transborder data flows
- Common insurance policies and imposed conditions
- Information security process improvement
- Recovery time objectives (RTO) for information resources
- Cost-benefit analysis techniques for mitigating risks to acceptable levels
- Security metrics design, development and implementation
- Information security management due to diligence activities and reviews of the infrastructure
- Events affecting security baselines that may require risk reassessments
- Changes to information security requirements in security plans, test plans and reperformance
- Disaster recovery testing for infrastructure and critical business applications
- External vulnerability reporting sources
- CISM information classification methods
- Life-cycle-based risk management principles and practices
- Security baselines and configuration management in the design and management of business applications and infrastructure
- Acquisition management methods and techniques
- Evaluation of vendor service level agreements and preparation of contracts

# What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

**Michelle Jemmott**
Pentagon

---

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam … but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

**John Peck**
EPA

---

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

**Sylvia Swinson**
Texeltek

## Skill up and get certified, guaranteed

### Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

### 100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

### Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

# CISM details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

| | Day 1 | Day 2 | Day 3 | Day 4 | Day 5 |
|---|---|---|---|---|---|
| Morning session | Information security governance (i) | Risk management (i) | Information security program development and management (i) | Information security program development and management (iii) | Information security incident management (i) |
| Afternoon session | Information security governance (ii) | Risk management (ii) | Information security program development and management (ii) | Information secu Information security program development and management (iv) | Information security incident management (ii) |
| Evening session | Optional group & individual study | Optional group & individual study | Optional group & individual study | Optional group & individual study | |

*Schedule may vary from class to class*

## Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills, including an in-depth CISM prep course, the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

## During your boot camp

### Day 1: Information security governance

- Information security concepts
- 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 (e.g., 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 (e.g., 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 (e.g., crime or fidelity insurance, business interruption)
- Requirements for the content and retention of business records and compliance
- Process for linking policies to enterprise business objectives
- Function and content of essential elements of

an information security program (e.g., 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, security architecture development and modeling, and 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 (e.g., architectural alignment, organizational positioning, change management, benchmarking, market/competitive analysis)
- Methodology for business case development and computing enterprise value propositions

## Day 2: 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

## Day 3: Information security program development and 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 (e.g., single sign-on, rules-based as opposed to list-based system access control for systems, limited points of systems administration)
- Information security technologies (e.g., cryptographic techniques and digital signatures, enabling management to select appropriate controls)
- Security procedures and guidelines for business processes and infrastructure activities
- Systems development life cycle methodologies (e.g., traditional SDLC, prototyping)
- Planning, conducting, reporting and follow-up of security testing
- Assessing and authorizing 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 (e.g., evaluation of vendor service level agreements, preparation of contracts)

## Day 4: Information security program development and management (continued)

- 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 reperformance
- Information security problem management practices
- Information security manager facilitative roles as change agents, educators and consultants
- Ways in which cultural and socially acceptable differences affect the behavior of staff
- Activities that can change cultural and socially acceptable behavior of staff
- Methods and techniques for security awareness training and education

## Day 5: Information security incident management

- Components of an incident response capability
- Information security emergency management practices (e.g., 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
- 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
- Notification process in managing security incidents and recovery (e.g., automated notice and recovery mechanisms in response to virus alerts in a real-time fashion)
- Requirements for collecting and presenting evidence: rules for evidence, admissibility of evidence, quality and completeness of evidence
- Post-incident reviews and follow-up procedures

## After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

## About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.



INFOSEC