Cybersecurity Certifications – Course Details

Cybersecurity certifications validate a professional's ability to **protect information systems, manage cyber risks, ensure compliance, and defend against cyber threats**. These globally recognized credentials from **ISACA®, EC-Council®, and (ISC)²®** are designed for professionals across technical, managerial, and governance roles.

📘 Courses Covered

- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Ethical Hacker (CEH)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)

🔹 Course Overview

Cybersecurity courses provide in-depth knowledge of **information security, risk management, ethical hacking, security governance, and compliance**.
These programs focus on **real-world scenarios**, helping professionals build resilient security strategies aligned with business goals.

https://www.icertglobal.com/cyber-security

1️⃣ Certified Information Systems Auditor (CISA)

Course Overview

CISA certification focuses on **auditing, controlling, and assuring information systems**. It validates expertise in **IT governance, risk management, and compliance**.

https://www.icertglobal.com/cyber-security/cisa

Key Learning Objectives

- Audit information systems effectively
- Assess IT governance and risk management
- Evaluate system controls
- Ensure compliance with standards and regulations

Target Audience

- IT auditors
- Compliance professionals
- Risk and assurance managers

Prerequisites

- 5 years of work experience in IS auditing, control, or security (experience waivers available)

Tools & Technologies Covered

- IT audit frameworks
- Risk assessment tools
- Control and compliance models
- Governance standards

Exam Format

- Online, proctored exam

Number of Questions

- 150 MCQs

Time Duration

- 4 hours

Passing Score

- 450 out of 800

Question Types

- Multiple Choice Questions (MCQs)
- Scenario-based questions

Exam Tips & Strategies

- Focus on audit and governance principles
- Understand ISACA frameworks
- Practice scenario-based questions

2️⃣ Certified in Risk and Information Systems Control (CRISC)

Course Overview

CRISC certification validates expertise in **enterprise risk management**, focusing on identifying, assessing, and mitigating IT risks.

https://www.icertglobal.com/cyber-security/crisc

Key Learning Objectives

- Identify and analyze IT risks
- Implement risk response strategies
- Monitor and report risks
- Align risk management with business objectives

Target Audience

- Risk management professionals
- IT managers
- Security analysts

Prerequisites

- Minimum 3 years of work experience in risk management

Tools & Technologies Covered

- Risk assessment frameworks
- Control monitoring tools
- Governance and compliance models

Exam Format

- Online, proctored exam

Number of Questions

- 150 MCQs

Time Duration

- 4 hours

Passing Score

- 450 out of 800

Question Types

- Scenario-based MCQs
- Risk analysis case studies

Exam Tips & Strategies

- Focus on risk scenarios
- Understand business impact analysis
- Practice decision-based questions

3️⃣ Certified Ethical Hacker (CEH)

Course Overview

CEH certification focuses on **ethical hacking and penetration testing techniques** used to identify and prevent cyber threats.

https://www.icertglobal.com/cyber-security/certified-ethical-hacker

Key Learning Objectives

- Understand hacking methodologies

- Perform vulnerability assessments
- Identify security weaknesses
- Implement countermeasures

Target Audience

- Ethical hackers
- Penetration testers
- Security analysts

Prerequisites

- Basic networking and security knowledge recommended

Tools & Technologies Covered

- Kali Linux
- Metasploit
- Nmap
- Wireshark
- Vulnerability scanning tools

Exam Format

- Online, proctored exam

Number of Questions

- 125 questions

Time Duration

- 4 hours

Passing Score

- Approximately 60%–70% (varies)

Question Types

- MCQs
- Scenario-based questions

Exam Tips & Strategies

- Practice hacking tools hands-on
- Understand attack vectors
- Revise security fundamentals

4️⃣ Certified Information Security Manager (CISM)

Course Overview

CISM certification focuses on **information security governance and management**, bridging the gap between technical security and business leadership.

https://www.icertglobal.com/cyber-security/cism

Key Learning Objectives

- Develop security governance frameworks
- Manage security risk

- Design security programs
- Handle incident management

Target Audience

- Security managers
- IT managers
- CISOs and security leaders

Prerequisites

- 5 years of information security management experience

Tools & Technologies Covered

- Security governance frameworks
- Risk management tools
- Incident response models

Exam Format

- Online, proctored exam

Number of Questions

- 150 MCQs

Time Duration

- 4 hours

Passing Score

- 450 out of 800

Question Types

- Scenario-based questions
- Management-focused MCQs

Exam Tips & Strategies

- Focus on governance over technical depth
- Understand business-aligned security decisions
- Practice situational questions

5️⃣ Certified Information Systems Security Professional (CISSP)

Course Overview

CISSP is an advanced cybersecurity certification covering **security architecture, engineering, and operations** across multiple domains.

https://www.icertglobal.com/cyber-security/cissp

Key Learning Objectives

- Understand end-to-end security concepts
- Design secure systems and architectures
- Manage identity and access
- Implement security operations

Target Audience

- Security architects
- Senior security professionals
- Cybersecurity consultants

Prerequisites

- 5 years of work experience in at least two CISSP domains

Tools & Technologies Covered

- Security architecture frameworks
- IAM tools
- Cryptography technologies
- Security operations platforms

Exam Format

- Computer Adaptive Test (CAT)

Number of Questions

- 100–150 questions

Time Duration

- 3 hours

Passing Score

- 700 out of 1000

Question Types

- Adaptive MCQs
- Scenario-based questions

Exam Tips & Strategies

- Focus on concept understanding, not memorization
- Think like a security manager
- Practice adaptive test scenarios