Training: ISC2
ISC2 CISSP Certification Prep Course

ISC2

TRANING TERMS

2026-11-16 | 5 days | Virtual Classroom
2026-11-23 | 5 days | Virtual Classroom
2026-12-07 | 5 days | Virtual Classroom
2026-12-14 | 5 days | Virtual Classroom

TRAINING GOALS:

Official ISC2 CBK Training Seminar for the CISSP (Certified Information Systems Security Professional)

Official ISC2 Online Instructor-Led Training offers the structure of a classroom along with the flexibility of remote learning. Updated course content aligns with the recently refreshed CISSP exam outline and features live virtual instruction by an ISC2 Authorized Instructor, a verified security expert who holds the CISSP.

*Each participant in an authorized training **CISSP Certification Prep Course** held in Compendium CE will receive a free CISSP Certification Exam voucher.*

This course is designed for information security professionals with deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization. Led by an ISC2 authorized instructor, this training seminar provides a comprehensive review of information systems security concepts and industry best practices, covering the following eight domains of the CISSP Common Body of Knowledge (CBK®)

- Domain 1: Security and Risk Management
- Domain 2: Asset Security
- Domain 3: Security Architecture and Engineering
- Domain 4: Communication and Network Security
- Domain 5: Identity and Access Management (IAM)
- Domain 6: Security Assessment Testing
- Domain 7: Security Operations
- Domain 8: Software Development Security

Course objectives

At the end of this course, learners will be able to:

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Apply fundamental concepts and methods related to the fields of information technology and security.
- Align overall organizational operational goals with security functions and implementations.
- Determine how to protect assets of the organization as they go through their lifecycle.
- Leverage the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.
- Apply security design principles to select appropriate mitigations for vulnerabilities present in common information system types and architectures.
- Explain the importance of cryptography and the security services it can provide in today's digital and information age.
- Evaluate physical security elements relative to information security needs.
- Evaluate the elements that comprise communication and network security relative to information security needs.
- Leverage the concepts and architecture that define the associated technology and implementation systems and protocols at Open Systems Interconnection (OSI) model layers 1–7 to meet information security needs.
- Determine appropriate access control models to meet business security requirements.
- Apply physical and logical access controls to meet information security needs.
- Differentiate between primary methods for designing and validating test and audit strategies that support information security requirements.
- Apply appropriate security controls and countermeasures to optimize an organization's operational function and capacity.
- Assess information systems risks to an organization's operational endeavors.
- Determine appropriate controls to mitigate specific threats and vulnerabilities.
- Apply information systems security concepts to mitigate the risk of software and systems vulnerabilities throughout the systems' lifecycles.

Intended audience.

This course is for individuals planning to pursue the CISSP certification. The CISSP is intended for professionals who have a minimum of 5 years' cumulative work experience in 2 or more of the 8 domains of the CISSP Common Body of Knowledge (CBK). Earning a 4-year college degree or regional equivalent or a recognized credential from the ISC2 approved list will satisfy 1 year of the required experience. Education credit will only satisfy 1 year of experience.

Prior to taking this course the learner should have the following experience, skills, or knowledge in: obtained while serving in the following roles:

- Chief Information Officer

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Chief Information Security Officer
- Chief Technology Officer
- Compliance Manager/ Officer
- Director of Security
- Information Architect
- Information Manager / Information Risk Manager or Consultant
- IT Specialist/Director/Manager
- Network/System Administrator
- Security Administrator
- Security Architect / Security Analyst
- Security Consultant
- Security Manager
- Security Systems Engineer/ Security Engineer

CONSPECT:

- The Information Security Environment
  - Justify an organizational code of ethics.
  - Relate confidentiality, integrity, availability, non-repudiation, authenticity, privacy and safety to due care and due diligence.
  - Relate information security governance to organizational business strategies, goals, missions, and objectives.
  - Apply the concepts of cybercrime to data breaches and other information security compromises.
  - Relate legal, contractual, and regulatory requirements for privacy and data protection to information security objectives.
  - Relate transborder data movement and import-export issues to data protection, privacy, and intellectual property protection.
- Information Asset Security
  - Relate the IT asset management and data security lifecycle models to information security.
  - Explain the use of information classification and categorization, as two separate but related processes.
  - Describe the different data states and their information security considerations.
  - Describe the different roles involved in the use of information, and the security considerations for these roles.
  - Describe the different types and categories of information security controls and their use.
  - Select data security standards to meet organizational compliance requirements.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Identity and Access Management (IAM)
  - Explain the identity lifecycle as it applies to human and nonhuman users.
  - Compare and contrast access control models, mechanisms, and concepts.
  - Explain the role of authentication, authorization, and accounting in achieving information security goals and objectives.
  - Explain how IAM implementations must protect physical and logical assets.
  - Describe the role of credentials and the identity store in IAM systems.
- Security Architecture and Engineering
  - Describe the major components of security engineering standards.
  - Explain major architectural models for information security.
  - Explain the security capabilities implemented in hardware and firmware.
  - Apply security principles to different information systems architectures and their environments.
  - Determine the best application of cryptographic approaches to solving organizational information security needs.
  - Manage the use of certificates and digital signatures to meet organizational information security needs.
  - Discover the implications of the failure to use cryptographic techniques to protect the supply chain.
  - Apply different cryptographic management solutions to meet the organizational information security needs.
  - Verify cryptographic solutions are working and meeting the evolving threat of the real world.
  - Describe defenses against common cryptographic attacks.
  - Develop a management checklist to determine the organization’s cryptologic state of health and readiness.
- Communication and Network Security
  - Describe the architectural characteristics, relevant technologies, protocols, and security considerations of each of the layers in the OSI model.
  - Explain the application of secure design practices in developing network infrastructure.
  - Describe the evolution of methods to secure IP communications protocols.
  - Explain the security implications of bound (cable and fiber) and unbound (wireless) network environments.
  - Describe the evolution of, and security implications for, key network devices.
  - Evaluate and contrast the security issues with voice communications in traditional and VoIP infrastructures.
  - Describe and contrast the security considerations for key remote access technologies.
  - Explain the security implications of software-defined networking (SDN) and network virtualization technologies.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Software Development Security
  - Recognize the many software elements that can put information systems security at risk.
  - Identify and illustrate major causes of security weaknesses in source code.
  - Illustrate major causes of security weaknesses in database and data warehouse systems.
  - Explain the applicability of the OWASP framework to various web architectures.
  - Select malware mitigation strategies appropriate to organizational information security needs.
  - Contrast the ways that different software development methodologies, frameworks, and guidelines contribute to systems security.
  - Explain the implementation of security controls for software development ecosystems.
  - Choose an appropriate mix of security testing, assessment, controls, and management methods for different systems and applications environments.
- Security Assessment and Testing
  - Describe the purpose, process, and objectives of formal and informal security assessment and testing.
  - Apply professional and organizational ethics to security assessment and testing.
  - Explain internal, external, and third-party assessment and testing.
  - Explain management and governance issues related to planning and conducting security assessments.
  - Explain the role of assessment in data-driven security decision-making.
- Security Operations
  - Show how to gather and assess security data efficiently and effectively.
  - Explain the security benefits of effective change management and change control.
  - Develop incident response policies and plans.
  - Link incident response to needs for security controls and their operational use.
  - Relate security controls to improving and achieving required availability of information assets and systems.
  - Understand the security and safety ramifications of various facilities, systems, and infrastructure characteristics.
- Putting It All Together
  - Explain how governance frameworks and processes relate to the operational use of information security controls.
  - Relate the process of conducting forensic investigations to information security operations.
  - Relate business continuity and disaster recovery preparedness to information security operations.
  - Explain how to use education, training, awareness, and enagagement with all members of the organization as a way to strengthen and enforce information security processes.
  - Show how to operationalize information systems and IT supply chain risk management.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

REQUIREMENTS:

Candidates for CISSP must have a minimum of five years cumulative paid work experience in two or more of the eight domains of the CISSP CBK. Earning a four-year college degree or regional equivalent or an additional credential from the ISC2 approved list will satisfy one year of the required experience. Education credit will only satisfy one year of experience.

A candidate who doesn't have the required experience to become a CISSP may become an Associate of ISC2 by successfully passing the CISSP examination. The Associate of ISC2 will then have six years to earn the five years required experience.

Your work experience must fall within two or more of the eight domains of the ISC2 CISSP CBK:

- Domain 1. Security and Risk Management
- Domain 2. Asset Security
- Domain 3. Security Architecture and Engineering
- Domain 4. Communication and Network Security
- Domain 5. Identity and Access Management (IAM)
- Domain 6. Security Assessment and Testing
- Domain 7. Security Operations
- Domain 8. Software Development Security

More information https://www.isc2.org/Certifications/CISSP/experience-requirements

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by ISC2 (course completion).

In order to complete the course, receive a certificate of completion and earn ISC2 continuing professional education (CPE) credits learners must:

- Complete all learning activities within the course.
- Complete a course evaluation.
- Score 70% or higher on the final assessment.

A Certificate of Completion will be provided in class by your instructor once you have completed a course by meeting all the requirements. Please retain the certificate of completion as proof of credits earned.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

This course will help prepare you also for the CISSP certification exam available at Pearson VUE test centers.

*Each participant in an authorized training **CISSP Certification Prep Course** held in Compendium CE will receive a free CISSP Certification Exam voucher.*

TRAINER:

ISC2 Authorized Instructor

ADDITIONAL INFORMATION:

Participating in this training you get 40 CPE (Continuing Professional Education) credits.

CPE credits for ISC2 credentials must be self-reported by members and associates through the ISC2 CPE Portal accessible via www.isc2.org using your member login credentials.

CPE credits earned for this course may be eligible for continuing professional education credits for non-ISC2 certifications. Please visit the continuing education requirements established by the credentialing organization for eligibility.

For specific questions related to your CPE credits or the CPE portal please contact member support - membersupport@isc2.org.

The Official ISC2 CBK Training Seminar for the CISSP has earned ACE CREDIT. Students who complete the course can apply for two hours of lower division credit at participating universities and colleges. For more information https://www.acenet.edu/national-guide/Pages/default.aspx

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007