



ISC2 TRAINING

Certified Information Systems Security Professional (CISSP)

Become a Certified Information Systems Security Professional (CISSP). Master the 8 domains to design, implement, and manage enterprise security architectures.

DURATION

40 hours

LEVEL

Expert

FORMAT

Instructor-Led

- Globally Recognized Certification

- Expert-Led Hands-On Training

- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

The Certified Information Systems Security Professional (CISSP) certification is globally recognized as the gold standard for information security professionals. This expert-level course provides an intensive, comprehensive deep dive into the eight domains of the ISC2 CISSP Common Body of Knowledge (CBK), equipping participants with the advanced technical skills and management methodologies required to effectively design, implement, and manage an enterprise-wide information security program. You will master critical aspects of security and risk management, asset security, security architecture and engineering, communication and network security, identity and access management (IAM), security assessment and testing, security operations, and software development security. This training goes beyond theoretical knowledge, preparing you for real-world challenges.

Completing the CISSP course at Computer Pride signifies your commitment to excellence in the cybersecurity field and provides a clear pathway to leadership roles. You will develop the strategic and tactical expertise necessary to protect organizations from sophisticated cyber threats, ensure business continuity, and maintain compliance with global regulatory frameworks. The course leverages practical scenarios and in-depth discussions to solidify understanding, making you adept at identifying vulnerabilities, mitigating risks, and responding to incidents effectively. This certification is invaluable for professionals aiming to elevate their careers and become pivotal assets in securing digital assets and infrastructure.

With CISSP, you gain a globally recognized credential that validates your expertise across a broad range of security functions. It not only enhances your professional credibility but also significantly boosts your career trajectory and earning potential in the highly competitive information security market. You will learn to articulate complex security concepts to both technical and non-technical stakeholders, develop robust security policies, and implement resilient security architectures that safeguard organizational information against evolving threats.

Duration	40 hours
Level	Expert
Vendor	ISC2
Exam Code	CISSP

PREREQUISITES

- Basic understanding of IT concepts
- Familiarity with operating systems
- Basic networking knowledge

COURSE CURRICULUM

01 Module 1: Security and Risk Management

- Security Governance Principles
- Compliance and Legal Issues (GDPR, HIPAA, local regulations)
- Risk Management Concepts and Frameworks (NIST, ISO 27005)
- Business Continuity and Disaster Recovery Planning
- Personnel Security and Security Awareness Training

02 Module 2: Asset Security and Security Architecture & Engineering

- Information Classification and Ownership

- Data Security (Encryption, Data Loss Prevention - DLP)
- Security Models and Architectures (Bell-LaPadula, Biba, SABSA)
- Cryptography Principles and Applications (Symmetric, Asymmetric, Hashing)
- Physical Security Controls and Design

03 Module 3: Communication & Network Security and Identity & Access Management

- Secure Network Components and Topologies
- Network Protocols and Security Issues (TCP/IP, DNS, VPNs, Firewalls)
- Identity Management Systems (Single Sign-On - SSO, Federation)
- Access Control Models and Techniques (RBAC, DAC, MAC)
- Authentication Methods (Multi-Factor Authentication - MFA, Biometrics)

04 Module 4: Security Assessment & Testing and Security Operations

- Security Assessment Strategies and Methodologies
- Vulnerability Management and Penetration Testing
- Security Operations Management and Incident Response
- Forensics Investigations and E-discovery
- Monitoring and Logging Security Events

05 Module 5: Software Development Security

- Secure Software Development Life Cycle (SDLC)
- Security Testing in SDLC (SAST, DAST, IAST)
- Database Security and Web Application Security
- Software Supply Chain Security
- Cloud Security (IaaS, PaaS, SaaS considerations)

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

- > **Chief Information Security Officer (CISO)**
- > **Security Architect**
- > **Information Security Manager**

FREQUENTLY ASKED QUESTIONS

Q: What specific leadership and strategic skills will I gain that are crucial for executive-level cybersecurity roles after completing the CISSP course?

The CISSP course is meticulously designed to cultivate not just technical proficiency, but also strategic leadership abilities. You will gain expertise in developing and implementing comprehensive security governance frameworks, performing enterprise-wide risk management, formulating effective security policies, and leading incident response teams. These skills are critical for roles like CISO, enabling you to align security initiatives with business objectives, communicate risk effectively to executive boards, and drive strategic decision-making in a rapidly evolving threat landscape.

Q: How does the CISSP certification address the practical experience requirements for its accreditation, and what kind of real-world application will I be equipped for?

While the CISSP course provides the essential knowledge to pass the exam, the certification itself requires a minimum of

five years of cumulative paid work experience in at least two of the eight CISSP domains. This course bridges the gap between theory and practice by equipping you with the understanding of how to apply security principles in real-world scenarios. You'll learn to design secure architectures, implement robust security controls, manage security operations, and conduct thorough security assessments, preparing you to practically fulfill the experience requirements and excel in hands-on security roles within complex enterprise environments.

Q: Given the dynamic cybersecurity landscape in Kenya, how does the CISSP curriculum remain relevant and equip professionals to tackle emerging local and regional cyber threats?

The CISSP curriculum is globally recognized and vendor-neutral, focusing on foundational and strategic principles of information security rather than specific tools or regional regulations. This broad and deep understanding equips professionals to adapt to new technologies and emerging threats, whether they are global or specific to the Kenyan and East African context. You will learn to implement international best practices for risk management, incident response, and data protection, enabling you to build resilient cybersecurity postures that can effectively counter the evolving threat landscape faced by organizations in the region, ensuring compliance and data integrity.

ABOUT COMPUTER PRIDE



East Africa's Premier IT Training Center

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+

Years of Excellence

10,000+

Professionals Trained

50+

Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location

1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email

info@computer-pride.co.ke

Phone

+254 705 900 900

www.computer-pride.co.ke