# Certified Information Systems Security Professional Training

CISSP®

Certified Information
Systems Security Professional

(ISC)²®

KiTS
Technologies
...your kitted ICT partner

# Certified Information Systems Security Professional Training

## The Next Generation of Security Leaders

Certified Information Systems Security Professional (CISSP®) is the most globally recognized certification in the information security market. Required by some of the world's most security conscious organizations, the CISSP is considered the gold standard credential that assures information security leaders possess the breadth of knowledge, skills and experience required to credibly build and manage the security posture of an organization.

Backed by (ISC)2®, the global leader in information security certifications, CISSPs have earned their place as trusted advisors. Their expertise plays a critical role in helping organizations integrate stronger security protocols and protect against threats in an increasingly complex cyber security landscape.

CISSP was the first credential in the field of information to meet the stringent requirements of ISO/IEC Standard 17024. Not only is the CISSP an objective measure of excellence, but also a globally recognized standard of achievement.

## Training Objective:

Upon completion, participants will have the in-dept knowledge of the entire CISSP curriculum and become confident in dealing with real life data security issues as it applies to various business environment and requirements. Additionally, participants will able to pass the rigorous CISSP examination at first attempt.

## Our guarantee:

Pass the CISSP exam the first time. This is our guarantee. We are confident that attendees will be adequately prepared to pass CISSP course the first time. But if (for some reasons) any attendee has any issue, he/she will be re-trained FREE within 12 months.

## The CISSP Helps You:

- Demonstrate your ability to effectively define the architecture, design, management and controls that assure the security of business environments.
- Validate your experience, skills and commitment as an information security professional.
- Advance your career with the most globally recognized information security certification in the industry.
- Affirm your commitment to continued competence in the most current information security practices through (ISC)2's Continuing Professional Education (CPE) requirement.
- Fulfill government and organization requirements for information security certification mandates.

## CISSP Insights

> “*The CISSP certification I got after attending the official (ISC)2 [review] seminar greatly added to my competitive edge and, as a result, I won my current position.*
> *I am now making the (ISC)2 certification a requirement for the members of my team, confident in the knowledge that their skills are genuine and current.*”
>
> Daniel, *CISSP*
> *The Netherlands*

> “*Obtaining the CISSP certification opened up doors I thought inviolable. My career - both professional and academic - grew dramatically!*”
>
> Claudi, *CISSP, CIA, CISA, CISM*
> *Italy*

## The CISSP Helps Employers:

- Increase credibility of the organization when working with vendors and contractors.
- Position candidates on a level playing field as the CISSP is internationally recognized.
- Ensure their employees use a universal language, circumventing ambiguity with industry-accepted terms and practices.
- Increase confidence that job candidates and employees possess the knowledge and experience to do the job right.
- Increase confidence that information security personnel are current and capable through CISSP's CPE credits requirement.
- Confirm their employee's commitment and years of experience gained in the industry.

## Who Should Become a CISSP

If you fall into any of the following categories, then CISSP is for you:

- Security Consultant & Security Analyst
- Security Manager & Security Systems Engineer
- IT Consultants/Director/Manager & Information Security Professionals.
- Security Auditor & Director of Security
- Network & Security device administrators / Security Architect
- Mid-career IT professionals seeking to specialize in information security.
- Engineers and other security professionals whose positions require CISSP certification.
- Young graduate with a background in information technology.
- Anyone interested in understanding the principles, best practices, and core concepts of information systems security.

### *CISSP in the News*

*"Today's Most In-Demand Certifications"*

- Certification Magazine

*"The top five in-demand IT certifications for 2013"*

- TechRepublic

*"The Most In-Demand Certifications in IT for 2013"*

- IT Strategy News

## The CISSP CBK

The CISSP® domains are drawn from various information security topics within the (ISC)$^{2}$® CBK®. Update annually, the domains reflect the most up-to –date best practices worldwide, while establishing a common framework of teams and principles to discuss, debate and resolve matters pertaining to the profession.

### The CISSP CBK consists of the following 8 domains:

- *Security and Risk Management (Security, Risk, Compliance, Law, Regulations, and Business Continuity)*
  - Confidentiality, integrity, and availability concepts
  - Security governance principles
  - Compliance
  - Legal and regulatory issues
  - Professional ethic
  - Security policies, standards, procedures and guidelines

- *Asset Security (Protecting Security of Assets)*
  - Information and asset classification
  - Ownership (e.g. data owners, system owners)
  - Protect privacy
  - Appropriate retention
  - Data security controls
  - Handling requirements (e.g. markings, labels, storage)

- *Security Engineering (Engineering and Management of Security)*
  - Engineering processes using secure design principles
  - Security models fundamental concepts
  - Security evaluation models
  - Security capabilities of information systems
  - Security architectures, designs, and solution elements vulnerabilities
  - Web-based systems vulnerabilities
  - Mobile systems vulnerabilities
  - Embedded devices and cyber-physical systems vulnerabilities
  - Cryptography
  - Site and facility design secure principles
  - Physical security

- *Communication and Network Security (Designing and Protecting Network Security)*
  - Secure network architecture design (e.g. IP & non-IP protocols, segmentation)
  - Secure network components
  - Secure communication channels
  - Network attacks

- *Identity and Access Management (Controlling Access and Managing Identity)*
  - Physical and logical assets control
  - Identification and authentication of people and devices
  - Identity as a service (e.g. cloud identity)
  - Third-party identity services (e.g. on-premise)
  - Access control attacks
  - Identity and access provisioning lifecycle (e.g. provisioning review)

- *Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)*
  - Assessment and test strategies
  - Security process data (e.g. management and operational controls)
  - Security control testing
  - Test outputs (e.g. automated, manual)
  - Security architectures vulnerabilities

- *Security Operations (Foundational Concepts, Investigations, Incident Management, and Disaster Recovery)*
  - Investigations support and requirements
  - Logging and monitoring activities
  - Provisioning of resources
  - Foundational security operations concepts
  - Resource protection techniques
  - Incident management
  - Preventative measures
  - Patch and vulnerability management
  - Change management processes
  - Recovery strategies
  - Disaster recovery processes and plans
  - Business continuity planning and exercises
  - Physical security
  - Personnel safety concerns

- *Software Development Security (Understanding, Applying, and Enforcing Software Security)*
  - Security in the software development lifecycle
  - Development environment security controls
  - Software security effectiveness
  - Acquired software security impact

## *Mode of Training:*

The Intensive 5-Days Program (Boot Camp) is aimed at providing professionals with a fully immersed training and certification experience.