NETWORK INTELLIGENCE
Global cybersecurity provider

Certified Information Systems Security Professional (CISSP)

A 4-day training workshop for Americas

- Dates: **July 19 -22, 2021**
- **Timings – 9:00 AM – 4:00 PM ET**
- Duration : 7 hours for 4 days (28 hours)
- Mode: Online via Microsoft teams
- Course Fees: USD **$ 350**

What's Included?

4 days of instructor-led Online training

Courseware pack with slides and exercises

Refund Policy

100% of the training fees will be refunded to any participant who has appeared for the CISSP examination within 6 months of the training and failed to clear the certification

INTRODUCTION

Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the International Information Systems Security Certification Consortium, commonly known as (ISC)².

CISSP is considered a global standard that proves an individual's proficiency in several security disciplines and is acknowledged worldwide as a professional achievement.

OBJECTIVE OF THE CISSP TRAINING PROGRAM

If you're planning to appear for the CISSP exam and need to undergo a training that will help you cover the gaps in your knowledge or if you're looking to build a career in information security and wish to get all your key concepts in place or if you're someone wanting to get a broad-based view of the key aspects of information security, this is the course for you.

WHO SHOULD ATTEND THE CISSP TRAINING PROGRAM

- Security Consultant
- Security Analyst
- Security Manager
- Security Systems Engineer
- IT Director/Manager
- Chief Information Security Officer
- Security Auditor
- Director of Security
- Security Architect
- Network Architect

NETWORK INTELLIGENCE
Global cybersecurity provider

WHY CISSP ?

Created by (ISC)², the CISSP certification is the gold standard for security certifications and an internationally acknowledged benchmark for info security professionals. It is one of the world's most valued information technology and information security certification.

CISSP has a widespread recognition in a variety of information security management roles and this type of industrywide acceptance is valuable for everyone who holds this designation. The CISSP helps to demonstrates that you are at the top of your cybersecurity game in terms of both knowledge and experience.

Here are a few reasons why CISSP certification could be the right certification for you.

- It will help you to gain credibility as a security expert.
- You will become a member of the largest association of cybersecurity professionals in the world today
- It will help you to maximize your career & earning potential.
- The certification validates a professional's hands-on cybersecurity experience.

Those looking to appear for the CISSP exam should possess at least five years of paid, full-time employment in cybersecurity or related positions. The participants must also have detailed experience in two of the eight domains that are covered by the CISSP exam.

By passing the exam or earning the title of CISSP, you demonstrate you have the following:

- Technical security expertise along with managerial capabilities
- Expertise in eight crucial security areas ranging from access control to software development.
- Proven comfort with the technology and controls that improve a company's security posture.
- Readiness to participate in the creation of policies that set the framework for enterprise level cybersecurity.

In line with these objectives, we are pleased to announce a 4-day 7-hour online training on "Certified Information Systems Security Professional (CISSP)".

Certified Information Systems Security Professional (CISSP) Training

Course Content :

Domain 1 : Security and Risk Management

This is the largest domain in CISSP, providing a comprehensive overview of the things you need to know about information systems management. It covers:

- Understanding and applying concepts of confidentiality, integrity and availability
- Evaluating and applying security governance principles
- Determining compliance requirements
- Understanding legal and regulatory issues that pertain to information security in a global context
- Identifying, analysing, and prioritizing Business Continuity (BC) requirements
- Understanding and applying risk management concepts
- Applying risk-based management concepts to your environment
- Establishing and maintaining a security awareness, education, and training program

Domain 2 : Asset Security

This domain addresses the physical requirements of information security. It covers:

- Identifying and classifying ownership of information and assets
- Determining and maintaining information and asset ownership
- Protecting privacy
- Ensuring appropriate asset retention
- Determining data security controls
- Establishing information and asset handling requirements

NETWORK INTELLIGENCE
Global cybersecurity provider

Domain 3 : Security Architecture and Engineering

This domain covers several important information security concepts, including:

- Implementing and managing processes using secure design principles
- Understanding the fundamental concepts of security models
- Understanding security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assessing and mitigating the vulnerabilities of security architectures, designs, and solution elements
- Applying security principles to site and facility design
- Designing and implementing physical security

Domain 4 : Communication and Network Security

This domain covers the design and protection of an organization's networks. This includes:

- Implementing secure design principles in network architectures
- Securing network components
- Implementing secure communication channels according to design

Certified Information Systems Security Professional (CISSP) Training

Course Content :

Domain 5 : Identity and Access Management (IAM)

This domain helps information security professionals understand how to control the way users can access data. It covers:

- Controlling physical and logical access to assets
- Managing identification and authentication of people, devices, and services
- Integrating identity as a service and third-party identity services
- Implementing and managing authorization mechanisms
- Managing the identity and access provisioning lifecycle

Domain 6 : Security Assessment and Testing

It covers:

- Creating and updating security policy
- Conducting document review
- Implementing risk identification
- Conducting vulnerability scan
- Understanding data analysis
- Managing reports & briefing

Please note that this is not an $(ISC)^2$ endorsed course, although it is conducted by our Principal Consultant and international security expert, K. K. Mookhey, who is a CISA, CISSP and CISM certified professional. The participants will receive 28 CPE points for this training.

NETWORK INTELLIGENCE
Global cybersecurity provider

Domain 7 : Security Operations

Basic objective is to focus on how to make data available to the user without any problems. It covers:

- Understanding and supporting investigations (forensics)
- Understanding requirements for investigation types
- Understanding administrative security
- Conducting incident response management
- Operating and maintaining detective and preventative measures
- Implementing and supporting patch and vulnerability management
- Understanding and participating in change management processes
- Implementing Disaster Recovery (DR) processes
- Testing Disaster Recovery Plans (DRP)
- Participating in Business Continuity (BC) planning and exercise

Domain 8 : Software Development Security

This domain dives deep into the world of software development. Covers some key programming concepts like:

- Understanding the concepts of compilers, interpreters, Assemblers.
- Understanding the Concepts of object-oriented programming
- Understand and integrate security Development methodologies
- Understanding the database concepts
- Assess the effectiveness of software security

“ Prevent a security breach by keeping data out of reach “

NETWORK INTELLIGENCE
Global cybersecurity provider

Lead Trainer

KK Mookhey,
Founder & CEO
Network Intelligence

KK provides the vision and direction for the company and has steered it from a one-man consulting firm started in 2001 to a global cybersecurity firm with an expansive portfolio of services. A technologist at heart, he enjoys dealing with complex security problems and developing solutions to client challenges. He is a qualified PCI QSA, CISA and CISSP.

Rajeev Andharia,
IITL Experts, PMP, CISA, CISSP, COBIT
Director - Digital Risk & Benefit Optimization

Rajeev specializes in good practices like COBIT, Agile / Scrum, ITIL, DevOps, PMBOK and relevant ISO standards for IT governance, enterprise architecture, service management, information security, business continuity and information risk management. He has Co-Authored ITSM library book “Six Sigma for IT Management” published by itSMF, Netherland. He regularly delivers thought leadership talks at ISACA and PMI conferences / chapters.

Registration link: https://forms.office.com/r/nVPRAN6XdS