NETWORK INTELLIGENCE

introducing

Certified Information Systems Security Professional (CISSP)

A 36 Hours Online Information System Security Training

Dates: 18th Dec – 21st Dec 2023

Time: 6:00 AM To 1:00 PM (EST)

Mode: Online

Course Fees:

Regular Participant : USD $ 550

Early bird discount : USD 450 (Register before 30th November)

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.

Who should attend?

- 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

Why CISSP?

- 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.

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)".

CISSP Certified Information Systems Security Professional

NETWORK INTELLIGENCE

DOMAIN- 1

- Understand and apply concepts of confidentiality, integrity and availability
- Evaluate and apply security governance principles
- Determine compliance requirements
- Understand legal and regulatory issues that pertain to information security in a global context
- Identify, analyse, and prioritize Business Continuity (BC) requirements
- Understand and apply risk management concepts
- Apply risk-based management concepts to your environment
- Establish and maintain a security awareness, education, and training program

DOMAIN- 2

- Identify and classify ownership of information and assets
- Determine and maintain information and asset ownership
- Protect privacy
- Ensure appropriate asset retention
- Determine data security controls
- Establish information and asset handling requirements

DOMAIN- 3

- Implement and manage processes using secure design principles
- Understand the fundamental concepts of security models
- Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Apply security principles to site and facility design
- Designing and implementing physical security

DOMAIN- 4

- Implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design

DOMAIN- 5

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Integrating identity as a service and third-party identity services
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle

DOMAIN- 6

- Security policy creation and update
- Conduct document review.
- Implement risk identification.
- Conduct vulnerability scan.
- Understand data analysis.
- Manage Report & briefing.

DOMAIN- 7

- Understand and support investigations (forensics)
- Understand requirements for investigation types
- Understand administrative security
- Conduct incident response management
- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercise

DOMAIN- 8

- Understand and support investigations (forensics)
- Understand requirements for investigation types
- Understand administrative security
- Conduct incident response management
- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercise

Trainer Details

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/c7EE3PumKy

NETWORK INTELLIGENCE