Solutions Security Strategies

RC:1270765

SEC-CONCEPTS NETWORKS®

It's Possible

Consultancy | Solutions | Security | Strategies

(ISC)²

CERTIFICATIONS

- CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)
- SYSTEMS SECURITY CERTIFIED PRACTITIONER (SSCP)
-

PROGRAMME GUIDE

(ISC)² CERTIFICATIONS PROGRAMME GUIDE

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP) CERTIFICATION

Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the not-for-profit International Information Systems Security Certification Consortium, (ISC)2. The CISSP was the first credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. It is approved by the U.S. Department of Defense (DoD) in both their Information Assurance Technical (IAT) and Managerial (IAM) categories.

CISSP certification is not only an objective measure of excellence, but a globally recognized standard of achievement. Koenig provides comprehensive CISSP training for participants who wish to gain expertise in defining the design, architecture, management and controls leading to a secure business environment.

Course Objectives

•Understand the bascis of telecommunication and network security concepts, required components for minimizing security risks, securing channels of communication, and techniques for preventing and detecting network-based attacks.

•Identify the key terms and processes of security operations and how to protect and control information processing assets in a centralized or distributed environment.

•Define and apply information security governance and Risk Management Framework including the policies, concepts, principles, structures and standards that are established for the protection of information assets and how to assess the effectiveness of that protection

•Gain the required skills to design the architecture and manage IT security in an enterprise environment through this authorized CISSP course

Course Contents

•Security and Risk Management
•Asset Security
•Security Engineering
•Communication and Network Security
•Identity and Access Management
•Security Assessment and Testing
•Security Operations
•Software Development Security

Call/WhatsApp: 08039134906
training@sec-conceptsnetworks.com
www.sec-conceptsnetworks.com

SYSTEMS SECURITY CERTIFIED PRACTITIONER (SSCP) CERTIFICATION

Overview

SSCP Training at Koenig will prepare participants for Systems Security Certified Practitioner (SSCP) certification, which is an vendor neutral information security credential governed by the not-for-profit International Information Systems Security Certification Consortium (ISC)2. The SSCP Course will help participants get an understanding of information security strategies for a business enterprise so that they can protect and manage sensitive corporate information.

Course Prerequisites

Valid experience includes information systems security-related work performed, or work that requires information security knowledge and involves direct application of that knowledge. For the SSCP certification, a candidate is required to have a minimum of 1 year of cumulative paid full-time work experience in one or more of the 7 domains of the SSCP CBK.

Benefits of Systems Security Certified Practitioner (SSCP)

Upon Completion of this Course, you will accomplish following:-

• Understand Access Control policies, procedures and standards to define operations and user controls.
• Implement security operations provide for the availability, integrity, and confidentiality of organizational assets.
• Identify and define the processes and methods based on IT criteria for the continuous monitoring and analysis of system access results.
• Collect information for identification of, and response to, security breaches or events.
• Identify the Business Continuity and Disaster Recovery Planning requirements necessary to ensure the preservation of the business.
• Identify the concepts and the requirements within cryptography, certificate and key management and secure protocols.
• Provide the basic understanding of Telecommunication and Network Security Concepts.
• Define and explain the countermeasures and techniques for dealing with viruses, worms, logic bombs, Trojan horses and other related forms of intentionally created damaging code.