Certified Information Systems Security Professional

Duration: 5 Days       Course Code: CISSP

Overview:

A CISSP is an information assurance professional who defines the architecture, design, management and/or controls that assure the security of business environments. The vast breadth of knowledge and the experience it takes to pass the exam is what sets the CISSP apart.

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

Target Audience:

IT professionals seeking to enhance their careers and gain credibility as information security specialists

Objectives:

- Best-practice information security management practices, including IS technical skills, risk management and business continuity planning.
- Cryptography
- Security architecture for applications and networks.
- Access control and physical security

Prerequisites:

The Seminar offers a high-level review of the main topics and identifies areas that students need to study and includes:

- Post-Seminar Self-Assessment
- 100% up-to-date material
- An overview of the scope of the information security field
Content:

- Access Control - a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.
- Application Development Security - addresses the important security concepts that apply to application software development. It outlines the environment where software is designed and developed and explains the critical role so
- Business Continuity and Disaster Recovery Planning – for the preservation and recovery of business operations in the event of outages.
- Cryptography - the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.
- Information Security Governance and Risk Management - the identification of an organization’s information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines. Management
- Legal, Regulations, Investigations and Compliance
- Computer crime laws and regulations
- The measures and technologies used to investigate computer crime incidents
- Operations Security - used to identify the controls over hardware, media, and the operators and administrators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools, and facilities that
- Physical (Environmental) Security - provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.
- Security Architecture and Design - contains the concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications and those controls used to enforce various
- Telecommunications and Network Security
- Network structures
- Transmission methods
- Transport formats
- Security measures used to provide availability, integrity, and confidentiality
- Authentication for transmissions over private and public communications networks and media

Further Information:

For More information, or to book your course, please call us on 00 966 92000 9278
training@globalknowledge.com.sa
www.globalknowledge.com.sa

Global Knowledge - KSA, 393 Al-Uroubah Road, Al Woorood, Riyadh 3140, Saudi Arabia