

Hands-on course , 5
day(s)
Ref : CIS

Participants

IS security manager or any other person who plays a role in IS security policy.

Pre-requisites

Basic knowledge of networks and operating systems as well as information security. Basic knowledge of auditing and business continuity standards.

2018 Price : 3030€ excl. VAT

Next sessions

GENEVE

sep. 17 2018, dec. 10 2018

LUXEMBOURG

sep. 17 2018, dec. 10 2018

CISSP, IS security, certification preparation

OBJECTIVES

This training details security concepts for obtaining CISSP certification. It will prepare you to take the exam by covering the entire Common Body of Knowledge (CBK), the shared core security knowledge defined by the International Information Systems Security Certification Consortium (ISC)².

1) IS security and the (ISC)²'s CBK

2) Security management and operations security.

3) Architecture, security models, and access control

4) Cryptography and development security

5) Telecom and network security

6) Continuity of business, laws, ethics, and physical security.

Certification

To take the certification exam, you must register on the ISC2 website and submit an eligibility packet.

1) IS security and the (ISC)²'s CBK

- Information system security.
- The why of CISSP certification.
- Overview of the scope covered by the CBK.

2) Security management and operations security.

- Security management practices. Writing policies, directives, procedures, and standards for security.
- The security awareness program, management practices, risk management, etc.
- Operations security: Preventive, detective, and corrective measures, roles and responsibilities of those involved.
- Best practices, security when hiring, etc.

3) Architecture, security models, and access control

- Architecture and security models: System architecture, theoretical informational security models.
- System evaluation methods, operational security modes, etc.
- Access control systems and methodologies. Categories and types of access controls.
- Access to data and systems, intrusion prevention systems (IPS) and intrusion detection systems (IDS).
- Audit trails, threats and attacks related to access control, etc.

4) Cryptography and development security

- Cryptography. Concepts, symmetrical and asymmetrical cryptography.
- Hash functions, public key infrastructure, etc.
- Security of application and system developments. Databases, data warehouses.
- The development cycle, object-oriented programming, expert systems, artificial intelligence, etc.

5) Telecom and network security

- Telecom and network security. Basic concepts, TCP/IP model, network and security equipment.
- Security protocols, attacks on networks, data backups, wireless technologies, VPNs, etc.

6) Continuity of business, laws, ethics, and physical security.

- Continuity of operations and disaster recovery plan.
- Business continuity plan, disaster recovery plan.
- Emergency measures, training and awareness program, crisis communications, exercises and tests, etc.
- Law, investigations, and ethics: Civil, criminal, and administrative law, intellectual property.
- Legal framework of investigations, evidence admissibility rules, etc.
- Physical security. Threats and vulnerabilities related to the environment of a place, scope of security.
- Layout requirements, site monitoring, staff protection, etc.