+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 16/09/2024

Sign up

CISMP Certification Preparation Course

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

3 days (21 hours)

Presentation

Our preparation for CISMP (Certified Information Security Management Principles) certification will help you provide a solid grounding in IT security principles, covering technical and managerial aspects for effective security risk management.

The CISMP training program will introduce you to key information security concepts such as risk management, control frameworks, legislation and compliance. You will also learn how to identify, mitigate and assess risks in a professional environment.

Preparedness covers other concepts such as business continuity, incident response and third-party vendor management. This approach includes an understanding of network infrastructure, access control measures and the protection of sensitive data.

With CISMP, you'll master information security management best practices, develop incident auditing skills and understand how to ensure security while meeting an organization's legal and regulatory requirements.

As with all our training courses, this one will bring you up to date with the latest CISMP developments.

Objectives

- Understand the fundamentals of information security
- Identify and manage information systems risks
- Applying a security framework tailored to organizations

- Implement technical and human safety controls
- Develop disaster recovery and continuity plans

Target audience

- **Cybersecurity analysts**
- IT security managers
- IT professionals

Prerequisites

General understanding of information systems and risk management concepts.

Note: Ambient IT is not the owner of CISMP, this certification belongs to BCS The Chartered Institute for IT.

OUR CISMP TRAINING PROGRAM

INFORMATION SECURITY PRINCIPLES

- Concepts and definitions
- The need for and benefits of information security
- Sample questions

INFORMATION RISKS

- Information systems threats and vulnerabilities
- Risk management
- Sample questions
- References and further reading

INFORMATION SECURITY FRAMEWORK

- Organization and responsibilities
- Organizational policies, standards and procedures
- Information security governance
- Implementation of the information assurance program
- Security incident management
- Legal framework
- Safety standards and procedures
- Sample questions
- References

SAFETY LIFECYCLES

- The information life cycle
- Test, audit and revision
- Systems development and support

CHECKS ON THE SAFETY OF PROCEDURES AND PEOPLE

- General controls
- Personal safety
- User access controls
- Training and awareness-raising

TECHNICAL SAFETY CHECKS

- Technical safety
- Malware protection
- Networks and communications
- Operational technology
- External services
- Cloud computing
- IT infrastructure
- Sample questions

PHYSICAL AND ENVIRONMENTAL SAFETY

- Physical security
- Different uses for controls
- Sample questions

DISASTER RECOVERY AND BUSINESS CONTINUITY MANAGEMENT

- Relationship between disaster recovery and business continuity management, risk assessment and impact analysis
- Resilience and redundancy
- Approaches to drawing up and implementing plans
- Documentation, maintenance and testing required
- Need to establish links with managed service provision and outsourcing
- Need for secure off-site storage of vital equipment
- Need to involve staff, suppliers and IT system providers
- Relationship with security incident management
- Compliance with standards
- Sample questions

OTHER TECHNICAL ASPECTS

- Investigation and forensics
- The role of cryptography
- Information on threats
- Conclusion

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.