Course : Cloud computing, governance and security

Seminar - 3d - 21h00 - Ref. CCG
Price : 2990 CHF E.T.

★★★★⯪   **4,6 / 5**

(BEST)

Cloud computing enables companies to simplify IT management and save money, but it also raises security concerns. This rich training course explains how to assess the risks (particularly regulatory) and what solutions need to be put in place to meet the cybersecurity challenge.

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Learn how to secure virtual environments and network access to the Cloud
- ✓ Assessing and managing cloud computing risks in accordance with ISO 27005
- ✓ Controlling and monitoring cloud security
- ✓ Learn about legal aspects and regulatory compliance

Intended audience

CIOs, CISOs, IT architects, network/storage/system engineers, security managers, project managers, consultants.

Prerequisites

Basic knowledge of Cloud SaaS, PaaS, IaaS models and IT security. Project management skills.

Course schedule

1 Introduction to cloud computing security

- Definition of Cloud Computing (NIST) and ISO 17788 standard.
- The main suppliers and the main failures already observed.
- SecaaS (Security as a Service) offers.
- The keys to a secure cloud architecture.

PARTICIPANTS
CIOs, CISOs, IT architects, network/storage/system engineers, security managers, project managers, consultants.

PREREQUISITES
Basic knowledge of Cloud SaaS, PaaS, IaaS models and IT security. Project management skills.

TRAINER QUALIFICATIONS
The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS
The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

2 Security in virtual environments

- Risks associated with server virtualization (VM Escape, VM Hopping, VM Theft and VM Sprawl).
- The problem of anti-malware protection in a virtualized infrastructure.
- Risks linked to vulnerabilities, APIs and software (Openstack, Docker, VmWare...).

3 Cloud network access security

- Secure access via IPsec, VPN, https and SSH.
- Specific Cloud access solutions (Intercloud, AWS Direct connect, etc.).
- CASB (Cloud Access Security Broker) solutions.
- Vulnerabilities in cloud clients (PCs, tablets, smartphones) and browsers.

4 The work of the Cloud Security Alliance (CSA)

- Security Guidance for Critical Areas of Focus in Cloud Computing.
- The twelve main threats identified in the Cloud.
- The OCF framework and the STAR (Security, Trust & Assurance Registry) directory.
- How do I use the Cloud Controls Matrix (CCM) and the CAIQ questionnaire?
- Certificate of Cloud Security Knowledge (CCSK).

5 Cloud computing security according to ENISA

- Cloud risk assessment and management using ISO 27005.
- The thirty-five risks identified by ENISA.
- ENISA recommendations for the security of government clouds.

6 Controlling cloud security

- How to control security in the cloud: auditing, penetration testing, qualification, certification?
- What is the value of the Secure Cloud, CSA STAR and Cloud confidence security labels?
- How do you ensure continuous safety monitoring throughout the life of the contract?
- How are security incidents detected and reported in the cloud?

7 The Cloud contract

- The essential security clauses to be included in a Cloud contract (monitoring committee, confidentiality, etc.).
- Reversibility clauses (upstream & downstream) to avoid being trapped by a supplier.
- The security audit clause: can it still be negotiated? What to do in a public cloud
- The importance of data localization and jurisdiction.
- Cloud service level agreements (SLAs).
- Penalties and indemnities: understanding the differences.

8   Legal aspects and regulatory compliance

- What are the supplier's legal responsibilities? What about the supplier's subcontractors?
- Supplier nationality and Datacenter location.
- The legal framework for personal data (Directive 95/46 EC, GDPR, CCT, BCR...).
- Following the cancellation of the Safe Harbor agreement, what are the new guarantees provided by the Privacy Shield?
- An update on the USA Patriot Act. Does it threaten data in the Cloud outside the USA?
- The legal framework for personal health data (law of January 26, 2016).
- Health data hosts (ASIP accreditation, security obligations, data localization, etc.).

9   Cloud security standards

- What is the value of suppliers' ISO 27001 security certification?
- ISO/IEC 17788:2014 (vocabulary) and ISO/IEC 17789:2014 (reference architecture).
- The new ISO/IEC standards (27017 & 27018) dedicated to security in the Cloud.
- How does ISO 27018 help protect personal data in the cloud?
- ISO 27017 and its ideal complement CSA Cloud Control Matrix.

10   License management in the cloud

- Understand why license management is more complex in the cloud.
- How do you ensure compliance?
- The limits of software asset management tools in the cloud.
- Inventory and reconcile licenses installed, acquired and used in the Cloud.

Dates and locations

REMOTE CLASS
2026 : 24 Mar., 19 May, 13 Oct., 15 Dec.