Professional Cloud Security Manager

Duration: 3 Days Course Code: GKPCS Version: 1.0

Overview:

Cloud computing is an emerging technology paradigm that helps organizations deliver IT services faster, with more agility, and with a lower cost of ownership. IT organizations are becoming more cognizant of the associated risks that come with cloud environments. Trusting information assets to the cloud requires a thorough understanding of security and of its associated risks, legal considerations and design of a governance structure.This course is designed for senior security, audit, and compliance professionals who are architecting policies and strategies to ensure compliance with and secure use of cloud computing. It includes comprehensive reference materials that help to continue the participants educational experience post the course. The course prepares you for the Professional Cloud Security Manager certification (PCS) exam provided by the Cloud Credential Council. The PCS is endorsed, recognized and supported by several key technology vendors and standards bodies. The content for this course, as well as the PCS certification is based on and aligned with cloud standards developed by the National Institute of Standards and Technology (NIST). The cost of the examvoucher is € 300,00 and is not included in the courseprice.

Target Audience:

Governance, Risk & Amp; Compliance (GRC) professionals, IT auditors, Compliance specialists, IT security professionals, cloud computing specialists.

Objectives:

- **After completing this course you should be able to understand:**
- Security and governance concepts and challenges in cloud computing
- What is new in security in the cloud?
- Contract management, terms, and conditions and legal
- IaaS specific security and governance policies
- PaaS specific security and governance policies
- SaaS specific security and governance policies

Prerequisites:

It is recommended that participants have achieved the Cloud Technology Associate certification (or its equivalent) from the Cloud Credential Council (and that participants are conversant with cloud concepts and vocabulary).

Having achieved the COBIT Foundation and relevant ISO/IEC 27000 certifications (or equivalents) is also recommended

Testing and Certification

Recommended as preparation for the following exams:

- **PCS** - Professional Cloud Security Manager

Content:

Security and Governance Concepts in Cloud Computing

- Key security concepts relevant to cloud computing
- Impact of cloud security on existing legacy data, systems and business
- Costs, trade-offs and consequences of severity of risks relative to the types of cloud computing scenarios in XaaS

Security Threats and Challenges in Cloud Computing

- Security risk in cloud computing
- Risks of various cyber attacks on data held in cloud environments
- Transparency, accountability and viability in relation to cloud computing

Physical Security and the Impact of Cloud Computing

- Critical physical security threats associated with data held in cloud environments
- Ownership and access issues in both on-premise and off-premise hardware

Virtualization Management and Security in the Cloud

- Critical virtual security threats associated with data held in cloud environments
- Issues specific to corporate and non-corporate resources and environments

What Security Does the Cloud Solve or Shift?

- Compliance and audit provisions relevant to operating in the cloud
- Balance of responsibility and liability between client and service provider

What Security Does the Cloud Change or Introduce?

- Relates the implications of core cloud features on security and governance
- Impact of cloud computing on legal issues, such as copyright, legislative compliance, and ownership

Existing Security Reference Models and Standards

- Explains the key current security standards that apply to cloud computing

Identifying the Delta in Your IT and Business Architecture for Cloud Security

- Security issues and risks in a given scenario

Risk Management and the Cloud

- Design features that are required for a secure cloud environment
- Security management components and tools currently available

IT Governance and Security

- Core principles of governance in a cloud environment

Monitoring-Users and Systems

- Issues of systems and business monitoring for on premise and off premise, remote services monitoring scenarios
- Monitoring systems in relation to the various cloud deployment possibilities
- Tools for User and systems monitoring using scenarios for on premise, off premise and hybrid combinations

Contract Management and TS and CS: Terms and Conditions

- Key concepts and types of contracts for technology and business and the impact of cloud on contracts management
- Hosting models ranging from onsite, CoLoc, Outsourcing, Managed hosting, Cloud Managed Hosting and the impact of cloud computing on these models
- Contract options for the different cloud deployments, the use of contract templates and types of contract between single and multiple parties
- Types of monetization, metering and charging and subscription mechanisms, and the impact on Terms and Conditions of service for different types of cloud computing scenarios

Legal Controls, Intelectual Property and Privacy

- Key legislative control issues that apply to cloud computing environments

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.be