Cloud Management & Security

Duration: 4 Days

Language: en

Course Code: PI1-113

Objective

Upon completion of this course, participants will be able to:

- Identify and assess cloud services.
- Audit and adjust security settings.
- Encrypt data.
- Use the Cloud vendor service contracts to ensure their data's confidentiality, integrity, and availability.
- Identify cybersecurity risks and cyber-attacks and how to defend them.
- Optimise Cloud practices.
- Adhere to data regulations and compliance.

Audience

This course is designed for any professional who requires a greater understanding of potential cybersecurity breaches, managing data encryption, and legal compliance regarding the Cloud. It would be most beneficial for:

- Technology Engineers, Chief Technology Officer (CTO) and Chief Information Officer (CIO)
- Key Application Development and Data Research Personnel
- Strategic Development Directors
- Crisis Management
- Team leaders
- Senior Managers
- Technical professionals
- IT specialists
- Legal Personnel

Training Methodology

This course will use various adult learning techniques to ensure a maximum understanding, comprehension and retention of the information presented.

The highly interactive training course is carefully designed to provide the best mix of experience, theory, and practice in a professional learning environment. It will provide real case studies and practical applications through “hands-on” action learning. Delivery will be through presentations, group investigations, training DVDs, and interactive seminars.

Summary

Major public cloud vendors are enhancing their services and improving cloud security, such as stopping distributed denial-of-service attacks. Experts note that cloud attacks are less devastating than on-premises ones, often limited to a single misconfigured service. However, organisations must remain vigilant against security threats, as vendors like Google, AWS, and Microsoft do not fully protect cloud data. Users must understand their shared responsibility and follow cloud security best practices, including configuration management, automated security updates, and improved logging and access management.

Despite advancements in security, breaches still occur. Cloud administrators should regularly test environments and review security audits. Business owners must be cautious with new technologies like AI and machine learning, which expand potential attack surfaces.

Compliance alone does not guarantee security. Organisations must align regulations with a robust cloud governance framework. Successful cloud management relies on proper tool use, automation, and a competent IT staff. Collaboration between IT and business teams is crucial to adapting to a cloud culture and achieving business goals.

Course Content & Outline

Section 1: Introduction to Cloud Computing

- Learn delivery models such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
- Understand Cloud types (Public, Private, Hybrid).
- How to choose a cloud service provider.
- What are the Cloud computing costs?

Section 2: Evolution of IT Security

- How to categorise physical and electronic risks.
- Understanding the legal and regulatory considerations.
- What are the current threats and trends an organisation faces?
- Learn different networking and communication technologies.
- Understanding different computer system designs.

Section 3: Compliance & Legal Considerations

- Understanding compliance challenges for the Cloud.
- What are the privacy concerns?
- What is data sovereignty?
- Understanding Cloud supplier agreements.

Section 4: Crisis Management & Risk Assessment

- How to approach risk assessments for the Cloud.
- Understanding Internal and external assessments.
- Understanding data security in the Cloud.

- Leaning encryption architectures.

Section 5: Identifying & Responding to Data Breaches

- How to recover from data loss or a data breach.
- Understanding key factors to identify a security breach.
- Learning crisis management planning.
- How to deal with the initial crisis and media management.

Certificate Description

Upon successful completion of this training course, delegates will be awarded a Holistique Training Certificate of Completion. For those who attend and complete the online training course, a Holistique Training e-Certificate will be provided.

Holistique Training Certificates are accredited by the British Accreditation Council (BAC) and The CPD Certification Service (CPD), and are certified under ISO 9001, ISO 21001, and ISO 29993 standards.

CPD credits for this course are granted by our Certificates and will be reflected on the Holistique Training Certificate of Completion. In accordance with the standards of The CPD Certification Service, one CPD credit is awarded per hour of course attendance. A maximum of 50 CPD credits can be claimed for any single course we currently offer.

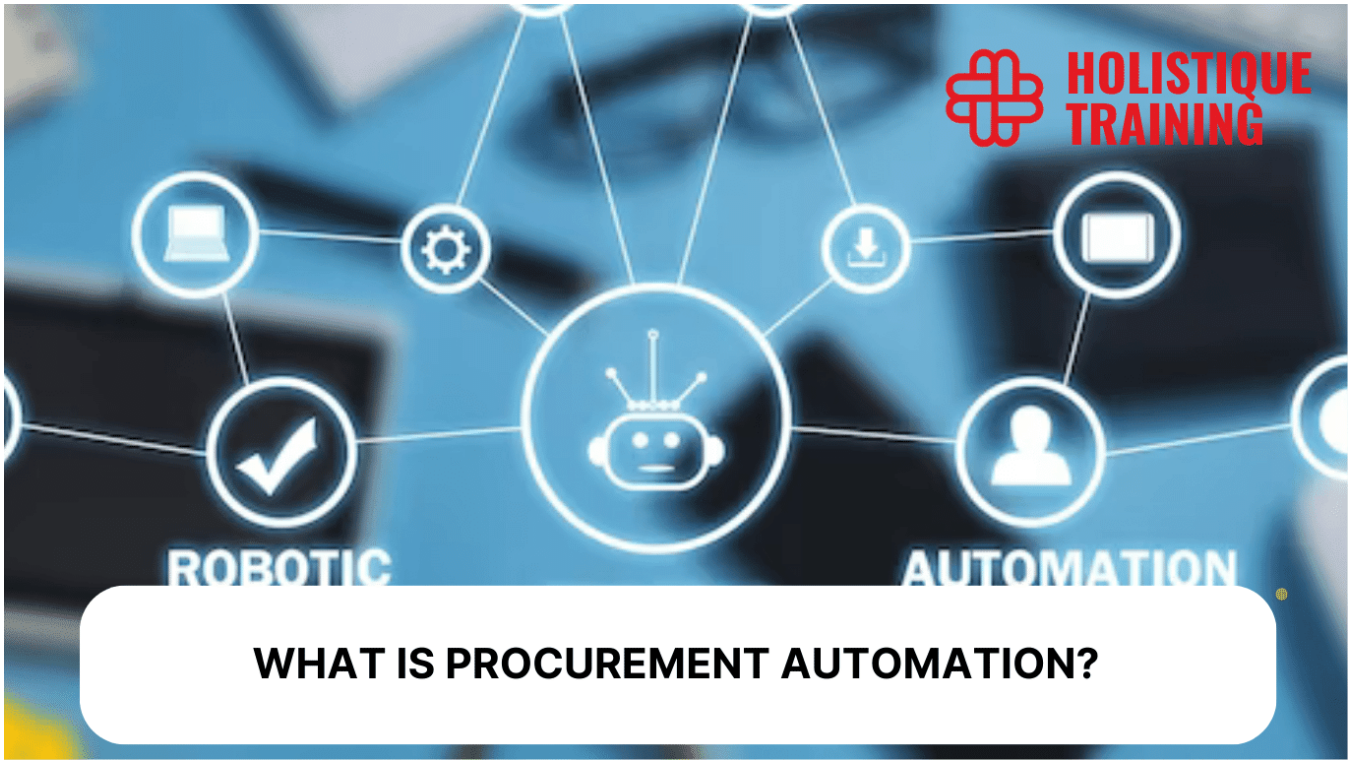
Categories

IT & Computer Application, Technology, Project Management

Tags

security , technology , IT , Cloud , Cyber security

Related Articles



Harnessing Cloud Computing: Embracing a New Era of Technology

Embark on a journey into the world of cloud computing, where remote servers redefine data management. Explore 5 key benefits, from scalability to security, and learn how to transition seamlessly. Stay ahead in this dynamic tech era!