Encryption and Data Protection in Cloud ERP Training Course

Professional Development Training Course Outline

Category	Enterprise Resource Planning (ERP)	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid digital transformation of enterprises, powered by the shift to Cloud ERP systems (Enterprise Resource Planning), has made data the most critical business asset. While Cloud ERP offers unparalleled scalability, agility, and cost-efficiency, it introduces complex new vectors for cyber threats, demanding a specialized focus on Cloud Security Architecture and Data Governance. This course addresses the modern imperative: securing sensitive business data including PII (Personally Identifiable Information), financial records, and intellectual property across the entire cloud lifecycle. Strong keywords: Cloud ERP Security, Data Governance, Cybersecurity Compliance, Zero Trust, Data Sovereignty.

Encryption and Data Protection in Cloud ERP Training Course is engineered to provide IT professionals, security architects, and compliance officers with actionable, hands-on expertise to deploy and manage advanced encryption and Data Loss Prevention (DLP) strategies within major Cloud ERP environments. The focus moves beyond mere theoretical understanding to practical implementation of Access Controls, Key Management Systems (KMS), and compliance with stringent global regulations like GDPR and HIPAA. Graduates will be equipped to mitigate risks from both external threats and insider threats, thereby establishing a robust, future-proof data protection posture that supports business continuity and maintains stakeholder trust in the hyper-connected, multi-cloud enterprise. Strong keywords: Encryption Key Management, Cloud DLP, Incident Response, Risk Mitigation, Multi-Cloud Security.

Programme Curriculum

Encryption and Data Protection in Cloud ERP Training Course

Introduction

The rapid digital transformation of enterprises, powered by the shift to Cloud ERP systems (Enterprise Resource Planning), has made data the most critical business asset. While Cloud ERP offers unparalleled scalability, agility, and cost-efficiency, it introduces complex new vectors for cyber threats, demanding a specialized focus on Cloud Security Architecture and Data Governance. This course addresses the modern imperative: securing sensitive business data including PII (Personally Identifiable Information), financial records, and intellectual property across the entire cloud lifecycle. Strong keywords: Cloud ERP Security, Data Governance, Cybersecurity Compliance, Zero Trust, Data Sovereignty.

Encryption and Data Protection in Cloud ERP Training Course is engineered to provide IT professionals, security architects, and compliance officers with actionable, hands-on expertise to deploy and manage advanced encryption and Data Loss Prevention (DLP) strategies within major Cloud ERP environments. The focus moves beyond mere theoretical understanding to practical implementation of Access Controls, Key Management Systems (KMS), and compliance with stringent global regulations like GDPR and HIPAA. Graduates will be equipped to mitigate risks from both external threats and insider threats, thereby establishing a robust, future-proof data protection posture that supports business continuity and maintains stakeholder trust in the hyper-connected, multi-cloud enterprise. Strong keywords: Encryption Key Management, Cloud DLP, Incident Response, Risk Mitigation, Multi-Cloud Security.

Couse Duration

5 days

Course Objectives

1. Master the principles of Cloud Data Sovereignty and Data Residency in a global ERP context.
2. Design and implement a Zero Trust Security Model specifically for Cloud ERP access.
3. Evaluate and select robust SaaS ERP and PaaS encryption techniques.
4. Develop a compliant strategy for Encryption Key Management using HSMs and native Cloud KMS.
5. Apply Dynamic Data Masking and Tokenization to protect sensitive data in non-production environments.
6. Establish effective Data Loss Prevention (DLP) policies for Cloud ERP data both at rest and in transit.
7. Configure Granular Access Controls to enforce the Principle of Least Privilege.
8. Navigate and ensure adherence to major Cybersecurity Compliance frameworks.
9. Integrate Security Information and Event Management (SIEM) for Continuous Controls Monitoring.
10. Formulate an advanced Cloud Incident Response and Disaster Recovery plan for ERP data breaches.
11. Secure API Integrations and third-party vendor access points within the Cloud ERP ecosystem.
12. Utilize Cloud Security Posture Management (CSPM) tools for proactive risk assessment and remediation.
13. Leverage AI/ML for Threat Detection and predictive analytics against emerging cloud-native vulnerabilities.

Target Audience

1. Cloud Security Architects
2. IT/ERP Security Administrators
3. Data Protection Officers (DPO)
4. Compliance and Risk Managers
5. Chief Information Security Officers (CISO)
6. ERP Implementation Consultants
7. Cloud Engineers (AWS, Azure, GCP)
8. Internal IT Auditors

Course Modules

1. Cloud ERP Security Fundamentals & Data Governance

- Shared Responsibility Model in IaaS, PaaS, and SaaS ERP.
- Data Classification and Lifecycle Management
- Case Study: Analyzing a major Cloud ERP vendor's security certifications and compliance reports.
- Data residency, jurisdiction, and the challenge of global data transfer.
- Implementing a comprehensive Cloud Data Governance Framework.

2. Encryption Technologies and Best Practices

- Comparison of data-at-rest and data-in-transit encryption.
- Detailed review of AES-256 and TDE (Transparent Data Encryption) in ERP databases.
- Case Study: The technical implementation of "Encrypt-at-Host" for cloud-hosted ERP virtual machines.
- Understanding and mitigating the risks of weak cryptographic keys and algorithms.
- Exploring advanced data protection: Homomorphic Encryption and Confidential Computing.

3. Key Management Strategies (KMS)

- Architecture of Cloud Provider Key Management Services (KMS)
- Principles of Cryptographic Key Lifecycle Management
- Case Study: Transitioning from a self-managed key system to a centralized, cloud-native HSM solution.
- Best practices for using Customer-Managed Keys and Customer-Provided Keys
- Securing access to the KMS vault and ensuring non-repudiation.

4. Identity, Access, and Privilege Management

- Implementing Multi-Factor Authentication and Adaptive Authentication for ERP access.
- Designing Role-Based Access Control matrices specific to core ERP functions
- Case Study: A financial services firm using Privileged Access Management (PAM) to restrict super-user access to the ERP system.
- Enforcing the Principle of Least Privilege using Attribute-Based Access Control
- Securing Single Sign-On and Identity Federation with the Cloud ERP.

5. Data Loss Prevention (DLP) and Threat Mitigation

- Setting up DLP policies to monitor and block exfiltration of sensitive ERP data
- Techniques for Dynamic Data Masking and Data Scrambling in sandbox or testing environments.
- Case Study: A multinational manufacturer preventing a potential insider threat by deploying ERP-level DLP on financial reports.
- Vulnerability assessment and penetration testing best practices for Cloud ERP.
- Protecting against SQL injection, cross-site scripting, and other web application vulnerabilities.

6. Regulatory Compliance and Audit in the Cloud

- Mapping Cloud ERP data protection controls to GDPR and HIPAA Security Rule requirements.
- Conducting internal and external Compliance Audits on the cloud environment.
- Case Study: A healthcare provider successfully passing a HIPAA audit by demonstrating TDE and robust access logging on their cloud ERP database.
- Achieving and maintaining compliance with regional data protection laws
- Utilizing automated tools for Continuous Compliance Monitoring and reporting.

7. Cloud Security Architecture and Integration

- Securing the network perimeter.
- Securing API Gateways and Microservices that connect to the Cloud ERP core.
- Case Study: Implementing a Zero Trust Network Access solution for remote employees connecting to the Cloud ERP.
- Hardening the underlying operating systems and containers
- Leveraging cloud-native services for network and application-level DDoS protection.

8. Incident Response and Business Continuity Planning

- Developing a Cloud Incident Response playbook for a data breach in the ERP system.
- Techniques for Digital Forensics and evidence collection in a volatile cloud environment.
- Case Study: Simulating a ransomware attack on the ERP backup storage and executing a successful, encrypted data recovery plan.
- Implementing Secure Backup and Disaster Recovery strategies with immutable storage.
- Post-incident analysis, system hardening, and continuous improvement cycles.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com