Security Auditing for Data Storage Systems Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the current hyper-connected digital economy, data is the most critical asset, making Data Storage Security Auditing an indispensable discipline. Organizations face an escalating volume of sophisticated cyber threats, including ransomware and Advanced Persistent Threats, that specifically target massive, centralized data repositories. The integrity, confidentiality, and availability of sensitive information, whether residing in on-premises storage, cloud environments, or hybrid systems, are constantly at risk. Security Auditing for Data Storage Systems Training Course provides security professionals with the practical, in-depth knowledge and technical expertise required to systematically assess, audit, and fortify modern data storage infrastructure.

This program moves beyond theoretical concepts to focus on real-world application of auditing standards, compliance frameworks, and Zero Trust principles across the entire data lifecycle. Participants will master risk-based auditing methodologies, including the use of modern tools for vulnerability assessment, configuration review, and access control governance. By integrating trending topics like Cloud Security Posture Management and DevSecOps integration, this course ensures practitioners can implement robust, compliant, and resilient security controls that proactively mitigate data breaches and satisfy stringent global regulatory compliance requirements like GDPR and HIPAA.

Programme Curriculum

Security Auditing for Data Storage Systems Training Course

Introduction

In the current hyper-connected digital economy, data is the most critical asset, making Data Storage Security Auditing an indispensable discipline. Organizations face an escalating volume of sophisticated cyber threats, including ransomware and Advanced Persistent Threats, that specifically target massive, centralized data

repositories. The integrity, confidentiality, and availability of sensitive information, whether residing in on-premises storage, cloud environments, or hybrid systems, are constantly at risk. Security Auditing for Data Storage Systems Training Course provides security professionals with the practical, in-depth knowledge and technical expertise required to systematically assess, audit, and fortify modern data storage infrastructure.

This program moves beyond theoretical concepts to focus on real-world application of auditing standards, compliance frameworks, and Zero Trust principles across the entire data lifecycle. Participants will master risk-based auditing methodologies, including the use of modern tools for vulnerability assessment, configuration review, and access control governance. By integrating trending topics like Cloud Security Posture Management and DevSecOps integration, this course ensures practitioners can implement robust, compliant, and resilient security controls that proactively mitigate data breaches and satisfy stringent global regulatory compliance requirements like GDPR and HIPAA.

Course Duration

5 days

Course Objectives

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

1. Strategically audit and assess security controls across Multi-Cloud and Hybrid Storage architectures.
2. Implement and verify Zero Trust Architecture principles for data access and storage segmentation.
3. Perform Risk-Based Auditing using industry-standard frameworks like NIST CSF and ISO 27001.
4. Master techniques for auditing Advanced Encryption at rest and in transit, including Key Management Systems.
5. Validate Cloud Security Posture Management tool configurations to detect storage misconfigurations.
6. Analyze and remediate vulnerabilities in Containerized Storage using DevSecOps practices.
7. Design and audit effective Data Loss Prevention (DLP) and Data Classification policies for sensitive data.
8. Conduct Forensic Audits on storage logs to identify the root cause of a simulated Data Breach or Insider Threat.
9. Review and harden Identity and Access Management (IAM) policies, focusing on Privileged Access Management (PAM).
10. Ensure Regulatory Compliance for data storage with key global mandates like GDPR, HIPAA, and PCI DSS.
11. Audit Data Resilience and Business Continuity Planning (BCP) for disaster recovery and protection against Ransomware.
12. Scrutinize Storage Area Network (SAN) and Network Attached Storage (NAS) security and segmentation controls.
13. Prepare comprehensive, actionable Audit Reports with evidence-based findings and Remediation roadmaps.

Target Audience

1. Information Security Auditors
2. Cybersecurity Analysts and Consultants
3. Data Protection Officers and Compliance Managers
4. Cloud Security Engineers and Architects
5. System Administrators and Storage Engineers
6. IT Risk Managers and Governance Professionals

7. DevSecOps Practitioners focused on data pipelines
8. IT Managers responsible for data retention and security policies

Course Modules

Module 1: Foundational Storage Architectures & Risk Modeling

- Review of SAN, NAS, and Object Storage security differences.
- Mapping the Data Lifecycle to key security controls.
- Introduction to Risk-Based Auditing methodology.
- Threat Modeling for storage environments: identifying common attack vectors.
- Defining the Audit Scope for complex hybrid environments.
- Case Study: Analyzing a major bank's transition to hybrid cloud and the inherent risk of misconfigured S3 Buckets causing a data leak.

Module 2: Access Control & Identity Governance

- Auditing IAM policies, roles, and permissions for storage systems
- Verifying implementation of Least Privilege and Segregation of Duties
- Reviewing Privileged Access Management solutions for administrative storage accounts.
- Assessing Multi-Factor Authentication and strong password policies on storage access.
- Auditing third-party and service account access to critical data stores.
- Case Study: The compromise of a service account leading to unauthorized data modification, focusing on a post-incident PAM system audit.

Module 3: Data Encryption & Key Management

- Auditing compliance of Encryption at Rest and Encryption in Transit.
- Deep dive into Key Management Systems, key rotation, and access policies.
- Verifying the use of Hardware Security Modules for root of trust.
- Auditing database-level encryption and tokenization controls.
- Reviewing data destruction policies and secure erasure verification.
- Case Study: Auditing a company's migration to a new KMS, identifying weak key access policies that violated FIPS 140-2 standards.

Module 4: Compliance and Regulatory Frameworks

- Auditing data residency and cross-border transfer compliance
- Reviewing controls for protecting Protected Health Information and financial data
- Mapping technical controls to regulatory requirements
- Developing an Audit Checklist based on common compliance standards
- Handling of Data Subject Access Requests and audit trails.
- Case Study: A comprehensive audit for a healthcare provider to achieve HIPAA compliance for their archival and live patient data storage systems.

Module 5: Storage Configuration & Vulnerability Assessment

- Auditing secure configuration baselines for operating systems and storage appliance firmware.
- Conducting Vulnerability Assessment and penetration testing against exposed storage interfaces
- Auditing network segmentation, Firewall rules, and port access for storage networks
- Reviewing patch and Vulnerability Management processes for storage infrastructure.
- Assessing security controls for Containerized and Virtual Machine storage volumes.

- Case Study: Identifying and exploiting a critical vulnerability in outdated NAS firmware during a Penetration Test and proposing a remediation plan.

Module 6: Log Analysis & Incident Response Auditing

- Auditing the integrity, retention, and collection of Audit Logs for all storage access events.
- Verifying effectiveness of Security Information and Event Management correlation rules for storage events.
- Reviewing the Incident Response Plan specifically for a storage security event
- Practicing Forensic Data Collection techniques from compromised storage systems.
- Auditing controls for detecting and alerting on Insider Threat and data exfiltration attempts.
- Case Study: Using a SIEM to trace a Ransomware infection back to its initial access point via a compromised file share, analyzing the dwell time.

Module 7: Cloud Storage Security

- Auditing Cloud Security Posture Management output and resolving misconfigurations.
- Deep-level auditing of cloud storage security features
- Securing and auditing serverless and cloud-native database storage.
- Implementing and auditing Immutable Storage for ransomware protection.
- Reviewing and optimizing Cloud Data Loss Prevention and data discovery tools.
- Case Study: Auditing a company's public cloud migration, discovering and fixing over 100 critical CSPM alerts related to publicly accessible data.

Module 8: Data Resilience, BCP, and Final Reporting

- Auditing the security of Data Backup and Disaster Recovery processes and off-site storage.
- Verifying the effectiveness of Data Resilience against catastrophic failures and cyberattacks.
- Developing a concise, evidence-based Executive Summary Report and detailed technical findings.
- Proposing Remediation steps, prioritizing risks based on business impact.
- Presenting and communicating audit results to both technical teams and Executive Leadership.
- Case Study: Reviewing the aftermath of a major regional outage, auditing the BCP and DR processes to ensure future Data Resilience compliance.

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.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now