Insider Threat Management for Banks Training Course

Professional Development Training Course Outline

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

Course Introduction

Insider Threat Management for Banks Training Course is designed to equip banking professionals with advanced knowledge and practical capabilities to identify, prevent, detect, investigate, and respond to insider risks, employee-related cyber threats, privileged access abuse, data leakage, fraud, and operational vulnerabilities. As financial institutions accelerate digital transformation, cloud adoption, open banking, artificial intelligence (AI), remote work, and cybersecurity modernization, insider threats have become a critical priority for banking resilience, information security, regulatory compliance, and customer trust. This course integrates modern Cybersecurity Risk Management, Zero Trust Security, Identity Governance, Behavioral Analytics, Data Loss Prevention (DLP), Security Operations, and Threat Intelligence frameworks.

The program provides a comprehensive understanding of how banks can develop proactive Insider Risk Programs using people, processes, and technology to safeguard sensitive financial data and critical banking systems. Participants will explore global best practices, regulatory expectations, incident response strategies, and real-world banking case studies involving malicious insiders, negligent employees, compromised credentials, third-party risks, and privileged user misuse. Through practical exercises and scenario-based learning, participants will gain the skills required to build a strong insider threat prevention culture and cyber-resilient banking environment.

Programme Curriculum

Insider Threat Management for Banks Training Course

Introduction

Insider Threat Management for Banks Training Course is designed to equip banking professionals with advanced knowledge and practical capabilities to identify, prevent, detect, investigate, and respond to insider

risks, employee-related cyber threats, privileged access abuse, data leakage, fraud, and operational vulnerabilities. As financial institutions accelerate digital transformation, cloud adoption, open banking, artificial intelligence (AI), remote work, and cybersecurity modernization, insider threats have become a critical priority for banking resilience, information security, regulatory compliance, and customer trust. This course integrates modern Cybersecurity Risk Management, Zero Trust Security, Identity Governance, Behavioral Analytics, Data Loss Prevention (DLP), Security Operations, and Threat Intelligence frameworks.

The program provides a comprehensive understanding of how banks can develop proactive Insider Risk Programs using people, processes, and technology to safeguard sensitive financial data and critical banking systems. Participants will explore global best practices, regulatory expectations, incident response strategies, and real-world banking case studies involving malicious insiders, negligent employees, compromised credentials, third-party risks, and privileged user misuse. Through practical exercises and scenario-based learning, participants will gain the skills required to build a strong insider threat prevention culture and cyber-resilient banking environment.

Course Duration

5 days

Course Objectives

By the end of this training course, participants will be able to:

1. Understand the evolving landscape of insider threats and cybersecurity risks in banking environments.
2. Develop effective Insider Threat Management Frameworks aligned with banking security standards.
3. Identify malicious insiders, negligent users, compromised accounts, and third-party threats.
4. Implement Zero Trust Security Models to reduce insider risk exposure.
5. Apply Identity and Access Management (IAM) and privileged access controls.
6. Strengthen Data Loss Prevention (DLP) strategies for protecting confidential banking information.
7. Utilize User and Entity Behavior Analytics (UEBA) for early threat detection.
8. Improve Security Operations Center (SOC) capabilities for insider threat monitoring.
9. Conduct effective insider threat investigations and digital forensics analysis.
10. Develop robust incident response and cyber crisis management procedures.
11. Enhance compliance with financial regulations, cybersecurity standards, and governance requirements.
12. Build employee awareness programs promoting cybersecurity culture and ethical behavior.
13. Design proactive strategies for continuous insider risk assessment and banking resilience.

Target Audience

1. Chief Information Security Officers (CISOs)
2. Information Security Managers and Analysts
3. Cybersecurity Operations Teams
4. Risk Management Professionals
5. Compliance and Internal Audit Officers
6. IT Administrators and System Engineers
7. Fraud Prevention and Investigation Teams
8. Banking Executives and Digital Transformation Leaders

Course Modules

Module 1: Fundamentals of Insider Threat Management in Banking

- Understanding the insider threat landscape in modern banking.
- Types of insider threats: malicious, negligent, accidental, and compromised insiders.
- Impact of insider incidents on financial institutions and customers.
- Insider threat lifecycle and risk management principles.
- Building a proactive insider threat governance framework.
- **Case Study:** Analysis of a global bank data breach caused by unauthorized employee access and lessons learned.

Module 2: Insider Risk Identification and Threat Assessment

- Conducting insider threat risk assessments in banking environments.
- Identifying high-risk users and sensitive business processes.
- Employee behavior patterns and risk indicators.
- Third-party and contractor insider risks.
- Developing insider risk scoring models.
- **Case Study:** Assessment of contractor access abuse in a financial institution.

Module 3: Identity Governance and Privileged Access Management

- Implementing Identity and Access Management (IAM) controls.
- Privileged Access Management (PAM) strategies.
- Role-Based Access Control (RBAC) and Least Privilege principles.
- Access certification and user lifecycle management.
- Managing administrator and privileged user risks.
- **Case Study:** Preventing unauthorized database access through PAM implementation.

Module 4: Zero Trust Security and Insider Threat Prevention

- Zero Trust architecture principles for banks.
- Continuous authentication and authorization.
- Device trust and adaptive access controls.
- Micro-segmentation for reducing internal exposure.
- Implementing risk-based security decisions.
- **Case Study:** A bank implementing Zero Trust to protect digital banking platforms.

Module 5: Data Protection, Monitoring, and Behavioral Analytics

- Data Loss Prevention (DLP) strategies.
- Monitoring user activities and abnormal behavior.
- User and Entity Behavior Analytics (UEBA).
- Security Information and Event Management (SIEM) integration.
- Protecting customer data and financial records.
- **Case Study:** Detection of unusual employee downloads using behavioral analytics.

Module 6: Insider Threat Investigation and Incident Response

- Insider threat detection and investigation processes.
- Digital evidence collection and forensic analysis.
- Incident response frameworks for insider incidents.
- Coordination between cybersecurity, HR, legal, and compliance teams.
- Post-incident reviews and corrective actions.

- **Case Study:** Investigation of employee credential misuse affecting banking operations.

Module 7: Governance, Compliance, and Insider Risk Culture

- Regulatory expectations for insider risk management.
- Developing insider threat policies and procedures.
- Ethical responsibilities and employee accountability.
- Security awareness and cybersecurity culture programs.
- Measuring insider threat program effectiveness.
- **Case Study:** Building a cybersecurity culture program after repeated employee security violations.

Module 8: Advanced Insider Threat Management Technologies and Future Trends

- Artificial Intelligence (AI) in insider threat detection.
- Machine Learning (ML) risk analytics.
- Threat Intelligence and predictive security models.
- Cloud security and remote workforce challenges.
- Future trends in banking cyber resilience.
- **Case Study:** Using AI-powered analytics to predict insider risk behavior in a digital bank.

Training Methodology

- 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