



Insider Threat Programme Management Course: Detection, Personnel Security and Investigation



Insider Threat Programme Management Course: Detection, Personnel Security and Investigation

Introduction:

Insider threat programme management, covering detection, personnel security and investigation, is a 5-day course for corporate security, information security and human resources managers in critical infrastructure and public bodies, ending with an Insider Risk Programme Plan for a case organisation. Staff, contractors and vendors with legitimate access commit fraud, data theft and sabotage when screening, access signals and grievance reports sit in separate departments. Nominees already manage security, HR or access functions and work through anonymised case studies at practitioner level. CoreConcept Training Center delivers this insider threat programme management course.

Course Objectives:

- Classify malicious, negligent and compromised insiders and map the harm pathways that apply to the organisation's critical assets and privileged roles
- Establish an insider risk hub with a charter, decision rights and data-sharing rules across security, HR, IT and legal functions
- Design pre-employment screening tiers and continuous vetting triggers proportionate to the sensitivity of each role
- Configure detection use cases that combine behavioural indicators, UEBA anomaly scores, DLP alerts and privileged access events
- Triage insider referrals and run proportionate investigations that preserve evidence and respect employee privacy safeguards
- Produce an Insider Risk Programme Plan with owners, controls, measures and a review cycle for senior approval

Target Audience:

- Managers responsible for corporate security and protective functions in critical infrastructure operators and public bodies
 - Managers responsible for information security, security operations and monitoring of privileged users
 - Human resources managers responsible for recruitment screening, employee relations and disciplinary cases
 - Managers responsible for identity, access and privileged account governance
 - Managers responsible for internal investigations, ethics reporting and legal risk in employee matters
-

Course Outline:

Day 1: Insider Threat Landscape, Insider Types and Programme Baseline

- Malicious, Negligent and Compromised Insider Typology With Case Examples
- Insider Harm Pathways Across Fraud, Data Theft and Sabotage
- Critical Pathway Model of Personal Predispositions and Stressors
- Crown Jewels Inventory and Privileged Role Exposure Mapping
- Insider Programme Maturity Baseline Across HR, Security and IT

Day 2: Mitigation Frameworks, Governance and the Converged Insider Risk Hub

- Define, Detect, Assess and Manage Insider Mitigation Cycle
- CERT Common Sense Guide Best Practices Mapped to Owners
- ISO/IEC 27002 People Controls for Screening and Disciplinary Process
- Insider Risk Hub Charter With HR, Legal and IT Roles
- ISO 31000 Insider Risk Register and Appetite Statement

Day 3: Personnel Security, Behavioural Indicators and Technical Signals

- Pre-Employment Screening Matrix by Role Sensitivity Tier
- Continuous Vetting Triggers and Periodic Aftercare Review Cycle
- Behavioural Indicator Catalogue and Line Manager Reporting Channel
- UEBA Baselines and Anomaly Scoring for Privileged Users
- DLP and Privileged Access Management Alert Correlation Rules

Day 4: Case Triage, Proportionate Investigation and Privacy Safeguards

- Insider Case Triage Matrix With Severity and Confidence Scoring
- MITRE ATT&CK Technique Mapping for Insider Data Exfiltration
- Proportionate Investigation Plan and Evidence Chain of Custody
- Privacy Impact Assessment for Employee Monitoring Activities
- Departing Employee Offboarding Controls and Access Revocation Checklist

Day 5: Case Study Work and the Insider Risk Programme Plan

- Case Organisation Briefing Pack With Personnel and Access Data
 - Case Insider Risk Register and Role Sensitivity Tiering
 - Case Detection Use Cases Combining HR and UEBA Signals
 - Case Triage Exercise on Three Anonymised Insider Referrals
 - Insider Risk Programme Plan Completion and Peer Defence
-

Skills You Will Gain:

- Insider Typology Analysis
- Insider Risk Hub Governance
- Role Sensitivity Tiering
- Continuous Vetting Design
- Behavioural Indicator Recognition
- UEBA Use Case Design
- Insider Case Triage
- Privacy-Proportionate Investigation

Why Attend This Course:

- Deliver an Insider Risk Programme Plan to the chief security officer, the head of human resources and legal counsel for approval
- Decide which roles need enhanced screening, which signals justify a referral and when a case moves to formal investigation
- Avoid data loss, sabotage and unlawful monitoring claims caused by unshared warning signs or disproportionate surveillance
- Equip line managers, HR advisers and analysts with the indicator catalogue, triage matrix and reporting channel from the course

Conclusion:

Back at work, the participant presents the Insider Risk Programme Plan to the chief security officer, the head of human resources and legal counsel, who use it to approve the insider risk hub charter, the screening tiers and the detection use cases to fund first. Line managers receive the indicator reporting channel and investigators receive the triage matrix. After the first quarter of operation, the hub should review referral volumes, false positive rates, case outcomes and privacy complaints, then adjust thresholds, vetting triggers and owners in the plan.

Frequently Asked Questions FAQ:

What should participants know before an insider threat programme management course?

Participants should already manage security, information security, HR or access functions. No prior insider threat training is needed. Anonymised examples of screening policies, access reviews or past employee cases help participants relate the case study to their own organisation.

How does insider threat programme management differ from a physical security or information security management course?

It concentrates on people with legitimate access: personnel vetting, behavioural and technical signals, case triage and proportionate investigation run by a joint HR, security, IT and legal hub. Site protection design and security management system fundamentals appear only as background.

Why does insider threat programme management need privacy safeguards?

Monitoring staff without proportionality, transparency and legal review creates employee relations and legal exposure and erodes the trust that reporting depends on. Privacy impact assessments, data minimisation and documented decision rights keep detection lawful and defensible.

What do participants take back from the insider threat programme management course?

Participants take back an Insider Risk Programme Plan for a case organisation, with a hub charter, a role sensitivity tiering, screening and vetting triggers, detection use cases, a triage matrix and a review cycle, ready to adapt to their own organisation.
