
Insider and Application Fraud in IT Systems: Controls, Log Monitoring and Response Training Course

27 September – 1 October 2027
Geneva





Insider and Application Fraud in IT Systems: Controls, Log Monitoring and Response Training Course

Ref: 417_24667 **Date:** 27 September – 1 October 2027 **Location:** Geneva **Fees:** 5500 GBP

Programme Summary

Insider and Application Fraud in IT Systems, covering controls, log monitoring and response, is the subject of this five-day training course for IT risk, security, audit and fraud leaders at strategic level, ending in a control and response blueprint for one application. Such fraud often uses legitimate rights and passes access checks. The programme moves from fraud mechanics in systems, through diagnosis of control and log gaps, to design of detection and response, then to application on one application. Mars Training Centre UK delivers this Insider and Application Fraud in IT Systems programme for senior risk and security leaders.

The Business Case

When fraud runs through privileged accounts or application logic, losses are found late, evidence is incomplete and responsibility is disputed between IT, audit and fraud teams. Leaders who understand how misuse leaves traces in systems can set clearer controls, agree what to log and prepare an evidence-ready response before an incident occurs.

- Detection Time: Shortens as logs and alerts are designed around known misuse patterns.
- Evidence Quality: Improves as collection and preservation steps are agreed in advance.
- Control Ownership: Becomes clearer as IT, audit and fraud teams share one control map.

Principles and Evidence Base

- ISO/IEC 27001 access control and logging controls: they structure the control review in Sessions 2 and 3.
- ISO/IEC 27001 collection of evidence control: it frames the evidence readiness design in Session 4.
- ISO/IEC 27037 guidance on digital evidence: it guides identification and preservation steps in Session 4.
- Segregation of duties principles: they shape the privileged access analysis in Session 2.

Intended Participants

- Information security leaders who set access, logging and monitoring standards.
- Internal audit leaders who test controls over critical applications.
- Fraud and investigation leaders who receive alerts and referrals from systems.
- IT risk owners who sponsor control changes in business applications.

The programme serves banks, utilities, government agencies and insurers, and suits mixed groups from risk, security and audit functions.



Learning Outcomes

1. Participants will be able to classify the ways insiders and application users misuse legitimate system rights.
2. Participants will be able to evaluate privileged access and segregation of duties for conflicts that enable fraud.
3. Participants will be able to diagnose gaps in application controls and log coverage.
4. Participants will be able to design monitoring rules and alert routes for specific misuse patterns.
5. Participants will be able to construct an evidence preservation and escalation routine.
6. Participants will be able to justify a prioritised control and response blueprint for one application.

Programme Structure

Day 1: Insider and Application Fraud in IT Systems Principles

How does fraud exploit legitimate rights in a system?

- Fraud Triangle Applied to Systems
- Insider Misuse Pattern Catalogue
- Application Logic Abuse Examples
- Privileged Account Lifecycle Map
- ISO/IEC 27001 Control Overview

Day 2: Diagnosing Access and Application Control Gaps

Where do access rights and application rules allow misuse?

- Segregation of Duties Conflict Matrix
- Privileged Access Review Sheet
- Transaction Approval Flow Walkthrough
- Shared and Service Account Audit
- Control Gap Heat Map

Day 3: Diagnosing Log and Monitoring Gaps

Would current logs show the misuse when it happens?

- Log Source Coverage Inventory
- Audit Trail Integrity Check
- Alert Noise and Blind Spot Review
- Reconstruction of a Misuse Timeline
- Monitoring Gap Register



Day 4: Designing Detection, Evidence and Response

What should be detected, preserved and escalated, and by whom?

- Misuse Detection Rule Template
- Alert Triage and Escalation Path
- ISO/IEC 27037 Evidence Handling Steps
- Roles Matrix for IT, Audit and Fraud Teams
- Containment Decision Checklist

Day 5: Applying the Controls to One Application

Is the blueprint ready for the application owner?

- Applying the Session 2 Conflict Matrix to the Application
- Testing the Session 3 Log Inventory on Sample Events
- Checking the Session 4 Rules Against a Misuse Scenario
- Rehearsing the Escalation Briefing
- Completing the Fraud Control and Response Blueprint

Methodology

The programme uses a case analysis method built on anonymised incident narratives, sample log extracts and control descriptions from several sectors. Participants map misuse paths, test whether logs would reveal them, draft detection rules and rehearse escalation in small groups, with feedback on each work product.

- Suggested activity: Reconstructing a misuse timeline from a sample log extract.
- Suggested activity: Finding segregation conflicts in a payment approval workflow.
- Suggested activity: Drafting an escalation routine for a privileged account alert.

Capstone Output

Each participant completes a fraud control and response blueprint for one business application. It holds a conflict matrix, a log coverage inventory, detection rules, an evidence handling routine and an escalation path. The blueprint is used to brief the application owner, guide control changes and align IT, audit and fraud teams.



Frequently Asked Questions

Is insider and application fraud in IT systems suitable for leaders without a technical background?

Yes. Insider and application fraud in IT systems is taught at strategic level, assuming responsibility for controls, audit or fraud decisions rather than hands-on system administration.

Which references does insider and application fraud in IT systems rest on?

Insider and application fraud in IT systems rests on ISO/IEC 27001 access, logging and evidence controls, ISO/IEC 27037 and segregation of duties principles.

How is the blueprint from insider and application fraud in IT systems used at work?

You use the blueprint to brief the application owner, guide control changes and align IT, audit and fraud teams on detection and response.

How does insider and application fraud in IT systems differ from a programme on fraud analytics?

Insider and application fraud in IT systems centres on controls, logs and evidence in systems, while a fraud analytics programme centres on statistical and machine learning models.