# Insider Threat Program Management (NITTF standards) Training Course

Professional Development Training Course Outline

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

## Course Introduction

Insider threats represent a critical risk to organizational security, data integrity, and operational continuity. These threats can arise from employees, contractors, or other trusted personnel who misuse access to information systems, facilities, or sensitive assets. The Insider Threat Program Management course provides participants with the knowledge and skills to identify, mitigate, and manage insider risks while adhering to National Insider Threat Task Force (NITTF) standards. Insider Threat Program Management (NITTF standards) Training Course emphasizes building a comprehensive insider threat program, integrating risk assessment, behavioral analysis, and security controls to prevent unauthorized disclosures, fraud, or sabotage. Participants will also explore cutting-edge tools and strategies for monitoring, detecting, and responding to potential insider threats in real-time.

In today’s high-risk digital and physical environments, organizations require robust insider threat programs to protect classified information, intellectual property, and operational systems. This course combines policy frameworks, operational procedures, technological solutions, and employee awareness techniques to strengthen organizational resilience. Through interactive modules, case studies, and hands-on exercises, participants will learn to design, implement, and evaluate insider threat programs that comply with NITTF standards, enhance situational awareness, and minimize internal security risks.

## Programme Curriculum

**Insider Threat Program Management (NITTF standards) Training Course**

**Introduction**

Insider threats represent a critical risk to organizational security, data integrity, and operational continuity. These threats can arise from employees, contractors, or other trusted personnel who misuse access to information systems, facilities, or sensitive assets. The Insider Threat Program Management course provides

participants with the knowledge and skills to identify, mitigate, and manage insider risks while adhering to National Insider Threat Task Force (NITTF) standards. Insider Threat Program Management (NITTF standards) Training Course emphasizes building a comprehensive insider threat program, integrating risk assessment, behavioral analysis, and security controls to prevent unauthorized disclosures, fraud, or sabotage. Participants will also explore cutting-edge tools and strategies for monitoring, detecting, and responding to potential insider threats in real-time.

In today's high-risk digital and physical environments, organizations require robust insider threat programs to protect classified information, intellectual property, and operational systems. This course combines policy frameworks, operational procedures, technological solutions, and employee awareness techniques to strengthen organizational resilience. Through interactive modules, case studies, and hands-on exercises, participants will learn to design, implement, and evaluate insider threat programs that comply with NITTF standards, enhance situational awareness, and minimize internal security risks.

**Course Objectives**

1. Understand the fundamentals of insider threat programs and NITTF standards.
2. Identify potential insider threat indicators, behaviors, and risk factors.
3. Develop policies and procedures to prevent, detect, and mitigate insider threats.
4. Implement monitoring tools and analytics to track insider activities.
5. Conduct risk assessments and vulnerability analyses within the organization.
6. Integrate physical, technical, and administrative controls for insider threat mitigation.
7. Establish reporting mechanisms and escalation protocols for suspicious activities.
8. Build employee awareness and training programs to reduce insider risk.
9. Coordinate with human resources, legal, and IT departments for holistic program management.
10. Apply NITTF standards for program design, evaluation, and compliance.
11. Conduct investigations and respond effectively to confirmed insider incidents.
12. Measure program effectiveness through metrics and continuous improvement.
13. Maintain confidentiality, legal compliance, and ethical standards in insider threat management.

**Organizational Benefits**

- Enhanced detection and mitigation of internal security risks
- Improved compliance with NITTF and regulatory standards
- Strengthened data protection and information security posture
- Reduced operational disruptions and insider-caused losses
- Better integration of security, HR, and IT functions
- Increased employee awareness and proactive risk reporting
- Effective incident response and investigation capabilities
- Protection of intellectual property and sensitive organizational assets
- Enhanced leadership and governance in risk management
- Data-driven insights for continuous program improvement

**Target Audiences**

- Security managers and risk officers
- Human resource professionals
- IT and cybersecurity personnel
- Compliance and legal officers
- Operational managers with access to sensitive systems

- Investigators and auditors
- Policy makers and organizational leadership
- Consultants in security and risk management

**Course Duration:** 5 days

**Course Modules**

**Module 1: Introduction to Insider Threats**

- Define insider threats and categories of insiders
- Overview of NITTF standards and guidelines
- Identify risks and potential organizational impacts
- Understand insider threat life cycles and phases
- Discuss case examples of insider incidents
- Case Study: Analysis of a real insider data breach incident

**Module 2: Risk Assessment & Vulnerability Analysis**

- Conduct organizational risk assessments for insider threats
- Identify critical assets and information systems
- Map vulnerabilities and potential attack vectors
- Prioritize risks based on likelihood and impact
- Integrate assessment results into program design
- Case Study: Risk assessment for a financial institution

**Module 3: Policy & Program Development**

- Develop insider threat program policies aligned with NITTF standards
- Establish roles and responsibilities for program governance
- Design reporting, monitoring, and escalation procedures
- Integrate HR, IT, and legal considerations
- Define acceptable use policies and employee agreements
- Case Study: Implementing a program policy framework in a corporate setting

**Module 4: Monitoring & Detection Tools**

- Use behavioral analytics to identify anomalies
- Implement access monitoring for systems and facilities
- Apply technical controls for data and network security
- Monitor communications, transactions, and user activity
- Combine physical and digital monitoring approaches
- Case Study: Detection of unauthorized access in a government agency

**Module 5: Incident Response & Investigations**

- Establish insider incident response teams and procedures
- Investigate alerts and suspicious behaviors effectively
- Document findings while maintaining confidentiality
- Coordinate with internal and external stakeholders
- Apply ethical and legal standards during investigations
- Case Study: Investigation of insider fraud in a multinational company

**Module 6: Employee Awareness & Training**

- Design awareness campaigns to reduce insider risk
- Train staff on security policies, reporting mechanisms, and ethical practices
- Conduct workshops and simulations for proactive learning
- Monitor effectiveness of training programs
- Encourage employee participation in threat mitigation
- Case Study: Successful insider risk awareness program in a bank

**Module 7: Metrics & Program Evaluation**

- Define key performance indicators for insider threat programs
- Measure program effectiveness and risk reduction outcomes
- Conduct periodic audits and compliance assessments
- Review program successes and areas for improvement
- Implement continuous improvement cycles for program maturity
- Case Study: Evaluating program effectiveness in a government organization

**Module 8: Governance, Compliance & Legal Considerations**

- Ensure compliance with NITTF standards and relevant regulations
- Address privacy, legal, and ethical considerations in monitoring
- Establish governance structures and oversight committees
- Integrate legal counsel in program development
- Document compliance efforts and maintain audit readiness
- Case Study: Compliance challenges in a multinational financial institution

**Training Methodology**

- Instructor-led presentations on NITTF standards and best practices
- Interactive workshops with real-world scenarios
- Hands-on exercises using monitoring and detection tools
- Case study analysis of insider incidents and program implementation
- Group discussions, simulations, and role-playing exercises
- Development of action plans for organizational insider threat programs

**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