Counter-Intelligence (CI) Fundamentals and Methodology Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Counter-Intelligence (CI) is a critical component of national security and organizational protection, aimed at detecting, preventing, and neutralizing espionage, sabotage, and insider threats. In today's complex geopolitical and technological environment, CI professionals require advanced analytical, investigative, and operational skills to identify adversarial intelligence activities and protect sensitive assets. Counter-Intelligence (CI) Fundamentals and Methodology Training Course provides a comprehensive understanding of CI fundamentals, operational methodologies, threat analysis, and strategic frameworks to mitigate risks posed by both internal and external actors. Participants will learn to integrate intelligence collection, countermeasures, and risk mitigation strategies effectively within organizational structures.

The course combines theoretical foundations with practical exercises, real-world case studies, and hands-on operational simulations to strengthen participants' capabilities in CI planning, threat assessment, and investigative techniques. Emphasis is placed on analytical reasoning, legal and ethical considerations, operational security, and the effective use of technological tools in CI operations. By the end of the training, participants will be equipped to design, implement, and oversee robust counter-intelligence programs that safeguard organizational integrity and national security interests.

Programme Curriculum

Counter-Intelligence (CI) Fundamentals and Methodology Training Course

Introduction

Counter-Intelligence (CI) is a critical component of national security and organizational protection, aimed at detecting, preventing, and neutralizing espionage, sabotage, and insider threats. In today's complex geopolitical and technological environment, CI professionals require advanced analytical, investigative, and operational skills to identify adversarial intelligence activities and protect sensitive assets. Counter-Intelligence (CI)

Fundamentals and Methodology Training Course provides a comprehensive understanding of CI fundamentals, operational methodologies, threat analysis, and strategic frameworks to mitigate risks posed by both internal and external actors. Participants will learn to integrate intelligence collection, countermeasures, and risk mitigation strategies effectively within organizational structures.

The course combines theoretical foundations with practical exercises, real-world case studies, and hands-on operational simulations to strengthen participants' capabilities in CI planning, threat assessment, and investigative techniques. Emphasis is placed on analytical reasoning, legal and ethical considerations, operational security, and the effective use of technological tools in CI operations. By the end of the training, participants will be equipped to design, implement, and oversee robust counter-intelligence programs that safeguard organizational integrity and national security interests.

Course Objectives

1. Understand the fundamentals and principles of counter-intelligence operations.
2. Identify key threats to organizational and national security.
3. Develop skills in intelligence collection and operational analysis.
4. Apply investigative techniques to detect espionage and insider threats.
5. Integrate CI methodologies into organizational security strategies.
6. Utilize threat assessment and risk management tools effectively.
7. Strengthen operational security and protective measures.
8. Implement ethical and legal frameworks in CI operations.
9. Leverage technological tools for CI detection and prevention.
10. Conduct CI reporting, documentation, and communication protocols.
11. Enhance decision-making through analytical reasoning and evidence-based methods.
12. Plan, coordinate, and manage CI operations efficiently.
13. Evaluate CI program effectiveness and propose continuous improvements.

Organizational Benefits

- Enhanced protection against espionage and insider threats
- Improved threat detection and response capabilities
- Strengthened organizational and national security posture
- Increased operational readiness and situational awareness
- Better integration of CI methodologies into security frameworks
- Reduced risk of sensitive information compromise
- Strengthened legal and ethical compliance in operations
- Improved decision-making based on actionable intelligence
- Enhanced staff capacity and CI professional development
- Reduced vulnerabilities through continuous CI program evaluation

Target Audiences

- Counter-Intelligence officers and analysts
- Security and intelligence managers
- Law enforcement and national security professionals
- Threat assessment and risk management specialists
- Cybersecurity and technical intelligence staff
- Policy makers and government officials
- Security consultants and investigators

- Military and defense intelligence personnel

Course Duration: 10 days

Course Modules

Module 1: Introduction to Counter-Intelligence

- History and evolution of counter-intelligence
- Core principles and objectives of CI operations
- Types of threats: espionage, sabotage, insider risks
- CI organizational structures and responsibilities
- Legal and ethical considerations in CI
- Case Study: Historical espionage case impacting national security

Module 2: Threat Assessment and Analysis

- Identifying potential adversaries and vulnerabilities
- Analyzing threat intelligence and risk indicators
- Assessing operational impact of security breaches
- Prioritizing threats for CI focus
- Integrating analytical tools for threat evaluation
- Case Study: Threat assessment in a corporate espionage scenario

Module 3: Intelligence Collection Techniques

- Human intelligence (HUMINT) collection methods
- Open-source intelligence (OSINT) applications
- Technical and electronic intelligence collection
- Surveillance strategies and operational planning
- Documentation and validation of intelligence sources
- Case Study: OSINT application in detecting insider threats

Module 4: Investigative Methodologies

- Planning and conducting CI investigations
- Interviewing techniques and interrogation strategies
- Gathering evidence for CI operations
- Monitoring and surveillance of suspects
- Coordinating with law enforcement and regulatory bodies
- Case Study: Investigation of internal data leakage in a financial institution

Module 5: Operational Security (OPSEC)

- Principles and implementation of OPSEC
- Identifying critical information and vulnerabilities
- Implementing security countermeasures
- Monitoring and controlling information flow
- Evaluating OPSEC effectiveness in operations
- Case Study: OPSEC failure leading to compromise of sensitive operations

Module 6: Insider Threat Detection

- Recognizing patterns and behaviors indicative of insider threats
- Monitoring internal communications and activities
- Risk mitigation strategies for insider threats
- Policy development to manage insider risks
- Collaboration with HR and compliance teams
- Case Study: Insider threat detection in a multinational organization

Module 7: Counter-Espionage Measures

- Identifying espionage tactics and techniques
- Applying counter-surveillance and deception strategies
- Disrupting adversarial intelligence operations
- Protecting sensitive data from foreign intelligence threats
- Coordination with national intelligence agencies
- Case Study: Counter-espionage operations in a defense sector organization

Module 8: Cyber Counter-Intelligence

- Cyber threats and espionage risks
- Securing digital assets and networks
- Monitoring for insider and external cyber threats
- Cyber investigative techniques and tools
- Cyber incident response and reporting protocols
- Case Study: Detecting and mitigating cyber espionage in an MFI

Module 9: Legal and Ethical Frameworks

- National and international CI laws and regulations
- Ethical considerations in CI operations
- Balancing operational secrecy with transparency
- Compliance with human rights and organizational policies
- Documentation and reporting standards
- Case Study: Legal challenges in CI operations

Module 10: Analytical Techniques for CI

- Data collection and synthesis for intelligence analysis
- Pattern recognition and anomaly detection
- Predictive analytics for threat anticipation
- Reporting and presenting intelligence findings
- Decision-making based on analytical insights
- Case Study: Analytical assessment preventing a security breach

Module 11: Counter-Intelligence Program Management

- Designing and implementing CI programs
- Resource allocation and operational planning
- Monitoring program effectiveness
- Staff training and professional development
- Risk and performance evaluation frameworks
- Case Study: Implementation of a CI program in a large organization

Module 12: Technical Counter-Intelligence Tools

- Use of surveillance technology and sensors
- Communication monitoring and encryption analysis
- Cybersecurity software for CI applications
- Integration of technical tools into operations
- Maintaining operational security of technical assets
- Case Study: Use of technical tools to uncover espionage activities

Module 13: Crisis Management and Response

- CI role in organizational crisis management
- Incident response planning and coordination
- Communication strategies during CI crises
- Containment and mitigation of security breaches
- Post-incident review and improvement
- Case Study: Response to a multi-level security breach

Module 14: International CI Operations

- Global CI practices and collaboration
- Intelligence sharing with allied organizations
- Monitoring transnational threats
- Managing diplomatic and legal considerations
- Applying international standards in CI operations
- Case Study: Cross-border CI operation disrupting espionage network

Module 15: Evaluation and Continuous Improvement

- Measuring CI program effectiveness
- Key performance indicators and metrics
- Lessons learned and operational refinement
- Institutionalizing continuous improvement processes
- Updating CI protocols and strategies
- Case Study: Continuous improvement in CI operations in a government agency

Training Methodology

- Instructor-led presentations and expert briefings
- Practical exercises and role-play scenarios
- Case study analysis and group discussions
- Hands-on workshops with threat assessment and intelligence tools
- Real-world simulations of CI operations
- Development of actionable CI strategies and operational plans

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com