Defense Industrial Base Resilience and Supply Chain Security 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

The modern defense industrial base faces increasingly complex threats, including cyber-attacks, geopolitical disruptions, natural disasters, and supply chain vulnerabilities. Organizations must strengthen resilience and security across production, procurement, logistics, and technology integration to ensure operational continuity and national security. Defense Industrial Base Resilience and Supply Chain Security Training Course provides participants with advanced knowledge, frameworks, and best practices to mitigate risks, maintain critical supply chain integrity, and enhance the overall robustness of defense industrial operations. Emphasis is placed on practical strategies for identifying vulnerabilities, assessing risk, and implementing proactive resilience measures while leveraging emerging technologies and policy frameworks.

Participants will explore methodologies for risk management, continuity planning, cyber resilience, supplier monitoring, and regulatory compliance within defense supply networks. Through real-world case studies, interactive exercises, and scenario-based learning, attendees will develop actionable insights to safeguard supply chains against disruptions, improve decision-making under uncertainty, and build institutional capability for long-term resilience. The course ensures that learners acquire the skills to evaluate critical suppliers, secure logistics operations, and maintain operational readiness in both routine and crisis situations.

Programme Curriculum

Defense Industrial Base Resilience and Supply Chain Security Training Course

Introduction

The modern defense industrial base faces increasingly complex threats, including cyber-attacks, geopolitical disruptions, natural disasters, and supply chain vulnerabilities. Organizations must strengthen resilience and

security across production, procurement, logistics, and technology integration to ensure operational continuity and national security. Defense Industrial Base Resilience and Supply Chain Security Training Course provides participants with advanced knowledge, frameworks, and best practices to mitigate risks, maintain critical supply chain integrity, and enhance the overall robustness of defense industrial operations. Emphasis is placed on practical strategies for identifying vulnerabilities, assessing risk, and implementing proactive resilience measures while leveraging emerging technologies and policy frameworks.

Participants will explore methodologies for risk management, continuity planning, cyber resilience, supplier monitoring, and regulatory compliance within defense supply networks. Through real-world case studies, interactive exercises, and scenario-based learning, attendees will develop actionable insights to safeguard supply chains against disruptions, improve decision-making under uncertainty, and build institutional capability for long-term resilience. The course ensures that learners acquire the skills to evaluate critical suppliers, secure logistics operations, and maintain operational readiness in both routine and crisis situations.

Course Objectives

1. Understand the key concepts of defense industrial base resilience and supply chain security.
2. Identify critical vulnerabilities within defense supply chains.
3. Analyze risks from cyber threats, geopolitical shifts, and natural disasters.
4. Apply risk assessment frameworks for supply chain continuity.
5. Develop contingency and crisis response plans for critical operations.
6. Implement security policies and compliance measures across suppliers.
7. Assess supplier reliability and performance under stress conditions.
8. Integrate technology solutions to monitor and secure supply chains.
9. Strengthen cybersecurity resilience in manufacturing and logistics networks.
10. Evaluate supply chain dependencies and interdependencies for mitigation planning.
11. Apply incident response protocols and continuity exercises.
12. Build institutional capacity for long-term resilience and sustainability.
13. Measure and improve resilience metrics and supply chain performance indicators.

Organizational Benefits

- Improved operational continuity in defense supply networks
- Enhanced risk management and mitigation capability
- Stronger supplier engagement and compliance oversight
- Reduced vulnerability to cyber threats and physical disruptions
- Greater preparedness for natural disasters and geopolitical crises
- Increased visibility and monitoring of critical supply chains
- Improved decision-making through data-driven risk assessment
- Strengthened organizational resilience culture and policies
- Enhanced regulatory compliance and reporting capabilities
- Better alignment of strategic planning with operational security goals

Target Audiences

- Defense industrial base managers and executives
- Supply chain and logistics professionals
- Risk management and resilience officers
- Cybersecurity and IT specialists in defense organizations
- Procurement and contract management teams

- Government and defense regulators
- Crisis management and continuity planners
- Consultants and advisors in defense operations

Course Duration: 5 days

Course Modules

Module 1: Overview of Defense Industrial Base Resilience

- Key concepts and frameworks for resilience in defense industries
- Threat landscape and emerging risks
- Critical infrastructure and supply chain dependencies
- Regulatory and compliance considerations
- Best practices for operational resilience
- Case Study: Lessons from a defense supply chain disruption

Module 2: Supply Chain Risk Assessment

- Identifying critical nodes and suppliers
- Risk mapping and prioritization techniques
- Evaluating supplier financial, operational, and security risks
- Integration of risk assessment into decision-making
- Scenario planning for supply chain disruptions
- Case Study: Risk assessment of multi-tier defense suppliers

Module 3: Cybersecurity and Data Protection

- Cyber threat landscape for defense supply chains
- Securing digital communications and data exchanges
- Vendor and supplier cybersecurity requirements
- Incident detection and response protocols
- Implementing cyber resilience frameworks
- Case Study: Cyber attack on a defense logistics network

Module 4: Supplier Management and Compliance

- Supplier vetting and performance monitoring
- Contractual obligations for resilience and security
- Compliance with defense regulations and standards
- Supplier audits and continuous improvement
- Collaborative approaches to risk mitigation
- Case Study: Supplier compliance program improvement

Module 5: Crisis Management and Continuity Planning

- Developing operational continuity plans
- Crisis response teams and communication strategies
- Resource allocation during disruptions
- Testing and exercising continuity plans
- Coordination with internal and external stakeholders
- Case Study: Response to natural disaster affecting supply chain

Module 6: Technology Solutions for Resilient Supply Chains

- Digital tools for monitoring and risk detection
- Predictive analytics for supply chain performance
- IoT and blockchain applications in defense logistics
- Data visualization and reporting dashboards
- Integrating technology into risk management processes
- Case Study: Implementation of supply chain monitoring software

Module 7: Physical Security and Infrastructure Protection

- Securing facilities and critical assets
- Access control and perimeter protection measures
- Emergency response for physical threats
- Integration with cybersecurity and operational plans
- Employee training and awareness programs
- Case Study: Securing a critical manufacturing site

Module 8: Performance Measurement and Continuous Improvement

- Resilience metrics and KPIs for defense supply chains
- Continuous monitoring and evaluation approaches
- Lessons learned and feedback integration
- Benchmarking against best practices
- Developing improvement roadmaps for supply chain security
- Case Study: KPI-driven improvement program in defense operations

Training Methodology

- Instructor-led presentations and discussions
- Interactive scenario-based exercises and simulations
- Case study analysis of real-world supply chain disruptions
- Group work and problem-solving workshops
- Hands-on tools for risk assessment and monitoring
- Continuous feedback, reflection sessions, and action planning

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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