Aviation Cyber-Physical Security Training Course

Professional Development Training Course Outline

Category	Aviation and Airport Management	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Aviation Cyber-Physical Security Training Course equips aviation professionals with advanced knowledge and practical skills to protect airports, airlines, air traffic management systems, and critical aviation infrastructure from evolving cyber-physical threats. As digital transformation, smart airports, Industrial Control Systems (ICS), Operational Technology (OT), Internet of Things (IoT), Artificial Intelligence (AI), cloud computing, and connected aviation ecosystems become standard, organizations require resilient cybersecurity strategies that integrate physical security, risk management, threat intelligence, regulatory compliance, and operational resilience. This course emphasizes global best practices, cyber resilience, digital transformation, zero-trust architecture, incident response, and secure aviation operations while supporting ICAO standards and international cybersecurity frameworks.

Participants will explore emerging cyber risks affecting airport operations, baggage handling systems, biometric technologies, air navigation services, aviation communication systems, unmanned aircraft integration, and smart infrastructure. Through practical exercises and international case studies, learners will strengthen capabilities in cyber risk assessment, vulnerability management, security governance, crisis management, business continuity, digital forensics, threat detection, and coordinated incident response to ensure safe, secure, and resilient aviation operations in an increasingly connected global environment.

Programme Curriculum

Aviation Cyber-Physical Security Training Course

Introduction

Aviation Cyber-Physical Security Training Course equips aviation professionals with advanced knowledge and practical skills to protect airports, airlines, air traffic management systems, and critical aviation infrastructure from evolving cyber-physical threats. As digital transformation, smart airports, Industrial Control Systems (ICS),

Operational Technology (OT), Internet of Things (IoT), Artificial Intelligence (AI), cloud computing, and connected aviation ecosystems become standard, organizations require resilient cybersecurity strategies that integrate physical security, risk management, threat intelligence, regulatory compliance, and operational resilience. This course emphasizes global best practices, cyber resilience, digital transformation, zero-trust architecture, incident response, and secure aviation operations while supporting ICAO standards and international cybersecurity frameworks.

Participants will explore emerging cyber risks affecting airport operations, baggage handling systems, biometric technologies, air navigation services, aviation communication systems, unmanned aircraft integration, and smart infrastructure. Through practical exercises and international case studies, learners will strengthen capabilities in cyber risk assessment, vulnerability management, security governance, crisis management, business continuity, digital forensics, threat detection, and coordinated incident response to ensure safe, secure, and resilient aviation operations in an increasingly connected global environment.

Course Objectives

By the end of this course, participants will be able to:

1. Understand aviation cyber-physical security principles.
2. Identify emerging cyber threats affecting aviation infrastructure.
3. Conduct comprehensive cyber risk assessments.
4. Strengthen Operational Technology (OT) and ICS security.
5. Secure airport IoT and smart infrastructure.
6. Implement Zero Trust cybersecurity frameworks.
7. Improve cyber incident response capabilities.
8. Apply aviation cybersecurity governance standards.
9. Protect aviation communication and navigation systems.
10. Enhance digital resilience and business continuity.
11. Utilize cyber threat intelligence for proactive defense.
12. Develop integrated cyber-physical security strategies.
13. Promote regulatory compliance and organizational resilience.

Organizational Benefits

- Strengthened aviation cybersecurity posture.
- Reduced cyber and operational risks.
- Improved regulatory compliance.
- Enhanced resilience of critical infrastructure.
- Faster incident detection and response.
- Better protection of passenger information.
- Increased operational continuity.
- Stronger stakeholder confidence.
- Improved cross-functional security coordination.
- Greater organizational preparedness against emerging threats.

Target Audiences

- Airport Security Managers
- Airport Operations Managers
- Aviation Safety Officers
- IT and Cybersecurity Professionals
- Air Traffic Management Personnel
- Airline Security Teams
- Critical Infrastructure Managers
- Government Aviation Regulators

Course Duration: 5 days

Course Modules

Module 1: Aviation Cyber-Physical Security Fundamentals

- Aviation cyber-physical security concepts
- Aviation threat landscape
- Critical aviation infrastructure
- Cybersecurity governance principles
- Global aviation security standards
- Case Study: Heathrow Airport cyber resilience initiatives

Module 2: Cyber Risk Assessment and Threat Management

- Cyber risk identification
- Vulnerability assessment techniques
- Threat intelligence integration
- Risk mitigation planning
- Cybersecurity maturity assessment
- Case Study: Colonial Pipeline cyberattack lessons for critical infrastructure

Module 3: Protecting Airport Operational Technology

- Industrial Control Systems security
- SCADA protection strategies
- Airport automation security
- Secure network architecture
- OT vulnerability management
- Case Study: Ukraine power grid cyberattack implications for airport operations

Module 4: Smart Airports and IoT Security

- Smart airport technologies

- IoT device protection
- Biometric security systems
- Cloud security integration
- AI-enabled threat detection
- Case Study: Singapore Changi Airport smart security implementation

Module 5: Incident Response and Digital Resilience

- Cyber incident response planning
- Digital forensics fundamentals
- Business continuity planning
- Disaster recovery strategies
- Crisis communication management
- Case Study: Maersk NotPetya recovery lessons for aviation resilience

Module 6: Aviation Communication and Navigation Security

- Air traffic communication security
- Navigation system protection
- Satellite communication security
- Data integrity assurance
- Secure aviation information exchange
- Case Study: FAA cybersecurity modernization initiatives

Module 7: Governance, Compliance and Security Leadership

- ICAO cybersecurity guidance
- ISO 27001 implementation
- Regulatory compliance management
- Security auditing techniques
- Security awareness culture
- Case Study: European Aviation cybersecurity governance framework

Module 8: Future Aviation Cybersecurity Strategies

- Artificial Intelligence security
- Quantum computing implications
- Emerging cyber threats
- Zero Trust implementation roadmap
- Continuous security improvement
- Case Study: Dubai International Airport digital transformation security practices

Training Methodology

- Interactive expert-led presentations
- Practical aviation cybersecurity simulations
- Hands-on cyber risk assessment exercises
- International aviation case study discussions
- Group workshops and collaborative learning
- Incident response tabletop exercises
- Security policy development activities
- Digital resilience planning sessions
- Knowledge assessments and feedback
- Action planning for workplace implementation

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