Vital Installations and Buildings Security – IAOSHE Certification

4 – 15 January 2027
London (UK)



Vital Installations and Buildings Security – IAOSHE Certification

Ref: 3254923_326023 **Date:** 4 – 15 January 2027 **Location:** London (UK) **Fees:** 11000 GBP

Introduction

In a world of increasing threats to critical infrastructure and sensitive facilities, ensuring the security of vital installations is more important than ever. This comprehensive course—Vital Installations and Buildings Security - IAOSHE Certification—equips security managers, safety officers, and facility managers with the skills and knowledge to assess threats, implement robust physical and procedural security measures, and respond effectively to incidents.

Drawing on international best practices and aligned with regulatory standards such as ISO 31000 and ASIS guidelines, this program combines practical strategies and real-world scenarios to build a complete security management plan for safeguarding high-risk and high-value sites.

Course Objectives

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

- Identify and assess potential threats to vital installations and critical infrastructure.
- Design and implement physical security and procedural security measures tailored to site-specific risks.
- Understand and apply modern technologies for intrusion detection and surveillance.
- Coordinate incident response with internal stakeholders and emergency services.
- Develop and manage a comprehensive security management plan that aligns with organizational goals and industry standards.

Course Outlines

Day 1: Introduction to Critical Infrastructure Security

- Definition and types of vital installations and critical infrastructure.
- Internal vs external threat landscape.
- Conducting a site-specific risk analysis.
- Overview of regulatory standards ISO 31000, ASIS, etc..
- Role and responsibilities of the security officer in infrastructure protection.



Day 2: Risk Assessment and Vulnerability Analysis

- Components of threat, vulnerability, and consequence assessment.
- Using risk matrices and prioritization techniques.
- Conducting security audits and site surveys.
- Case studies of past security breaches and lessons learned.
- Developing a threat profile for installations.

Day 3: Perimeter and Physical Security Controls

- Physical security design principles.
- Barriers: fencing, gates, bollards, barriers.
- Entry/exit systems, airlocks, and control points.
- Enhancing lighting, signage, and access control zones.
- Anti-vehicle and anti-intrusion technologies.

Day 4: Access Control and Identity Management

- Access control systems: keycards, biometrics, smart systems.
- Managing visitors and contractors securely.
- Role-based access and zoning policies.
- Physical controls: turnstiles, mantraps, door security.
- Common access control failures and mitigation strategies.

Day 5: Surveillance and Monitoring Systems

- Best practices in CCTV planning and placement.
- Camera types: PTZ, thermal, infrared, AI-powered.
- Integrating surveillance with alarm systems and access control.
- Control rooms and centralized monitoring strategies.
- Using video analytics and intelligent threat detection.

Day 6: Emergency Response and Incident Management

- Developing and coordinating emergency response plans.
- Protocols for fire, bomb threats, and sabotage.
- Incident reporting and escalation procedures.
- Roles of private security, police, and civil defense agencies.
- Conducting tabletop exercises and communication planning.



Day 7: Cybersecurity for Physical Infrastructure

- Convergence of cybersecurity and physical security.
- Common vulnerabilities in building automation and control systems.
- Securing SCADA and access control networks.
- Conducting awareness training for staff and contractors.
- Coordinating with IT and cybersecurity teams.

Day 8: Human Factor and Insider Threat Mitigation

- Screening and vetting employees and contractors.
- Monitoring employee behavior and reporting suspicious activities.
- Promoting ethics and whistleblowing channels.
- Training staff in security awareness.
- Real-life insider threat examples and mitigation tactics.

Day 9: Security Planning and Documentation

- Developing a site-specific security plan.
- Writing policies, SOPs, and emergency procedures.
- Integrating security with health, safety, and fire regulations.
- Defining roles and responsibilities of security personnel.
- Collaboration with facility managers and risk managers.

Day 10: Case Studies, Drills, and Wrap-Up

- Reviewing global incidents at vital installations.
- Group project: designing a security plan for a sensitive facility.
- Conducting drills and simulations for emergency preparedness.
- Open discussion of challenges, best practices, and next steps.
- Certificate presentation and closing session.



Why Attend This Course: Wins & Losses!

- Acquire actionable knowledge: Learn how to identify, assess, and mitigate threats to vital installations.
- Boost your practical skills: Hands-on exercises to implement robust physical security and access control measures.
- Leverage modern technologies: Explore the latest intrusion detection and surveillance tools for site protection.
- Enhance coordination: Master effective incident response in collaboration with emergency services and internal stakeholders.
- Develop a comprehensive plan: Create a security management plan aligned with international standards like ISO 31000.
- Learn from real-world scenarios: Case studies and drills to test your readiness.
- Build your professional credibility: Earn a recognized IAOSHE certification to advance your career.
- Prepare for evolving risks: Stay ahead in securing critical infrastructure and sensitive facilities in a changing threat landscape.

Conclusion

Protecting vital installations and sensitive facilities is crucial to maintaining business continuity and public safety. This IAOSHE-certified course provides the skills and confidence to design, implement, and manage a holistic security management plan.

Whether you're a security manager, facility leader, or responsible for safeguarding critical infrastructure, this program equips you to respond to today's challenges and anticipate future threats. Start your journey now to build a safer, more resilient organization!

