Integrated Security Systems Management and Administration Training Course



21 - 25 Dec 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM4868_131883

Course Introduction / Overview:

In today's complex threat landscape, a siloed approach to security is no longer viable. This course provides a comprehensive framework for managing and administering modern integrated security systems, where physical security technologies and cybersecurity protocols converge. Participants will explore the entire lifecycle of security systems, from initial risk assessment and design to implementation, operation, and future-proofing. The curriculum delves into the critical interplay between access control, video surveillance, intrusion detection, and information management platforms. As discussed by security expert Martin Gill in his seminal work, "The Handbook of Security," effective security management requires a holistic understanding of both technology and human factors. This principle is central to the training provided by BIG BEN Training Center. We move beyond simple technical training to foster strategic thinking, enabling participants to build resilient, intelligent, and cohesive security ecosystems that protect assets, people, and information effectively. This course is designed to equip professionals with the advanced skills needed to lead security integration projects and manage sophisticated security operations centers with confidence and foresight.

Target Audience / This training course is suitable for:

- Security Managers and Directors.
- IT Security Professionals.
- Facility and Building Managers.
- Security System Integrators and Installers.
- Corporate Security Personnel.
- Law Enforcement and Government Security Officials.
- Security Consultants and Advisors.
- Risk and Compliance Managers.
- Project Managers overseeing security installations.
- Operations Managers with security responsibilities.

Target Sectors and Industries:

- Banking and Financial Services.
- Critical Infrastructure and Utilities.
- Transportation and Logistics, including airports and seaports.
- Government, Public Sector, and Defense Agencies.
- Healthcare and Pharmaceutical.
- Corporate and Commercial Real Estate.
- Retail and Hospitality.
- Education and University Campuses.
- Telecommunications and Data Centers.
- Manufacturing and Industrial Facilities.

Target Organizations Departments:

- Corporate Security Department.
- Information Technology (IT) and Cybersecurity Department.
- Facilities Management.
- Operations and Logistics.
- Risk Management and Compliance.
- Physical Security and Asset Protection.
- Health, Safety, and Environment (HSE).
- Internal Audit and Investigations.
- Human Resources.
- Project Management Office (PMO).

Course Offerings:

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

- Develop a comprehensive strategy for integrating disparate security systems.
- Conduct thorough security risk assessments to inform system design and policy.
- Evaluate, select, and procure appropriate security technologies for specific needs.
- Manage the full project lifecycle of a security system implementation from start to finish.
- Administer advanced access control systems and video management systems (VMS).
- Create and implement effective Standard Operating Procedures (SOPs) for security operations.
- Understand the convergence of physical security and cybersecurity and mitigate associated risks.
- Operate and leverage Physical Security Information Management (PSIM) platforms.
- Plan for system maintenance, upgrades, and technology lifecycle management.
- Ensure security systems comply with relevant data privacy and industry regulations.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive. We believe that adult learning is most effective when it combines expert knowledge with hands-on application. This course moves beyond traditional lectures to include a dynamic blend of training techniques. Participants will engage in detailed case study analyses of real-world security integration projects, dissecting both successes and failures to draw actionable insights. Facilitated group discussions and brainstorming sessions encourage peer-to-peer learning and the sharing of diverse industry experiences. A significant portion of the course is dedicated to practical exercises and simulations, where participants will work in teams to design a security system for a model facility, develop an incident response plan, and configure key parameters in a mock management platform. Our expert instructors provide continuous guidance and personalized feedback, ensuring that theoretical concepts are firmly grounded in practical, real-world application. This approach guarantees that participants leave not just with knowledge, but with the confidence and skills to implement what they have learned immediately in their professional roles.

Course Agenda (Course Units):

Unit One: Foundations of Integrated Security Management

- The evolution from siloed to integrated security systems.
- Core components: Access Control, CCTV, Intrusion Detection, and Alarms.
- Understanding the convergence of physical and cybersecurity.
- Benefits and challenges of security system integration.
- Key industry standards and protocols (e.g., ONVIF).
- The role of the Security Operations Center (SOC) in an integrated environment.
- Fundamental principles of security risk assessment.

Unit Two: Security System Design and Technology Evaluation

- Conducting a comprehensive site survey and needs analysis.
- Developing a security operational requirement (OR).
- Principles of Crime Prevention Through Environmental Design (CPTED).
- Designing a multi-layered security architecture.
- Evaluating and comparing different security technologies and vendors.
- Understanding Video Management Systems (VMS) and their capabilities.
- Introduction to Physical Security Information Management (PSIM) platforms.

Unit Three: Project Management for Security System Implementation

- The security project management lifecycle.
- Defining project scope, budget, and timelines.
- Stakeholder management and communication planning.
- Managing vendors and system integrators effectively.
- Best practices for system installation, cabling, and configuration.
- System commissioning, testing, and acceptance procedures.
- Developing comprehensive user training and documentation.

Unit Four: Administration and Operation of Integrated Systems

- Developing and implementing Standard Operating Procedures (SOPs).
- User and credential management for access control systems.
- Effective video surveillance monitoring and evidence handling.
- Alarm management, verification, and response protocols.
- Managing system health, diagnostics, and preventative maintenance.
- Generating and analyzing security reports and metrics.
- Conducting drills and exercises for incident response readiness.

Unit Five: Advanced Topics and Future Trends in Security

- Cybersecurity for physical security devices and networks.
- Integrating IoT devices and sensors into the security ecosystem.
- The role of Artificial Intelligence (AI) and video analytics.
- Cloud-based security solutions (VSaaS and ACaaS).
- Compliance with data privacy regulations like GDPR.
- Developing a long-term security technology roadmap.
- Crisis management and business continuity planning.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As AI and machine learning become more integrated into security systems, how can organizations balance the benefits of predictive analytics with the ethical implications of constant surveillance and potential algorithmic bias?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by adopting a holistic, strategic management perspective rather than focusing solely on the technical configuration of individual devices. While many programs teach how to operate a camera or a door controller, we teach how to build, manage, and lead a cohesive security ecosystem. Our curriculum is uniquely structured around the complete project and operational lifecycle, bridging the critical gap between IT, physical security, and facilities management. We place a strong emphasis on the convergence of cyber and physical security, a crucial and often overlooked area that is paramount in today's threat environment. The course content is forward-looking, preparing participants not just for current challenges but also for future trends like IoT integration, AI-driven analytics, and cloud-based security platforms. By integrating principles from risk management, project management, and operational best practices, we provide a multi-disciplinary skill set. Participants leave with the ability to think strategically, justify security investments to senior leadership, and manage the complex interplay of technology, people, and processes that defines modern security excellence.