# Comprehensive Security Risk and Mitigation Strategies Training Course



21 - 25 Dec 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM1230_132585

## Course Introduction / Overview:

In today's interconnected and dynamic environment, the ability to proactively identify, assess, and mitigate security risks is no longer a specialized function but a core business necessity. This course provides a comprehensive framework for mastering security risk assessment and developing robust mitigation strategies that protect organizational assets, ensure operational continuity, and maintain stakeholder confidence. Drawing upon established principles outlined in seminal works like "The Security Risk Assessment Handbook" by Douglas J. Landoll, this program moves beyond theoretical concepts to deliver practical, actionable skills. Participants will delve into the complete risk management lifecycle, from initial asset identification and threat modeling to the implementation and monitoring of effective security controls. BIG BEN Training Center has designed this immersive experience to equip professionals with the methodologies needed to conduct thorough vulnerability assessments, perform both qualitative and quantitative risk analysis, and align security initiatives with strategic business objectives. This training course is essential for building a resilient security posture capable of withstanding the complex and evolving threats facing modern organizations.

## Target Audience / This training course is suitable for:

- Security Managers and Directors.
- IT Professionals and System Administrators.
- Risk Analysts and Compliance Officers.
- Corporate Security Personnel.
- Facility and Operations Managers.
- Business Continuity and Disaster Recovery Planners.
- Internal and External Auditors.
- Project Managers responsible for security-sensitive projects.
- Law Enforcement and Government Security Officials.
- Consultants specializing in security and risk management.

## Target Sectors and Industries:

- Financial Services and Banking.
- Information Technology and Telecommunications.
- Healthcare and Pharmaceuticals.
- Government Agencies and Public Sector Bodies.
- Critical Infrastructure including Energy and Utilities.
- Retail and E-commerce.
- Manufacturing and Supply Chain Logistics.
- Transportation and Aviation.
- Education and Research Institutions.
- Hospitality and Entertainment.

## Target Organizations Departments:

- Corporate Security Department.
- Information Technology (IT) and Cybersecurity.
- Risk Management and Strategy.
- Compliance and Legal Affairs.
- Operations and Facilities Management.
- Internal Audit and Assurance.
- Human Resources.
- Procurement and Supply Chain Management.
- Finance and Asset Management.

## Course Offerings:

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

- Conduct comprehensive security risk assessments using industry-standard frameworks.
- Identify, classify, and valuate critical organizational assets.
- Analyze and model potential threats from various internal and external sources.
- Perform systematic vulnerability assessments across physical, technical, and administrative domains.
- Apply both qualitative and quantitative methods for risk analysis and prioritization.
- Develop and evaluate effective risk mitigation and treatment strategies.
- Design and implement appropriate security controls to reduce risk to acceptable levels.
- Create robust incident response and business continuity plans.
- Establish metrics for monitoring security performance and reporting to senior management.
- Foster a proactive, risk-aware culture within their organization.

## Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, practical, and engaging, ensuring that participants can immediately apply the learned concepts in their professional roles. We move beyond traditional lectures by integrating a dynamic blend of expert-led presentations, real-world case study analyses, and collaborative group workshops. Participants will actively engage in hands-on exercises, such as conducting a mock risk assessment on a hypothetical organization, developing a risk treatment plan, and participating in incident response simulations. These practical sessions are designed to reinforce theoretical knowledge and build tangible skills. Facilitated discussions and peer-to-peer learning are central to our approach, allowing attendees to share experiences and gain diverse perspectives on security challenges. Continuous feedback is provided by the instructor throughout the course to guide learning and ensure a deep understanding of the material. This immersive, application-focused methodology guarantees that participants leave with not just knowledge, but also the confidence and competence to implement effective security risk management programs.

## Course Agenda (Course Units):

### Unit One: Foundations of Security Risk Management

- Introduction to Security Risk Management Concepts.
- Key Terminology. Threats, Vulnerabilities, Risks, and Controls.
- The Importance of a Proactive Security Posture.
- Overview of International Standards and Frameworks (ISO 31000, ISO 27005, NIST SP 800-30).
- The Risk Management Lifecycle.
- Defining Risk Appetite and Tolerance.
- Legal, Regulatory, and Compliance Considerations.

### Unit Two: The Comprehensive Risk Assessment Process

- Phase 1. Context Establishment and Scoping the Assessment.
- Phase 2. Asset Identification, Classification, and Valuation.
- Phase 3. Threat Source Identification and Threat Modeling.
- Phase 4. Vulnerability Identification and Analysis.
- Techniques for Information Gathering. Interviews, Surveys, and Document Review.
- Physical Security Assessments.
- Cybersecurity and Technical Vulnerability Scans.

### Unit Three: Qualitative and Quantitative Risk Analysis Techniques

- Understanding the Difference Between Qualitative and Quantitative Analysis.
- Qualitative Analysis Methods. Risk Matrices, Heat Maps, and Ordinal Scales.
- Conducting Impact and Likelihood Assessments.
- Prioritizing Risks Based on Qualitative Data.
- Quantitative Analysis Methods. Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE).
- Calculating Return on Security Investment (ROSI).
- Integrating Both Approaches for a Hybrid Risk Analysis.

## Unit Four: Developing and Implementing Mitigation Strategies

- The Four Risk Treatment Strategies. Avoidance, Transference, Mitigation, and Acceptance.
- Selecting and Designing Security Controls.
- Administrative, Technical, and Physical Controls.
- Developing a Risk Treatment Plan.
- Aligning Mitigation Strategies with Business Objectives.
- Cost-Benefit Analysis of Proposed Controls.
- Communicating the Mitigation Plan to Stakeholders.

## Unit Five: Reporting, Monitoring, and Continuous Improvement

- Documenting the Risk Assessment Findings and Recommendations.
- Creating a Formal Risk Assessment Report.
- Presenting Risk Data to Senior Management and Decision-Makers.
- Developing Key Risk Indicators (KRIs) and Security Metrics.
- Establishing a Continuous Monitoring Program.
- The Role of Security Audits and Reviews.
- Integrating Risk Management into the Organizational Culture.

# 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:

In an era of constantly evolving cyber and physical threats, how can an organization balance proactive risk mitigation with the need for operational agility and innovation?

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

This course distinguishes itself by offering a holistic and integrated perspective on security risk management, seamlessly blending the domains of physical, cyber, and operational security into a unified framework. Unlike programs that focus narrowly on a single aspect, our curriculum emphasizes the interconnectedness of threats and the need for a comprehensive, multi-layered defense strategy. We prioritize practical application over abstract theory, dedicating significant time to hands-on workshops, simulations, and case studies drawn from recent, real-world security incidents. This approach ensures participants develop tangible skills in conducting assessments and creating actionable mitigation plans. Furthermore, the course places a strong emphasis on the strategic dimension of risk management, teaching participants how to communicate risk in business terms and align security initiatives with overarching organizational goals. The focus is not just on identifying risks, but on developing the critical thinking and decision-making capabilities required to manage them effectively, fostering a proactive and resilient security culture that becomes a competitive advantage rather than just a cost center.