Strategic Corporate Security and Risk Management Training Course



21 - 25 Dec 2026

Cape town

4600 € (Per Person)

Ref: #SM3586_282180

Course Introduction / Overview:

This advanced training course is designed for executives and senior leaders tasked with protecting corporate assets, personnel, and reputation in a complex global landscape. The curriculum moves beyond traditional security protocols to instill a strategic, forward-thinking mindset essential for modern leadership. Participants will delve into the principles of Enterprise Security Risk Management (ESRM), learning to align security functions directly with overarching business objectives to create value and resilience. Drawing on concepts from seminal works like Philip P. Purpura's "Security and Loss Prevention: An Introduction," the course emphasizes a proactive, intelligence-led approach to threat mitigation. We will explore the convergence of physical and cybersecurity, the psychology of insider threats, and the leadership required to navigate high-stakes crises. At BIG BEN Training Center, our focus is on empowering leaders to build a robust security culture, make informed decisions based on comprehensive risk analysis, and effectively manage resources to counter emerging threats. This program equips executives with the strategic acumen to transform the security department from a cost center into a vital business enabler, safeguarding the organization's future growth and stability.

Target Audience / This training course is suitable for:

- Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs).
- C-Suite Executives (CEOs, COOs, CFOs).
- Vice Presidents and Directors of Security and Risk Management.
- Senior managers with responsibility for corporate security or asset protection.
- Heads of business continuity and crisis management teams.
- Legal and compliance executives.
- Operations directors and senior facility managers.
- Board members involved in risk and governance oversight.

Target Sectors and Industries:

- Financial services and banking.
- Technology, data centers, and telecommunications.
- Critical infrastructure including energy, oil and gas, and utilities.
- Healthcare and pharmaceutical.
- Manufacturing and industrial supply chains.
- Retail and consumer goods.
- Transportation and logistics.
- Government agencies and public sector organizations.
- Hospitality and large-scale event management.

Target Organizations Departments:

- Corporate Security and Asset Protection.
- Executive Management and Leadership.
- Risk Management and Compliance.
- Legal and General Counsel.
- Operations and Facilities Management.
- Human Resources.
- Information Technology (IT) and Cybersecurity.
- Internal Audit.
- Business Continuity and Crisis Management.

Course Offerings:

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

- Develop and implement a comprehensive Enterprise Security Risk Management (ESRM) framework.
- Align security strategies with core business objectives and executive-level priorities.
- Conduct sophisticated threat intelligence analysis and vulnerability assessments.
- Lead and manage effective crisis management and incident response protocols.
- Integrate physical security, personnel security, and cybersecurity into a converged program.
- Master the principles of security budgeting, resource allocation, and demonstrating ROI.
- Design and champion a proactive corporate security culture across the organization.
- Evaluate and leverage emerging security technologies and innovations strategically.
- Develop robust policies for workplace violence prevention and insider threat mitigation.
- Enhance personal leadership and communication skills for high-stakes security situations.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and directly applicable to the challenges faced by senior leaders. This course eschews traditional lecture-based formats in favor of a dynamic learning environment centered on executive-level problem-solving. A significant portion of the program is dedicated to analyzing real-world case studies of corporate security failures and successes, allowing participants to deconstruct complex scenarios and strategic decisions. Facilitated group discussions and peer-to-peer brainstorming sessions encourage the sharing of diverse experiences and perspectives. The course features sophisticated, interactive simulations of crisis events, such as data breaches, physical security threats, or supply chain disruptions, requiring participants to make critical decisions under pressure. Expert-led presentations will introduce cutting-edge frameworks and strategic models, which are then immediately applied in practical workshops. Participants will receive continuous feedback from instructors and peers, ensuring that the learned concepts are translated into actionable strategies they can implement within their own organizations. This hands-on, collaborative approach ensures a deep and lasting understanding of strategic corporate security management.

Course Agenda (Course Units):

Unit One The Strategic Framework of Corporate Security

- Foundations of modern corporate security management.
- Understanding the Enterprise Security Risk Management (ESRM) model.
- Aligning security initiatives with corporate strategy and business goals.
- The role of the executive in security governance and oversight.
- Legal, regulatory, and ethical considerations in corporate security.
- Developing a comprehensive security policy and procedure framework.
- Key performance indicators (KPIs) and metrics for security effectiveness.

Unit Two Advanced Threat and Risk Assessment

- Methodologies for comprehensive security risk assessments.
- Conducting vulnerability analysis for physical and digital assets.
- The intelligence cycle and its application in a corporate context.
- Identifying and analyzing internal and external threats.
- Understanding the convergence of physical and cyber threat landscapes.
- Techniques for supply chain and third-party risk management.
- Introduction to protective intelligence for executive protection.

Unit Three Integrating Physical, Technical, and Cyber Security

- Principles of layered security and Crime Prevention Through Environmental Design (CPTED).
- Advanced access control and surveillance technologies.
- Cybersecurity fundamentals for non-technical executives.
- Strategies for protecting intellectual property and sensitive data.
- Developing a robust insider threat mitigation program.
- Managing travel security and duty of care for a global workforce.
- Evaluating and implementing new security technologies and systems.

Unit Four Executive Leadership in Crisis Management and Business Continuity

- Developing a proactive crisis management and incident response plan.
- Leading a crisis management team during a critical event.
- Strategic communication with stakeholders, media, and employees.
- Fundamentals of Business Continuity Planning (BCP) and disaster recovery.
- Conducting effective post-incident reviews and implementing lessons learned.
- Managing workplace violence prevention and response strategies.
- Simulation exercises for crisis decision-making.

Unit Five The Future of Security Leadership and Governance

- Building and sustaining a positive security culture throughout the organization.
- Mastering security budget development and demonstrating return on investment (ROI).
- Managing investigations and liaising with law enforcement.
- The impact of artificial intelligence and machine learning on corporate security.
- Addressing emerging threats such as corporate espionage and activism.
- Developing personal leadership and influence skills for security executives.
- Creating a strategic roadmap for the future of the security function.

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 converged physical and cyber threats, how can an executive leader champion a truly holistic security culture that transcends departmental silos?

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

This course distinguishes itself by focusing exclusively on the strategic, executive-level dimension of corporate security, a perspective often overlooked in technically-focused or operational training. Unlike programs that concentrate on specific tools or tactical procedures, our curriculum is engineered to cultivate the strategic mindset required to lead a security function as an integral part of the business. We emphasize the critical skill of aligning security initiatives with core business objectives, teaching participants how to articulate security's value in the language of the C-suite—risk reduction, business enablement, and return on investment. The content is built around advanced, interdisciplinary concepts like Enterprise Security Risk Management (ESRM) and the convergence of physical and cyber domains. A key differentiator is our heavy reliance on sophisticated, real-world case studies and crisis simulations that force participants to make high-stakes decisions, honing their leadership and judgment under pressure. The program is not about becoming a security technician; it is about becoming a security strategist and a trusted business advisor who can navigate complexity, govern risk, and build organizational resilience from the top down.