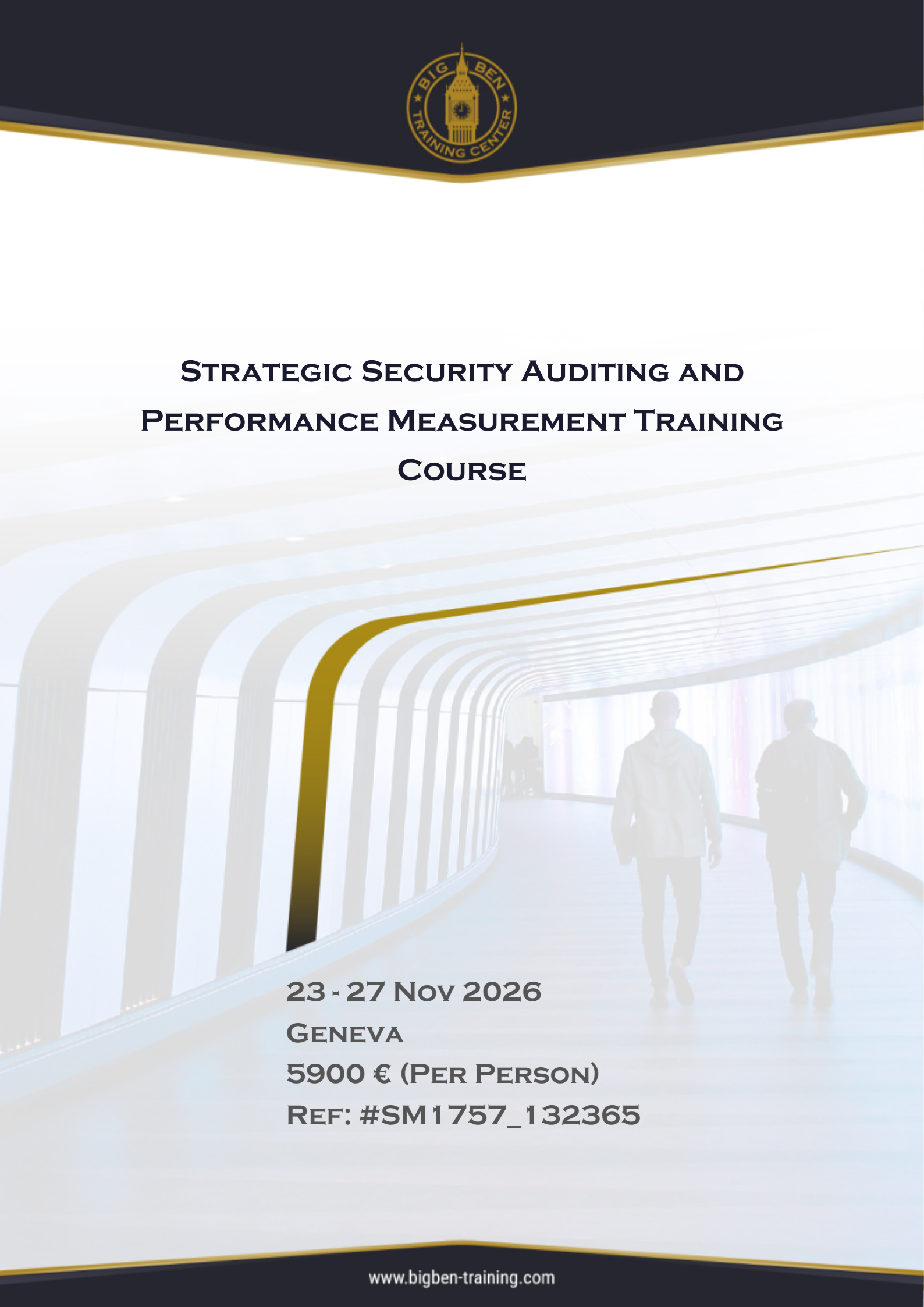
Strategic Security Auditing and Performance Measurement Training Course



23 - 27 Nov 2026

Geneva

5900 € (Per Person)

Ref: #SM1757_132365

Course Introduction / Overview:

In today's complex digital landscape, simply implementing security controls is no longer sufficient. Organizations must be able to verify their effectiveness and demonstrate value through rigorous security auditing and precise performance measurement. This course provides a comprehensive framework for mastering both disciplines, moving beyond simple compliance checklists to a strategic, data-driven approach to cybersecurity management. We will explore how to design, execute, and report on security audits that provide meaningful insights into an organization's risk posture. Drawing on principles from leading frameworks and the work of figures like Ron Ross, a key architect of the NIST Risk Management Framework, participants will learn to translate technical findings into business-relevant metrics. This program, offered by BIG BEN Training Center, delves into the methodologies outlined in seminal works like "Security Metrics: A Beginner's Guide," equipping professionals to not only identify vulnerabilities but also to measure the performance of their security programs over time. This training is essential for building a resilient and accountable security function that can effectively communicate its value and drive continuous improvement across the enterprise.

Target Audience / This training course is suitable for:

- Information Security Professionals.
- IT Auditors and Internal Auditors.
- Compliance and Risk Managers.
- IT Managers and Team Leaders.
- Security Analysts and Consultants.
- System and Network Administrators.
- Professionals preparing for security audit certifications.
- Anyone responsible for cybersecurity governance and oversight.

Target Sectors and Industries:

- Banking and Financial Services.
- Healthcare and Pharmaceuticals.
- Information Technology and Telecommunications.
- Government and Public Sector Agencies.
- Energy, Oil, and Gas.
- Retail and E-commerce.
- Consulting and Professional Services.
- Manufacturing and Industrial Control Systems.

Target Organizations Departments:

- Internal Audit Department.
- Information Security and Cybersecurity Department.
- Information Technology Operations.
- Risk Management Department.
- Legal and Compliance Department.
- Governance and Corporate Strategy.
- Finance and Operations.

Course Offerings:

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

- Develop a comprehensive security audit plan based on risk assessment and business objectives.
- Master various auditing techniques, including technical testing and policy review.
- Effectively collect, manage, and analyze audit evidence to support findings.
- Design and implement a security performance measurement program using relevant KPIs and KRIs.
- Align security metrics with internationally recognized frameworks like NIST and ISO 27001.
- Create compelling audit reports and performance dashboards for executive leadership.
- Communicate the business value and ROI of the security program to key stakeholders.
- Facilitate a culture of continuous security improvement through data-driven insights.

Course Methodology:

This training course employs a dynamic and interactive learning methodology designed to foster practical skills and deep understanding. The approach at BIG BEN Training Center is centered on participant engagement, moving beyond traditional lectures to a hands-on, workshop-style environment. Each session combines expert-led instruction with real-world case studies, allowing participants to analyze complex security audit scenarios and performance measurement challenges. A significant portion of the training is dedicated to collaborative group exercises and simulations where attendees will work together to scope an audit, develop security KPIs, and draft an audit report. These activities are designed to reinforce theoretical concepts and build practical problem-solving abilities. Throughout the course, there will be ample opportunity for open discussions, Q&A sessions, and peer-to-peer knowledge sharing. Participants will receive continuous feedback from the instructor, ensuring they can apply the learned techniques and frameworks directly to their own organizational context upon completion of the course.

Course Agenda (Course Units):

Unit One Foundations of Security Auditing and Governance

- Introduction to Security Auditing Principles.
- The Role of Auditing in Governance, Risk, and Compliance (GRC).
- Key Differences Between Audits, Assessments, and Tests.
- Understanding Major Security Frameworks (NIST CSF, ISO 27001, COBIT).
- The Legal, Ethical, and Professional Responsibilities of an Auditor.
- Defining Audit Scope and Objectives.
- Stakeholder Management and Communication in the Audit Process.

Unit Two The Security Audit Lifecycle in Practice

- Phase 1: Planning and Preparation for a Security Audit.
- Phase 2: Conducting Fieldwork and Gathering Evidence.
- Techniques for Evidence Collection (Interviews, Observation, Documentation Review).
- Sampling Methodologies for Effective Auditing.
- Assessing the Design and Effectiveness of Security Controls.
- Documenting Workpapers and Audit Trails.
- Managing the Audit Project and Team.

Unit Three Technical Auditing and Control Assessment

- Auditing Network Infrastructure and Firewalls.
- Assessing Identity and Access Management (IAM) Controls.
- Reviewing Application Security and Secure SDLC Practices.
- Auditing Cloud Security Environments (IaaS, PaaS, SaaS).
- Vulnerability Assessment and Penetration Testing for Auditors.
- Log Management and Security Information and Event Management (SIEM) Auditing.
- Evaluating Physical and Environmental Security Controls.

Unit Four Security Performance Measurement and Metrics

- Introduction to Security Performance Measurement.
- Developing Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs).
- The GQM (Goal, Question, Metric) Approach to Metric Development.
- Measuring the Effectiveness of Security Controls.
- Creating and Maintaining Security Performance Dashboards.
- Quantifying Security Risk and Calculating Security ROI.
- Benchmarking Performance Against Industry Standards.

Unit Five Reporting, Remediation, and Continuous Improvement

- Structuring and Writing an Effective Audit Report.
- Communicating Findings to Technical and Executive Audiences.
- Developing Actionable Recommendations for Remediation.
- The Audit Follow-Up and Remediation Tracking Process.
- Integrating Audit Findings into the Risk Management Lifecycle.
- Establishing a Continuous Auditing and Monitoring Program.
- The Future of Security Auditing: Automation and AI.

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:

How can an organization effectively measure the human element of its security posture, and can these qualitative aspects ever be fully represented by quantitative performance metrics?

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

This training course distinguishes itself by uniquely integrating the distinct but interconnected disciplines of security auditing and performance measurement into a single, cohesive curriculum. While many programs focus solely on the procedural aspects of conducting an audit, this course goes a step further by dedicating significant attention to the science of security metrics. It teaches participants not just how to find a control deficiency, but how to measure its impact and track the performance of remediation efforts over time. The methodology is framework-agnostic, providing attendees with universal principles and techniques that can be applied across various environments, whether they use NIST, ISO, COBIT, or a hybrid model. Furthermore, the course places a strong emphasis on communication, equipping professionals with the skills to translate complex technical findings into the language of business risk and value. Rather than just focusing on tools, it builds strategic competence, enabling participants to design and manage a data-driven security assurance program that supports business objectives and fosters a culture of continuous improvement.