Integrated Security Audit and Compliance for Financial Institutions Training Course

18 - 22 May 2026

Milan

5700 € (Per Person)

Ref: #SM7682_475496

Course Introduction / Overview:

The financial sector is a top target for cyber threats and fraud, making robust security audits and compliance essential for protecting customer data and maintaining public trust. This training course provides a comprehensive framework for conducting security audits and ensuring compliance with the complex web of financial regulations. We will cover key standards like PCI DSS, GDPR, and other local and international requirements. Participants will learn how to plan an audit, identify vulnerabilities, and report findings to management and regulators. We will explore academic work by authors like Richard E. Cascarino, whose book Auditing Information Systems provides a foundational framework for understanding the process. The curriculum is designed to equip professionals with the knowledge to manage security risks, protect sensitive financial data, and maintain a strong compliance posture. BIG BEN Training Center is committed to providing a program that helps financial institutions navigate the complex landscape of security and compliance. By the end of this course, participants will be able to perform thorough security audits, minimize risks, and make sure their organization is prepared for any regulatory scrutiny.

Target Audience / This training course is suitable for:

- Security auditors and compliance officers.
- IT and cybersecurity managers.
- Internal and external auditors.
- Risk management professionals.
- Financial institution executives.
- Legal and regulatory affairs specialists.
- Data protection officers.

Target Sectors and Industries:

- Banking and finance.
- Investment and wealth management.
- Insurance.
- Fintech companies.
- Credit unions.
- Payment processors.
- Government agencies and their equivalents.

Target Organizations Departments:

- Internal Audit.
- Cybersecurity and Information Security.
- Risk and Compliance.
- Legal.
- IT Operations.
- Finance.
- Operations.

Course Offerings:

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

- Plan and conduct a comprehensive security audit.
- Identify and test for vulnerabilities in financial systems.
- Ensure compliance with key regulations like PCI DSS and GDPR.
- Develop a security audit report with actionable recommendations.
- Understand the legal and financial consequences of non-compliance.
- Use best practices for data protection and access control.
- Communicate audit findings to both technical and non-technical stakeholders.
- Implement a continuous monitoring program to maintain compliance.

Course Methodology:

This training course uses a mix of instructional and hands-on methods to make sure the content is engaging and practical for financial professionals. The program begins with instructor-led sessions that provide a clear understanding of the core principles of security auditing and financial compliance. A key component of our approach is the use of real-world case studies and examples of audit findings in financial institutions. Participants will analyze these scenarios to understand the risks and how to address them. We also use interactive workshops and group exercises where participants work together to plan and execute a mock security audit. This collaborative learning model encourages teamwork and allows participants to practice their decision-making skills under pressure. Instructors at BIG BEN Training Center are experienced professionals who provide continuous feedback and guidance throughout the course. Our goal is to prepare professionals to face the complex challenges of financial security and compliance. By focusing on practical, actionable knowledge, we are making sure that every participant leaves the course ready to protect their organization's assets and reputation.

Course Agenda (Course Units):

Unit One: The Foundation of Financial Security Audits.

- Understanding the purpose and scope of a security audit.
- The role of governance in audit and compliance.
- Key security risks in the financial sector.
- The difference between internal and external audits.
- Planning an audit: scope, resources, and timeline.

Unit Two: Regulatory and Legal Compliance.

- An overview of key financial regulations.
- Understanding PCI DSS requirements.
- The impact of GDPR on financial data.
- Compliance with local and international laws.
- The legal implications of non-compliance.

Unit Three: Audit Methodologies and Vulnerability Testing.

- The steps of a security audit.
- Technical testing: vulnerability scanning and penetration testing.
- The importance of physical security audits.
- Auditing access control and identity management systems.
- Social engineering and human factors in security.

Unit Four: Data Protection and Privacy.

- Data classification and protection.
- Secure data storage and transmission.
- The principles of data privacy by design.
- Auditing controls for sensitive financial data.
- The process of a privacy impact assessment.

Unit Five: Reporting, Remediation, and Continuous Monitoring.

- Writing a comprehensive security audit report.
- Presenting findings to stakeholders.
- Developing a remediation plan.
- The importance of continuous monitoring.
- The future of security auditing in finance.

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 financial institutions effectively integrate the findings of security audits into their daily operations and business strategy, moving beyond a one-time compliance check to a culture of proactive and continuous security improvement?

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

This training course is unique because it provides an integrated approach to security auditing and regulatory compliance specifically for the financial sector. While many audit courses exist, they often don't address the unique and complex web of regulations that financial institutions must follow. Our program bridges the gap between technical auditing skills and the practical, legal, and business context of finance. It is not just about finding vulnerabilities; it is about understanding how those vulnerabilities impact the business and its compliance posture. The course uses a hands-on, scenario-based methodology, allowing participants to work through real-world audit dilemmas. We place strong emphasis on communication and reporting skills, which are critical for an effective audit. BIG BEN Training Center is committed to providing a program that gives financial professionals the knowledge and skills they need to protect their organization from both cyber threats and regulatory fines. By providing a comprehensive and practical approach, this course sets itself apart from other generic security training programs.