Financial Sector Cyber Security Audit and Assurance Training Course

14 - 18 Dec 2026

Milan

5900 € (Per Person)

Ref: #CYB5226_88476

Course Introduction / Overview:

The financial sector remains the primary target for sophisticated cyber-attacks, driven by the immense value of the assets and data it protects. This landscape necessitates a specialized approach to cybersecurity, one that integrates deep technical knowledge with a thorough understanding of complex regulatory frameworks. This intensive training course is meticulously designed to equip professionals with the advanced skills required to conduct effective cybersecurity audits and provide robust assurance within financial institutions. As discussed by authors like Chris Davis in works such as "IT Auditing: Using Controls to Protect Information Assets," the role of the auditor has evolved from a compliance checker to a strategic advisor on cyber risk management. This program, offered by BIG BEN Training Center, bridges that gap by covering everything from foundational audit principles and regulatory compliance with FFIEC and GLBA to advanced technical assessments of cloud infrastructure, fintech platforms, and incident response capabilities. Participants will gain a holistic perspective, enabling them to not only identify vulnerabilities but also to evaluate the overall maturity and resilience of an institution's cybersecurity posture, ensuring they can protect critical assets and maintain stakeholder trust in an era of persistent digital threats.

Target Audience / This training course is suitable for:

- IT Auditors and Internal Auditors.
- Information Security Managers and Analysts.
- Risk Management Professionals.
- Compliance Officers and Managers.
- IT Professionals working in the financial sector.
- External Auditors specializing in financial institutions.
- Regulatory and Supervisory Staff.
- Cybersecurity Consultants.

Target Sectors and Industries:

- Commercial and Retail Banking.
- Investment Banking and Asset Management.
- Insurance and Reinsurance Companies.
- Credit Unions and Cooperative Banks.
- Financial Technology (Fintech) and Payment Processors.
- Brokerage Firms and Stock Exchanges.
- Government Financial Regulatory Bodies and Central Banks.
- Private Equity and Venture Capital Firms.

Target Organizations Departments:

- Internal Audit Department.
- Information Technology (IT) and IT Security.
- Risk Management Department.
- Compliance and Legal Departments.
- Operations and Treasury Departments.
- Fraud Prevention and Investigation Units.
- Corporate Governance and a Board Audit Committee.

Course Offerings:

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

- Develop a comprehensive audit plan for cybersecurity within a financial institution.
- Assess compliance with key financial regulations such as GLBA, SOX, and PCI DSS.
- Evaluate the effectiveness of cybersecurity governance and risk management frameworks like NIST and ISO 27001.
- Conduct technical audits of critical infrastructure, including networks, operating systems, and core banking applications.
- Analyze and audit cloud security controls and third-party vendor risk management programs.
- Master techniques for auditing incident response, business continuity, and disaster recovery plans.
- Assess security controls for emerging technologies like mobile banking, fintech, and blockchain.
- Prepare impactful audit reports and communicate findings effectively to senior management and boards of directors.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to foster a dynamic and immersive learning experience that goes beyond theoretical knowledge. This course emphasizes a hands-on, practical approach to mastering cybersecurity audit and assurance in the financial sector. We utilize a blend of expert-led instruction, interactive group discussions, and detailed analysis of real-world case studies drawn from actual financial institution breaches and regulatory enforcement actions. Participants will engage in collaborative workshops to develop audit plans, conduct risk assessments, and simulate the evaluation of IT general controls (ITGC). Practical exercises will challenge attendees to apply learned concepts to realistic scenarios, such as auditing a cloud service provider or testing an incident response plan. Our trainers facilitate a continuous feedback loop, ensuring that every participant can connect the material to their professional context. This interactive and application-focused methodology ensures that attendees leave not just with knowledge, but with the confidence and competence to immediately enhance the cybersecurity posture of their organizations.

Course Agenda (Course Units):

Unit One: Foundations of Financial Cybersecurity Auditing

- The Evolving Threat Landscape in the Financial Sector.
- Core Principles of Information Systems Auditing.
- Key Regulatory and Compliance Frameworks (FFIEC, GLBA, SOX, NYDFS).
- Understanding IT General Controls (ITGC) in a Banking Context.
- The Role of the Cybersecurity Auditor in the Three Lines of Defense Model.
- Developing a Risk-Based Cybersecurity Audit Universe.
- Audit Planning, Scoping, and Engagement Management.

Unit Two: Governance, Risk, and Compliance (GRC) Audit

- Auditing the Cybersecurity Governance Framework.
- Evaluating the Information Security Policy and Standards.
- Conducting a Cybersecurity Risk Assessment Audit.
- Assessing the Third-Party and Vendor Risk Management Program.
- Auditing Data Governance and Privacy Compliance (e.g., GDPR).
- Evaluating the Security Awareness and Training Program.
- Techniques for Reporting GRC Findings to the Audit Committee.

Unit Three: Auditing Technical Security Controls

- Auditing Network Security Architecture and Controls (Firewalls, IDS/IPS).
- Vulnerability Management and Penetration Testing Program Audit.
- Auditing Identity and Access Management (IAM) and Privileged Access.
- Assessing Security for Core Banking and Financial Applications.
- Data Loss Prevention (DLP) and Encryption Control Audits.
- Auditing Security for Cloud-Based Services (IaaS, PaaS, SaaS).
- Reviewing Security Operations Center (SOC) and SIEM effectiveness.

Unit Four: Business Resilience and Incident Response Assurance

- Auditing the Business Continuity Management (BCM) Program.
- Evaluating the Disaster Recovery (DR) Plan and Testing Results.
- Assessing the Cyber Incident Response Plan and Playbooks.
- Reviewing Digital Forensics and Investigation Readiness.
- Auditing Crisis Management and Communication Protocols.
- Validating Backup and Recovery Capabilities.
- Assurance over Operational Resilience in Financial Market Infrastructures.

Unit Five: Advanced Auditing and Reporting

- Auditing Security in Fintech and Open Banking (API Security).
- Assessing Risks in Mobile Banking and Payment Systems.
- Emerging Challenges: Auditing Blockchain and AI/ML Systems.
- Consolidating Audit Evidence and Formulating Findings.
- Developing Effective Audit Recommendations.
- Writing a Compelling and Actionable Cybersecurity Audit Report.
- Presenting Audit Results to Executive Management and the Board.

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 financial services become increasingly decentralized through technologies like blockchain and DeFi, how must the traditional cybersecurity audit and assurance paradigm evolve to remain effective?

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

This course distinguishes itself by its exclusive and deep focus on the financial services industry, a sector with unparalleled security challenges and regulatory scrutiny. Unlike generic cybersecurity audit courses, every module, case study, and exercise is tailored to the specific context of banking, insurance, and investment firms. We move beyond theoretical frameworks to provide practical, actionable guidance on auditing the very technologies and processes that define modern finance, from core banking systems and SWIFT controls to emerging fintech and cloud-based platforms. The curriculum is uniquely structured to integrate three critical pillars: stringent regulatory compliance, in-depth technical control assessment, and strategic risk management. Participants will not only learn how to find a vulnerability but also how to assess its business impact within a financial context and communicate that risk effectively to the board. This holistic approach, blending governance with hands-on technical validation, ensures graduates are prepared to provide true assurance, not just a compliance checklist, making them invaluable assets in protecting the integrity and stability of their financial institutions.