Strategic IT Risk Management in Finance and Government Training Course



28 Dec 2026 - 01 Jan 2027

Boston

7500 € (Per Person)

Ref: #IT3558_158100

Course Introduction / Overview:

This intensive training course provides a comprehensive exploration of IT risk management frameworks tailored specifically for the unique challenges of the financial and public sectors. In an era of escalating cyber threats and stringent regulatory demands, establishing a robust IT risk management program is no longer optional but a critical component of organizational resilience and strategic success. This course delves into the practical application of globally recognized frameworks such as COBIT, NIST, and ISO 27005, moving beyond theoretical knowledge to equip participants with actionable skills. As discussed by author David L. Olson in works like "Enterprise Risk Management", a holistic approach is essential for integrating IT risk into the broader business context. Participants will learn to identify, assess, mitigate, and monitor IT risks effectively, ensuring alignment with business objectives and compliance with complex legal and regulatory landscapes. BIG BEN Training Center has designed this program to empower professionals to build and manage a resilient IT infrastructure that supports public trust and financial stability, fostering a proactive risk-aware culture within their organizations.

Target Audience / This training course is suitable for:

- IT Risk Managers and Analysts.
- Information Security Professionals.
- Compliance and Audit Officers.
- IT Managers and Team Leaders.
- Government and Public Sector IT Officials.
- Financial Sector Technology Executives.
- Operational Risk Managers.
- Business Continuity Planners.
- Consultants specializing in GRC (Governance, Risk, and Compliance).
- Project Managers overseeing technology initiatives.

Target Sectors and Industries:

- Commercial and Investment Banking.
- Insurance and Asset Management.
- Financial Technology (FinTech) and Payment Services.
- Government Ministries and Federal Agencies.
- State and Local Government Bodies.
- Public Utilities and Critical Infrastructure.
- Public Healthcare Organizations.
- Regulatory and Supervisory Authorities.
- Non-profit and Non-governmental Organizations (NGOs).

Target Organizations Departments:

- Information Technology (IT) and Information Security.
- Risk Management.
- Internal Audit and aompliance.
- Legal and Regulatory Affairs.
- Operations and Business Units.
- Finance and Treasury.
- Strategic Planning.
- Procurement and Vendor Management.

Course Offerings:

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

- Develop and implement a tailored IT risk management framework using COBIT, NIST, or ISO standards.
- Conduct comprehensive IT risk assessments to identify and prioritize threats and vulnerabilities.
- Align IT risk management strategies with organizational goals and risk appetite.
- Navigate the specific regulatory and compliance requirements of the financial and public sectors.
- Establish effective risk monitoring, reporting, and communication channels for stakeholders.
- Integrate third-party risk management into the overall IT security posture.
- Develop robust incident response and business continuity plans to ensure operational resilience.
- Foster a proactive, risk-aware culture across all departmental levels.
- Evaluate and select appropriate risk mitigation controls and strategies.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, engaging, and practical, ensuring that participants can immediately apply their learning in their professional roles. We believe in an experiential learning approach that moves beyond traditional lectures. The course combines expert-led instruction with intensive case studies drawn from real-world scenarios in the financial and public sectors, allowing participants to analyze complex problems and devise effective solutions. Collaborative group discussions and workshops are a core component, fostering peer-to-peer learning and the exchange of diverse perspectives. Participants will engage in hands-on exercises, including risk assessment simulations and framework development activities. Our trainers facilitate a dynamic environment where questions are encouraged, and practical challenges are addressed directly. Continuous feedback is provided throughout the sessions to reinforce key concepts and ensure a deep understanding of the material. This blended approach guarantees a comprehensive learning experience that bridges theory with practical, real-world application.

Course Agenda (Course Units):

Unit One Foundations of IT Risk Management

- Introduction to IT Risk Management Concepts and Terminology.
- The Strategic Importance of IT Risk Management in Finance and Government.
- Understanding the Relationship Between Risk, Threats, and Vulnerabilities.
- Key Principles of Governance, Risk, and Compliance (GRC).
- Defining Risk Appetite and Risk Tolerance.
- The IT Risk Management Lifecycle.
- Roles and Responsibilities in IT Risk Management.

Unit Two Core IT Risk Management Frameworks

- Deep Dive into the COBIT Framework for IT Governance and Management.
- Exploring the NIST Cybersecurity Framework (CSF) and Risk Management Framework (RMF).
- Understanding the ISO/IEC 27005 Standard for Information Security Risk Management.
- Comparing and Contrasting Major Frameworks.
- Selecting and Customizing a Framework for Your Organization.
- Integrating Multiple Frameworks for Comprehensive Coverage.
- Practical Exercise in Mapping Controls to Framework Requirements.

Unit Three Risk Assessment and Analysis Techniques

- Methodologies for IT Risk Identification and Discovery.
- Qualitative vs. Quantitative Risk Analysis.
- Conducting a Business Impact Analysis (BIA).
- Threat Modeling and Vulnerability Assessment Techniques.
- Risk Evaluation and Prioritization using Heat Maps and Risk Registers.
- Scenario Analysis and Stress Testing for IT Risks.
- Documenting and Communicating Risk Assessment Findings.

Unit Four Regulatory Compliance and Governance

- Key Regulations in the Financial Sector (e.g., SOX, GLBA, Basel III).
- Data Privacy Regulations (e.g., GDPR, CCPA) and Their Impact on IT Risk.
- Public Sector Compliance and Information Security Mandates.
- The Role of the IT Audit in Ensuring Compliance.
- Building a Compliance-Driven IT Risk Program.
- Managing Regulatory Change and Its Impact on IT Controls.
- Reporting on Compliance to Regulators and Senior Management.

Unit Five Advanced Risk Mitigation and Management

- Developing and Implementing Risk Treatment Plans.
- Third-Party and Supply Chain Risk Management.
- Strategies for Managing Cloud and Emerging Technology Risks.
- Developing an Effective Incident Response Plan.
- Integrating IT Risk with Business Continuity and Disaster Recovery Planning.
- Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) for IT Risk.
- Cultivating a Strong Risk-Aware Culture within the Organization.

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 digital transformation accelerates, how can public and financial sector organizations balance innovation with the inherent IT risks without stifling growth or compromising security?

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

This course distinguishes itself through its specialized dual-focus on the financial and public sectors, two of the most highly regulated and targeted industries globally. Unlike generic IT risk courses, every module, case study, and discussion is tailored to address the specific compliance landscapes, threat profiles, and operational realities of these unique environments. The curriculum emphasizes the practical application of globally recognized frameworks like COBIT and NIST, not just their theoretical components. Participants will learn how to select, customize, and implement these frameworks to solve real-world challenges, from navigating complex government mandates to securing sensitive financial data. Furthermore, the course content is built on a strategic perspective, teaching participants how to align IT risk management with overarching business objectives and communicate risk effectively to executive leadership. It moves beyond a purely technical viewpoint to foster a holistic understanding of how IT risk impacts organizational resilience, public trust, and financial stability. The interactive methodology ensures that participants leave with actionable strategies and a robust toolkit they can deploy immediately within their organizations.