Comprehensive IT Auditing: Mastering Modern Techniques

2026 □□□□□□ 11 – 7
Edinburgh (UK)



Comprehensive IT Auditing: Mastering Modern Techniques

Ref: 20262420_235789 Duration: Edinburgh (UK) Fees: 5200 GBP

Why This Course

IT auditing plays a vital role in strengthening governance, managing technology risks, and ensuring that information systems are secure, reliable, and aligned with organizational objectives. As digital environments become more complex, auditors need practical knowledge of IT controls, cybersecurity risks, data analytics, cloud environments, emerging technologies, and recognized audit frameworks.

This intensive 1-week IT Auditing Training program provides participants with a comprehensive understanding of modern IT audit techniques, methodologies, and practical tools. The course covers IT governance, risk assessment, IT general controls, application controls, cybersecurity audits, cloud and emerging technology audits, audit reporting, and follow-up activities. Through real-world case studies, practical exercises, and framework-based discussions, participants will develop the skills needed to conduct effective, risk-based IT audits and communicate findings clearly to management.

What You'll Learn and Practice

By joining this program, you will:

- Understand the IT audit process and its role in organizational governance.
- Apply risk assessment techniques to identify critical IT audit areas.
- Plan and execute IT audit engagements efficiently.
- Evaluate IT controls using frameworks such as COBIT, NIST, and ISO 27001.
- Assess access controls, identity management, change management, and IT operations.
- Review data backup, recovery, and service management controls.
- Evaluate application controls, including input, processing, and output controls.
- Audit database management systems and data-related controls.
- Use data analytics to improve IT audit effectiveness.
- Explore continuous auditing and monitoring techniques.
- Assess cybersecurity, cloud, virtualization, IoT, mobile, AI, and machine learning risks.
- Analyze audit evidence and prepare clear, actionable audit reports.



The Program Flow

Day 1: Introduction to IT Auditing

- Understand IT audit fundamentals, objectives, and scope.
- Explore the role of IT audit in governance, risk management, and compliance.
- Review IT governance and management frameworks.
- Apply IT risk assessment techniques to prioritize audit focus areas.
- Plan an IT audit engagement based on organizational risks and objectives.

Day 2: IT General Controls

- Evaluate access controls and identity management practices.
- Review change management and system development controls.
- Assess IT operations and service management processes.
- Examine data backup, recovery, and continuity-related controls.
- Identify weaknesses in IT general controls and recommend improvements.

Day 3: Application Controls and Data Analytics

- Understand input, processing, and output controls in business applications.
- Audit database management systems and related data controls.
- Apply data analytics techniques to support audit testing.
- Use continuous auditing and monitoring concepts to improve audit coverage.
- Interpret audit results and connect findings to business and technology risks.

Day 4: Cybersecurity and Emerging Technologies

- Assess network security controls and penetration testing outcomes.
- Understand audit considerations for cloud computing and virtualization.
- Explore audit risks related to IoT and mobile devices.
- Review how artificial intelligence and machine learning affect IT audits.
- Identify emerging technology risks and suitable audit approaches.

Day 5: Audit Reporting and Follow-Up

- Evaluate audit evidence and determine the significance of findings.
- Write clear, structured, and impactful IT audit reports.
- Present audit findings and recommendations to management.
- Develop practical action plans for remediation and improvement.
- Conduct post-audit follow-up to monitor corrective actions and progress.



Individual Impact

- Build confidence in conducting structured and risk-based IT audits.
- Strengthen understanding of IT governance, controls, cybersecurity, and audit frameworks.
- Improve skills in audit planning, evidence evaluation, and control assessment.
- Gain practical awareness of data analytics and continuous auditing techniques.
- Enhance the ability to communicate findings clearly and professionally.

Work Impact

- Improve the organization's ability to identify and manage IT risks.
- Strengthen IT governance, compliance, and control effectiveness.
- Enhance audit coverage through better use of frameworks and data analytics.
- Support stronger cybersecurity, application, and infrastructure control environments.
- Drive positive change through clear audit reports and actionable recommendations.

Training Methodology

This program combines IT audit concepts with practical application through:

- Instructor-led sessions on IT audit methodologies and frameworks.
- Real-world case studies covering IT risks, controls, and audit findings.
- Practical exercises on audit planning, risk assessment, and control evaluation.
- Data analytics activities for IT audit testing and monitoring.
- Cybersecurity, cloud, and emerging technology audit scenarios.
- Audit reporting workshops and management presentation practice.

Beyond the Course

Upon completion, participants will be able to:

- Conduct risk-based IT audits aligned with organizational objectives.
- Evaluate IT controls using recognized frameworks such as COBIT, NIST, and ISO 27001.
- Use data analytics to improve audit efficiency and effectiveness.
- Assess IT general controls, application controls, cybersecurity, and emerging technology risks.
- Produce clear, actionable audit reports that support better IT governance and control improvement.

