BLACKBIRD FOR TRAINING

Comprehensive Course in Technology Auditing



Comprehensive Course in Technology Auditing

Introduction

As digital transformation accelerates across industries, organizations are increasingly dependent on cloud computing, artificial intelligence, automation, digital platforms, and interconnected technologies. These advancements introduce significant opportunities for innovation and growth but also create complex risks related to cybersecurity, regulatory compliance, operational resilience, data governance, and emerging technology adoption.

Today's technology auditor must move beyond traditional audit methodologies and develop the ability to assess sophisticated digital ecosystems, evaluate emerging risks, and provide strategic assurance to executive leadership. Modern auditing requires a comprehensive understanding of advanced technologies, cyber threats, governance frameworks, and evolving regulatory requirements.

This intensive program is designed for experienced auditors, risk professionals, compliance specialists, cybersecurity practitioners, and technology leaders seeking to enhance their expertise in auditing modern digital environments. Through practical exercises, case studies, simulations, and real-world scenarios, participants will learn how to evaluate emerging technologies, assess security and governance controls, and provide assurance across complex technology landscapes.

The course combines advanced auditing techniques with leading frameworks including COBIT 2019, NIST Cybersecurity Framework, NIST SP 800-53, ISO/IEC 27001, ISO/IEC 27005, CIS Controls, Cloud Security Alliance guidance, and emerging governance standards for artificial intelligence and digital trust.

Course Objectives

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



- Conduct risk-based audits within complex digital environments.
- Develop strategic technology audit plans aligned with organizational objectives.
- Evaluate cybersecurity governance and security control effectiveness.
- Assess artificial intelligence systems and machine learning governance frameworks.
- Audit cloud computing environments and hybrid infrastructure architectures.
- Evaluate identity and access management controls.
- Assess governance practices for automation and digital transformation initiatives.
- Analyze technology risks associated with connected devices and distributed environments.
- Apply advanced data analytics techniques during audit engagements.
- Integrate threat intelligence into audit planning and risk assessment activities.
- Conduct forensic reviews and incident response assessments.
- Evaluate business continuity and cyber resilience capabilities.
- Audit blockchain solutions and distributed ledger technologies.
- Assess compliance with international cybersecurity and technology regulations.
- Communicate audit findings effectively to executive management and boards.
- Develop future-ready audit strategies for emerging technologies.

Course Outlines

Day 1: Strategic Technology Audit Planning and Risk Intelligence

- Evolution of technology auditing in digital organizations.
- Enterprise digital transformation risks and assurance requirements.
- Risk-based audit planning methodologies.
- Enterprise technology risk assessment frameworks.
- Integrating threat intelligence into audit planning.
- Auditing cloud-native and digital-first environments.
- Mapping controls using COBIT 2019 and NIST frameworks.
- Case study: Building a technology audit universe.

Day 2: Digital Governance and Technology Risk Management

- Technology governance frameworks and oversight models.
- Enterprise risk management integration.
- Governance of digital transformation initiatives.
- Third-party technology risk management.
- Vendor and service provider assurance.
- Regulatory compliance requirements for digital organizations.
- Technology policy and control framework assessments.
- Workshop: Digital governance maturity assessment.



Day 3: Advanced Cybersecurity Auditing

- Cybersecurity audit methodologies.
- Security architecture reviews.
- Network security control assessments.
- Vulnerability management and penetration testing oversight.
- Security monitoring and threat detection capabilities.
- Security Operations Center effectiveness reviews.
- Security information and event management assessments.
- Case study: Enterprise cybersecurity audit engagement.

Day 4: Auditing Artificial Intelligence and Intelligent Automation

- AI governance frameworks and emerging regulations.
- Auditing machine learning systems.
- Model risk management.
- Explainability, transparency, and fairness assessments.
- AI ethics and responsible AI controls.
- Auditing robotic process automation environments.
- Governance of intelligent automation initiatives.
- Practical exercise: AI governance assessment.

Day 5: Cloud Security and Hybrid Infrastructure Auditing

- Auditing cloud computing environments.
- Cloud governance and security responsibilities.
- Hybrid and multi-cloud risk management.
- Auditing Azure, AWS, and Google Cloud environments.
- Identity governance in cloud ecosystems.
- Data protection and privacy controls.
- Cloud compliance assessments.
- Case study: Multi-cloud security audit.

Day 6: Auditing Data Governance, Privacy and Digital Trust

- Data governance frameworks.
- Data classification and lifecycle management.
- Privacy regulations and compliance requirements.
- Auditing data protection controls.
- Data integrity and quality assurance reviews.
- Digital trust frameworks.
- Cross-border data transfer requirements.
- Workshop: Privacy impact audit assessment.



Day 7: Forensic Auditing and Incident Response Assessment

- Digital forensic principles for auditors.
- Incident response governance.
- Cyber breach investigation methodologies.
- Evidence collection and preservation requirements.
- Reviewing security incident management processes.
- Post-incident recovery assessments.
- Lessons learned and continuous improvement reviews.
- Hands-on simulation: Technology breach investigation.

Day 8: Auditing Emerging Technologies and Connected Ecosystems

- Internet of Things governance and security.
- Edge computing audit considerations.
- Blockchain auditing methodologies.
- Smart contract assurance reviews.
- Digital asset governance.
- Operational technology and industrial control systems auditing.
- Emerging technology risk assessment models.
- Case study: Blockchain governance audit.

Day 9: Continuous Auditing, Data Analytics and Intelligent Assurance

- Continuous auditing frameworks.
- Continuous controls monitoring.
- Audit analytics platforms and technologies.
- Data-driven audit methodologies.
- Predictive risk analytics.
- Visualization and dashboard reporting.
- Automation of audit procedures.
- Workshop: Developing intelligent audit programs.

Day 10: Executive Reporting, Audit Leadership and Future Technologies

- Executive-level audit reporting.
- Technology risk communication strategies.
- Reporting to boards and audit committees.
- Risk prioritization and strategic recommendations.
- Ethical considerations in emerging technology audits.
- Quantum computing implications for auditors.
- Zero Trust architectures and future assurance models.
- Capstone exercise: Presenting a strategic technology audit report.



Why Attend This Course: Wins & Losses!

- Master advanced auditing techniques for modern digital environments.
- Strengthen expertise in cybersecurity, cloud, and artificial intelligence auditing.
- Improve technology risk assessment capabilities.
- Develop practical skills in forensic auditing and incident response evaluation.
- Gain experience auditing emerging technologies and digital ecosystems.
- Enhance regulatory compliance and governance assessment capabilities.
- Improve executive reporting and stakeholder communication skills.
- Learn industry-recognized frameworks and best practices.
- Build strategic assurance capabilities for digital transformation initiatives.
- Increase professional value as a technology audit leader.

Conclusion

Technology auditing has become a strategic function that directly supports organizational resilience, governance, cybersecurity, and digital transformation success. As organizations continue to adopt advanced technologies such as artificial intelligence, cloud computing, automation, connected devices, and blockchain solutions, auditors must possess the skills required to evaluate risks, assess controls, and provide assurance across increasingly complex environments.

This course provides participants with a comprehensive framework for auditing modern technologies, combining governance, cybersecurity, compliance, risk management, forensic investigation, and emerging technology assessment into a unified audit approach. Through practical exercises, simulations, and real-world case studies, participants develop the knowledge and confidence required to perform advanced technology audits that deliver measurable value to their organizations.

By integrating internationally recognized frameworks, advanced auditing methodologies, and forward-looking technology risk practices, the program prepares professionals to lead audit innovation, strengthen organizational resilience, and support executive decision-making in a rapidly evolving digital world.

FAQ

What is Information Technology Audit and why is it important?

Information Technology Audit is an independent and systematic process used to evaluate IT governance, security controls, technology risks, and operational effectiveness within an organization. For those asking what is Information Technology Audit, it helps ensure that digital systems are secure, compliant, reliable, and aligned with business objectives while supporting operational resilience and regulatory compliance.



What is the Information Technology Audit process?

The Information Technology Audit process typically begins with defining the audit scope, assessing technology risks, reviewing IT controls, testing security and operational effectiveness, and reporting findings with practical recommendations. Modern Information Technology Auditing follows internationally recognized frameworks, including the Global Technology Audit Guide GTAG, to provide risk-based assurance across complex digital environments.

What is the difference between Information Technology Audit and Information Technology Security Audit?

While Information Technology Audit evaluates the overall governance, operations, and effectiveness of IT systems, an Information Technology Security Audit specifically focuses on cybersecurity controls, access management, network security, data protection, and vulnerability management. Together, these audit disciplines help organizations strengthen security, reduce technology risks, and improve compliance.

Who should attend an Information Technology Audit course?

An Information Technology Audit course is ideal for internal and external auditors, IT professionals, cybersecurity specialists, compliance officers, risk managers, and governance practitioners. It equips participants with the knowledge required to assess emerging technologies, evaluate technology risks, apply audit technology solutions, and perform effective audits in modern digital environments.

What skills will participants gain from an Information Technology Audit course?

Participants will develop practical skills in risk-based technology audit planning, cybersecurity auditing, cloud security assessment, IT governance evaluation, data governance reviews, incident response assessment, and executive audit reporting. The course also strengthens the ability to apply international frameworks, assess emerging technologies, and provide strategic assurance that supports digital transformation and organizational resilience.

