IT AUDIT FOR NON-IT AUDITORS



GENTEX®
TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Introduction

IT Audit for Non-IT Auditors Training Course gives general auditors the confidence to examine technology controls without a technical background. Participants work through IT fundamentals in plain language, IT general controls, application controls, access and change management, cybersecurity basics, cloud and third-party arrangements, analytics, and technology findings reporting as one connected discipline. The programme links the technology risk an organisation carries with the audit questions and evidence a non-specialist can gather. As a result, learners gain a practical, jargon-free IT audit method. Furthermore, the course strengthens technical literacy, questioning technique, and reporting confidence.

IT Audit for Non-IT Auditors Course Objectives

- Explain core IT concepts in plain, non-technical language.
- Apply the IIA standards and COBIT principles at a practical level.
- Audit IT general controls: access, change, and operations.
- Audit application controls and basic interface controls.
- Assess user access, privileged accounts, and segregation of duties.
- Review change management and patch management controls.
- Apply cybersecurity and data protection basics to audit work.
- Audit cloud services and third-party technology arrangements.
- Apply simple data analytics to technology audit evidence.
- Write technology findings and reporting for non-specialist audiences.

Course Methodology

- Interactive sessions built on non-technical IT audit cases.
- Workshops on ITGC concepts, access review, and question design.

GENTEX® TRAINING CENTER

- Group exercises on access testing, change review, and findings drafting.
- Hands-on practice with access listings, audit programmes, and checklists.
- Simulation of an IT audit interview and an exit meeting.
- Facilitator coaching and peer review on personal IT audit plans.

Who Should Take This Course

- Generalist internal auditors and audit assistants.
- Finance, operations, and compliance auditors.
- Risk and internal control professionals.
- Finance and operations managers supporting audit work.
- Quality assurance and governance professionals.
- Consultants advising on IT controls and audit support.

IT Audit for Non-IT Auditors Course Outlines

Day 1: IT Concepts in Plain Language

- Hardware, software, networks, and databases explained simply.
- Systems, applications, and interfaces at a practical level.
- Servers, cloud, and how systems are hosted.
- Users, accounts, roles, and permissions.
- Data, records, and information flows.
- Common IT terminology auditors will hear.
- Case discussion: an audit halted by technical jargon.

Day 2: IT General Controls Access and Operations

- Access management: provisioning, changes, and termination.
- Privileged accounts, administrator access, and superuser risk.
- Segregation of duties in systems and roles.
- Access reviews and recertification practice.
- Backup, restore, and job scheduling controls.
- Incident handling and operations monitoring.
- Workshop: testing user access and privileged accounts.

Day 3: Change Management and Application Controls

- Change management process and release control.
- Emergency changes and their risk.
- Patch management and vulnerability basics.
- Application controls: input, processing, output, and interfaces.
- System interfaces and reconciliation controls.
- Testing application controls without technical tools.
- Exercise: auditing a change and an application control.

Day 4: Cybersecurity, Cloud, and Third Parties

- Cybersecurity basics: threats, controls, and responsibilities.
- Identity, passwords, and multi-factor authentication.
- Data protection, privacy, and records obligations.
- Cloud service models and shared responsibility.
- Third-party and vendor assurance and SOC reports.
- Basic data analytics for technology audit evidence.
- Simulation: reviewing a cloud arrangement and access logs.

Day 5: Findings, Reporting, and Working with IT

- Structuring technology findings with root cause analysis.
- Translating technical issues into business impact.
- Writing findings for management and the board.
- Interviewing IT staff and asking the right questions.
- Working with IT specialists and external experts.
- Follow-up, remediation tracking, and closure validation.
- Capstone: presenting an IT-audit report for a non-technical audience.

Conclusion

By successfully completing IT Audit for Non-IT Auditors, participants will gain a practical command of core IT concepts, IT general controls, application control basics, access and change review, cybersecurity and cloud awareness, simple analytics, and technology findings reporting. They will acquire skills in access testing, change review, risk-based questioning, and non-technical reporting that bring technology risk within audit scope. Gentex Training Center designs the programme to help auditors examine IT controls with confidence.

FAQs

Q1 What is the "IT Audit for Non-IT Auditors" course about?

It gives general auditors the confidence to examine technology controls without a technical background. The course spans IT concepts in plain language, IT general controls for access and operations, change management and application controls, cybersecurity, cloud and third parties, and findings, reporting and working with IT.

Q2 What are the key benefits of the "IT Audit for Non-IT Auditors" course?

You gain a practical, jargon-free IT audit method that links technology risk with the audit questions and evidence a non-specialist can gather. The course improves technical literacy and access review practice, strengthens change and application control testing, sharpens cybersecurity and cloud awareness, and gives you reporting practice that translates technical issues into business impact.

Q3 What skills will I gain from the "IT Audit for Non-IT Auditors" course?

You will develop four core skills: core IT concept and terminology literacy, IT general control testing for access, change and operations, application control and cybersecurity awareness review, and technology findings development with non-technical reporting.

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q4 What tools, methods, or standards are covered in the "IT Audit for Non-IT Auditors" course?

The course covers hardware, software, networks and databases explained simply, systems, applications and interfaces, servers, cloud and hosting, users, accounts, roles and permissions, data, records and information flows, common IT terminology, access management covering provisioning, changes and termination, privileged accounts, administrator access and superuser risk, segregation of duties in systems and roles, access reviews and recertification, backup, restore and job scheduling controls, incident handling and operations monitoring, the change management process and release control, emergency changes, patch management and vulnerability basics, application controls for input, processing, output and interfaces, system interfaces and reconciliation controls, cybersecurity threats, controls and responsibilities, identity, passwords and multi-factor authentication, data protection, privacy and records obligations, cloud service models and shared responsibility, third-party and vendor assurance and SOC reports, basic data analytics for technology audit evidence, technology findings with root cause analysis, translating technical issues into business impact, writing findings for management and the board, interviewing IT staff, working with IT specialists and external experts, and follow-up, remediation tracking and closure validation.

Q5 How is the "IT Audit for Non-IT Auditors" course applied in real-world practice?

Participants apply it to real work such as testing user access and privileged accounts, reviewing a change management record, auditing a basic application control, assessing a cloud arrangement with SOC reports, running a simple analytics test over access data, and drafting technology findings for a non-technical audit committee. The same methods support remediation tracking and working alongside IT specialists.