CONCEPT

IT Audit and Information Systems Assurance: IT General Controls, Application Controls and Reporting

IT Audit and Information Systems Assurance: IT General Controls, Application Controls and Reporting

Introduction:

When IT audit coverage stops at policies and questionnaires, weak user access, untested program changes and failed backups stay hidden until a system outage, data error or breach exposes them. Audit committees then receive assurance that no one can trace to evidence from the systems themselves. This Core Concept course equips auditors to plan and perform IT audit work on information systems, testing IT general controls, application controls and interfaces, and to report rated findings with follow-up. Participants leave with an IT General Controls Audit Programme and Findings Report built on their own systems.

Course Objectives:

- Plan a risk-based IT audit by mapping systems, infrastructure layers and data flows to IT risks and control objectives
- Use COBIT 2019 and IIA GTAG guidance as audit criteria for IT governance and IT general controls
- Test logical access, program change, IT operations and backup controls with walkthroughs, evidence requests and sampling
- Evaluate application input, processing and output controls, interfaces, database and ERP settings, and service organisation reports
- Apply data analytics to full populations of access, change and job logs to detect control exceptions
- Report IT audit findings with risk ratings, agreed management actions and follow-up evidence ready for the audit committee

Target Audience:

- Internal auditors who extend assurance engagements into systems and technology controls
- IT auditors who plan and test IT general and application controls
- Risk and control staff who assess technology risk and monitor remediation
- Compliance and second-line reviewers who rely on IT control evidence in their own work
- Audit team members who review service organisation reports and third-party IT assurance

Course Outline:

Day 1: IT Audit Process and the IT Risk Landscape

- IT Audit Types: General Control Reviews Versus Application Control Reviews
- Preventive, Detective and Corrective IT Control Classification
- Confidentiality, Integrity and Availability Objectives in IT Audit Scoping
- IT Audit Universe of Applications, Infrastructure Layers and Data Flows
- Risk-Based IT Audit Plan and Engagement Scoping Memo

Day 2: IT Governance and Control Frameworks for Auditors

- COBIT 2019 Governance and Management Objectives as Audit Criteria
- IIA GTAG 1 Information Technology Controls Structure
- IIA GTAG 17 Approach to Auditing IT Governance
- ITGC Domain Map: Logical Access, Change, Operations, Backup and Physical Security
- IT Risk and Control Matrix Template for Systems in Scope

Day 3: Testing IT General Controls

- Logical Access Testing: Provisioning, Leavers and Privileged Accounts Using GTAG 9
- Program Change, Patch and Development Life Cycle Testing Using GTAG 2
- IT Operations Testing: Job Scheduling, Incident Records and Data Centre Physical Security
- Backup and Recovery Testing: Restore Evidence and Retention Checks
- IT Audit Evidence Standards and Attribute Sampling by Control Frequency

Day 4: Application Controls, ERP, Cloud and Cyber Assurance

- Application Input, Processing and Output Controls and Interface Reconciliation Testing
- Database and ERP Environment Review at Overview: Roles, Configuration and Audit Trails
- Service Organisation Assurance: SOC 1 and SOC 2 Type I and Type II Reports at Overview
- Cybersecurity Audit Basics: Vulnerability Scans, Security Logs and Patch Status Review
- Data Analytics in IT Audit: Full-Population Tests of Access, Change and Job Logs

Day 5: IT Audit Case Work, Reporting and Follow-Up

- ERP Access and Change Case Study: Exceptions and Compensating Controls
- Cloud Provider Case Study: SOC 2 Type II Exceptions and Complementary User Entity Controls
- IT Audit Report Drafting: Rated Findings and Management Action Plans
- Remediation Follow-Up Tracker and Closure Evidence Review
- IT General Controls Audit Programme and Findings Report Presentation and Peer Challenge

Skills You Will Gain:

- IT Audit Planning
- IT Risk and Control Mapping
- Access Control Testing
- Change Management Review
- Application Control Evaluation
- Service Organisation Report Review
- Audit Data Analytics
- IT Audit Reporting

Why Attend This Course:

- Return with an IT General Controls Audit Programme and Findings Report prepared for one of your own systems
- Request the right system evidence from IT teams and judge whether it proves a control actually operated
- Read a SOC report or ERP access listing and spot the exceptions that matter to your audit opinion
- Compare IT audit practice with auditors from banking, energy, public services and manufacturing

Conclusion:

Reliable assurance over technology depends on testing controls inside the systems, not only reading policies about them. This course moves from IT audit types, control objectives and risk-based planning, through COBIT 2019 and GTAG guidance, to testing access, change, operations and backup controls, then to application controls, ERP and database environments, SOC reports, cybersecurity basics and audit analytics. The final day applies these methods to case material and produces an IT General Controls Audit Programme and Findings Report ready for review.