INFOSECTRAIN
Educate. Excel. Empower.

GRC IT Audit

(Governance Risk & Compliance)

Practical Approach Training

INFOSECTRAIN

Course Highlights

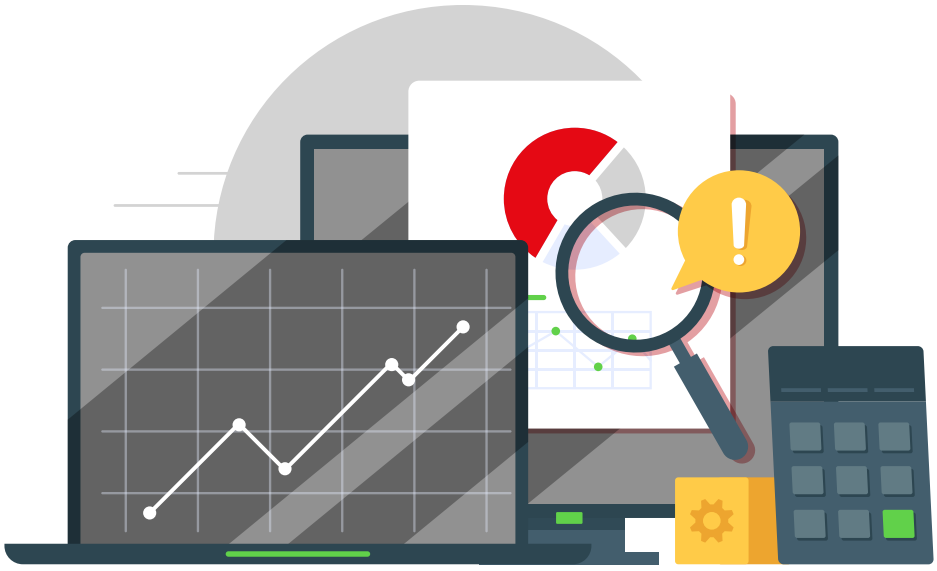
- 40-Hour LIVE Instructor-led Training
- Designed for CISA, CISM, CISSP professionals
- Hands-On End-to-End Audit Simulation
- SOC 2 Deep Dive — Type I, II & III
- Get Job Ready with Mock Interview Tips
- Immersive Learning via Industry Case Studies
- 5 Frameworks: ISO 27001, 22301, 27701, SOC 2 & ITGC
- Sample Templates: Risk Register, RCM, Audit Plan & more
- Extended Post Training Support & Access to Recorded Sessions

INFOSECTRAIN

About Course

The GRC IT Audit Practical Approach Training from InfosecTrain is tailored for IT professionals, Auditors, and Governance Specialists who aim to enhance their expertise in auditing IT systems, controls, and governance frameworks.

Learn to build hands-on capability across ITGC, SOC 2, ISO 27001, ISO 22301 and ISO 27701. Learn to plan risk-based audits, evaluate and challenge evidence, audit critical control domains, write executive-ready reports and manage stakeholders effectively. With sample templates, a full audit simulation, SOC 2 deep dive and a dedicated career readiness module, this course converts your existing knowledge into the audit competency that employers and clients actually hire for.



INFOSECTRAIN

Course Objectives

Upon successful completion of the training, participants will be able to:

- Build a real audit mindset, not just certification knowledge
- Design risk-based audit plans aligned to organisational risk registers
- Execute audits using walkthroughs, inquiry, inspection and reperformance
- Evaluate, challenge and detect fabricated or insufficient audit evidence
- Audit ITGC domains: access, privileged access, change, patch and incident management
- Audit BCP, DR, backup and physical security controls end-to-end
- Apply data privacy and vendor risk audit techniques aligned to GDPR and DPDPA
- Map and harmonise controls across ISO 27001, ISO 22301, ISO 27701 and SOC 2
- Write executive-ready audit findings using the Condition-Criteria-Cause-Impact framework
- Transition confidently into senior IT Audit and GRC roles with interview-ready skills

INFOSECTRAIN

Target Audience

This course is designed for working professionals who want to build or strengthen hands-on GRC / IT Audit capability.

Ideal participants include:

- GRC, Technology Risk, or Compliance professionals
- Cybersecurity professionals transitioning into audit/assurance roles
- Professionals preparing for Senior Auditor / Consultant roles
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- ISO/IEC 27001 Lead Implementer

Pre-requisites

- Basic understanding of IT systems, applications, and networks
- Familiarity with frameworks like ISO 27001, SOC 2, SOX, or ITIL (awareness level sufficient)
- Prior experience or certification, such as CISA, CISM, CISSP, or ISO 27001 Lead Implementer, is highly recommended
- Ideal for professionals transitioning into the GRC and IT Audit roles

INFOSECTRAIN

Course Content

Module 1

Foundations of IT & GRC Auditing (Why Audits Exist)

Objective: Build an audit mindset before tools & controls

- Overview of IT Audit
- Types of IT Audits
  - ITGC Audit
  - SOX Audit
  - IS Audit
- Role of GRC in organizations
- Auditor vs Consultant vs Risk Manager (implicit understanding)
- How experienced professionals fail in audits?
- Common Audit Misconceptions Among Certified Professionals

Module 2

Governance and Risk Auditing (How Organizations Are Structured and How Risks Are Managed)

Objective: Understand the environment being audited

- Auditing Governance Structures
- Auditing Risk Registers (Sample Risk register shared)
- Importance of:
  - ✓ RCM (Risk Control Matrix)
  - ✓ Observation Sheets

Module 3

Audit Planning (How Audits Are Designed)

Objective: Teach thinking before testing

- How to Develop an Effective Audit Plan (Sample Plan to be created)
- Identifying and Assessing Audit Risks
- Key considerations for Risk based audit planning
- Audit scope definition & prioritization

Module 4

Core Audit Execution Techniques (How Audits Are Performed)

Objective: Build strong execution fundamentals

- Audit techniques:
  - Walkthroughs
  - Inquiry
  - Observation
  - Inspection
  - Reperformance
- Design Effectiveness vs Operating Effectiveness
- Sampling Basics:
  - Population
  - Period
  - Sample size
  - Selection methods
- Audit Evidence:
  - Sufficiency & appropriateness
  - What evidence can be accepted / rejected
  - Screenshot pitfalls
  - Timestamp validation
  - Fabricated evidence detection

Module 5

Auditing Core IT General Controls (ITGC)

Objective: Hands-on audit exposure (What would you test? What would fail? What evidence is sufficient?)

Access & Identity

- Auditing User Access Management (UAM)
- Auditing Logical Access Controls
- Auditing Password Controls
- Auditing Privileged Access (PIM / PAM)
- Auditing HR Security Controls

Change & Operations

- Auditing Change Management Controls
- Auditing Configuration Management
- Auditing Patch Management Controls

IT Service Management

- Auditing Incident Management Controls
- Auditing Problem Management Controls

Module 6

Resilience, Continuity & Infrastructure Controls

Objective: Cover availability & operational risk

- Auditing Business Continuity Management (BCM)
- Auditing BIA, BCP, and DR
- Design vs Operational effectiveness difference in BCM
- Auditing Backup and Restoration Controls
- Auditing Physical and Environmental Controls

Module 7

Data Protection, Privacy & Third-Party Risk

Objective: Address modern regulatory and cyber risk

- Reviewing Information Security Policies
- Auditing Data Privacy Controls
- Auditing Vendor Management & Outsourcing Practices
- Cybersecurity Control Audits:
  - ✓ Data Protection Governance
  - ✓ Endpoint Security
  - ✓ Mobile Device Management (MDM)

Module 8

Standards & Framework Orientation

Objective: Teach how to use standards, not quote them

- Brief Overview of:
  - ISO 27001
  - ISO 22301
  - ISO 27701
  - SOC 2 Trust Criteria
- How auditors map controls to standards (conceptual)
- Practical hands-on Cross-framework harmonization by taking few controls

Module 9

SOC 2 Deep Dive

Objective: Job-ready SOC 2 capability

- What is SOC 2 & Why it Matters
- SOC 2 Type I vs Type II vs Type III
- Five Trust Service Criteria
- Key Control Areas
- Audit Readiness Phases
- Key Documents to Prepare
- Common SOC 2 Gaps

Module 10

Audit Reporting & Stakeholder Management

Objective: Convert findings into value

- Structure of an Audit Finding:
  - Condition
  - Criteria
  - Cause
  - Impact
  - Recommendation
- Rating Issues:
  - High / Medium / Low
- Remediation & Management Action Plans
- How to Draft Audit Observations
- Preparing a Comprehensive Audit Report
- How to talk to IT teams without conflict
- How to ask for evidence professionally
- Mini End-to-End Audit Simulation

INFOSECTRAIN

Module 11

Career & Interview Readiness (Outcome-Focused)

Objective: Convert learning → employability

- How to transition from GRC / Technical role to IT Audit
- Key Areas to Focus on for IT Audit Interviews
- Mock Interview Tips & Techniques
- How to write CV for IT Audit roles
- How to answer scenario-based questions

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on