Internal Audit, Cybersecurity & Risk Management Basic Training – 5 Days (40 Hours)

Day 1 – Basics of Internal Audit & Risk

- Introduction to Internal Audit
- Purpose and importance of Internal Audit
- Roles and responsibilities of an Internal Auditor
- Types of audits (Internal, External, Compliance, IT)
- Introduction to Risk Management
- Types of risks (Operational, Financial, IT, Compliance)
- Risk identification and assessment basics
- Overview of common audit and risk frameworks

Day 2 – Internal Audit Process & Controls

- Internal Audit lifecycle overview
- Audit planning and scoping
- Understanding business processes
- Internal controls – basic concepts
- Preventive vs Detective controls
- Control testing basics
- Audit documentation and working papers
- Writing basic audit observations and reports

Day 3 – Cybersecurity Fundamentals for Auditors

- Introduction to Cybersecurity
- Importance of cybersecurity for auditors
- Common cyber threats and attacks
- Basic IT and cybersecurity terminology
- Information security principles (CIA Triad)
- Overview of IT environments
- High-level cybersecurity frameworks (ISO 27001, NIST)
- Identifying basic cyber risks

Day 4 – IT & Cybersecurity Audit Basics

- Introduction to IT and Cybersecurity Audits
- Key IT and cybersecurity audit areas
- Access controls and user management basics
- Network and system security basics
- Data protection and privacy fundamentals
- Third-party and vendor risk basics
- Cyber incident overview
- Simple cybersecurity audit checklist

Day 5 – Integrated Risk, Compliance & Practical Overview

- Linking Internal Audit, Risk, and Cybersecurity
- Basic Governance, Risk & Compliance (GRC) concepts
- Regulatory and compliance overview (high level)
- Managing audit findings and follow-ups
- Introduction to continuous risk monitoring
- Common audit challenges and best practices
- Simple case study (Internal Audit + Cyber Risk)
- Course recap and Q&A;