MERCURY

Advanced IT Audit and Digital Risk Assurance Mastery Program

24 – 28 January 2027
Cairo (Egypt)



Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Advanced IT Audit and Digital Risk Assurance Mastery Program

Ref: 121462_1033643 **Date:** 24 – 28 January 2027 **Location:** Cairo (Egypt) **Fees:** 4000 Euro

Introduction:

In today's rapidly evolving digital landscape, organizations rely heavily on complex information systems, cloud infrastructures, and data-driven operations. This transformation has significantly elevated the importance of IT auditing as a strategic function that ensures governance, risk management, compliance, and operational integrity. Advanced IT Audit goes beyond traditional control verification and focuses on proactive risk identification, cybersecurity resilience, data analytics, and continuous auditing techniques. This program equips professionals with cutting-edge methodologies, frameworks, and tools required to audit modern IT environments effectively and provide strategic assurance to stakeholders.

Targeted Audience:

- IT Auditors and Senior Internal Auditors.
- Risk Management and Compliance Professionals.
- Information Security Specialists.
- IT Managers and System Administrators.
- Governance, Risk, and Compliance GRC Professionals.
- External Auditors dealing with IT systems.
- Professionals seeking advanced expertise in IT auditing.

Training Objectives:

At the end of this program, participants will be able to:

- Provide participants with advanced knowledge of IT audit frameworks and standards.
- Enhance the ability to identify and assess complex IT risks.
- Develop expertise in auditing emerging technologies and digital environments.
- Strengthen skills in data analytics for audit purposes.
- Enable participants to design and execute risk-based IT audit plans.
- Improve reporting, communication, and advisory capabilities in IT auditing.
- Understand and apply advanced IT audit methodologies and frameworks.
- Evaluate IT governance structures and align them with organizational objectives.
- Conduct risk-based IT audits across complex systems and infrastructures.
- Assess cybersecurity controls and incident response mechanisms.
- Utilize data analytics tools to enhance audit effectiveness.
- Audit cloud computing environments and emerging technologies.
- Provide actionable recommendations and strategic insights to management.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Targeted Competencies:

- Advanced IT Audit Planning and Execution.
- IT Risk Assessment and Management.
- IT Governance and Control Evaluation.
- Cybersecurity Audit Expertise.
- Data Analytics and Continuous Auditing.
- Regulatory Compliance and Standards Application.
- Strategic Thinking and Advisory Skills.

Course Content:

First Unit, Advanced IT Audit Frameworks and Methodologies:

- Understanding globally recognized IT audit frameworks, including COBIT, ISO 27001, NIST, and ITIL.
- Comparative analysis of frameworks and selecting the appropriate model for the organizational context.
- Designing risk-based IT audit methodologies aligned with enterprise risk management.
- Developing audit charters, policies, and procedures for IT audit functions.
- Integrating IT audit with corporate governance and internal audit functions.
- Advanced documentation techniques and audit evidence collection strategies.
- Establishing quality assurance and improvement programs for IT auditing.

Second Unit, IT Risk Assessment and Internal Controls Evaluation:

- Identifying and categorizing IT risks across infrastructure, applications, and data layers.
- Performing advanced risk assessments using qualitative and quantitative techniques.
- Evaluating general IT controls, including access management, change management, and operations.
- Assessing application controls and business process integration.
- Designing and testing internal controls for effectiveness and efficiency.
- Utilizing risk heat maps and scoring models for prioritization.
- Continuous monitoring and dynamic risk assessment approaches.

Third Unit, Cybersecurity and Information Security Auditing:

- Understanding modern cyber threats, vulnerabilities, and attack vectors.
- Auditing information security frameworks and control environments.
- Evaluating network security, endpoint protection, and identity management systems.
- Assessing incident response plans, disaster recovery, and business continuity strategies.
- Conducting penetration testing reviews and vulnerability assessments.
- Auditing compliance with cybersecurity regulations and standards.
- Measuring cybersecurity maturity and resilience.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Fourth Unit, Data Analytics and Technology-Driven Auditing:

- Introduction to data analytics in IT auditing and its strategic importance.
- Using advanced tools such as ACL, IDEA, Power BI, and Python for audit analysis.
- Designing audit tests using data extraction, transformation, and analysis techniques.
- Detecting anomalies, fraud indicators, and control weaknesses through data analysis.
- Implementing continuous auditing and continuous monitoring systems.
- Visualizing audit findings and creating dynamic dashboards.
- Integrating artificial intelligence and machine learning in audit processes.

Fifth Unit, Auditing Emerging Technologies and Digital Transformation:

- Auditing cloud computing environments, including SaaS, PaaS, and IaaS models.
- Evaluating cloud governance, security, and compliance risks.
- Auditing blockchain technology and distributed ledger systems.
- Assessing risks and controls in artificial intelligence and automation systems.
- Reviewing Internet of Things IoT environments and associated vulnerabilities.
- Addressing privacy, data protection, and regulatory challenges in digital ecosystems.
- Developing future-ready IT audit strategies for digital transformation initiatives.