

IT Audit and Information Systems Risk Controls Management

4 – 8 October 2027
Barcelona

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

IT Audit and Information Systems Risk Controls Management

Ref: 103600660_83288 **Date:** 4 – 8 October 2027 **Location:** Barcelona **Fees:** 5700 Euro

Course Overview:

The IT Audit and Information Systems Risk and Controls Management Course provides a structured professional framework for planning and conducting information technology and information systems audits across modern digital environments. It enables participants to understand the relationship between IT governance, IT risk management, internal control, information security, and cybersecurity while clarifying the responsibilities of IT auditors in protecting information assets and supporting reliable business operations.

The course progresses from the fundamentals of information systems auditing and audit scoping to IT risk assessment, risk and control matrix development, IT general controls, and application controls testing. It also addresses identity and access management, user access reviews, change management audits, database controls, IT infrastructure, cloud services, and third-party risk.

Drawing on recognized guidance covering electronic information systems auditing, essential cybersecurity controls, and audit data analytics, the course connects professional principles with organizational practice. Participants will explore electronic audit evidence, data analysis, control design and operating effectiveness, audit findings, and IT audit reporting. The course also covers information security audits, cybersecurity audits, business continuity, and disaster recovery, enabling participants to deliver objective assurance, identify control weaknesses, and recommend practical corrective actions.

Target Audience:

- IT Auditors and Information Systems Auditors
- Internal Auditors and Senior Auditors
- Information Security and Cybersecurity Auditors
- Governance, Risk, and Compliance Professionals
- IT Managers and Technology Professionals
- Internal Control and Risk Management Officers
- Information Security and Cybersecurity Analysts
- Identity and Access Management Professionals
- Business Continuity and Disaster Recovery Specialists
- Digital Systems and Electronic Process Auditors
- Data Quality and Electronic Accounting Systems Professionals

Targeted Organizational Departments:

- Internal Audit and Information Systems Audit
- Information Technology and Digital Transformation
- Cybersecurity and Information Security
- Governance, Risk, and Compliance
- Enterprise Risk and IT Risk Management
- Internal Control and Quality Assurance
- Business Continuity and Disaster Recovery
- Data Management, Databases, and Analytics
- IT Infrastructure and Technology Operations
- Cloud Services and Technology Vendor Management

Targeted Industries:

- Government Authorities and Public-Sector Organizations
- Ministries, Municipalities, and Public Institutions
- Banks, Financial Institutions, and Insurance Companies
- Telecommunications and Information Technology
- Oil, Gas, Energy, and Utilities
- Manufacturing and Industrial Organizations
- Healthcare Institutions and Hospitals
- Universities and Educational Institutions
- Transportation and Logistics
- Retail and E-Commerce
- Professional and Advisory Services

Course Objectives:

By the end of this course, participants will be able to:

- Explain the principles of IT auditing and information systems auditing.
- Define the responsibilities of IT auditors and relevant stakeholders.
- Align information systems audit objectives with IT governance and organizational priorities.
- Establish the scope, objectives, and criteria of an IT audit engagement.
- Apply a risk-based IT audit approach to engagement planning.
- Identify and assess inherent and residual IT risks.
- Develop a risk and control matrix linked to appropriate audit procedures.
- Evaluate the design and implementation of IT general controls.
- Test IT controls and assess their operating effectiveness.
- Review application controls over data input, processing, and output.
- Evaluate identity and access management and user access rights.
- Audit privileged accounts and segregation of duties.
- Assess change management, system development, and IT operations.
- Evaluate controls over databases, infrastructure, and cloud services.
- Conduct information security and cybersecurity audits systematically.

Training Methodology:

The course uses an interactive learning methodology that connects professional principles with realistic organizational situations. Each subject begins with a focused explanation before being translated into steps that an information systems auditor can apply during audit planning, examination, evaluation, and reporting. Case studies representing organizations that depend on electronic systems and cloud services will help participants analyze risks, identify relevant controls, and select suitable audit procedures.

Facilitated group discussions will explore IT governance, identity and access management, change management, database controls, cloud environments, and third-party risks. Participants will examine illustrative examples of risk and control matrices, interview questions, documentation reviews, control testing methods, and electronic audit evidence. Scenarios based on essential cybersecurity controls and electronic systems auditing will demonstrate how to distinguish between control design, implementation, and operating effectiveness.

The course will also include guided discussions on data analytics and its use in identifying anomalies, unusual transactions, and indicators of elevated risk. Participants will review examples of audit findings and learn to distinguish among the audit criterion, observed condition, root cause, risk impact, and recommendation. Each training day concludes with a structured review and feedback session that connects the topics to an end-to-end IT audit engagement.

AGILE LEADERS
Training Center

Course Resources:

The course does not include the provision of licensed software or operational technology tools. It provides professional insights, reference materials, and illustrative examples, including:

- Selected educational content from information systems audit references
- Illustrative IT audit scope and planning examples
- Sample IT risk register structure
- Example risk and control matrix
- Examples of IT general controls and application controls
- Illustrative identity and access management review points
- Sample questions for change management and IT operations audits
- Examples of electronic audit evidence and working-paper documentation
- Cloud services and third-party audit scenarios

Course Content:

Day 1: IT Audit and Information Systems Governance

- **Topic 1:** IT and information systems audit fundamentals
- **Topic 2:** Auditor roles and stakeholder responsibilities
- **Topic 3:** Independence, objectivity, and professional ethics
- **Topic 4:** IT governance and internal control
- **Topic 5:** Electronic systems and information assets
- **Topic 6:** Audit scope, objectives, and criteria
- **Reflection & Review:** Defining an information systems audit engagement

AGILE LEADERS
Training Center

Day 2: Risk-Based IT Audit Planning

- **Topic 1:** Understanding the organization and its IT environment
- **Topic 2:** Identifying critical systems, processes, and assets
- **Topic 3:** Recognizing IT threats and risks
- **Topic 4:** Assessing inherent and residual risk
- **Topic 5:** Developing a risk and control matrix
- **Topic 6:** Designing a risk-based audit plan and program
- **Reflection & Review:** Linking risks, controls, and audit procedures

Day 3: IT General and Application Controls

- **Topic 1:** IT general controls framework
- **Topic 2:** Identity, access, and user authorization
- **Topic 3:** Privileged accounts and segregation of duties
- **Topic 4:** Change management and system development audits
- **Topic 5:** Input, processing, and output controls
- **Topic 6:** IT operations, backups, and monitoring controls
- **Reflection & Review:** Evaluating control design and operating effectiveness

Day 4: Security, Infrastructure, and Digital Services Auditing

- **Topic 1:** Information security and cybersecurity audits
- **Topic 2:** Database controls and data integrity
- **Topic 3:** IT infrastructure and network auditing
- **Topic 4:** Cloud services and third-party audits
- **Topic 5:** Vulnerability, incident, and security log management
- **Topic 6:** Business continuity and disaster recovery
- **Reflection & Review:** Analyzing security and operational resilience gaps

AGILE LEADERS
Training Center

Day 5: Audit Execution, Data Analytics, and Reporting

- **Topic 1:** Collecting and evaluating electronic audit evidence
- **Topic 2:** Interviews, observation, and document examination
- **Topic 3:** Sampling and IT control testing
- **Topic 4:** Data analytics and exception detection
- **Topic 5:** Developing findings, causes, impacts, and recommendations
- **Topic 6:** Audit reporting and corrective-action follow-up
- **Reflection & Review:** Developing integrated IT audit results

FAQ:

What qualifications or prerequisites are required before attending the course?

No specific professional certification is required. A basic understanding of internal audit, risk management, internal control, information security, or information technology is beneficial. The course introduces technical concepts progressively, making it suitable for both audit professionals and IT specialists.

How long is each daily session, and what is the course's total duration?

Each daily session lasts approximately four to five hours, including breaks and interactive activities. The course is delivered over one week, providing a total of approximately 20 to 25 training hours.

What is the difference between IT general controls and application controls, and how are they tested?

IT general controls support the overall technology environment and include access management, change management, backups, and IT operations. Application controls operate within a particular system or business process and address the accuracy, completeness, authorization, and validity of inputs, processing, and outputs. Auditors test these controls through document examination, interviews, observation, reperformance, data analysis, and sampling before comparing the results with the established audit criteria.

AGILE LEADERS
Training Center

How This Course Differs from Other Courses:

This course distinguishes itself by integrating information systems auditing, IT risk management, cybersecurity, and organizational controls into a single learning journey that reflects the complete audit lifecycle. Instead of presenting IT audit concepts as isolated theoretical subjects, it demonstrates how auditors convert their understanding of systems and processes into assessable risks, testable controls, reliable evidence, and clearly communicated findings.

The content draws on specialized references covering electronic information systems auditing, essential cybersecurity controls, IT audit matrices, and the use of data analytics in assurance activities. This provides an effective balance between professional foundations and organizational application. Participants examine IT general controls and application controls alongside identity and access management, change management, databases, infrastructure, cloud services, and third-party arrangements.

The course places particular emphasis on the auditor's professional judgment: why a control should be tested, what constitutes sufficient evidence, how control effectiveness should be evaluated, and how findings and recommendations should be developed. It also addresses business continuity, disaster recovery, audit data analytics, and IT audit reporting. This integrated scope makes the course relevant across industries and suitable for professionals seeking a comprehensive understanding of technology-related assurance without limiting the training to one system, framework, or professional examination.