Global Horizon
TRAINING CENTER

Training Course:
Certified in Risk and Information Systems Control Training Program

16 - 20 November 2026
London (UK)

Training Course:
Certified in Risk and Information Systems Control Training Program

Training Course code: IT236612 From: 16 - 20 November 2026 Venue: London (UK) - Training Course Fees: 6300 Euro

Introduction

The Certified in Risk and Information Systems Control Training Program is designed by Global Horizon Training Center to provide professionals with comprehensive knowledge and practical capabilities in IT risk management, information systems controls, governance, risk response, and technology-related security principles.

As organizations become increasingly dependent on digital technologies, cloud environments, interconnected systems, and data-driven operations, managing technology-related risks has become a critical business priority. Professionals responsible for risk, governance, cybersecurity, audit, and information systems must be able to identify emerging threats, assess their potential business impact, establish appropriate controls, and continuously monitor risk exposure.

This intensive five-day training program provides participants with a structured approach to identifying, analyzing, evaluating, responding to, and monitoring IT-related risks. It also develops the skills required to design, implement, assess, and maintain effective information systems controls aligned with organizational objectives and recognized risk management practices.

The program combines conceptual knowledge with practical risk scenarios, control analysis, case studies, and assessment exercises, enabling participants to translate risk and control principles into effective organizational practices.

Training Objectives

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

- Understand the principles of IT risk management and information systems control.
- Explain the relationship between enterprise governance, business objectives, IT risk, and information systems controls.
- Identify internal and external events that may create technology-related risks.
- Conduct structured IT risk identification and assessment.
- Analyze risk likelihood, impact, exposure, and organizational consequences.
- Develop and maintain effective IT risk registers.
- Establish appropriate risk appetite and tolerance considerations.
- Evaluate alternative risk response and treatment strategies.
- Identify and recommend appropriate information systems controls.

- Understand preventive, detective, corrective, and compensating controls.
- Assess control design and operating effectiveness.
- Develop appropriate Key Risk Indicators KRIs and control metrics.
- Monitor changes in the technology and business environment that affect risk.
- Communicate IT risk effectively to management and relevant stakeholders.
- Integrate risk management and information systems control into organizational decision-making.

Course Methodology

The program uses an interactive and application-oriented methodology to ensure that participants can translate theoretical concepts into practical workplace capabilities.

The methodology includes:

- Instructor-led presentations and facilitated discussions.
- Practical explanations of IT risk and control concepts.
- Real-world business and technology risk scenarios.
- Case studies covering risk identification, assessment, and response.
- Risk assessment and control evaluation exercises.
- Group discussions and experience sharing.
- Practical development of risk registers and control matrices.
- Analysis of Key Risk Indicators and control performance measures.
- Scenario-based exercises for risk response and reporting.
- Knowledge reviews and assessment questions throughout the program.

Organizational Impact

Organizations whose professionals complete this training program can benefit from:

- Stronger alignment between IT risk management and organizational objectives.
- Improved identification and assessment of technology-related risks.

- More structured and consistent risk management practices.
- Enhanced design and implementation of information systems controls.
- Improved understanding of control effectiveness and control deficiencies.
- Stronger governance and accountability for technology-related risks.
- Better communication of IT risks to senior management and stakeholders.
- Improved monitoring through meaningful risk indicators and control metrics.
- Increased organizational resilience against technology disruptions and emerging threats.
- Better integration of cybersecurity, IT governance, risk, compliance, and assurance activities.
- More informed risk-based decision-making across technology environments.

Target Audience

This training program is suitable for professionals involved in IT risk management, governance, cybersecurity, compliance, audit, and information systems control, including:

- IT Risk Managers and Officers
- Enterprise Risk Management Professionals
- IT Governance Professionals
- GRC Managers and Specialists
- Information Security Managers and Specialists
- Cybersecurity Professionals
- IT Auditors and Internal Auditors
- Information Systems Auditors
- Risk and Compliance Officers
- IT Managers and Supervisors
- Information Systems Managers
- IT Control and Assurance Professionals
- Business Continuity and Resilience Professionals
- Technology Consultants

- Professionals responsible for designing, implementing, or monitoring IT controls
- Professionals seeking to strengthen their knowledge of risk and information systems control

Training Outline

Day 1 - IT Risk Governance and Organizational Context

IT Risk and Enterprise Governance

- Understanding IT risk in the modern organization
- Relationship between business risk and technology risk
- Enterprise governance and IT governance
- Aligning IT risk management with business objectives
- Roles and responsibilities in IT risk governance
- Risk ownership and accountability
- Three Lines Model and risk oversight
- Establishing an effective risk management culture

Organizational Risk Context

- Internal and external business environments
- Understanding organizational strategy and objectives
- Technology dependencies and critical business services
- Regulatory, contractual, and compliance considerations
- Stakeholder expectations and risk perspectives
- Organizational risk capacity, appetite, and tolerance

Risk Management Framework

- Principles of enterprise risk management
- IT risk management lifecycle
- Establishing risk management policies and standards
- Risk taxonomy and classification

- Risk management roles and escalation structures
- Integrating IT risk with enterprise risk management

Day 2 - IT Risk Identification and Assessment

Risk Identification

- Understanding risk scenarios
- Identifying threats, vulnerabilities, assets, and business impacts
- Internal and external risk sources
- Cybersecurity and information security risks
- Technology infrastructure risks
- Application and data risks
- Third-party and supply-chain risks
- Cloud and outsourced service risks
- Emerging technology risks

Risk Assessment

- Inherent versus residual risk
- Qualitative and quantitative assessment approaches
- Assessing likelihood and impact
- Financial, operational, regulatory, and reputational impact
- Risk scoring and prioritization
- Risk matrices and heat maps
- Understanding risk aggregation and concentration

Risk Analysis and Documentation

- Developing effective risk scenarios
- Root cause and contributing-factor analysis
- Establishing risk registers

- Documenting assumptions and dependencies
- Prioritizing risks for management attention

Day 3 - Risk Response and Risk Treatment

Risk Response Strategies

- Risk avoidance
- Risk mitigation
- Risk transfer and sharing
- Risk acceptance
- Selecting appropriate risk responses
- Cost-benefit considerations in risk treatment
- Evaluating response effectiveness
- Understanding residual risk after treatment

Developing Risk Action Plans

- Defining risk treatment objectives
- Establishing actions, responsibilities, and timelines
- Assigning risk and control ownership
- Resource requirements
- Prioritizing remediation initiatives
- Risk acceptance and exception processes
- Management approval and escalation

Risk and Control Integration

- Translating risk scenarios into control requirements
- Mapping risks to controls
- Identifying control gaps
- Control rationalization

- Managing excessive or redundant controls
- Risk-based control selection

Risk Communication

- Communicating risk to business stakeholders
- Management-level risk reporting
- Executive risk dashboards
- Escalation of significant risks
- Communicating residual risk and control weaknesses

Day 4 - Information Systems Controls: Design and Implementation

Fundamentals of Information Systems Controls

- Purpose and importance of information systems controls
- Relationship between risks and controls
- Control objectives
- Control design principles
- Manual versus automated controls
- Preventive controls
- Detective controls
- Corrective controls
- Compensating controls

Key Information Systems Control Areas

- Identity and access management
- Privileged accen
- Control matrices
- Implementing controls within business and IT processes
- Integrating controls into technology operations

Day 5 - Control Assessment, Risk Monitoring and Reporting

Control Assessment

- Understanding control design effectiveness
- Assessing operating effectiveness
- Control testing concepts
- Evidence and documentation
- Identifying control deficiencies
- Evaluating the significance of control weaknesses
- Root cause analysis of control failures
- Developing corrective actions

Risk and Control Monitoring

- Continuous risk monitoring
- Continuous control monitoring
- Key Risk Indicators KRIs
- Key Performance Indicators KPIs
- Key Control Indicators KCIs
- Establishing thresholds and triggers
- Monitoring changes in risk exposure
- Emerging risk identification
- Tracking remediation activities

Risk Reporting and Communication

- Designing effective risk reports
- Risk dashboards and heat maps
- Reporting to senior management
- Communicating significant control deficiencies

- Risk escalation mechanisms
- Providing actionable risk information
- Supporting risk-informed decision-making

Maintaining an Effective Risk and Control Environment

- Periodic reassessment of risks
- Reviewing control effectiveness
- Responding to changes in technology and business processes
- Lessons learned from incidents and control failures
- Continuous improvement of risk management practices
- Building organizational risk awareness

Registration form on the Training Course: Certified in Risk and Information Systems Control Training Program

Training Course code: IT236612 From: 16 - 20 November 2026 Venue: London (UK) - Training Course Fees: 6300 Euro

Complete & Mail or fax to Global Horizon Training Center (GHTC) at the address given below

Delegate Information

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Company Information

Company Name: .....
Address: .....
City / Country: .....

Person Responsible for Training and Development

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Payment Method

- ☐ Please find enclosed a cheque made payable to Global Horizon
- ☐ Please invoice me
- ☐ Please invoice my company

Easy Ways To Register

Telephone: +201095004484 to provisionally reserve your place.	Fax your completed registration form to: +20233379764	E-mail to us : info@gh4t.com or training@gh4t.com	Complete & return the booking form with cheque to:Global Horizon 3 Oudai street, Aldouki, Giza, Giza Governorate, Egypt.