Advanced in AI Risk Training

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Duration: **2 Day**

Advanced in AI Risk is an expert-led program focused on helping experienced professionals manage the governance, security, compliance and operational risks emerging as artificial intelligence becomes increasingly embedded within modern organisations.

Over two days, learners develop specialist knowledge and practical skills for identifying, assessing, classifying and controlling AI-related risks. The course examines how AI risk can be incorporated into existing Enterprise Risk Management (ERM) structures and how vulnerabilities can be evaluated throughout the AI lifecycle.

The program considers AI risk across areas including model design, algorithms, training, model drift, validation, data and asset management, third-party relationships and eventual decommissioning. It also extends beyond technical threats to consider regulatory obligations, ethics, privacy, intellectual property, societal impact and ESG considerations.

An important focus is the operational integration of AI risk management. Learners examine how AI-related considerations can be embedded into risk registers, control frameworks, incident management, business continuity, disaster recovery, change management, supply chains and third-party governance.

The course also prepares learners for the **ISACA Advanced in AI Risk (AAIR)** certification. An exam voucher is included, with the examination scheduled directly through ISACA following course completion.

Prerequisites

Learners should have a strong foundation in governance, risk management and information security principles. Previous professional experience within risk, compliance or security functions is recommended.

The course is intended for experienced governance, risk and security professionals looking to extend their existing expertise into AI risk management.

It is particularly relevant to professionals holding certifications such as:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Certified in Governance, Risk and Compliance (CGRC)
- Certified Information Systems Security Professional (CISSP)

Advanced in AI Risk Training

BILGINC IT Academy
info@bilginc.com
bilginc.com

Duration: **2 Day**

What You Will Learn

By the end of the course, learners will be able to:

- Evaluate risks associated with AI model design, algorithms, training, drift and lifecycle management.
- Integrate AI risk management into enterprise risk management programs.
- Develop an AI risk management framework covering responsibilities, accountability and risk tolerance.
- Conduct structured assessments to identify and classify AI risks.
- Recommend and justify suitable risk treatment strategies.
- Evaluate compliance with AI-related regulations, standards and legal obligations.
- Incorporate AI risks into governance structures, risk registers and control frameworks.
- Assess AI use cases against organisational risk appetite.
- Monitor and test processes to identify emerging AI risks.
- Collaborate across organisational functions to improve AI risk awareness.
- Develop AI risk metrics and reporting for operational and executive audiences.
- Perform threat and vulnerability assessments for AI initiatives.
- Incorporate AI risk into incident management, business continuity and disaster recovery.
- Continuously monitor changes in the AI risk landscape.
- Evaluate and validate controls to maintain risk within acceptable tolerance.
- Advise on contractual AI risks, including data usage and intellectual property.
- Evaluate AI risks within supply chains and third-party relationships.
- Address ethical, societal and ESG considerations, including bias, privacy and safety.
- Use AI capabilities to strengthen risk management processes.
- Integrate AI risk considerations into change management.
- Evaluate human oversight controls at critical decision points.

Training Outline

Domain 1: AI Risk Governance and Framework Integration

This domain establishes the governance foundations required for effective AI risk management and considers how AI initiatives can be aligned with organisational strategy.

- AI models and approaches
- AI frameworks and strategies
- AI use cases
- Organisational processes for AI
- Alignment with organisational objectives
- AI ownership and accountability
- Oversight responsibilities
- AI policies and procedures
- Organisational training and risk awareness
- Regulatory compliance
- Legal considerations
- AI trustworthiness
- Ethical and societal implications
- ESG considerations

Advanced in AI Risk Training

BILGINC IT Academy
info@bilginc.com
bilginc.com

Duration: **2 Day**

Domain 2: AI Lifecycle Risk Management

This domain examines how risk should be considered throughout the complete AI lifecycle, from initial design through to retirement.

- AI design risks
- Development and procurement
- AI documentation
- Model training
- Testing and validation
- Model performance and change
- AI implementation
- Maintenance and lifecycle management
- Decommissioning
- AI data management
- AI asset management

Domain 3: AI Risk Program Management

This domain focuses on operationalising AI risk management through structured programs, controls, metrics and continuous monitoring.

- AI risk scenario identification
- Threat, vulnerability and attack assessment
- Structured AI risk assessment
- Risk treatment strategies
- AI control selection
- Control evaluation and validation
- AI risk metrics
- Continuous monitoring
- Risk reporting
- AI supply chain risk management
- Third-party resources and services
- AI incident response
- Business Impact Analysis (BIA)
- Business continuity
- Disaster recovery

Exam and Certification

The course prepares learners for the **ISACA Advanced in AI Risk (AAIR)** certification examination.

ISACA Product Access Changes

Effective **16 April 2026**, ISACA is reducing access periods for certain products from **12 months to 6 months**, including exams, QAE, Online Review Courses, non-sponsored webinars and Virtual Workshops.

The revised model uses two primary access windows:

1. **Assignment and Redemption Window:** Products must be assigned and redeemed within six months of purchase.
2. **Access and Completion Window:** Once redeemed, learners receive six months of access. This period includes accessing learning materials, scheduling examinations and sitting applicable exams.

For learners:

- **Review Manuals:** Long-term access will continue.
- **QAE Databases and Online Review Courses:** Available for six months following redemption.
- **Exams:** Must be scheduled and completed within six months of redemption.

Learners are therefore encouraged to redeem products promptly and plan their study and examination schedule early enough to make full use of the available access period.