Certified Lead AI Risk Manager Training

Duration: **4 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Build and integrate a comprehensive AI risk management programme across your organisation.

Develop practical expertise for navigating rapidly evolving AI regulations in risk and compliance roles.

Work through nine hands-on exercises covering real AI risk scenarios, from the AI lifecycle through to risk treatment.

Certified Lead AI Risk Manager equips professionals with the knowledge, methods, and practical tools required to identify, assess, and manage risks associated with the use of artificial intelligence in modern organisations. The course examines AI governance, regulatory compliance, and ethical considerations through internationally recognised approaches such as the **NIST AI Risk Management Framework** and the **EU AI Act**.

Participants gain practical experience applying these approaches to realistic AI risk scenarios, including bias, security vulnerabilities, and transparency concerns. A central focus of the course is understanding AI risk management not simply as a technical control activity, but as an ongoing discipline that should be embedded within organisational strategy and governance.

The programme examines standards that support the development, deployment, and governance of AI systems, including **ISO 42001, ISO 42005, ISO 22989, ISO 23894, ISO 38507, ISO 24028, and ISO 23053**. It also covers important risk management resources and frameworks such as the**NIST AI Risk Management Framework** and the **MIT AI Risk Repository**.

By the end of the course, participants will be better prepared to establish an organisational approach to AI risk that supports responsible, compliant, and ethical AI adoption.

Prerequisites

Participants should have a foundational understanding of:

- Artificial intelligence concepts and data governance principles,
- Organisational risk management or information security practices,
- Compliance and governance structures within a business environment.

Certified Lead AI Risk Manager Training

Duration: **4 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

This course is designed for:

- Risk, compliance, and governance professionals responsible for AI-related initiatives,
- IT and security specialists involved in assessing AI systems and associated controls,
- Data scientists, AI developers, and engineers incorporating responsible AI practices into their work,
- Consultants advising organisations on AI risk management and mitigation,
- Legal, ethical, and compliance advisors specialising in AI regulation.

What You Will Learn

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

- Explain the fundamental concepts and principles of AI risk management and governance,
- Apply frameworks such as the NIST AI Risk Management Framework and the EU AI Act when considering compliance and ethical requirements,
- Identify and assess key AI risks, including bias, data security, transparency, and accountability,
- Develop and implement AI risk mitigation and incident response strategies,
- Integrate AI risk management into broader business, risk, and compliance frameworks,
- Analyse real-world cases to identify lessons learned and good practices for controlling AI risk,
- Support responsible AI use across the organisation through governance and continual improvement.

Training Outline

Introduction to AI Risk Management

This section examines both the opportunities created by artificial intelligence and the risks and challenges it introduces for modern organisations.

- Opportunities and challenges associated with AI in modern organisations
- Essential terminology, definitions, and risk management concepts
- Overview of global AI risk management standards and regulations

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

- Recognise how international AI standards and frameworks support the governance, development, and deployment of AI systems,
- Explain the global AI regulatory landscape and consider alignment across regions including the EU, UK, U.S., and beyond.

AI Risk Identification, Assessment, and Measurement

This section focuses on how AI risks emerge, how they can be classified, and the methods available for assessing them.

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Techniques for identifying and categorising AI-related risks
- Quantitative and qualitative approaches to risk assessment
- Assessment of AI model reliability, data integrity, and ethical exposure

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

- Identify fundamental AI components and understand how risks, impacts, and harms can emerge from AI use,
- Evaluate major sources of AI risk and explain the benefits of structured AI risk management practices,
- Outline the stages of the AI lifecycle and assess how risks can change across different phases.

AI Risk Mitigation, Governance, and Incident Response

This section examines how identified risks can be treated and how an organisational AI risk management programme can be established.

- Design mitigation strategies aligned with compliance frameworks
- Establish governance structures that support ethical AI deployment
- Plan incident response and escalation procedures for AI failures and bias events

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

- Explain the structure and purpose of an AI risk management programme, including how essential controls and frameworks contribute to risk reduction,
- Establish AI risk governance structures, define AI system scope and boundaries, and conduct gap analyses to support effective oversight,
- Apply AI risk criteria and context-setting methods to align governance with organisational objectives,
- Identify AI-related risks, sources, events, and outcomes while mapping risks across systems and processes,
- Assign AI risk ownership to strengthen accountability, responsibility, and traceability.

AI Risk Monitoring and Continual Improvement

This section considers how AI risks and controls can be measured, monitored, and improved after implementation.

- Establish metrics and KPIs for AI risk performance
- Continuously evaluate AI systems through audits and impact assessments
- Incorporate lessons learned into organisational governance frameworks

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

- Apply qualitative and quantitative AI risk analysis methods to assess probability, impact, and overall risk levels,
- Evaluate AI-related risks against defined criteria, including EU AI Act categories, and prioritise them for treatment,
- Develop structured AI risk treatment plans using appropriate strategies and post-deployment activities,
- Determine suitable controls for AI risk treatment and integrate them into organisational processes,
- Review the effectiveness of implemented controls on an ongoing basis to support risk mitigation

and organisational resilience.

AI Risk Management in Business Strategy

The final section explores how AI risk management can become part of wider organisational strategy, governance, and enterprise risk practices.

- Connect AI risk management with strategic planning and enterprise risk frameworks
- Maintain accountability and ethical oversight within AI operations
- Develop a culture that supports responsible and transparent AI innovation

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

- Implement AI risk monitoring and reporting practices using performance metrics, recordkeeping, and lessons learned to support transparency and accountability,
- Establish competence and awareness programmes that address workforce skill gaps, encourage professional development, and sustain responsible AI operations,
- Evaluate the effectiveness of AI risk management through monitoring, internal audits, and performance reviews,
- Apply continual improvement practices to optimise AI risk management and strengthen organisational resilience.

Exams and Assessments

Participants complete a **formal certification examination administered by PECB** after the course.