Cybersecurity Specialization: AI Risk Management Framework Training

Duration: **2 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Exclusive - Learn to navigate global AI risk and regulatory frameworks with confidence and clarity.

As artificial intelligence becomes increasingly embedded in critical systems, managing its risks is no longer optional—it's essential. This two-day, hands-on course is designed to equip AI practitioners, cybersecurity professionals, risk managers, and compliance leaders with the tools and frameworks needed to navigate the complex landscape of AI risk. Participants will explore the structure and application of the NIST AI Risk Management Framework (AI RMF), compare it with global standards such as the EU AI Act and Saudi Arabia's NCA AI & Data Governance Framework, and learn how to apply these principles to real-world scenarios.

Through a blend of expert-led instruction, interactive activities, and case-based exercises, learners will gain practical experience in identifying, assessing, and mitigating AI risks such as bias, explainability, and data privacy. The course emphasizes ethical governance and regulatory compliance, guiding participants in designing unified risk strategies that align with international standards. Whether you're building AI systems or overseeing their deployment, this course offers a comprehensive foundation for responsible and secure AI implementation.

Who Should Attend?

This course is designed for AI practitioners, risk managers, cybersecurity professionals, compliance officers, policymakers, and organizational leaders involved in the development, deployment, or oversight of AI systems.

Prerequisites

- Participants should have a foundational understanding of AI systems and basic knowledge of risk management or cybersecurity principles.
- Familiarity with regulatory concepts or frameworks (such as GDPR or NIST CSF) is helpful but not required.

Cybersecurity Specialization: AI Risk Management Framework Training

Duration: **2 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

- Identify key risks associated with AI systems, including bias, explainability, privacy, and robustness.
- Describe the structure and components of the NIST AI Risk Management Framework (AI RMF).
- Compare global AI governance frameworks, including the EU AI Act, NIST AI RMF, Saudi NCA AI Framework and OECD AI Principles.
- Explain how AI risk categories (e.g., high-risk, unacceptable risk) are determined under the EU AI Act.
- Analyze the alignment and divergence between NIST AI RMF, Saudi NCA AI Framework and the EU AI Act in addressing AI risk.
- Apply NIST AI RMF functions (Map, Measure, Manage, Govern) to real-world AI use cases.
- Evaluate AI governance strategies for ethical alignment and regulatory compliance.
- Design a unified AI risk management strategy that addresses global compliance and cybersecurity needs.
- Construct practical mitigation plans for identified AI risks, including monitoring and control mechanisms.
- Collaborate in teams to assess AI risk scenarios and recommend strategy improvements.
- Interpret real-world case studies to extract best practices and lessons learned for AI risk implementation.

Training Outline

1. **Introduction to AI Risk Management and Global Frameworks**
   - Introduction to AI Risk Management
   - Overview of Key Global AI Frameworks
   - Mapping Global Frameworks to AI Risk Management Practices
   - AI Governance, Ethics, and Accountability
2. **Advanced AI Risk Management Strategies and International Compliance**
   - Advanced Risk Management Strategies for AI Systems
   - Regional Variations
   - Case Studies: AI RMF and EU AI Act Implementation
   - Designing a Global AI Risk Management Strategy