Advanced in AI Security Management (AAISM) Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

Advanced in AI Security Management (AAISM) eğitimi, yapay zekâ sistemlerinin güvenli yönetimi, risk kontrolü ve kurumsal yönetişimi üzerine odaklanan ileri seviye bir siber güvenlik programıdır. ISACA tarafından geliştirilen bu sertifika programı, kurumların AI teknolojilerini güvenli, etik ve uyumlu şekilde kullanmasını sağlar.

Bu yoğunlaştırılmış eğitim programı, katılımcılara şu konularda derin bilgi kazandırır:

- Yapay zekâ yönetişim (AI Governance) süreçleri
- AI risk yönetimi ve kontrol mekanizmaları
- Güvenli ve etik AI kullanım prensipleri
- Kurumsal düzeyde AI güvenlik stratejileri

Ayrıca eğitim, ISACA'nın global standartları ile uyumlu olarak hazırlanmıştır.

Neden AAISM Eğitimi Almalısınız?

- AI güvenliği alanında uzmanlaşma
- Kurumsal riskleri minimize etme
- Uluslararası geçerliliğe sahip sertifika
- Kariyer gelişimi ve liderlik fırsatları

Prerequisites

Eğitime katılmak için önerilen kriterler:

- ISACA CISM veya ISC2 CISSP sertifikasına sahip olmak
- Güvenlik alanında deneyim
- AI sistemleri hakkında temel bilgi

Who Should Attend

Bu eğitim özellikle aşağıdaki profesyoneller için uygundur:

- Bilgi güvenliği yöneticileri ve danışmanlar
- GRC (Governance, Risk, Compliance) uzmanları
- Siber güvenlik liderleri
- AI güvenlik altyapısı kurmak isteyen kurumlar

Advanced in AI Security Management (AAISM) Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

What You Will Learn

Eğitim sonunda katılımcılar:

- AI yönetişim framework'lerini yönetebilir
- Risk analizleri yapabilir ve çözüm planı oluşturabilir
- AI sistemlerini güvenlik açısından değerlendirebilir
- KPI ve KRI metrikleri oluşturabilir
- AI güvenlik programları tasarlayabilir

Outline

Domain 1. AI governance and program management

- Stakeholder considerations, frameworks, and regulatory requirements
- Organisational structure, roles, and governance models
- Defining charters and establishing AI steering committees
- Risk appetite, tolerance, and framework alignment
- Selecting and applying appropriate AI governance frameworks
- Developing AI business use cases and managing privacy implications
- Establishing AI strategies, policies, and procedures
- Responsible and acceptable use of AI systems
- Managing AI assets and data lifecycles
- Creating AI asset inventories and data management protocols
- Model documentation, classification, and storage practices
- Implementing AI data protection and destruction measures
- Building an AI security management program
- Establishing documented plans, team roles, and proficiency standards
- Integrating AI-enabled security tools and performance metrics
- Developing KRIs and KPIs to measure AI security effectiveness
- Managing business continuity and incident response for AI
- Implementing AI-specific detection, notification, and escalation processes
- Designing AI response playbooks and red-button protocols
- Defining recovery objectives (RTO and RPO) from an AI perspective

Domain 2. AI risk management

- Conducting AI risk assessments and defining acceptable risk thresholds
- Performing impact, conformity, and privacy impact assessments (PIAs)
- Developing treatment plans and documenting AI-specific risk responses
- Implementing AI-focused penetration testing, vulnerability testing, and red teaming
- Managing adversarial and insider threats within AI ecosystems
- Identifying AI-enabled threats, deepfakes, and synthetic data misuse
- Applying threat intelligence to AI-based attack chains and anomaly detection
- Managing AI vendor and supply chain risk
- Conducting due diligence and defining accountability between provider and deployer
- Managing dependencies in AI software packages and libraries
- Establishing SLAs, ownership, and IP considerations for AI systems
- Implementing access control, liability, and vendor monitoring processes

Advanced in AI Security Management (AAISM) Eğitimi

Süre: **2 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Domain 3. AI technologies and controls

- Designing AI security architecture aligned with secure-by-design principles
- Managing AI change control and secure development lifecycles (SDL)
- Securing infrastructure-as-code and model interconnectivity
- Managing AI model lifecycles, including selection, training, validation, and regression testing
- Implementing technical evaluation, verification, and validation (TEVV) of AI models
- Applying data management controls to mitigate data poisoning, bias, and accuracy issues
- Managing privacy, ethical, trust, and safety controls within AI systems
- Ensuring explainability, consent, transparency, and fairness in AI decision-making
- Maintaining human oversight (human-in-the-loop) in automated processes
- Applying trust and safety measures such as content moderation and harm prevention
- Monitoring environmental impact and ensuring data minimisation and anonymisation
- Designing and implementing AI security controls and continuous monitoring processes
- Mapping AI security threats to controls and metrics
- Implementing control life cycles and self-assessments (CSA)
- Delivering AI security awareness training to drive organisational readiness