https://cloudsecurityalliance.org/artifacts/ai-risk-management-thinking-beyond-regulatory-boundaries

标题：AI风险管理：超越监管界限的思考

发布日期：2024年11月13日

虽然人工智能（AI）提供了巨大的好处，但它也引入了重大的风险和挑战，这些尚未得到解决。一个全面的AI风险管理框架是我们能够真正信任AI的唯一途径。这种方法需要主动考虑超越监管必要性的合规性改进。

为了满足这一需求，本出版物提出了一种全面的方法，用于公正地评估AI系统，超越单纯的合规性。它涉及AI技术的关键方面，包括数据隐私、安全和信任。这些审计考虑适用于广泛的行业，并建立在现有的AI审计最佳实践之上。这种创新的方法涵盖了整个AI生命周期，从开发到退役。

第一部分建立了对用于端到端评估AI的组件的全面理解。它分享了对广泛技术的考虑，使批判性思维成为可能，并支持风险评估活动。

第二部分由附录组成，附录中包含与第一部分涵盖的每项技术相对应的潜在问题。这些问题并非穷尽无遗，但作为识别潜在风险的指导方针。目的是激发非传统思维和挑战现有假设，从而增强AI风险评估实践，提高智能系统的整体可信度。

关键要点：

用于端到端评估AI的基本概念、原则和词汇

评估智能系统的关键指标

超越监管合规性的AI可信度的价值

如何在AI生命周期的所有阶段评估风险，包括开发、部署、监控和退役

有助于有效AI治理的关键因素

如何遵守全球AI法规，如通用数据保护条例（GDPR）和欧盟AI法案

评估AI系统时需要考虑的具体方面，包括AI基础设施、传感器、数据存储、通信接口、控制系统、隐私方法等

与上述概念相关的评估问题