DOI: doi.org/10.47363/JAICC/ICADCCS2026/2026(5)5

International Conference on AI, Data Science, Cybersecurity, Cloud Architectures, and Software Engineering

Conference Proceedings April 22, 2026 - Germany

Audit Ready AI Agentic Coding: ISO 27001 Governance for GitHub Copilot in Financial Services

Ibrahim Diab

Senior IT Security Manager, Germany

Abstract
Fintechs increasingly rely on fast software delivery while facing bank grade expectations for auditability, change control, and data protection. Agentic AI coding is evolving the Software development cycle and in the same time is introducing new governance & compliance challenges. This session presents a practical, ISO/IEC 27001 aligned governance model for deploying GitHub Copilot in GitHub.com (chat and platform features) with "audit ready by design" evidence.

We translate ISO 27001 risk treatment and the Statement of Applicability (SoA) into enforceable controls across three layers: (1) Copilot policy governance (enterprise/org policy enforcement for feature availability and model access), (2) agentic visibility and audit trails using GitHub's AI Controls, including agent session visibility and agentic audit log events to answer "what happened, when, and on whose behalf," and (3) secure operating practices for regulated SDLC—segregation of duties, mandatory reviews, and evidence collection for audits.

Attendees will get a repeatable blueprint: a Copilot-specific SoA pattern, a control to evidence map (policies → logs → audit artifacts), and a minimal governance checklist that preserves developer velocity while strengthening compliance posture. We also discuss how vendor assurance artifacts support third party risk conversations, noting GitHub's published statement that Copilot Business and Copilot Enterprise are included in the scope of GitHub's ISMS.