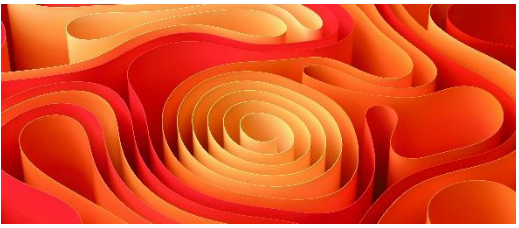
Pills

Regulatory/Supervisory Pills | N.92 June 2025



TOPICS:

Technology

SOURCE

Federal Office for Information Security - Germany

Federal Office for Information Security - Germany: Test Criteria Catalogue for AI Systems in Finance

- The **Test Criteria Catalogue for AI Systems in Finance** - prepared by the Federal Office for Information Security (BSI) - provides a structured framework for evaluating the security, trustworthiness, and compliance of AI systems used in the financial sector. Developed under the BSI's AICRIV Finance project, **the catalogue aims to align AI applications with the** EU AI Act while addressing sector-specific risks and regulatory expectations.
- The catalogue introduces a **risk-based, holistic, and adaptable audit approach,** allowing both self-assessment and external audits. It employs an initial questionnaire to tailor the evaluation process based on system characteristics and risk profile, ensuring relevance across diverse financial use cases.
- **Ten dimensions** form the backbone **of the evaluation: AI Security & Robustness** – Evaluates resilience against attacks (e.g., evasion, backdoor, model theft), robustness under corner cases, and handling of AI-specific incidents; **IT Security** – Covers classical IT safeguards like access controls, network protection, and supply chain security; **Monitoring** – Focuses on ongoing performance tracking, anomaly detection, and incident response; **Performance** – Ensures functional correctness, efficiency, reliability, and resistance to overfitting; **Governance** - Addresses organizational structures, AI policy reviews, competency management, and legal implications; **Human Oversight** – Examines the presence and effectiveness of human-in-the-loop mechanisms; **Fairness** – Assesses bias, ethical considerations, and accessibility; **Transparency** – Promotes explainability, user awareness, and documentation of AI processes; **Data Quality & Management** – Mandates high standards for data sourcing, integrity, consent management, and documentation; **Development** – Stipulates comprehensive technical documentation, model selection transparency, and controlled deployment practices.
- **Each criterion is clearly mapped to relevant EU AI Act articles** - particularly those on risk management, transparency, robustness, and quality management - providing practical pathways towards regulatory compliance.