Curating AI Tools That Are Secure, Compliant and Enterprise Ready

Transforming financial services through strategic AI implementation with robust security frameworks

Parinita Kothari

Engineering Lead, Lloyds Banking Group

Why Risk Assessment & Security Controls Matter

Confidential Customer Data

Protecting Privacy, Preserving Trust

Cyber Threat Reality

AI-driven cyber attacks surge: 93% of companies expect daily AI attacks in 2025

Regulatory Compliance

GDPR, CCPA, and SEC regulations demand transparent, secure AI deployment

Big Fintechs' Strategic AI Curation

Key Components for Success

01

Scalable Infrastructure

One Standard, Maximum Uptime and Optimal Cost

02

Multi-Layered Security Controls

Policy Driven Security, Automated by Design

03

Embedded Observability

Automated monitoring, robust Infrastructure management and proactive threat detection

04

Continuous Updates

Staying Ahead with Continuous Updates

End-to-End AI Product Curation Workflow

1. Define Business Objectives

Clear Objectives, Measurable Outcomes

2.Product Enterprise Readiness Assessment

Ensuring Confidence, Before Enterprise Adoption

3. Offering AI tools & Services as Code

Declarative, Scalable and Intelligent

4. Security & Compliance Integration

Integrating Trust, Enforcing Standards

5. Deployment & Monitoring

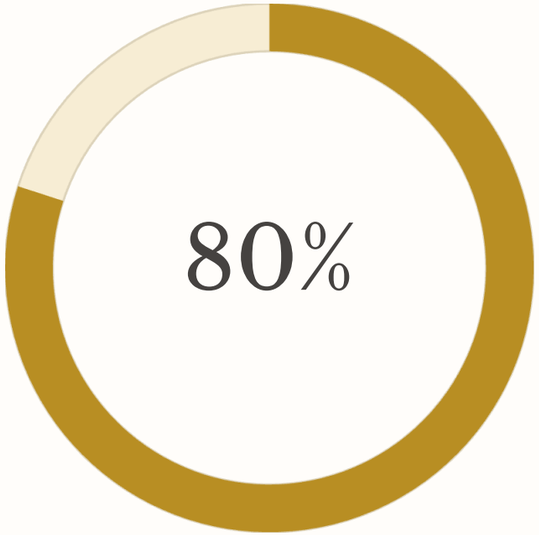
Human oversight with continuous performance metrics and improvement

6. Self Serve

Empower Teams, Unlock Agility - Internal Developement Portal & Backstage

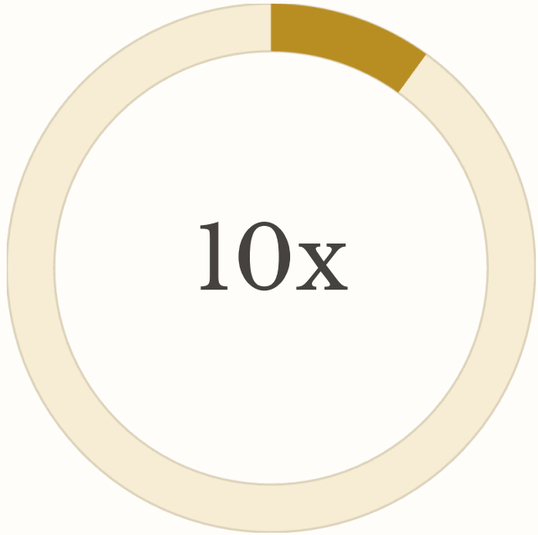
Benefits Delivered by Curation Workflow

Transformative Impact in Big Fintechs



Cost Reduction

Operational savings via standardization of curation workflow



Faster Adoption

Build once for use by multiple teams

Speeding AI Innovation: Making AI products accessible across the Bank, faster than ever

Scaling AI tools to multiple teams: Our 'Self Serve, Curate Once, Use Anywhere' approach empowers multiple teams to innovate faster

Challenges & The Road Ahead

Evolving Threat Landscape

Investing in continuous Threat Modelling of your existing products

Product Maturity

Maturity Matters: Not all AI tools are ready to handle enterprise scale production workloads

Keeping up with the latest Change & Pace

AI tools and Open Source communities are constantly evolving