CASE STUDY 02 · CONFIDENTIAL CLIENT ENGAGEMENT

NIST AI Risk Management Framework for a real-time detection platform

Setting up model risk governance for a platform that makes automated decisions from live behavioural signals.

CLIENT SECTOR Behavioural analytics and anomaly detection platform	MY ROLE Embedded AI risk adviser, from design to deployment
WORKED WITH Product leadership, data science and data protection	FOCUS NIST AI RMF and model risk management

The situation

The platform made automated calls about customer behaviour in real time. Its model risk needed to be monitored continuously once it was live, not reviewed once at launch.

What I did

1. **Risk taxonomy and governance charter**
   Risks specific to the detection use case, mapped to the four NIST AI RMF functions (Govern, Map, Measure, Manage) and agreed with product and data science before build.
2. **Model inventory and risk tiers**
   A full list of the detection engine's signal models, tiered by their potential impact on the business and its customers.
3. **Monte Carlo risk model**
   A simulation that expressed detection accuracy and false-positive risk in cost terms, so leadership could compare the cost of good and bad decisions.
4. **Validation and monitoring schedule**
   A recurring validation timetable with triggers for model drift and falling performance.

HOW I APPROACHED IT

I combined the NIST functions with model risk management practice, so each new model or signal falls under an agreed structure instead of needing a fresh review.

Similar work I take on

- Machine learning platforms preparing for enterprise or regulated customers
- Teams that need model risk expressed in commercial terms
- Organisations starting an AI risk register

The client's name and working documents are withheld under confidentiality.

Adenola Adegbesan · adenolaadegbesan.co.uk · adenola.adegbesan@gmail.com