

Enterprise AI Governance & Risk Management Wiki

The Policy & Control Repository for AI in Financial Services

Designed & Created by **Jayson Forde**

The governance backbone for AI model risk: the policies, validation standards, fairness controls, escalation rules, and review cadence that keep AI systems compliant, transparent, and accountable, aligned to SR 11-7, Basel, and the EU AI Act.

SR 11-7

MODEL RISK

Basel

STRESS TESTING

EU AI Act

FAIRNESS & RISK TIERING

Jayson Forde

Enterprise AI Transformation & Program Operations

CONFIDENTIAL

PURPOSE & SCOPE

Governance Built for a Financial AI Function

As the business expands AI into a stronger financial presence, this wiki is the governance infrastructure beneath it, the single, transparent record of how every model is documented, validated, monitored, and governed across its lifecycle.

WHAT THIS WIKI GOVERNS	
Business Objective	Expand AI into a stronger financial presence, safely, transparently, and in full regulatory compliance.
Purpose	Keep documentation of all model practices, ensure clear transparency, and establish collective governance knowledge, regulation guidelines, fraud-detection model guidelines, audit history and record-keeping principles, and the risk-management procedure, committee guidelines, and expected standards.
Regulatory Basis	SR 11-7 (model risk management), Basel (stress testing), and the EU AI Act (fairness and risk classification).
Function	The policy and control repository. Operational governance tools execute these rules; this wiki defines them.
Prepared & Created By	Jayson Forde Enterprise AI Transformation & Program Operations

GOVERNING PRINCIPLE

Governance is not documentation after the fact. **It is the standing control layer that decides what is validated, who is accountable, when humans review, and how evidence is retained**, before a model ever reaches production.

Contents

01

Risk Assumptions
The known risk scenarios this governance framework is built to catch.

02

Validation Methods
Back-testing, benchmarking, fairness analysis, and stress testing.

03

Data Lineage
Transparent record of data sources, transformations, and quality checks.

04

Escalation Rules
Who escalates, on what triggers, and how, within 48 hours.

05

Review Cadence
Risk-tiered review frequency across the model portfolio.

01

RISK ASSUMPTIONS

The Scenarios This Framework Catches

Governance begins by naming the risks it exists to detect. These are the known failure scenarios the validation, monitoring, and escalation controls in this wiki are built to surface early.

#	RISK ASSUMPTION	GOVERNANCE RESPONSE
1	Model spikes show fraud risk over the Christmas holidays.	Seasonal monitoring & stress testing
2	Model risk from digital fraud deposits during peak summer seasons.	Seasonal monitoring & stress testing
3	System triggers a threshold showing bias and unfair loan-approval methods.	Fairness analysis & bias testing (EU AI Act)
4	Data drifts with real-world changes and no oversight or updates.	Drift monitoring & review cadence
5	Documentation has poor escalation methods and procedures.	Formal escalation rules & audit trail

WHY THIS MATTERS

Each assumption maps to a specific control later in this wiki. **A risk that is named and mapped is a risk that is governed;** an unnamed risk is the one that reaches production unchecked.

02

VALIDATION METHODS

How Models Are Proven Sound

Every model is validated against a defined set of methods before and during production, each tied to a regulation and a monitoring control.

Back-testing

Conduct back-testing against historical data to validate predictive accuracy, and stress-test the validations in accordance with Basel regulations to ensure a sound system.

Benchmarking

Benchmark performance against industry standards or challenger models. Dashboards are set in place to monitor data-drift risk and fairness gaps, with oversight held accountable under strong governance. Stress-test systems against risk failures, and maintain documentation logs and record-trail keeping for clear audit logs, ensuring compliance with **SR 11-7, Basel, and the EU AI Act**. Escalation points and ownership are set for key responses and mitigation actions.

Fairness Analysis (EU AI Act)

Implement a dashboard to track and measure financial fairness across the organization. Measures assist credit approvals, loan approvals, fee-waiver ratios, and timely account responses, so all clients are treated fairly. A team member is assigned the role of monitoring and assessing fairness across the organization. Bias and fairness testing identifies disparate impacts with stakeholder accounts, and the same standards apply internally to teams handling accounts and to team leads.

Stress Testing (Basel)

Models and systems are placed under extreme but plausible scenarios to assess resilience. For each financial model, periodic stress-test scenarios, reviews, and methodologies confirm every model and system is sound and documented, across the loan department, credit department, and AI financial-questions department. The greater the risk, the more frequently it is monitored, with a periodic stress-test and review mark **every 6 to 12 weeks**. All documentation is retained for record trail and audit logs, supporting data-quality assessments, sound model concepts, and early prediction of potential risk and data-drift scenarios.

03

DATA LINEAGE

A Transparent Record of the Data

Principle: Provide a transparent record of data sources, transformations, and quality checks.

DATA SOURCES & HANDLING

Data Sources

Loan-approval records and KPI metric data; credit-card approval records and KPI metrics; client account sign-ups; customer-support ticket data; online loan and credit application record data. Quality checks are performed and clear record logs are kept. These sources follow risk-management and governance SOPs.

Transformation

Always follow the transformation principle: look for duplicated records, fill in missing values, correct formatting errors, and ensure all system information is held with privacy and under encryption guidelines.

Quality Checks

Duplicate detection, missing-value handling, format correction, and encryption/privacy validation, logged for traceability.

WHY LINEAGE GOVERNS RISK

A model is only as sound as the data beneath it. **Transparent lineage is what makes drift detectable, fairness measurable, and an audit defensible.**

Supporting Documentation

The following governance artifacts support this wiki and are maintained for traceability, audit readiness, and regulatory compliance:

- ◆ Validation Reports
- ◆ Audit Logs
- ◆ KPI Monitoring Dashboards
- ◆ Fairness Assessment Reports
- ◆ Model Validation Records

04

ESCALATION RULES

Who Acts, When, and How

When a control threshold is breached, escalation is not left to judgment, it follows a defined rule with named owners, concrete triggers, and a fixed response window.

RULE	DEFINITION
Who	The fraud team, the risk and governance committee, and the senior managers overseeing the department, for immediate oversight and risk action. These are the responsible parties.
When	When KPI compliance dashboards and risk flags hit a 6% mark ; when financial-fairness-gap governance reports are conducted and executed; when compliance auditing is requested; and when system performance drifts more than 0.7% .
How	Communicate to all assigned senior personnel, the regulation committee, and team leaders via email and team conference meeting, with complete, organized documentation and assessment prepared, escalated to all responsible members within 48 hours .

THE ESCALATION THRESHOLDS

6% KPI / risk-flag breach · 0.7% performance drift · 48-hour escalation window. Concrete triggers remove hesitation: when the number is hit, the escalation is mandatory, not discretionary.

05

REVIEW CADENCE

Review Frequency Scaled to Risk

Review frequency is governed by risk tier: the higher the risk a model carries, the more often it is reviewed. This is the core of a mature model-risk function.

MODEL / SYSTEM	RISK TIER	REVIEW FREQUENCY	REGULATORY BASIS
Financial Loan Risk Model & credit applications	HIGH	Every 3 months	Basel, EU AI Act, SR 11-7
Credit-line inquiry risk system & monitoring	MEDIUM	Every 6 months	SR 11-7
Standard SOP across the organization	STANDARD	Once a year	Internal governance

THE CADENCE PRINCIPLE

The loan risk model is the highest-risk scenario for the organization, so all loan activity is monitored on a **3-month cycle** to ensure it holds to Basel, the EU AI Act, and SR 11-7. Medium-risk systems review at 6 months; standard SOPs annually.

NEXT REVIEW	
Next Review Date	November 5, 2026
Frequency Basis	Periodic frequency principle: 3 months (high risk), 6 months (medium risk), 12 months (standard).

06

REGULATORY REFERENCES

The Compliance Backbone

This governance framework is built on three regulatory pillars. Every validation method, escalation rule, and review cadence in this wiki traces back to one of them.

REGULATION	WHAT IT GOVERNS	WHERE IT APPLIES HERE
SR 11-7	Federal Reserve guidance on model risk management, validation, and governance.	Validation, benchmarking, review cadence
Basel	Capital and stress-testing standards for financial resilience.	Back-testing, stress testing (6-12 wk mark)
EU AI Act	Risk classification and fairness requirements for AI systems.	Fairness analysis, bias testing, risk tiering

Version History

DATE	AUTHOR	CHANGES MADE
2026-07-18	Jayson Forde	Wiki governance update

HOW THIS WIKI IS USED

This wiki is the **policy and control repository**. It defines what policies apply, who owns decisions, how AI systems are classified, what controls are required, and when human review is triggered. Operational governance tools, such as a Governance & Risk Review Board, execute these rules against live initiatives.