

# ENTERPRISE.AI

SCALE · GOVERN · UNLOCK

## AI Governance Readiness Checklist

40-Point Assessment Against SR 11-7, SS1/23, NIST AI RMF & EU AI Act

|                             |   |
|-----------------------------|---|
| <b>Assessment Framework</b> | SR 11-7   SS1/23   NIST AI RMF   EU AI Act              |
| <b>Target Audience</b>      | Financial Services (Banks, Capital Markets, Sovereigns) |
| <b>Regions</b>              | Middle East, UK, Europe                                 |
| <b>Completion Time</b>      | Under 1 hour  |
| <b>Assessment Points</b>    | 40+ governance checkpoints                              |

Contact: [advisor@rodney-ai.com](mailto:advisor@rodney-ai.com)  
Generated: May 11, 2026

# Executive Summary

This comprehensive checklist guides financial institutions through a systematic assessment of their AI governance maturity across regulatory frameworks and organizational domains. Designed for Chief Risk Officers, Heads of AI, and Governance leaders, this tool evaluates 40+ critical governance dimensions.

## Why This Assessment Matters

- **Regulatory Convergence:** SR 11-7, SS1/23, NIST AI RMF, and EU AI Act establish increasingly consistent expectations for AI governance
- **Risk Concentration:** AI model failures in financial services create systemic risks requiring robust governance frameworks
- **Maturity Gap:** Many institutions lack comprehensive policies across the AI lifecycle from strategy through monitoring
- **Competitive Advantage:** Strong governance creates operational efficiency and stakeholder confidence

## How to Use This Checklist

1. **Self-Assessment:** Score each item from 1-5 based on your institution's current state
2. **Cross-Functional Review:** Engage Risk, Compliance, Model Risk, Technology, and Business teams
3. **Regulatory Mapping:** Each item references specific regulatory requirements for documented compliance
4. **Prioritization:** Use the scoring methodology to identify critical gaps and roadmap improvements
5. **Follow-Up:** Enterprise.AI advisory engagement can support remediation planning and implementation

## Assessment Domains

|                              |  |
|------------------------------|--|
| <b>Policy &amp; Strategy</b> | 8 items - Governance framework, AI strategy, risk appetite |
| <b>Model Risk Management</b> | 8 items - SR 11-7 alignment, model development, validation |
| <b>SS1/23 Compliance</b>     | 6 items - UK PRA operational resilience for AI systems     |
| <b>NIST AI RMF</b>           | 6 items - NIST AI Risk Management Framework alignment      |
| <b>EU AI Act Readiness</b>   | 6 items - EU AI Act compliance preparation and controls    |
| <b>Data Governance</b>       | 6 items - Data quality, lineage, bias detection, privacy   |
| <b>People &amp; Culture</b>  | 4 items - Skills, training, accountability, AI ethics      |

# Policy & Strategy

## **PS-1: Formal AI governance charter and board-approved AI strategy**

*Board-level charter defining AI governance structure, roles, accountabilities, and escalation procedures*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (governance framework), NIST AI RMF (governance), EU AI Act (AI Act compliance)

## **PS-2: Defined AI risk appetite statement aligned with institutional risk appetite**

*Documented risk appetite for different AI model types, use cases, and deployment contexts*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (risk governance), NIST AI RMF (risk determination)

## **PS-3: Comprehensive AI policy framework covering development through decommissioning**

*End-to-end policies covering AI strategy, development, testing, deployment, monitoring, and retirement*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SS1/23 (operational resilience), SR 11-7 (AI governance), EU AI Act (Article 9-13 controls)

## **PS-4: Three lines of defense model for AI governance and controls**

*Clear separation between business ownership (1st), risk/compliance oversight (2nd), and internal audit (3rd)*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (three lines model), Basel governance frameworks

## **PS-5: Board and senior management reporting on AI risk, performance, and incidents**

*Regular board-level and executive reports on AI portfolio health, emerging risks, and compliance status*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (governance), SS1/23 (senior management awareness)

## **PS-6: AI ethics principles and responsible AI framework**

*Documented principles covering fairness, transparency, accountability, and societal impact*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** EU AI Act (Article 2-3), NIST AI RMF (responsible AI)

## **PS-7: Model inventory and registry with ownership and metadata**

*Centralized registry of all AI models in production with owner, purpose, risk classification, data sources*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (model inventory), SS1/23 (system inventory)

**PS-8: Change management and versioning procedures for AI models**

*Documented procedures for model updates, retraining, versioning, and change approval workflows*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (governance), NIST AI RMF (continuous monitoring)

# Model Risk Management / SR 11-7

## **MRM-1: Model development standards and lifecycle governance framework**

*Documented standards for model development, including requirements, architecture, testing protocols*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (independent governance), NIST AI RMF (map, measure, manage)

## **MRM-2: Independent model validation and sign-off process**

*Segregated validation team independent from development, with documented validation plans and sign-off criteria*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (independent validation mandatory)

## **MRM-3: Backtesting, benchmarking, and performance monitoring framework**

*Regular backtesting against benchmarks, monitoring of actual vs. predicted performance, error analysis*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (ongoing monitoring), Basel III framework

## **MRM-4: Model documentation standards (including explainability requirements)**

*Comprehensive documentation of model purpose, inputs, methodology, assumptions, limitations, and explainability*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (model documentation), EU AI Act (technical documentation)

## **MRM-5: Stress testing and scenario analysis for AI models**

*Regular stress tests under adverse scenarios, sensitivity analysis, and edge case evaluation*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (stress testing), SS1/23 (resilience testing)

## **MRM-6: Model risk capital allocation and impact assessment**

*Quantification of model risk, capital allocation for model risk, and impact on institution's risk profile*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (risk management), Basel capital frameworks

## **MRM-7: Model governance for third-party/vendor models and frameworks**

*Due diligence, SLAs, performance monitoring, and risk assessment for external models and AI services*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (vendor risk), NIST AI RMF (supply chain)

**MRM-8: Incident management and remediation procedures for model failures**

*Rapid escalation, root cause analysis, client notification, and remediation procedures for model failures*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (incident handling), SS1/23 (incident reporting)

# SS1/23 Compliance (UK PRA)

## SS-1: Senior manager accountable for AI model risk (SMAR designation)

*Clear designation of senior manager with accountability for model risk governance*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: SS1/23 (SMAR requirement)

## SS-2: Operational resilience impact tolerance for AI-dependent processes

*Documented impact tolerance for critical functions supported by AI, with regular testing and monitoring*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: SS1/23 (impact tolerance), EMIR Article 31

## SS-3: AI model resilience testing and scenario analysis

*Regular testing of model performance under adverse conditions, data quality degradation, and operational stress*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: SS1/23 (operational resilience)

## SS-4: Data quality and availability controls for production AI models

*Monitoring of data quality metrics, availability thresholds, and contingency arrangements*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: SS1/23 (data resilience), NIST AI RMF (data governance)

## SS-5: Fallback arrangements and model override procedures

*Documented procedures for manual review, model override, and fallback to non-AI processes when needed*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: SS1/23 (operational resilience), EU AI Act (human oversight)

## SS-6: Regular reporting to PRA on model risk and resilience status

*Compliance with SS1/23 reporting requirements, including model inventory and resilience assessments*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: SS1/23 (reporting requirements)

# NIST AI RMF Alignment

## **NIST-1: NIST AI RMF governance and accountability structure**

*Roles and responsibilities aligned with NIST AI RMF framework (MAP, MEASURE, MANAGE, MONITOR)*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: NIST AI RMF (governance framework)

## **NIST-2: Risk mapping for AI models (MAP function)**

*Systematic identification and documentation of AI risks across the model lifecycle*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: NIST AI RMF (risk mapping)

## **NIST-3: Measurement of AI risks and performance metrics (MEASURE function)**

*Metrics and measurement protocols for model accuracy, bias, fairness, robustness, and other risk dimensions*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: NIST AI RMF (risk measurement)

## **NIST-4: Risk mitigation and control implementation (MANAGE function)**

*Active management of identified risks through controls, model updates, and process improvements*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: NIST AI RMF (risk management)

## **NIST-5: Continuous monitoring and feedback loops (MONITOR function)**

*Ongoing monitoring of model performance, feedback collection, and incorporation into improvement processes*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: NIST AI RMF (continuous monitoring)

## **NIST-6: Integration with enterprise risk management framework**

*AI risk management integrated with broader enterprise risk management and reporting structures*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

Regulatory Reference: NIST AI RMF (enterprise integration)

# EU AI Act Readiness

## **EU-1: Classification of AI systems by risk level (prohibited/high/limited/minimal)**

*Documented classification of AI systems according to EU AI Act risk categories*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** EU AI Act (Articles 6-10, risk classification)

## **EU-2: Risk assessment and mitigation for high-risk AI systems**

*Comprehensive risk assessments and mitigation strategies for AI systems classified as high-risk*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** EU AI Act (Article 9, risk assessment)

## **EU-3: Prohibited AI practices policy (compliance with Article 5)**

*Explicit policies prohibiting subliminal manipulation, exploiting vulnerable groups, social scoring systems*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** EU AI Act (Article 5, prohibited practices)

## **EU-4: Transparency and disclosure for AI-based decision making**

*Clear disclosure to customers when AI is used in decision-making, explainability of decisions*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** EU AI Act (Article 13-14, transparency)

## **EU-5: AI governance and compliance management system (Articles 16-29)**

*Documented compliance with Articles 16-29 including record-keeping, documentation, and quality management*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** EU AI Act (Articles 16-29)

## **EU-6: EU AI Act conformity assessment and CE marking readiness**

*Preparation for conformity assessment procedures and potential CE marking requirements*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** EU AI Act (Articles 43-49, conformity assessment)

# Data Governance & Quality

## DG-1: Data governance framework and data ownership structure

*Documented framework defining data stewardship, ownership, quality standards, and retention policies*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** GDPR (data governance), NIST AI RMF (data management)

## DG-2: Data quality monitoring and validation controls

*Automated and manual controls monitoring data completeness, accuracy, consistency, and timeliness*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SS1/23 (data quality), SR 11-7 (data governance)

## DG-3: Bias detection, measurement, and mitigation procedures

*Tools and processes to detect algorithmic bias, measure disparate impact, and implement mitigation strategies*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** EU AI Act (fairness), NIST AI RMF (bias assessment), Fair Lending rules

## DG-4: Data lineage, provenance, and traceability documentation

*Complete tracking of data sources, transformations, and flow through AI model pipeline*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** GDPR (data accountability), EU AI Act (documentation)

## DG-5: Privacy and consent management for training and operational data

*Controls ensuring proper consent, data minimization, and privacy protection for all AI data uses*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** GDPR (privacy), CCPA, financial services data regulations

## DG-6: Data retention, deletion, and versioning policies for model training

*Policies defining training data retention periods, secure deletion procedures, and version control*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** GDPR (data retention), SR 11-7 (record keeping)

# People, Culture & Training

## **PC-1: AI skills assessment and hiring plan for governance and risk roles**

*Identification of required AI governance, data science, and technical skills; hiring and development plans*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (governance capability), SS1/23 (senior manager requirements)

## **PC-2: Regular training program on AI risks for board, management, and staff**

*Tiered training covering AI fundamentals, governance frameworks, and role-specific AI risk knowledge*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (skills and knowledge), SS1/23 (senior manager awareness)

## **PC-3: Clear accountabilities and escalation procedures for AI incidents**

*Documented roles, responsibilities, and escalation paths for model failures, bias discoveries, and data issues*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** SR 11-7 (governance), SS1/23 (accountability)

## **PC-4: Ethical framework for AI development and decision-making**

*Ethics review processes, guidelines for responsible AI use, and protection of whistleblower concerns*

- Assessment Score: 1 (Not in place) to 5 (Fully implemented)

Score: \_\_\_\_ / 5

**Regulatory Reference:** EU AI Act (ethical AI), SR 11-7 (governance)

# Scoring Methodology & Interpretation

## Maturity Scoring Scale (1-5)

| Score | Level          | Definition   |
|-------|----------------|--|
| 1     | Initial/Ad-hoc | Practice is not in place or only ad-hoc; significant work required           |
| 2     | Developing     | Practice is partially implemented; many gaps remain                          |
| 3     | Defined        | Practice is documented and implemented; some gaps in consistency or coverage |
| 4     | Managed        | Practice is well-implemented and monitored; minor gaps only                  |
| 5     | Optimized      | Practice is fully implemented, monitored, and continuously improved          |

## Scoring Calculation

**Domain Scores:** Average the scores for all items within each governance domain (Policy & Strategy, Model Risk Management, etc.) to obtain domain-level maturity scores.

**Overall Governance Maturity Score:** Average all individual item scores to obtain an overall governance maturity rating.

**Gap Analysis:** Items scoring below 3 indicate significant control gaps requiring attention. Items scoring 3-4 benefit from enhancement. Items at 5 represent best practice benchmarks.

## Interpretation Guide

| Overall Score | Governance Posture | Recommended Actions  |
|---------------|--------------------|--|
| 1.0 - 2.0     | High Risk          | Urgent remediation required; significant regulatory exposure |
| 2.1 - 3.0     | Moderate Risk      | Material gaps; prioritize critical domain improvements       |
| 3.1 - 4.0     | Manageable Risk    | Solid foundation; continue maturation of controls            |
| 4.1 - 5.0     | Low Risk           | Strong governance posture; focus on continuous improvement   |

# Assessment Summary Scorecard

Complete this template to summarize your assessment results across governance domains.

| Domain  | # Items | Total Score | Average Score (÷ items)         | Rating |
|---|---------|-------------|---------------------------------|--------|
| Policy & Strategy                                     | ___     | ___         | ___                             |        |
| Model Risk Management / SR 11-7                       | ___     | ___         | ___                             |        |
| SS1/23 Compliance (UK PRA)                            | ___     | ___         | ___                             |        |
| NIST AI RMF Alignment                                 | ___     | ___         | ___                             |        |
| EU AI Act Readiness                                   | ___     | ___         | ___                             |        |
| Data Governance & Quality                             | ___     | ___         | ___                             |        |
| People, Culture & Training                            | ___     | ___         | ___                             |        |
| <b>&lt;b&gt;OVERALL GOVERNANCE MATURITY&lt;/b&gt;</b> |         |             | <b>&lt;b&gt;___/5&lt;/b&gt;</b> |        |

## Priority Gap Areas (Scores 1-2)

Identify and list the 5-10 most critical governance gaps for focused remediation planning.

- Gap 1: \_\_\_\_\_ (Score: \_\_\_/5)
- Gap 2: \_\_\_\_\_ (Score: \_\_\_/5)
- Gap 3: \_\_\_\_\_ (Score: \_\_\_/5)
- Gap 4: \_\_\_\_\_ (Score: \_\_\_/5)
- Gap 5: \_\_\_\_\_ (Score: \_\_\_/5)

## Next Steps & Remediation Planning

Based on your assessment, consider the following roadmap:

- Immediate (0-3 months):** Address critical gaps in high-risk areas (MRM, Policy & Strategy)
- Near-term (3-6 months):** Complete foundational governance framework and data governance
- Medium-term (6-12 months):** Build advanced monitoring, bias detection, and continuous improvement
- Ongoing:** Maintain alignment with evolving regulations (EU AI Act, NIST updates, emerging guidance)

**Enterprise.AI Advisory Support:** We specialize in accelerating governance maturity through strategic planning, framework development, control implementation, and regulatory alignment.

## About This Assessment

This AI Governance Readiness Checklist has been developed by Enterprise.AI to help financial institutions systematically assess their governance maturity across leading regulatory frameworks and best practices.

The assessment framework integrates guidance from:

- **SR 11-7:** Federal Reserve Guidance on Model Risk Management
- **SS1/23:** PRA Supervisory Statement on Operational Resilience
- **NIST AI RMF:** National Institute of Standards & Technology AI Risk Management Framework
- **EU AI Act:** European Union Artificial Intelligence Act (Regulation (EU) 2024/1689)

This document is designed for use by Chief Risk Officers, Heads of AI, Compliance leaders, and governance teams within financial institutions across Middle East, UK, and European markets.

## Contact Enterprise.AI

**Email:** advisor@rodney-ai.com

**Services:** Strategic AI advisory, governance frameworks, regulatory alignment, capability b

**Expertise:** Financial Services AI, Risk Management, Regulatory Compliance

### SCALE · GOVERN · UNLOCK

This assessment is provided for informational purposes. Results should be reviewed with appropriate legal, compliance, and risk management teams. Enterprise.AI recommendations are not legal or regulatory advice and should be validated against your specific jurisdiction and regulatory requirements.