4iGov

AI GOVERNANCE PRACTITIONER SERIES

ARTEFACT 2

Enterprise AI Governance, Risk and Compliance Framework

Applied to Regulated Financial Services | Reference Case: Apple Card and Goldman Sachs

A working governance framework for AI and automated systems in regulated financial environments. Incorporates EU AI Act, NIST AI RMF, DORA, and enterprise GRC standards.

Published by 4iGov | 4igov.cloud | 2026

4iGov.cloud

1. PURPOSE AND SCOPE

This framework defines the enterprise governance, risk, and compliance requirements for financial entities deploying AI or automated systems in regulated consumer-facing environments. It is derived from the governance failure analysis in Artefact 1 and maps controls to EU AI Act, NIST AI RMF, and DORA obligations.

The framework is structured as a working document. Each section is designed to support a governance practitioner, product owner, or risk officer in making, recording, and evidencing governance decisions across the AI use case lifecycle.

Framework Scope

- AI and automated systems processing consumer financial obligations — disputes, credit decisions, payments, fraud detection
- Third party AI and ICT providers integrated into regulated financial workflows
- Pre-deployment governance and post-deployment monitoring of AI use cases
- Reference case throughout: Apple Card — credit limit algorithm (2019) and dispute routing system (2024)

4iGov.cloud

2. AI GOVERNANCE PROCESS WORKFLOW

Every AI use case in a regulated financial environment must pass through six governance stages before and after deployment. The workflow below defines the required activities, accountable owner, and the gate condition that must be satisfied before proceeding to the next stage.

Gate conditions are non-negotiable. Commercial delivery timelines do not override governance gates. The Apple Card 2024 failure was directly caused by bypassing Stages 2, 3, and 4 under commercial pressure.

Stage	Name	Key Activities	Accountable Owner	Gate Condition — Must Be Met Before Proceeding
1	Use Case Intake and Classification	Document the AI use case: purpose, affected population, decision type, and regulatory context. Determine whether the system is automated, AI-assisted, or agentic.	Product Owner	Use case documented. Classification confirmed in writing.
2	Risk Tier Assessment	Apply EU AI Act risk classification. Assign NIST AI RMF risk profile. Identify all regulatory obligations triggered by the use case. Map third party dependencies.	Risk and Compliance Officer	Risk tier assigned. Regulatory obligations list signed off. Third party dependencies documented.
3	Controls Design	Map required controls to all identified risks. Define accountability matrix for integration boundaries. Design monitoring SLAs aligned to regulatory timeframes.	Governance Lead	Controls mapped. Accountability matrix complete. No unowned integration boundaries.
4	Pre-Deployment Governance Gate	Regulatory user journey testing completed — including all failure and incomplete paths. Independent compliance sign-off obtained. UX design validated against regulatory obligations.	Compliance Officer — independent of delivery	**Written compliance sign-off. All regulatory test cases passed including failure paths. UX error and confirmation states confirmed.**
5	Deployment and Monitoring	Deploy with monitoring controls active. Confirm real-time alerting on processing failures. SLAs documented and communicated to all accountable owners.	Technology Lead and Risk Officer	Monitoring confirmed active. SLA breach alerting tested. Deployment sign-off recorded.
6	Ongoing Governance and Review	Quarterly risk and controls review. Annual regulatory alignment assessment. Incident review and lessons learned documented in system of record.	AI Governance Committee	Quarterly review on record. Open issues tracked. No unreviewed incidents older than 30 days.

Apple Card reference — 2024 failure: The June 2020 workflow update bypassed Stages 2, 3, and 4. No risk tier assessment. No regulatory test cases for incomplete submission path. No compliance sign-off. The $25M quarterly penalty clause created a commercial incentive that effectively removed the governance gate from the process.

4igov.cloud

Apple Card reference — 2019 failure: The credit limit algorithm bypassed Stage 2 entirely. No disparate impact assessment was conducted before deployment. No bias risk was mapped. No proxy variable analysis was documented.

4iGov.cloud

3. EU AI ACT — RISK CLASSIFICATION AND OBLIGATIONS

3.1 Risk Tier Classification

Before deployment, every AI use case must be classified under the EU AI Act risk framework. Classification determines the compliance obligations that apply and must be documented as part of Stage 2 of the governance workflow.

Risk Tier	Definition	Financial Services Examples	Apple Card Classification
Prohibited	AI practices explicitly banned under Article 5. Deployment is not permitted under any circumstances.	Social scoring by public authorities; subliminal manipulation of consumers	Not applicable
High Risk	Systems listed in Annex III including credit, financial services, employment, and essential services.	Credit scoring, loan approval, automated dispute routing, fraud detection in consumer financial products	**2019 credit algorithm: High Risk. 2024 dispute routing: High Risk — Annex III financial services automated decision-making.**
Limited Risk	Systems with specific transparency obligations but not subject to full high-risk requirements.	Customer service chatbots, AI-generated content with disclosure requirement	Consumer-facing AI assistants without credit decision authority
Minimal Risk	All other AI systems. Subject to voluntary codes of practice only.	Spam filters, recommendation engines, internal analytics	Internal analytics with no direct consumer financial impact

3.2 High-Risk System Obligations and Controls Mapping

For systems classified as high-risk, the following Article obligations apply. Each is mapped to the required control and the specific Apple Card governance gap.

Article	Obligation	Required Control	Apple Card Gap — Both Failures
Art 9	Risk Management System	Continuous, documented risk management process for the lifetime of the system. Risk assessments before and after every material update.	2024: No risk management process for the updated dispute workflow. No post-deployment risk review. 2019: No risk management process for credit algorithm. No post-launch monitoring for discriminatory outcomes.
Art 10	Data Governance and Bias	Data used to train and operate high-risk AI must be assessed for quality, relevance, and potential bias including proxy variable effects.	2019: No proxy variable analysis conducted. Inputs correlated with gender produced discriminatory credit limit outcomes without explicit gender input.
Art 13	Transparency	Systems must be sufficiently transparent to allow deployers and users to interpret outputs appropriately. Decisions must be explainable.	2019: Credit limit decisions could not be explained to consumers or customer service representatives. Black box operation. 2024: Silent dead state produced no output to consumer or Goldman Sachs.
Art 14	Human Oversight	Systems must enable effective oversight by natural persons.	2019: No mechanism to flag or escalate potentially discriminatory credit decisions for

4iGov.cloud

Article	Obligation	Required Control	Apple Card Gap — Both Failures
		Override and intervention mechanisms must exist.	human review. 2024: No human escalation path for unprocessed disputes. No override mechanism.
Art 17	Quality Management System	QMS covering testing procedures, conformity assessment, and post-market monitoring. Test documentation retained.	2024: No regulatory test cases for incomplete submission path. No QMS for the dispute workflow.
Art 72	Post-Market Monitoring	Active monitoring of high-risk system performance post-deployment. Monitoring plan must be documented and maintained.	2024: No monitoring framework. Processing failure ran undetected for 12+ months. 2019: No post-launch monitoring for bias or disparate impact.

4iGov.cloud

4. NIST AI RISK MANAGEMENT FRAMEWORK — ALIGNMENT WORKSHEET

The NIST AI RMF structures AI risk management across four functions: Govern, Map, Measure, and Manage. This worksheet maps each function to the required governance activities, the evidence required, and the Apple Card gaps as worked examples.

Function	Sub-Category	Required Activity	Evidence Required	Apple Card Gap
GOVERN	Policies	Establish AI governance policies. Assign accountability for each AI use case. Maintain board-level visibility.	Governance policy document. Accountability matrix. Board reporting template.	No accountability matrix for Apple-Goldman integration boundary. No board-level AI governance reporting.
GOVERN	Risk Tolerance	Document organisational risk tolerance for AI systems. Define thresholds for acceptable failure rates in regulated workflows.	Risk tolerance statement approved by risk committee.	No documented risk tolerance. Commercial penalty clause ($25M/quarter) effectively set the risk threshold without governance input.
GOVERN	Incentive Alignment	Review commercial and organisational incentive structures for misalignment with responsible AI deployment.	Commercial contract review against governance standards. Sign-off that incentives do not override readiness gates.	$25M/quarter liquidated damages clause reviewed by legal but not assessed against governance readiness obligations.
MAP	Use Case Inventory	Maintain an inventory of all AI use cases with risk classification, regulatory obligations, and owner assigned.	AI use case register. Updated at each new deployment or material change.	No use case inventory. Credit algorithm and dispute routing system not registered as governed AI use cases.
MAP	Bias and Fairness	Identify and assess bias risks in training data, feature selection, and model outputs before deployment.	Bias assessment report. Proxy variable analysis. Disparate impact testing results.	2019: No bias assessment or proxy variable analysis before credit algorithm deployment.
MAP	Third Party Risk	Map third party AI and ICT dependencies as part of use case risk profile.	Third party risk assessment. Dependency map. Contract review against governance standards.	Apple not assessed as a critical third party provider for Goldman Sachs’ regulated dispute processing obligations.
MEASURE	KPIs and Monitoring	Define measurable performance indicators for each AI use case. Implement monitoring against regulatory SLAs.	KPI register. Monitoring dashboard. SLA breach alerting confirmed active.	No KPIs defined for dispute processing pipeline. No transmission failure monitoring.
MEASURE	Adverse Condition Testing	Test AI systems under failure, incomplete, and adverse conditions before deployment.	Adverse condition test results. Regulatory test case library including all failure paths.	No adverse condition testing for incomplete dispute submission. No failure path test cases.
MANAGE	Incident Response	Define and maintain incident response processes for AI system failures. Escalation paths and remediation workflows documented.	Incident response plan. Escalation matrix. Post-incident review template.	No incident response process. No detection mechanism meant no incident was declared for 12+ months.

Function	Sub-Category	Required Activity	Evidence Required	Apple Card Gap
MANAGE	Continuous Improvement	Conduct regular reviews of AI system risk profile. Apply lessons learned from incidents across all AI use cases.	Review cycle documentation. Cross-use case lessons learned register.	2019 NYDFS investigation produced no documented cross-use case governance review. 2024 failure occurred in the same governance vacuum.

4iGov.cloud

5. DORA — DIGITAL OPERATIONAL RESILIENCE REQUIREMENTS

DORA applies to financial entities operating in the EU and establishes binding obligations for ICT risk management, third party oversight, and operational resilience testing. For AI systems involving third party providers, DORA is the primary contractual governance framework.

Article	Requirement	Governance Action Required	Apple Card Application
Art 6	ICT Risk Management Framework	AI systems must be included in the ICT risk management framework. Risk assessments documented and updated for all material changes.	Dispute routing workflow and credit algorithm were not included in ICT risk scope. No ICT risk assessment conducted for either system.
Art 17	ICT Incident Management	Processes to detect, classify, manage, and report ICT-related incidents. AI system failures must be classified and escalated appropriately.	No incident detection process. Dispute transmission failure ran for 12+ months without classification or escalation.
Art 25	ICT Testing	Operational resilience testing of ICT systems including integration points with third party providers. Failure path testing required.	No integrated testing of the Apple-Goldman dispute submission pipeline. No failure path testing conducted before or after the June 2020 update.
Art 28	Third Party ICT Risk Management	Financial entities must manage third party ICT risk as part of the overall ICT risk framework. Critical third party providers must be identified, assessed, and monitored.	Apple was not assessed or managed as a critical ICT third party provider by Goldman Sachs despite Apple owning the consumer-facing interface for regulated financial workflows.
Art 30	Key Contractual Provisions	Contracts with critical ICT third party providers must include service levels, audit rights, incident notification, change management obligations, and resilience testing requirements.	Apple-Goldman contract lacked: change notification obligation for workflow updates, audit rights for Goldman over Apple’s dispute processing system, integrated resilience testing requirements, and SLAs tied to TILA regulatory timeframes.

DORA Implementation Note

- DORA entered into force on 17 January 2025. Financial entities with EU operations must comply with all DORA requirements. The Apple Card failures, had they occurred post-January 2025, would have triggered mandatory ICT incident reporting obligations under Article 17 within defined timeframes.
- The absence of the third party governance provisions in the Apple-Goldman contract would constitute a direct breach of Article 30 requirements for critical ICT third party providers.

4igov.cloud

6. CONTROLS CATALOGUE

The controls below are derived from the governance gap assessment in Artefact 1 and mapped to the regulatory frameworks in Sections 3, 4, and 5. Each control is assigned an owner, a frequency, and a reference to the failure it addresses.

ID	Control	Owner	Frequency	Framework Reference	Apple Card Failure Addressed
C-01	AI use case register maintained and updated at each new deployment or material change	Product Owner	Ongoing	NIST Map	No use case inventory for credit algorithm or dispute routing system
C-02	EU AI Act risk tier classification conducted before deployment of any AI or automated system	Risk Officer	Per deployment	EU AI Act Art 6	Neither Apple Card system was risk-classified before deployment
C-03	Bias and proxy variable assessment conducted before deployment of any model affecting consumer outcomes	Risk Officer	Per deployment	EU AI Act Art 10, NIST Map	No proxy variable analysis before 2019 credit algorithm deployment
C-04	Accountability matrix defined for all system integration boundaries. No unowned handoff states permitted	Governance Lead	Per deployment, reviewed quarterly	NIST Govern, EU AI Act Art 14	No owner assigned to Apple-Goldman dispute transmission boundary
C-05	Regulatory user journey testing conducted including all failure and incomplete paths before deployment	QA Lead + Compliance	Per deployment	EU AI Act Art 17, NIST Measure	No test case for incomplete dispute submission path in 2024
C-06	Independent compliance sign-off obtained before deployment. Commercial timelines do not override this gate	Compliance Officer	Per deployment	NIST Govern, EU AI Act Art 9	No independent compliance sign-off before June 2020 update deployment
C-07	Real-time monitoring active on all regulated AI workflows. SLA breach alerting tested before go-live	Technology Lead	Ongoing	EU AI Act Art 72, NIST Measure, DORA Art 6	No monitoring on dispute transmission pipeline. 12-month undetected failure.
C-08	UX design governance standard applied to all consumer-facing regulated workflows. Explicit error and confirmation states required	Product Owner + UX	Per deployment	EU AI Act Art 13, NIST Govern	Silent dead state with no consumer notification on incomplete submission
C-09	Third party ICT risk assessment conducted for all critical third party providers. Contract review against DORA Art 30 requirements	Risk Officer	Annual + per contract change	DORA Art 28, 30, NIST Map	Apple not assessed as critical ICT third party. Contract lacked change notification and audit rights.
C-1	Integrated end-to-end resilience testing of AI	Technology Lead	Annual minimum	DORA Art 25	No integrated testing of Apple-Goldman dispute

4igov.cloud

ID	Control	Owner	Frequency	Framework Reference	Apple Card Failure Addressed
0	workflows at critical integration boundaries				submission pipeline
C-11	AI governance incident response plan maintained. Escalation paths defined and tested	Governance Lead	Annual review	DORA Art 17, NIST Manage	No incident response process. No detection mechanism.
C-12	Cross-use case lessons learned review conducted following any regulatory investigation or incident	AI Governance Committee	Post-incident	NIST Manage	2019 NYDFS investigation produced no cross-use case governance review

This artefact is part of the 4iGov AI Governance Practitioner Series.

Artefact 3: AI Agent Capability and Risk Assessment | Artefact 4: Third Party AI Vendor Risk Assessment | 4igov.cloud

4iGov.cloud