4iGov

AI GOVERNANCE PRACTITIONER SERIES

ARTEFACT 4

Third Party AI Vendor Risk Assessment

Template and Worked Example | Reference Case: Apple Card and Goldman Sachs

A structured assessment template for governing third party AI and ICT providers in regulated financial environments. Aligned to DORA, EU AI Act, and NIST AI RMF.

Published by 4iGov | 4igov.cloud | 2026

Assessment ratings in the worked example are inferences from public regulatory findings only. See Section 2 disclaimer.

4iGov.cloud

1. PURPOSE AND STRUCTURE

This template provides a structured framework for assessing third party AI and ICT providers that are integrated into regulated financial workflows. It is designed to be completed at vendor onboarding, at contract renewal, following any material change to the vendor relationship, and as part of the annual third party risk review cycle.

The template is structured in five parts: vendor profile, governance and contractual assessment, technical integration controls, regulatory obligations mapping, and an overall risk rating. Each part produces a scored output. The final section applies the template to the Apple-Goldman Sachs relationship as a worked example.

When This Assessment Is Required

- Onboarding any new third party AI or ICT provider whose systems will process regulated consumer obligations
- Before any material change to an existing third party relationship — new system, new workflow, new data sharing arrangement
- Annual review of all critical ICT third party providers as required by DORA Article 28
- Following any incident or regulatory inquiry involving a third party provider
- When a third party provider deploys a material update affecting a regulated workflow without prior notification

4iGov.cloud

2. VENDOR PROFILE

Complete this section at the start of every assessment. The profile establishes the scope, the regulatory context, and the criticality classification that determines which assessment sections apply.

Field	Entry
Assessment Date	
Vendor Name	
Vendor Registered Jurisdiction	
Services Provided	
Regulated Workflows Affected	List all consumer-facing or regulated workflows that depend on this vendor
Financial Entity Conducting Assessment	
Assessment Conducted By	Name and role
Relationship Type	Select: Critical ICT Provider / Material ICT Provider / Standard ICT Provider
DORA Critical Provider Status	Confirmed critical / Under assessment / Not applicable
EU AI Act Applicability	Does the vendor operate AI systems classified as high-risk under Annex III? Yes / No / Under assessment
Previous Assessment Date	Date of last completed assessment or N/A if first assessment
Open Issues from Previous Assessment	Number and brief description, or None

Worked Example — Apple Card Vendor Profile

- Vendor: Apple Inc. | Jurisdiction: United States
- Services: Consumer-facing Apple Wallet application including dispute submission interface, automated dispute routing, and message transmission to Goldman Sachs backend
- Regulated Workflows Affected: Apple Card billing dispute submission — triggers TILA Regulation Z Billing Error Notice investigation obligations on Goldman Sachs
- Relationship Type: Critical ICT Provider — Goldman Sachs cannot fulfil its TILA obligations without Apple's system functioning correctly
- DORA Critical Provider Status: Would qualify as critical under DORA Article 28 — Goldman Sachs is entirely dependent on Apple for consumer dispute intake
- EU AI Act Applicability: High-risk — automated routing of consumer financial disputes falls under Annex III financial services obligations
- Note: All worked example assessments are inferences from publicly available regulatory findings. See cover page disclaimer.

4iGov.cloud

3. GOVERNANCE AND CONTRACTUAL ASSESSMENT

This section assesses whether the contractual and governance framework governing the vendor relationship meets the minimum standards required for a critical ICT provider under DORA and for a high-risk AI system provider under the EU AI Act.

#	Requirement	Assessment Criteria	Apple-Goldman Finding (Inferred)	Rating
G-01	Service Level Agreement for regulated workflows	SLA exists covering availability, processing time, and performance of all workflows affecting regulated consumer obligations. SLA timeframes aligned to regulatory deadlines (e.g. TILA 60-day resolution window).	No public evidence of an SLA for the dispute routing workflow aligned to TILA regulatory timeframes. Processing failures not governed by measurable SLA.	FAIL
G-02	Change notification obligation	Vendor is contractually required to notify the financial entity of any material change to systems affecting regulated workflows before deployment. Minimum notice period defined.	Apple deployed the June 2020 dispute workflow update without prior notification to Goldman Sachs. No contractual change notification obligation evidenced in public record.	FAIL
G-03	Audit rights	Financial entity has contractual right to audit vendor systems, processes, and controls relevant to regulated workflows. Audit frequency defined.	No public evidence of Goldman Sachs audit rights over Apple’s dispute processing systems. DORA Article 30 requires this for critical ICT providers.	FAIL
G-04	Incident notification obligation	Vendor is contractually required to notify the financial entity of any incident affecting regulated workflows within a defined timeframe.	No contractual incident notification obligation evidenced. Goldman Sachs was not notified when dispute transmission failed.	FAIL
G-05	Regulatory compliance allocation	Contract clearly allocates regulatory compliance responsibilities between vendor and financial entity. Both parties understand which obligations each is responsible for fulfilling.	Contract allocated consumer experience to Apple and investigation obligations to Goldman Sachs but did not define responsibility for system reliability at the handoff between the two.	CONDITIONAL
G-	Exit and continuity provisions	Contract includes provisions for business	Not determinable from public record. Scored as	CONDITIONAL

4iGov.cloud

#	Requirement	Assessment Criteria	Apple-Goldman Finding (Inferred)	Rating
06		continuity if vendor relationship ends. Financial entity can fulfil regulated obligations independently of the vendor within a defined transition period.	conditional given the complete dependency Goldman Sachs had on Apple for consumer dispute intake.	
G-07	Sub-contractor and fourth party disclosure	Vendor is required to disclose material sub-contractors or fourth party providers whose failure could affect regulated workflows.	Not assessed in public record. Scored as not evidenced.	**CONDITIONAL**

4iGov.cloud

4. TECHNICAL INTEGRATION CONTROLS

This section assesses whether the technical controls governing the integration between the financial entity and the vendor are sufficient to protect regulated workflows against failure, data loss, and processing gaps.

#	Control	Assessment Criteria	Apple-Goldman Finding (Inferred)	Rating
T-01	End-to-end integration testing	Complete workflow testing from consumer action through vendor system to financial entity backend. Includes failure paths and incomplete submission scenarios. Conducted before every material deployment.	No end-to-end integration test for the incomplete dispute submission path evidenced before the June 2020 deployment. The dead state was not identified before deployment.	FAIL
T-02	Transmission confirmation and acknowledgment	Vendor system provides confirmation to the financial entity that regulated data (e.g. consumer disputes) has been successfully transmitted. Financial entity confirms receipt. No silent failures permitted.	No transmission confirmation mechanism evidenced. Goldman Sachs received no signal when consumer disputes were not transmitted. Silent failure by design.	FAIL
T-03	Dead state detection and recovery	Integration workflow has no unhandled states. All incomplete or failed transactions are detected, logged, and escalated. Recovery mechanism exists for transactions stuck in intermediate states.	Dead state existed in the dispute submission workflow for 12+ months without detection or recovery. No state monitoring evidenced.	FAIL
T-04	Consumer-facing error and confirmation states	All consumer-facing workflows affecting regulated obligations present explicit confirmation on successful submission and explicit error notification on failure or incomplete submission.	No error state presented to consumers who submitted initial dispute message but did not complete secondary form. No confirmation that submission was incomplete or that further action was required.	FAIL
T-05	Cross-system audit trail	End-to-end audit trail exists covering all states from consumer action through vendor system to financial entity. Log entries from both systems can be correlated for any transaction.	Logs presumed to exist in both Apple and Goldman systems but no cross-system correlated audit trail evidenced. Processing history not reconstructable end-to-	CONDITIONAL

#	Control	Assessment Criteria	Apple-Goldman Finding (Inferred)	Rating
			end.	
T-06	Real-time monitoring at integration boundary	Monitoring is active at the integration boundary between vendor and financial entity systems. Transmission volumes, failure rates, and processing delays are monitored in real time against defined thresholds.	No monitoring at the Apple-Goldman integration boundary evidenced. Failure to transmit disputes was not detected for 12+ months.	FAIL
T-07	Data security at integration boundary	Data transmitted between vendor and financial entity systems is encrypted in transit and at rest. Access controls are defined and reviewed. Data minimisation principles applied.	Not determinable from public record. Scored as not evidenced pending confirmation.	CONDITIONAL

4iGov.cloud

5. REGULATORY OBLIGATIONS MAPPING

This section maps the applicable regulatory obligations to the vendor relationship and assesses whether those obligations are adequately addressed in the governance and contractual framework.

Framework	Obligation	Requirement for Third Party Relationship	Apple-Goldman Gap (Inferred)	Status
DORA	Art 28 — Third Party ICT Risk	Financial entity must identify, assess, and manage ICT third party risk. Critical providers must be subject to full risk management programme.	Apple not managed as a critical ICT provider by Goldman Sachs. No third party risk programme evidenced for the Apple relationship.	FAIL
DORA	Art 30 — Contractual Provisions	Contracts with critical ICT providers must include SLAs, audit rights, change notification, incident notification, and resilience testing obligations.	All four contractual provisions absent or not evidenced in public record.	FAIL
DORA	Art 25 — ICT Testing	Resilience testing must include integration points with critical ICT providers. Failure path testing required.	No integrated resilience testing of the Apple-Goldman dispute submission workflow evidenced.	FAIL
EU AI Act	Art 9 — Risk Management	Risk management system must cover third party AI components in high-risk systems. Vendor AI risk must be assessed as part of overall system risk.	No risk management system for the Apple Card dispute routing system. Third party AI risk not assessed.	FAIL
EU AI Act	Art 17 — Quality Management	QMS must cover third party components. Testing of third party AI systems required before deployment and after material changes.	No QMS covering Apple’s consumer-facing systems as a component of Goldman’s regulated AI workflow.	FAIL
NIST AI RMF	MAP — Third Party Context	Third party AI dependencies must be mapped as part of AI use case risk profile. Vendor risk must be assessed before deployment.	Apple not mapped as a third party dependency in the AI use case risk profile. Dependency risk not assessed.	FAIL
CFPB / TILA	Reg Z — Dispute Obligations	Financial entity is responsible for fulfilling TILA obligations regardless of whether a third party system fails. Adequate oversight of third party systems is required.	Goldman Sachs held responsible by CFPB for failure to investigate disputes that Apple’s system did not transmit. Third party system failure did not transfer the regulatory obligation.	FAIL

4igov.cloud

Key Regulatory Principle

- Regulatory obligations do not transfer to third party vendors. When a vendor system fails and a regulated obligation is not fulfilled, the financial entity remains liable. The Apple-Goldman case confirms this explicitly — Goldman Sachs was fined for disputes that Apple's system failed to transmit. Effective third party governance is not optional; it is the financial entity's primary defence against third party failure.

4iGov.cloud

6. OVERALL RISK RATING AND REMEDIATION PLAN

6.1 Score Summary

Rate each section from 1 (significant gaps) to 4 (fully compliant) based on the proportion of requirements meeting pass threshold. Apply the overall verdict using the table below.

Assessment Section	Template Score (1-4)	Apple-Goldman Score	Notes
Section 3 — Governance and Contractual		1	4 of 7 requirements FAIL. 3 CONDITIONAL. No critical contractual provisions in place.
Section 4 — Technical Integration Controls		1	5 of 7 controls FAIL. 2 CONDITIONAL. No transmission confirmation, no dead state detection, no boundary monitoring.
Section 5 — Regulatory Obligations		1	6 of 7 obligations assessed as FAIL. Fundamental DORA, EU AI Act, and TILA gaps.
OVERALL SCORE	/ 12	**3 / 12**	**VERDICT: HIGH RISK — Vendor relationship not adequately governed. Engagement with regulated workflows should not continue without remediation.**

Overall Score	Risk Rating	Recommended Action
10 to 12	Low Risk	Vendor relationship adequately governed. Proceed with standard annual review.
7 to 9	Medium Risk	Material gaps identified. Remediation plan required within 90 days. Heightened monitoring in interim.
4 to 6	High Risk	Significant governance failures. Remediation plan required within 30 days. Escalation to risk committee. Consider enhanced contractual obligations or vendor review.
1 to 3	Critical Risk	Fundamental governance failures. Immediate escalation to board and regulator notification consideration. Vendor engagement with regulated workflows should not continue until remediation is complete.

6.2 Minimum Remediation Requirements

For any requirement rated FAIL, the following minimum remediation actions apply before the vendor relationship can be rated as adequately governed.

Ref	Requirement	Minimum Remediation Action	Owner	Timeline
G-01	SLA for regulated workflows	Negotiate and execute SLA covering all regulated workflow processing times aligned to regulatory deadlines. Include breach notification and remediation obligations.	Legal and Risk Officer	60 days
G-02	Change notification	Amend contract to require minimum 10 business days prior notification of	Legal	30 days

4iGOV.cloud

Ref	Requirement	Minimum Remediation Action	Owner	Timeline
		material changes to systems affecting regulated workflows. Emergency change process defined.		
G-03	Audit rights	Amend contract to include right to audit vendor systems relevant to regulated workflows. Minimum annual audit. Financial entity can appoint third party auditor.	Legal	30 days
G-04	Incident notification	Amend contract to require vendor notification within 4 hours of any incident affecting regulated workflow processing. RCA required within 5 business days.	Legal	30 days
T-01	End-to-end integration testing	Establish joint testing protocol covering all regulated workflow paths including failure and incomplete submission scenarios. Conduct before every material deployment.	Technology Lead	45 days
T-02	Transmission confirmation	Implement transmission confirmation mechanism. Financial entity receives positive acknowledgment for every regulated transaction. Silent failures not permitted.	Technology Lead	45 days
T-03	Dead state detection	Implement state monitoring across full integration workflow. All incomplete transactions flagged within 24 hours. Recovery mechanism documented and tested.	Technology Lead	60 days
T-06	Integration boundary monitoring	Implement real-time monitoring at integration boundary. Volume anomalies and failure rates trigger automated alerting within defined thresholds.	Technology Lead	30 days

This is the final artefact in the 4iGov AI Governance Practitioner Series.

Artefact 1: Case Study | Artefact 2: Governance Framework | Artefact 3: AI Agent Risk Assessment | 4igov.cloud

4igov.cloud