INSTITUTIONAL AI
— SOVEREIGN INTELLIGENCE EDITION — CONFIDENTIAL

THE AI SOVEREIGNTY ASSESSMENT

ASSET SERVICING EDITION- PARTIAL

Governing AI Sovereignty Across Global Custody, Fund Administration, Securities Lending, Transfer Agency, and the Institutional Operations Chain

A Diagnostic Framework for Asset Servicing Leadership

APRIL 2026 | BOSTON, MA | GLOBAL ADVISORY SERVICES | www.institutionalai.net

FOR THE BOARD | EXECUTIVE BRIEF | ASSET SERVICING | CONFIDENTIAL

Your institution processes, safeguards, and reports on assets belonging to thousands of the world's largest investors. Every custody record, every NAV calculation, every corporate action, every securities lending transaction — these are fiduciary acts performed on behalf of clients who trust you with their most sensitive financial data. AI is now embedded in those operations. The question for the board is whether the governance of that AI matches the governance standard your clients expect of everything else you do.

THE NUMBERS THAT MATTER

$130T+
in combined AUC/A held by the three largest global custodians — BNY, State Street, and Northern Trust

100+
markets in which global asset servicers operate custody, settlement, and reporting operations

78%
of enterprises run mission-critical AI workloads on infrastructure they cannot independently audit

127 hrs.
mean time to detect incidents on provider-managed infrastructure vs. 34 hrs. with institution-controlled encryption

$4.7T
estimated global assets now influenced by AI-driven investment decisions — serviced by your operations

92%
of advanced AI chips fabricated by a single company in a geopolitically contested region

T+1
settlement acceleration — AI is now critical to meeting compressed settlement windows across global markets, making AI infrastructure reliability a direct operational risk

THE GOVERNANCE ARCHITECTURE

Score each cell 1 (Reactive) to 4 (Sovereign). Maximum total: 100 points. The distribution reveals whether your governance is balanced or structurally exposed — particularly in the Models and Agents columns where AI is now processing client portfolio data, executing reconciliations, and generating NAV calculations.

	Power	Compute	Data Centers	Models	Agents
Jurisdictional	___	___	___	___	___
Logical	___	___	___	___	___
Technical	___	___	___	___	___
Operational	___	___	___	___	___
Contractual	___	___	___	___	___

THE 5×5 CONTROL MATRIX

25 governance intersections | Score 1–4 per cell | Max total: 100 points

THE ASSET SERVICING SOVEREIGNTY IMPERATIVE

Asset servicers occupy a unique position in the financial ecosystem: you are the infrastructure layer. Your clients — asset managers, pension funds, sovereign wealth funds, insurance companies — depend on your operations as the foundation of their own governance. When your AI systems process their portfolio data, calculate their NAVs, execute their corporate

actions, and generate their regulatory reporting, the governance of those AI systems is not just your obligation — it is a link in every client's fiduciary chain.

If the AI systems performing your custody, fund administration, and transfer agency operations are running on infrastructure you cannot audit, in jurisdictions you cannot verify, under terms you have not negotiated for AI-specific processing — your clients' governance depends on assurances you cannot independently confirm.

THE GLOBAL OPERATIONS DIMENSION

Global asset servicers operate across 100+ markets, dozens of regulatory jurisdictions, and multiple time zones. AI deployed in these operations creates governance complexity that single-jurisdiction firms do not face:

Operational Domain	AI Governance Risk	Jurisdictional Complexity
Global Custody & Settlement	AI-driven trade matching, settlement prediction, and exception management processes client positions across jurisdictions with different data sovereignty laws	CSDR (EU), SEC 15c6-1 (US), HKMA, MAS — each with distinct data residency and audit requirements
Fund Administration & NAV	AI-assisted NAV calculation, pricing validation, and fair value estimation processes fund-level data that determines investor returns	UCITS (EU), SEC/ICA (US), CSSF, CBI, FINMA — fund domicile determines governing regulation
Transfer Agency	AI processes investor identity data, transaction records, and distribution payments across global investor bases	AML/KYC regimes vary by jurisdiction; GDPR, CCPA, and local privacy laws apply to investor PII
Securities Lending	AI-driven collateral optimization, borrower assessment, and automated lending programs process beneficial owner data	Beneficial owner data sovereignty; SFTR reporting (EU); SEC Rule 10c-1 (US)
Middle Office Outsourcing	AI performs reconciliation, trade confirmation, and position management on behalf of asset manager clients	Client data processed in your infrastructure under your AI governance — your governance becomes their governance
Regulatory Reporting	AI generates and validates regulatory filings across dozens of jurisdictions simultaneously	EMIR, MiFIR, SFTR, Form PF, CPO-PQR — accuracy obligations attach to your AI systems

THE CRITICAL REGULATORY CONTEXT

Framework	Implication for Asset Servicers
DORA (Digital Operational Resilience Act)	Directly applicable to custodians and fund administrators in the EU. ICT risk management, incident reporting, and third-party risk oversight requirements extend to AI infrastructure.
OCC / Fed / FDIC Guidance	Bank-regulated custodians face interagency guidance on AI risk management, model risk (SR 11-7), and third-party risk. AI in custody operations is subject to safety and soundness examination.
NIS2 Directive	Asset servicers designated as essential entities face mandatory cybersecurity and supply chain governance requirements, including AI system resilience.

Framework	Implication for Asset Servicers
GDPR / Global Privacy	Investor PII processed by AI in transfer agency, KYC, and client reporting operations must satisfy data residency, purpose limitation, and data subject rights.
CSDR / T+1 Settlement	AI systems supporting settlement must be operationally resilient. Settlement failures caused by AI system errors create direct financial liability.
UCITS / AIFMD	Fund administrators using AI for NAV calculation, pricing, and compliance monitoring must demonstrate governance of those AI systems to fund boards and regulators.
SEC Custody Rule / Form ADV	Qualified custodians using AI in custody operations face SEC examination of AI governance as part of custody rule compliance.
Basel III / G-SIB Requirements	G-SIB custodians face heightened operational resilience and risk management standards that extend to AI systems in critical operations.

FIVE QUESTIONS FOR THE BOARD

1.	When AI calculates a NAV, reconciles a position, or processes a corporate action on behalf of a client, can we prove — with technical evidence, not provider assurances — where that processing occurred and who had access?
2.	If our primary AI or cloud provider experienced a 48-hour outage, what happens to custody settlement, NAV publication, transfer agency processing, and securities lending operations across 100+ markets?
3.	Can we produce a complete audit trail of any AI-influenced operational decision from 18 months ago — a NAV calculation, a trade match, a corporate action election — for a regulator or a client within 24 hours?
4.	Do our clients know that AI is now processing their portfolio data, investor records, and fund calculations — and have we disclosed the governance framework governing that AI to their boards?
5.	Are we confident that our AI governance satisfies DORA, OCC examination standards, NIS2, GDPR, and every client's own due diligence requirements — simultaneously, across every jurisdiction we operate in?

Completion: 60–90 min | Score: 0–100 | 25 control questions | information@institutionalai.net

TABLE OF CONTENTS

1 EXECUTIVE OVERVIEW

What This Assessment Measures

The AI Sovereignty Assessment for Asset Servicing measures your institution's verified ability to own, govern, and audit the AI systems that execute custody operations, calculate net asset values, process corporate actions, manage securities lending programs, operate transfer agency functions, and generate regulatory reporting — across five governance control dimensions and five AI infrastructure layers.

The assessment produces a 5×5 matrix of 25 specific, answerable governance questions. A score of 1 to 4 per cell — maximum 100 total — produces a sovereignty profile revealing not just your overall governance posture, but exactly which infrastructure-governance intersections are exposed.

> *For asset servicers, the stakes are different from asset managers: you are processing thousands of clients' data simultaneously. A governance failure in your AI infrastructure is not a single-institution event — it is a systemic event affecting every client whose assets you service.*

The Infrastructure Layer Obligation

Asset servicers are the infrastructure layer of the global investment industry. BNY services over 96% of the world's top 100 banks. State Street's AUC/A reached $53.8 trillion in 2025. Northern Trust secured over 100 new mandates representing $385 billion in a single year. When AI is deployed in these operations, the governance obligation scales with the systemic importance of the institution.

The AI systems now embedded in your operations — reconciliation engines, NAV calculators, trade matching algorithms, corporate action processors, compliance monitors — are performing fiduciary acts on behalf of clients who selected you precisely because of your operational integrity. Those clients' boards are asking whether your AI governance matches the standard they expect of your non-AI operations. For most asset servicers today, it does not.

> *Your clients chose you because of operational excellence. If your AI governance does not match the standard of your non-AI operations, the trust that took decades to build can be undermined in a single regulatory examination or client audit.*

The Global Operations Imperative

A global custodian operating across 100+ markets faces AI governance complexity that is qualitatively different from a single-jurisdiction institution. Consider: a corporate action in Tokyo is processed by AI running on infrastructure in Ireland, using a model trained in the United States, with results delivered to a client in Singapore whose regulator requires data residency in

Asia-Pacific. That single operation touches four jurisdictional governance questions — and your AI governance framework must answer all of them simultaneously.

T+1 settlement has made this operational. AI is now critical to meeting compressed settlement windows — trade matching, exception prediction, and settlement instruction generation all rely on AI processing that must be resilient, auditable, and jurisdictionally compliant in real time. An AI system failure during a settlement cycle is no longer an inconvenience; it is a financial liability.

How to Score Each Cell

Level	Classification	Description
1	Reactive	No visibility or control. Relying entirely on provider assurances or standard contracts. Score: 1 point.
2	Evolving	Partial visibility or contractual controls only. Aware of the gap with some mitigating measures. Score: 2 points.
3	Governed	Active monitoring, enforced contractual rights, partial technical controls. Demonstrable to regulators and clients. Score: 3 points.
4	Sovereign	Full technical and contractual sovereignty. Cryptographically verifiable, continuously monitored, independently auditable. Score: 4 points.

2 THE ASSET SERVICING AI GOVERNANCE CHALLENGE

The AI Use Cases — and Their Governance Implications

Global Custody and Settlement

AI-driven trade matching, settlement prediction, exception management, and fails prevention are now operational at every major custodian. T+1 settlement has accelerated the dependency on AI for real-time processing across time zones.

Example: Your AI settlement prediction engine identifies 2,000 potential fails across 40 markets during the Asian trading day. The AI prioritises resolution actions, generates settlement instructions, and escalates exceptions — all before European markets open. If that AI system experiences model drift and begins misclassifying settlement risk, the cascading fails affect every client whose trades settle through your custody network.

Fund Administration and NAV Calculation

AI-assisted NAV calculation, pricing validation, fair value estimation, and fund accounting are transforming fund administration. When AI contributes to a published NAV that is later found to be incorrect, the liability chain runs from the fund administrator to the fund board to the end investor.

Example: An AI pricing engine validates 50,000 securities prices across your fund administration platform. It flags 200 prices as anomalous and auto-corrects 180 of them. Twenty corrections are wrong — affecting NAVs for 15 funds with combined AUM of $30 billion. The regulatory inquiry asks: what was the AI's correction logic? Who reviewed it? Can you produce the decision trail?

Transfer Agency and Investor Servicing

AI processes investor identity verification (KYC), transaction processing, distribution calculations, tax reporting, and anti-money laundering surveillance. Transfer agency AI processes the most sensitive personal data in the asset servicing chain — investor identities, bank account details, and transaction histories across jurisdictions with different privacy regimes.

Securities Lending and Collateral Management

AI-driven collateral optimisation, borrower assessment, automated lending programme management, and real-time collateral monitoring are standard. Securities lending AI processes beneficial owner data — which funds are lending, what collateral is accepted, what revenue is generated — that many clients consider highly confidential competitive intelligence.

Middle Office Outsourcing

AI performs reconciliation, trade confirmation, position management, and performance measurement on behalf of asset manager clients. When an asset manager outsources middle office to your institution, your AI governance becomes a direct link in their operational resilience chain. DORA explicitly requires financial entities to assess the ICT risk of their critical third-party providers — which is you.

Regulatory Reporting and Compliance

AI generates, validates, and submits regulatory filings across dozens of jurisdictions — EMIR, MiFIR, SFTR, Form PF, CPO-PQR, Annex IV. An AI system that generates an inaccurate regulatory filing creates direct regulatory exposure for your institution and your client.

Digital Asset Servicing

AI supports digital asset custody, tokenised asset administration, blockchain data integration, and on-chain reporting. BNY became the first G-SIB to offer regulated digital asset custody. State Street is implementing digital asset servicing infrastructure. AI governance in digital asset operations must address both traditional custody standards and emerging digital asset regulatory frameworks.

The Client Governance Chain

Asset servicers face a governance obligation that asset managers and asset owners do not: your AI governance is a dependency for thousands of other institutions' governance. When a pension fund board asks its custodian whether AI is being used to process their assets and whether that AI is governed to fiduciary standards, the custodian's answer determines the pension fund's own governance posture.

> *Your AI governance is not just your governance. It is a link in the fiduciary chain of every client whose assets you service. A governance failure at the infrastructure layer propagates to every institution that depends on you.*

3 THE FRAMEWORK

The Five AI Ecosystems in Asset Servicing

ECOSYSTEM 1 — POWER

Energy infrastructure powering global custody, fund administration, and settlement operations across data centres in multiple continents. Energy governance is operational resilience governance — power failure during a settlement cycle is a custody failure.

ECOSYSTEM 2 — COMPUTE

GPU clusters and computing infrastructure running reconciliation engines, NAV calculators, settlement prediction models, and compliance surveillance. For G-SIB custodians, compute governance is subject to bank supervisory examination.

ECOSYSTEM 3 — DATA CENTERS

The data centers and cloud infrastructure where client portfolio data, investor records, fund accounting data, and custody records reside. Multi-jurisdictional data center governance is the foundation of GDPR, DORA, and global privacy compliance.

ECOSYSTEM 4 — MODELS

The AI models processing custody operations, calculating NAVs, predicting settlement outcomes, monitoring compliance, and generating client reporting. This is the governance gap: models from external providers process client data that your institution is contractually and regulatorily obligated to protect.

ECOSYSTEM 5 — AGENTS

Autonomous AI agents executing multi-step operational workflows: trade matching sequences, corporate action processing chains, reconciliation exception resolution, and automated regulatory filing generation. State Street is implementing agentic AI across operations. BNY's Eliza platform integrates AI across client servicing.

The Five Pillars of Control

Pillar	Core Question	Asset Servicing Implication
1. Jurisdictional	Where does it execute, under which law?	100+ market operations; DORA, GDPR, NIS2, OCC guidance; fund domicile data residency
2. Logical	Who can access it, when, with what proof?	Client data segregation; multi-client processing; provider support access to custody systems

Pillar	Core Question	Asset Servicing Implication
3. Technical	Who holds the encryption keys?	Client portfolio data encryption; beneficial owner data protection; model provider access to client data during processing
4. Operational	Do you have real-time visibility?	24/7 global operations; settlement cycle monitoring; NAV publication deadlines; incident detection
5. Contractual	Do you have enforceable rights?	Cloud and AI provider terms; client SLA alignment; audit rights; DORA third-party provisions

How the Matrix Works

Scoring principle: Score each cell based on what you can demonstrate with evidence — not what contracts assert. For asset servicers, the critical honesty is in the Models and Agents columns: your AI providers' governance is your clients' governance.

THE 5×5 CONTROL MATRIX

Each cell is scored 1 (Reactive) to 4 (Sovereign) based on demonstrable evidence. Red-highlighted cells indicate critical governance intersections where most institutions score Level 1. The distribution across cells — particularly the gap between the Data Centers and Models columns — is more diagnostic than the total score.

4 THE ASSESSMENT

Complete all 25 questions. Score each cell 1–4 based on demonstrable evidence. Recommended team: COO, CTO, CISO, General Counsel, Chief Risk Officer, Head of Fund Administration, Head of Custody. Time: 60–90 minutes.

ECOSYSTEM 1 — POWER

Energy infrastructure

PILLAR 1 — JURISDICTIONAL CONTROL

Where does it execute, under which law?

Under which jurisdictions does the energy infrastructure powering your global custody, fund administration, and settlement operations reside — and do energy supply arrangements satisfy your operational resilience obligations under DORA, OCC, and FCA frameworks?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P1×E1 Score: _____ / 4

Notes: _____

PILLAR 2 — LOGICAL CONTROL

Who can access it, when, with what proof?

Who has privileged access to energy management systems for your custody and fund administration data centres — and is that access logged to institution-controlled systems?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P2×E1 Score: _____ / 4

Notes: _____

PILLAR 3 — TECHNICAL CONTROL

Who holds the encryption keys?

Do you control encryption keys for energy telemetry data across your global data center operations?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P3×E1 Score: _____ / 4

Notes: _____

PILLAR 4 — OPERATIONAL CONTROL

Do you have real-time visibility?

Do you have real-time visibility into energy consumption per operational function — custody, fund admin, transfer agency — sufficient for operational resilience reporting and client ESG disclosure?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P4×E1 Score: _____ / 4

Notes: _____

PILLAR 5 — CONTRACTUAL CONTROL

Do you have enforceable rights?

Do your energy contracts include resilience provisions, audit rights, and SLAs aligned to the operational continuity requirements of your custody and settlement obligations?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P5×E1 Score: _____ / 4

Notes: _____

ECOSYSTEM 1 — POWER SUBTOTAL: _____ / 20

ECOSYSTEM 2 — COMPUTE

GPU / chip infrastructure

PILLAR 1 — JURISDICTIONAL CONTROL

Where does it execute, under which law?

Under which jurisdictions do the compute resources running your settlement prediction, NAV calculation, reconciliation, and compliance AI models actually execute?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P1×E2 Score: _____ / 4

Notes: _____

PILLAR 2 — LOGICAL CONTROL

Who can access it, when, with what proof?

Who has access to compute environments processing client portfolio data, investor records, and fund accounting — including cloud provider support engineers — and is that access logged in your systems?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P2×E2 Score: _____ / 4

Notes: _____

PILLAR 3 — TECHNICAL CONTROL

Who holds the encryption keys?

Who controls the encryption keys for client data, fund accounting records, and investor PII processed on your compute infrastructure?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P3×E2 Score: _____ / 4

Notes: _____

PILLAR 4 — OPERATIONAL CONTROL

Do you have real-time visibility?

Do you have real-time visibility into compute utilization, performance, and availability across all AI systems supporting custody settlement, NAV publication, and regulatory reporting deadlines?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement

Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P4×E2 Score: _____ / 4

Notes: _____

PILLAR 5 — CONTRACTUAL CONTROL

Do you have enforceable rights?

Do your compute agreements protect client data from provider access and include workload portability sufficient to migrate custody operations to alternative infrastructure within your SLA obligations?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P5×E2 Score: _____ / 4

Notes: _____

ECOSYSTEM 2 — COMPUTE SUBTOTAL: _____ / 20

ECOSYSTEM 3 — DATA CENTERS

Cloud & physical infrastructure

PILLAR 1 — JURISDICTIONAL CONTROL

Where does it execute, under which law?

Can you demonstrate with technical evidence where every client portfolio, investor record, fund accounting workload, and custody record resides — satisfying DORA, GDPR, UCITS, and SEC data governance requirements across all jurisdictions you operate in?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P1×E3 Score: _____ / 4

Notes: _____

PILLAR 2 — LOGICAL CONTROL

Who can access it, when, with what proof?

Can you prove that no unauthorised person accessed client portfolio data, investor PII, fund accounting records, or custody positions in the past 18 months?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P2×E3 Score: _____ / 4

Notes: _____

PILLAR 3 — TECHNICAL CONTROL

Who holds the encryption keys?

Do you hold your own encryption keys (HYOK) for all client data, investor records, and fund accounting — or does your cloud provider manage them?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P3×E3 Score: _____ / 4

Notes: _____

PILLAR 4 — OPERATIONAL CONTROL

Do you have real-time visibility?

Can you detect an unauthorised access, data breach, or AI anomaly affecting client data within minutes — satisfying DORA incident reporting timelines and client notification obligations?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement

Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P4×E3 Score: _____ / 4

Notes: _____

PILLAR 5 — CONTRACTUAL CONTROL

Do you have enforceable rights?

Do your data center agreements include unlimited audit rights, subprocessor transparency, certified deletion, and exit terms exercisable within timelines that maintain custody service continuity?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P5×E3 Score: _____ / 4

Notes: _____

ECOSYSTEM 3 — DATA CENTERS SUBTOTAL: _____ / 20

ECOSYSTEM 4 — MODELS

LLMs & AI systems

PILLAR 1 — JURISDICTIONAL CONTROL

Where does it execute, under which law?

Under which jurisdictions are the AI models processing client portfolio data, fund NAVs, investor records, and custody operations trained, stored, and served?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P1×E4 Score: _____ / 4

Notes: _____

PILLAR 2 — LOGICAL CONTROL

Who can access it, when, with what proof?

Can your AI model providers access the client data, fund accounting information, and investor records your models process — and is that access logged in your own infrastructure?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P2×E4 Score: _____ / 4

Notes: _____

PILLAR 3 — TECHNICAL CONTROL

Who holds the encryption keys?

When AI models process client portfolio positions, fund NAVs, or investor PII, does the model provider process this data in plaintext on their infrastructure?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P3×E4 Score: _____ / 4

Notes: _____

PILLAR 4 — OPERATIONAL CONTROL

Do you have real-time visibility?

Do you have real-time visibility into AI model behavior across NAV calculation, settlement prediction, reconciliation, and compliance monitoring — including model drift detection and output quality?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement

Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P4×E4 Score: _____ / 4

Notes: _____

PILLAR 5 — CONTRACTUAL CONTROL

Do you have enforceable rights?

Do your AI model provider agreements give you explicit rights over client data processed, interaction logs, and outputs — or does the provider retain usage rights that conflict with your custody and fund administration obligations?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P5×E4 Score: _____ / 4

Notes: _____

ECOSYSTEM 4 — MODELS SUBTOTAL: _____ / 20

ECOSYSTEM 5 — AGENTS

Agentic applications

PILLAR 1 — JURISDICTIONAL CONTROL

Where does it execute, under which law?

Under which jurisdictions do your autonomous settlement processing, reconciliation, corporate action, and compliance monitoring agents execute — and where do their decision logs reside?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P1×E5 Score: _____ / 4

Notes: _____

PILLAR 2 — LOGICAL CONTROL

Who can access it, when, with what proof?

Who can approve, modify, or halt autonomous agents executing settlement instructions, processing corporate actions, or generating regulatory filings — and is every agent decision immutably logged?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P2×E5 Score: _____ / 4

Notes: _____

PILLAR 3 — TECHNICAL CONTROL

Who holds the encryption keys?

Do you have cryptographic enforcement over what autonomous agents can access across client portfolios, fund data, and investor records — preventing cross-client data exposure at the agent level?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P3×E5 Score: _____ / 4

Notes: _____

PILLAR 4 — OPERATIONAL CONTROL

Do you have real-time visibility?

Can you monitor, pause, or audit every autonomous agent processing settlements, reconciliations, corporate actions, or regulatory filings in real time — across all 100+ markets?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P4×E5 Score: _____ / 4

Notes: _____

PILLAR 5 — CONTRACTUAL CONTROL

Do you have enforceable rights?

Do your agentic AI vendor agreements include institutional liability for autonomous operational decisions, audit rights over every agent action, and data exit provisions protecting client data processed by agents?

Level 1 □ Reactive — no visibility; relying on provider assurances
Level 2 □ Evolving — partial contractual controls; limited technical enforcement
Level 3 □ Governed — active monitoring, enforced contractual rights, partial technical controls
Level 4 □ Sovereign — cryptographically verifiable, continuously monitored, independently auditable

P5×E5 Score: _____ / 4

Notes: _____

ECOSYSTEM 5 — AGENTS SUBTOTAL: _____ / 20

5 SCORING SUMMARY & HEAT MAP

Transfer your 25 cell scores below. The distribution tells you more than the total — specifically the gap between Data Centers and Models column scores.

PILLAR	POWER	COMPUTE	DATA CTR	MODELS	AGENTS	TOTAL
Jurisdictional	___	___	___	___	___	___ / 20
Logical	___	___	___	___	___	___ / 20
Technical	___	___	___	___	___	___ / 20
Operational	___	___	___	___	___	___ / 20
Contractual	___	___	___	___	___	___ / 20
ECO TOTAL	___/20	___/20	___/20	___/20	___/20	___ / 100

TOTAL SOVEREIGNTY SCORE: _____ / 100

Web: www.institutionalai.net/ai-strategy Email: information@institutionalai.net

All discussions covered under NDA. Assessment results and client data are never shared externally.

I N S T I T U T I O N A L A I

Sovereign Intelligence. Institutional Control.

www.institutionalai.net

LEGAL DISCLAIMER

This document is provided solely for informational and educational purposes. It does not constitute legal, regulatory, investment, or other professional advice, and it does not create an attorney-client or advisory relationship. Institutions should seek independent legal, regulatory, and technical counsel before making decisions related to AI infrastructure, governance, or compliance.

All assessments, scores, and recommendations contained herein are illustrative and intended to support internal discussion and strategic planning. They do not represent an official certification, audit, or regulatory determination. Institutional AI assumes no responsibility or liability for any decisions or outcomes resulting from reliance on this material.

All data cited from third-party sources are credited to publicly available publications (BIS, IOSCO, OCC, ESMA, SEC, IEA, OECD, Uptime Institute, and regulators) as of 2024–2026.