

INTRAGEN & ONE IDENTITY | FRAMEWORK

The wrong question: an IAM workload sovereignty framework for European buyers

INTRAGEN. by nomios

ONE™ IDENTITY

Executive summary

European IAM buyers keep asking the wrong question. **"Can we still trust US vendors?"** is not the question that protects the business.

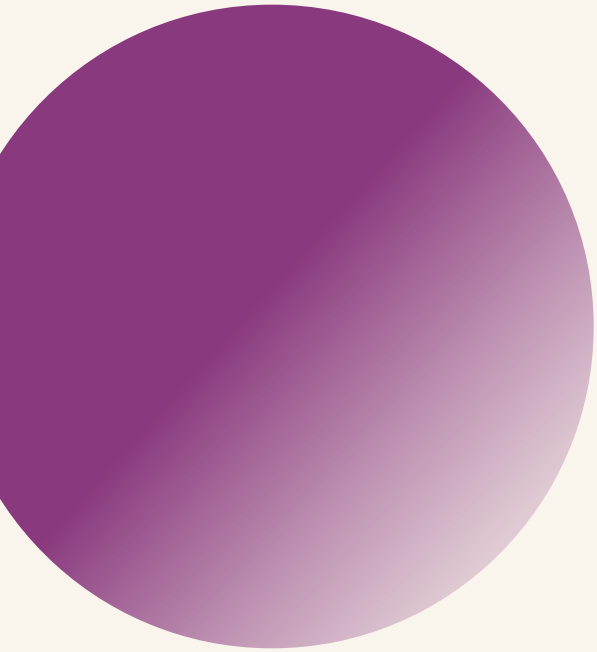
The right question is operational. If a vendor were ordered to stop selling, supporting, or licensing its product to you tomorrow, could you keep running long enough to build an alternative?

This paper turns that question into a working framework. It defines sovereignty in IAM across three dimensions: data, operational, and jurisdictional. It tests each one through three questions in order: classify the workload, model continuity under vendor lockout, and audit substrate control.

The framework starts from an honest fact. Mature IGA, PAM, and Access Management capability sits with a small number of mostly US vendors, and the infrastructure beneath them is mostly non-European too. Regulated buyers cannot suspend their obligations while the European market catches up.

So the answer is not to avoid US vendors. It is to know, configuration by configuration, where a deployment is sovereign and where it is exposed. We test the framework against one real deployment: One Identity Manager on customer-owned, on-premise infrastructure.

The headline finding holds across the paper. The same vendor can pass in one configuration and fail in another. Sovereignty in IAM is a measurable property of a configuration, not a label on a logo.



DISCLAIMER: This paper is a thought leadership framework, not legal or regulatory advice. It sets out a structured way to reason about sovereignty in IAM deployments. It does not interpret NIS2, DORA, or any national regime on your behalf, and it does not replace guidance from qualified legal, compliance, or regulatory advisors. Obligations vary by sector, jurisdiction, and circumstance. Validate any decision against your own advisors and your competent authority before acting on it.

The wrong question: an IAM workload sovereignty framework for European buyers

1. The wrong question

The question European IAM buyers keep asking is can we still trust US vendors? That is the wrong question. The right question is operational:

> *If a vendor were ordered tomorrow to stop selling, supporting, or licensing its product to a European customer, by sanctions, executive order, or licence revocation, could the customer keep running the system long enough to build an alternative?*

DORA gestures at exactly this concern for financial services. It already requires exit strategies, substitutability assessments, and ICT third-party concentration-risk management. It stops short in two places. It does not name geopolitical risk as a category. It applies only to financial services. Every other European IAM buyer is left to translate the same question into its own language without regulatory vocabulary to anchor it.

The European policy register has shifted. The Draghi report frames technology dependency on non-European providers as a strategic vulnerability. Procurement teams that used to treat sovereignty as a checkbox are starting to treat it as an architectural constraint.

The honest response is neither to avoid US vendors wholesale nor to carry on as before. It is a layered approach by workload class, anchored in a working definition of sovereignty in IAM, and tested against a specific deployment: One Identity Manager on customer-owned, on-premise infrastructure.

2. The honesty floor

Two facts have to be acknowledged before any framework is proposed.

- Mature Identity Governance and Administration (IGA), Privileged Access Management (PAM), and Access Management capability is concentrated in a small number of mostly US-headquartered vendors. European alternatives exist; for several enterprise workload classes their depth and integration coverage remain difficult to match today.

- Server, storage, network, operating-system, and middleware capability is concentrated in a small number of mostly non-European vendors. A complete European-supplied substrate is not a realistic procurement option for an enterprise European IAM buyer in 2026.

A buyer running NIS2-essential, DORA-regulated, or ISO 27001-certified processes cannot suspend the obligation while waiting for the European market to catch up. The responsible path is to use what works, in a configuration that minimises sovereignty exposure across the three dimensions defined below.

3. The regulatory frame, and where it stops

European IAM procurement vocabulary rests on two horizontal regulations and a layer of substrate-control regimes.

Instrument	What it gives the buyer	Where it stops
NIS2 (Article 21(2)(d), with 22(1))	Supplier-risk management for critical service providers; Union-level coordinated risk assessments of critical supply chains.	No specific test for suppliers headquartered outside the EU. Article 22(1) has not been activated for IAM.
DORA (Articles 28(3), 28(8), 28(9), 29)	Exit-strategy and substitutability requirements; ICT concentration-risk management; Register of Information with standardised templates.	Does not name geopolitical risk as a category. Applies only to financial services.
Substrate regimes (EUCS, GAIA-X, BSI C5, SecNumCloud, BIO, ENS, ACN)	A recognised vocabulary for hosting locus, contracting entity, key custody, and operational dependencies.	EUCS removed sovereignty-specific requirements from its highest tier in March 2024. National regimes apply only within their jurisdictions. ISO 27001 and SOC 2 do not address sovereignty by design.

The gap none of these parts closes is the one this paper takes up: a working definition of sovereignty in IAM, and a portable test for measuring it against any deployment.

4. What sovereignty means here

Sovereignty in IAM is the buyer's ability to retain control of three distinct things in the face of external pressure on the vendor, on the substrate, or on the surrounding legal regime. The three dimensions are not interchangeable. A deployment can satisfy one and fail another.

Dimensions	What it tests
Data sovereignty	Where the identity data resides, under whose legal regime, and who can be compelled to disclose it.
Operational sovereignty	The ability to keep the workload running independently of the vendor's continued cooperation.
Jurisdictional sovereignty	Which legal regime governs the contract, the contracting entity, and the operating environment.

The paper tests these dimensions through three questions, in order:

1. Classify the workload. Real-time sensitivity profile. Gating question only.
2. Continuity under vendor lockout. The operational-sovereignty test.
3. Substrate control. The data-sovereignty and jurisdictional-sovereignty test combined.

The same vendor can pass in one configuration and fail in another. The framework's output is a per-configuration map of where a stack is sovereign and where it is exposed.

5. Q1, Classify the workload

Workload class	Real-time sensitivity	Lockout window the business absorbs	Sovereignty toolkit
AM, SSO, MFA, PAM session brokering, CIAM authentication	High. Unavailability measured in minutes.	Minutes to tens of minutes.	Federation with customer-controlled IdP, customer-managed keys, EU-tenant SaaS under European contracting entity, sovereign-cloud substrate, and parallel-region resilience.
IGA: joiner-mover-leaver, provisioning, entitlement management, access reviews, certifications, and SoD	Low. Workflow is not real-time.	Days to weeks. Manual workarounds feasible.	Customer-owned substrate, on-premise deployment, customer-controlled keys, and customer-controlled identity store.

The Q1 insight is load-bearing. **IGA's low real-time sensitivity is not a limitation of the workload class. It is what makes IGA the workload class most amenable to substrate-control sovereignty patterns.** The same buyer who has limited substrate options for SSO may have substantially more substrate options for IGA, even when both products come from the same vendor.

Sovereignty cascades

A workload's operational sovereignty is bounded above by every layer it depends on. For most European enterprises today, the dominant non-European dependency is the productivity and hyperscaler substrate: Entra ID, Microsoft 365, Google Workspace, and the major hyperscaler clouds. Any IAM SaaS that runs on or federates with that substrate inherits its sovereignty profile, by construction.

Under a vendor-lockout scenario severe enough to remove a US-headquartered IAM SaaS from a European customer, the productivity substrate beneath it would already be removed too, and the IAM failure would be secondary to a much larger continuity event. IGA has the most architectural independence from that stack, and therefore the most sovereignty headroom.

> *For most European enterprises today, the dominant non-European dependency is the productivity and hyperscaler substrate… Any IAM SaaS that runs on or federates with that substrate inherits its sovereignty profile, by construction.*

6. Q2, Continuity under vendor lockout

> *If a vendor told the customer tomorrow that the customer cannot use the product, by sanctions, executive order, or licence revocation, could the existing system keep running while an alternative is built?*

The lawfulness of the lockout is irrelevant. The buyer plans for the operational consequences if it happens.

The six-month yardstick

Six months is long enough to plan a serious migration and short enough not to sound paranoid. It corresponds to the typical procurement and design phase of an enterprise IGA replacement, and sits within the range of migration windows observed across enterprise IAM transitions in Intragen's consultancy practice.

DORA Article 28(8) does not prescribe a duration for exit plans; six months is offered here as a working heuristic that regulated buyers can pressure-test against their own programme experience.

The five concrete checks

Q2 breaks into five operational checks:

1. Source-code or escrow access for the deployed version.
2. Certification cover for the migration window.
3. An engineer labour market outside the vendor's direct support.
4. Data-structure portability into alternative products.
5. Identity-directory survival when the vendor's runtime is unavailable.

Each check can be answered with the vendor under contract today. Each can be answered differently for two products from the same vendor on different substrates.



7. Q3, Substrate control

Substrate control breaks into four sub-properties. A Q3 audit assesses each in turn.

Sub-property	What the audit asks
Hosting locus	Where does the workload physically run? Customer-owned infrastructure is the least exposed; non-European hyperscaler region is the most exposed.
Contracting entity	Which legal entity signs the contract, and where is it registered? The contracting entity is the channel through which procurement, escalation, and dispute-resolution rights flow.
Key and identity custody	Where do the workload's secrets, credentials, and identity store live, and who can be compelled to disclose them? Physical location alone does not answer that.
Operational dependencies	What does the workload touch at runtime that the customer does not control? Telemetry endpoints, update channels, support tooling, third-party services, and licence-validation endpoints.

Two classes of operational dependency expose the workload over different timescales:

- Runtime-revocable dependencies. Vendor-operated cloud connectors, SaaS authentication tenants, telemetry endpoints that fail closed, and licence-validation endpoints that call home at start-up. The vendor can sever the dependency at its discretion. The workload stops at the moment of severance.

- Bounded refresh-cycle dependencies. Server hardware, operating system, middleware under perpetual licence, and firmware. A sanctioned hardware vendor cannot reach into the customer's data centre and stop a running asset. The customer loses future purchases, support, and the next refresh. The continuity tail is measured in years.

The Q2 six-month yardstick is far inside the refresh-cycle horizon and far outside the severance horizon for runtime-revocable dependencies. Q3 weighs them in proportion. ISO 27001 and SOC 2 are useful inputs but do not, on their own, answer any of the four sub-properties, because their scope is set by the assessed entity rather than by the buyer.

A sanctioned hardware vendor cannot reach into the customer's data centre and stop a running asset. The customer loses future purchases, support, and the next refresh. The continuity tail is measured in years.

8. Case study: One Identity Manager, on-premise

The case study tests one configuration of one product: One Identity Manager, deployed on customer-owned, on-premise infrastructure. This is the configuration the paper was commissioned to examine; the framework applies to any other deployment by running the same three questions.

Q1, Classify

The workload is enterprise IGA: joiner-mover-leaver lifecycle, provisioning, deprovisioning, roles, entitlements, certifications, SoD, and audit reporting. Real-time sensitivity is low. Queued provisioning, paused certification campaigns, and manual approval workarounds are feasible without material business impact.

Q2, Continuity

The on-premise deployment runs on customer-owned infrastructure. The vendor-controlled surface concentrates in software updates, technical support, and certification renewals. Under a six-month lockout, the deployed version continues to run from existing licensed binaries; updates pause; certifications already in place continue to apply, and renewals are deferrable. An independent partner network operates this product across Europe without direct vendor involvement on routine maintenance. Data is extractable in standard relational formats.

Connector mix is decisive. The core update and licence-validation channels can be operated in air-gapped configurations. Starling Connect, however, is a vendor-operated cloud connector platform. Any customer relying on Starling Connect for a target system has a runtime dependency on One Identity's cloud, and that dependency breaks operational continuity under a vendor-lockout scenario. Native and on-premise connectors preserve the verdict. Starling Connect reliance does not.

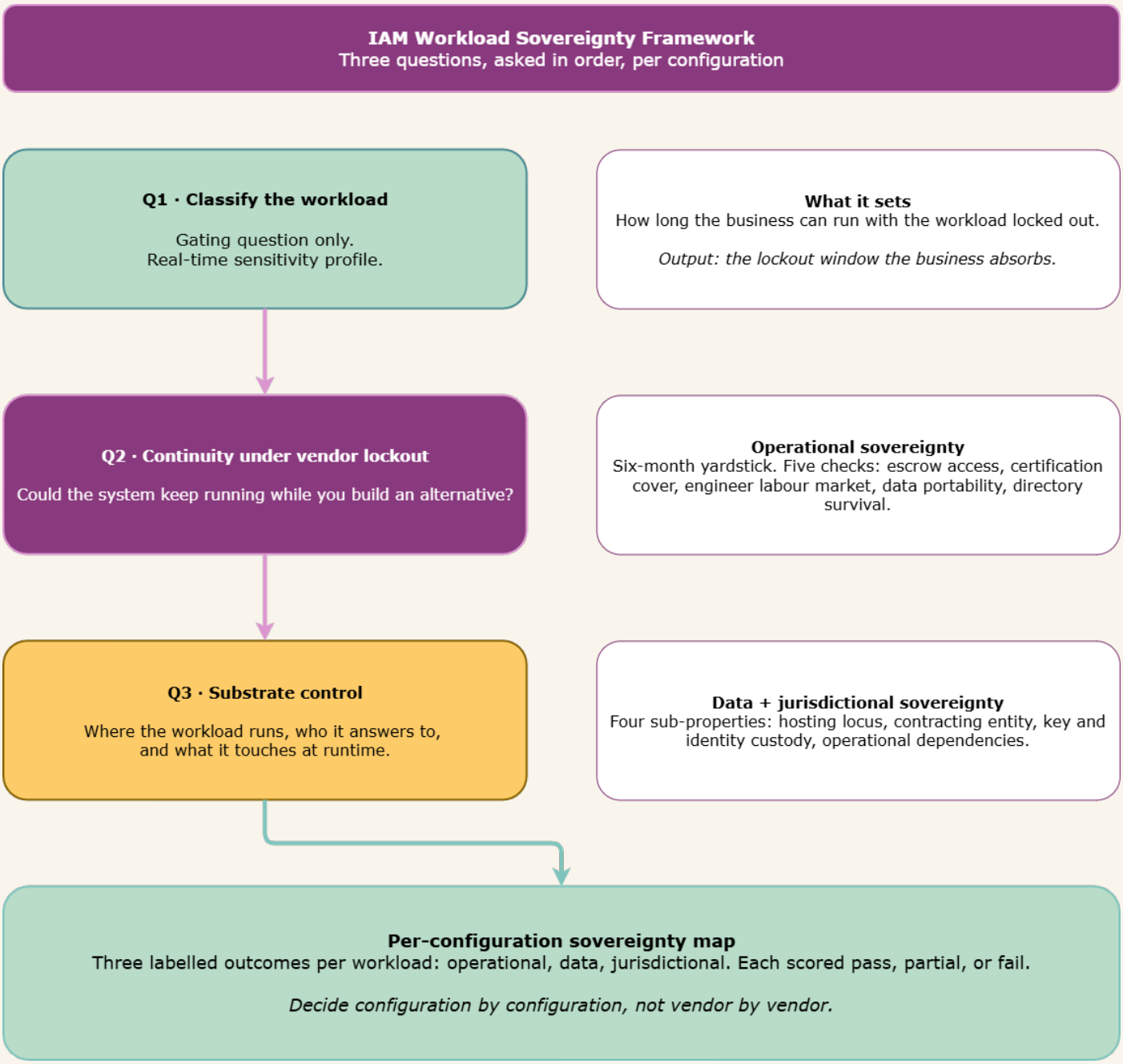
Q3, Substrate

The customer chooses the substrate. Identity store contents, role definitions, entitlement assignments, and audit logs all reside on customer infrastructure. Keys and credentials sit in customer-controlled key management. Identity data does not transit vendor infrastructure at runtime. On-premise deployment removes hosting-locus exposure at the application tier. Lower-tier substrate elements (operating system, hypervisor, and firmware) remain subject to their own export-control posture and are addressed at the customer's substrate-procurement layer, not by the IAM product choice. A contracting posture that minimises jurisdictional exposure looks like a European subsidiary as contracting entity, EU governing law, and an EU dispute-resolution forum.

Native and on-premise connectors preserve the verdict. Starling Connect reliance does not.

Case study verdict

Dimension	Result	Condition
Q1, Classify (gating)	Pass	Workload is enterprise IGA.
Q2, Operational sovereignty	Pass at six-month yardstick	Configuration-level audit required; broken by Starling Connect reliance.
Q3, Data sovereignty	Pass	Customer-owned substrate; customer-controlled keys.
Q3, Jurisdictional sovereignty	Pass at application tier	Contracting jurisdiction is a procurement negotiation between buyer and vendor.



9. How to apply this to your stack

1. Inventory the IAM workloads by class: AM, SSO, MFA, PAM, CIAM, IGA, identity directory services, audit, and analytics.
2. Run Q1 as a gating step. Determine the real-time sensitivity profile and the lockout window the business can absorb without material harm.
3. Run Q2 for operational sovereignty. Model the vendor-lockout scenario. Apply the six-month yardstick. Record the gaps that would need contingency planning.
4. Run Q3 for data and jurisdictional sovereignty. Audit the four sub-properties. Record substrate decisions and contracting decisions separately. Map the Q3 outputs onto the national substrate-control regime that applies in your jurisdiction (BSI C5, SecNumCloud, BIO, ENS, ACN, or others).
5. Record three labelled outcomes per workload (pass, partial, fail): operational sovereignty, data sovereignty, and jurisdictional sovereignty. The labelled format makes the result legible to procurement, architecture, legal, and audit functions in their own vocabularies.
6. Decide configuration by configuration, not vendor by vendor. The same vendor can pass the framework in one configuration and fail it in another. The decision-making unit is the configuration.

10. Closing

The right question is not can we trust US vendors. It is *which IAM workloads can absorb a lockout, and which configurations of which deployments are sovereign in the senses that matter: operational, data, and jurisdictional.*

Sovereignty in IAM is a measurable property of a configuration. The first step is an inventory of workload classes against the three dimensions. Intragen runs this assessment as a packaged engagement; buyers preferring to do it in-house have everything they need in this paper.



Where is your IAM stack sovereign, and where is it exposed?

You have the framework. The next step is to run it against your own workloads.

Run it with us: Intragen delivers this as a packaged engagement. We inventory your IAM workloads by class, run Q1, Q2, and Q3 against each one, and hand back a per-configuration sovereignty map that procurement, architecture, legal, and audit can all read in their own vocabulary.

Run it yourself: Everything you need is in this paper. Start with an inventory of workload classes, then score each against the three dimensions.

What you walk away with: A labelled outcome (pass, partial, fail) for operational, data, and jurisdictional sovereignty, per workload. A clear view of which configurations to keep, which to harden, and which to plan an exit from.

Which of your IAM workloads could absorb a vendor lockout tomorrow?

DISCLAIMER: This paper is a thought leadership framework, not legal or regulatory advice. It sets out a structured way to reason about sovereignty in IAM deployments. It does not interpret NIS2, DORA, or any national regime on your behalf, and it does not replace guidance from qualified legal, compliance, or regulatory advisors. Obligations vary by sector, jurisdiction, and circumstance. Validate any decision against your own advisors and your competent authority before acting on it.