emma

FOR CIOS · CTOS · HEADS OF CLOUD

EXECUTIVE GUIDE

Building the Business Case for Sovereign Cloud

A Decision Framework for CIOs. An executive guide for CTOs, CIOs, and VPs/Heads of Cloud navigating exit capability, concentration risk, audit readiness, and operational continuity across a complex cloud estate.

March 2026

CONTENTS

What This Guide Covers

The Sovereign Cloud Question Is Coming — Here's How to Frame It

> At some point in the next two quarters — likely sooner — someone in your leadership chain will ask about sovereign cloud. It might be your CISO, citing DORA's third-party risk requirements. It might be your General Counsel, flagging the EU Data Act's new switching provisions. It might be a board member who read about the European Commission's sovereign cloud procurement framework and wants to know what it means for your infrastructure.

The question, however it arrives, will sound simple: Should we move to a sovereign cloud?

The answer is not simple. And the instinct to frame it as a binary choice — stay with a hyperscaler for capability, or switch to a European provider for compliance — guarantees a suboptimal outcome. That framing presents sovereignty as a trade-off against innovation, forces a technology migration conversation when what's actually needed is a risk governance decision, and creates internal alignment problems because different stakeholders hear different versions of the same question.

In practice, most organisations do not face a binary choice between hyperscalers and sovereign providers. The real decision is whether their architecture can meet regulatory expectations for exit capability, concentration risk management, and operational resilience.

WHAT THIS GUIDE PROVIDES

A structured framework for evaluating sovereign, semi-sovereign, and regular public cloud options

This guide assesses the four dimensions that risk-oriented decision-makers actually need to evaluate. It includes a fillable decision matrix designed for internal use — in vendor evaluations, architecture reviews, and board presentations. The framework doesn't presuppose a single right answer. But it does lead to a clear conclusion about what "good" looks like architecturally for particular workloads and requirements.

Four Regulatory Developments Have Converged

> Four regulatory developments have converged to make sovereign cloud an operational decision, not just a strategic discussion point.

1. DORA entered enforcement in January 2025

The Digital Operational Resilience Act requires financial entities to manage ICT third-party risk as an integral component of their risk management framework. Article 28 requires firms to define an ICT third-party risk strategy and consider a multi-vendor approach where appropriate. Article 29 requires explicit assessment of concentration risk — evaluating the substitutability of each provider and the impact of their failure. Article 28(8) requires documented, tested exit strategies for ICT services supporting critical functions.

For any financial services company running predominantly or exclusively on a single hyperscaler, these are not future requirements. They are current supervisory expectations.

2. The EU Data Act's cloud switching provisions became applicable in September 2025

Chapter VI of the Data Act introduced mandatory switching rights for customers of cloud and data processing services. Cloud providers must now remove commercial, technical, and contractual obstacles to switching. Customers have a unilateral right to initiate switching with a maximum two-month notice period. Switching charges are being phased out entirely, with a complete ban taking effect in January 2027. Providers must support a 30-day transition period (extendable up to seven months where technically necessary).

This fundamentally changes the contractual dynamics of cloud provider relationships. Exit is no longer a theoretical option — it is a regulatory right with defined timelines and cost protections.

3. NIS2 transposition is creating supply chain security obligations across 18 sectors

NIS2's Article 21(2)(d) requires essential and important entities to evaluate the cybersecurity posture of their suppliers and service providers, including secure development procedures. This creates a direct compliance link between your cloud provider's security practices and your regulatory obligations. For organisations operating across multiple EU jurisdictions, the fragmented transposition landscape — with around 20 of 27 member states having completed national legislation — adds complexity to provider evaluation.

4. The EU Cloud and AI Development Act is signalling regulatory direction

The European Commission is expected to propose the Cloud and AI Development Act in Q1 2026. While not yet enforceable, the initiative signals clear policy direction on sovereign cloud standards, data centre capacity requirements, and procurement criteria. Organisations making multi-year cloud architecture decisions now should factor this directional signal into their planning.

KEY TAKEAWAY

The convergence of DORA, the EU Data Act, NIS2, and the forthcoming Cloud & AI Development Act makes sovereign cloud an operational decision — not a strategic discussion point

For any organisation running predominantly on a single hyperscaler, these are current supervisory expectations that require documented exit strategies, concentration risk assessments, and supply chain security evaluations.

The Four Dimensions That Matter

> Most cloud evaluations assess providers on technical capabilities, pricing, and service levels. For risk-oriented buyers — the CIOs, CISOs, and compliance leaders who need to defend cloud decisions to boards and regulators — four additional dimensions determine whether a cloud strategy is defensible.

1	2	3	4
Exit Capability	Concentration Risk	Audit Readiness	Operational Continuity

Dimension 1: Exit Capability

The question: If you needed to leave your current primary cloud provider — whether due to regulatory change, pricing pressure, service degradation, or strategic realignment — could you do it without unacceptable disruption?

Why it matters now: Exit capability has moved from a theoretical contingency to a regulatory requirement. DORA Article 28(8) requires documented exit strategies for ICT services supporting critical functions — plans that are "comprehensive, documented, and sufficiently tested and reviewed periodically." The EU Data Act now gives you the legal right to switch with two months' notice, but the right means nothing if your architecture cannot execute it.

What to assess:

- ✓ **Data portability**
  What percentage of your data can be exported in standard, portable formats? What data is stored in proprietary formats or structures that require transformation? What is the estimated volume of data requiring migration, and what are the egress costs at current provider pricing? Note: the Data Act's switching charge phase-out applies to provider-imposed switching charges, but egress fees remain a separate commercial consideration until the complete ban in January 2027.

- ✓ **Workload portability**
  What percentage of your workloads use provider-specific services (serverless functions, proprietary databases, provider-native AI/ML services) versus portable abstractions (containers, Kubernetes, standard APIs)? For each provider-specific service, what is the estimated refactoring effort to achieve portability?

- ✓ **Identity and access portability**
  Is your identity and access management federated through your own identity provider, or does it depend on the cloud provider's IAM as the root of trust? Can you replicate your access control model on an alternative provider?

- ✓ **Operational knowledge portability**
  How much of your team's operational expertise is tied to a specific provider's tooling, console, and operational patterns? What is the retraining cost and timeline to operate effectively on an alternative?

- ✓ **Contractual position**
  What are your current notice periods, termination rights, and any remaining contractual lock-in mechanisms? Have you reviewed these against the Data Act's mandatory provisions?

Exit Capability Scoring Guidance

SCORE	DESCRIPTION
1 — Critical exposure	>70% of workloads use provider-specific services; no tested migration path; data in proprietary formats; single-provider IAM dependency

Dimension 2: Concentration Risk

The question: What is the impact on your operations, compliance posture, and business continuity if your primary cloud provider experiences a sustained outage, a regulatory posture change, or a material pricing increase?

Why it matters now: DORA Article 29 requires financial entities to identify and assess concentration risk as part of their ICT risk management framework, specifically evaluating whether contractual arrangements create or increase dependency on a single provider. Beyond DORA's explicit requirements, concentration risk is increasingly recognised as a governance issue — equivalent to supply chain concentration, key-person dependency, or financial counterparty exposure. Boards that understand those risk categories can understand cloud concentration risk, if it's framed correctly.

What to assess:

- ☑ **Workload concentration**
  What percentage of your production workloads, by both count and criticality, run on a single provider? What percentage of your revenue-generating services depend on a single provider's infrastructure?

- ☑ **Service dependency depth**
  Beyond compute and storage, how many higher-level services (managed databases, identity services, monitoring, logging, networking, secrets management, CI/CD) depend on a single provider? Each dependency layer deepens the concentration.

- ☑ **Geographic concentration**
  Are your workloads distributed across multiple regions, or concentrated in one or two regions of a single provider? For data residency obligations, does all your EU data processing depend on one provider's EU regions?

- ☑ **Commercial concentration**
  What percentage of your total cloud spend goes to a single provider? At what point would a pricing increase from that provider materially affect your operating budget?

- ☑ **Substitutability assessment (DORA-specific)**
  For the ICT services your primary provider delivers — particularly those supporting critical or important functions — are alternative providers available? What is the switching timeline? What capabilities would you lose during transition?

Concentration Risk Scoring Guidance

SCORE	DESCRIPTION
1 — Critical exposure	>85% of production workloads on single provider; no alternative provider relationship established; single-region deployment; >80% of cloud spend with one vendor
2 — High risk	70–85% single-provider; alternative provider evaluated but not operational; limited geographic distribution; 65–80% spend concentration
3 — Moderate	50–70% single-provider; secondary provider operational for non-critical workloads; multi-region within primary provider; 50–65% spend concentration
4 — Good	30–50% single-provider; secondary provider operational for some critical workloads; multi-provider geographic distribution; 35–50% spend concentration
5 — Strong	Workloads distributed across providers by policy; no single provider >50% of critical workloads; multi-provider, multi-region; documented concentration risk assessment per DORA Art. 29

Dimension 3: Audit Readiness

The question: Can your current cloud infrastructure generate the compliance evidence your auditors, regulators, and internal risk functions actually require — not retrospectively, but continuously?

Why it matters now: The compliance evidence bar has risen materially. DORA requires financial entities to provide "complete and updated information on ICT risk and on their ICT risk management framework to the competent authorities upon their request" (Article 6(3)). The register of information on ICT service providers must be available for supervisory review. NIS2's Article 21(2)(f) requires "policies and procedures to assess the effectiveness of cybersecurity risk-management measures" — not just controls, but proof that controls work. GDPR's Article 32(1)(d) requires "a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures."

Across all three frameworks, the requirement is the same: demonstrate, don't just describe. An auditor asking "where is your data processed?" needs a verifiable answer from your infrastructure, not a reference to a contract.

What to Assess for Audit Readiness

Data residency evidence

Can you demonstrate, from operational data rather than contractual documentation, exactly where your workloads and data are deployed — by country, by region, by data centre? Can you prove that data residency policies are enforced at deployment time, not just documented?

Policy enforcement evidence

Do your governance controls generate evidence that policies are being actively enforced — that non-compliant deployments are blocked, that access controls match documented policies, that encryption is applied where required? Or does compliance evidence require manual assembly after the fact?

Third-party risk documentation

Can you produce a current view of all your cloud provider relationships, their service scope, deployment locations, and sub-processor chains? Does this documentation update automatically as your infrastructure changes, or does it require manual maintenance?

Incident and change audit trail

Do your cloud environments produce tamper-evident logs of all significant events — deployments, configuration changes, access events, incidents — that span all providers in a single, reviewable format?

Assessment cadence

How frequently do you assess the effectiveness of your technical controls? Is this assessment continuous, periodic (annual/quarterly), or reactive (only when triggered by an audit)?

Audit Readiness Scoring Guidance

SCORE	DESCRIPTION
1 — Critical exposure	Compliance evidence is assembled manually for each audit; no continuous monitoring; data residency relies on contract language, not infrastructure verification; no cross-provider audit trail
2 — High risk	Some automated evidence collection per provider, but siloed; cross-provider view requires manual correlation; data residency checked periodically, not enforced at deployment
3 — Moderate	Monitoring operational across environments; data residency enforced for some workloads; audit trail exists per provider but not unified; effectiveness assessments conducted annually
4 — Good	Unified monitoring across providers; data residency enforced by policy at deployment; cross-provider audit trail; effectiveness assessed quarterly; evidence can be produced for regulatory requests within days
5 — Strong	Continuous governance generating audit-ready evidence from live infrastructure; data residency provable

Dimension 4: Operational Continuity

The question: If your primary cloud provider's regulatory posture, service availability, pricing model, or regional presence changes materially, can your operations continue without unacceptable disruption?

Why it matters now: This dimension extends beyond traditional disaster recovery to encompass scenarios that are increasingly plausible in the current geopolitical and regulatory environment. The convergence of DORA, NIS2, and evolving EU sovereignty requirements means that a provider's compliance posture can change in ways that affect your own compliance. Regulatory decisions in non-EU jurisdictions — such as the US CLOUD Act's extraterritorial data access provisions — can create compliance risk for EU data processed through US-headquartered providers, even when data is stored in the EU. Provider pricing decisions can materially affect operating budgets, and single-provider dependency means no competitive leverage to negotiate.

What to assess:

- ✓ **Multi-provider operational capability**

  Can your team actually operate across multiple providers today, or is multi-cloud a strategic intent rather than an operational reality? Are deployment, monitoring, and governance processes provider-agnostic, or do they require provider-specific tooling and expertise?

- ✓ **Failover capability**

  For your critical workloads, can you fail over to an alternative provider (or to on-premises infrastructure) with defined recovery time and recovery point objectives? Has this been tested?

- ✓ **Regulatory scenario planning**

  Have you evaluated the impact on your operations if: (a) a key provider's regulatory posture changes (e.g., loss of an adequacy decision affecting data transfers); (b) new sovereignty requirements restrict use of non-EU-headquartered providers for certain workloads; (c) your primary provider exits a region or changes service availability?

- ✓ **Commercial resilience**

  If your primary provider increases pricing by 20–30%, what is your response? Can you redistribute workloads to alternative providers, or are you structurally locked into the pricing relationship?

- ✓ **Team capability**

  Does your engineering and operations team have the skills, tooling, and documented procedures to operate across multiple providers, or is operational knowledge concentrated on a single platform?

Operational Continuity Scoring Guidance

SCORE	DESCRIPTION
1 — Critical exposure	Single-provider operations; no failover capability; no regulatory scenario planning; team skills concentrated on one platform; commercially locked in via long-term commitments
2 — High risk	Secondary provider identified but not operational; failover untested; some awareness of regulatory scenarios but no formal assessment; team skills mostly single-provider
3 — Moderate	Secondary provider operational for some workloads; failover tested for non-critical systems; regulatory scenarios documented; some team cross-training; commercial terms allow flexibility
4 — Good	Multi-provider operations for critical and non-critical workloads; failover tested for critical systems; regulatory scenarios assessed and response plans documented; team competent across providers
5 — Strong	Full multi-provider operational capability; failover tested periodically for critical workloads with defined RTO/RPO; regulatory scenarios assessed and integrated into architecture planning; team operates provider-agnostically; commercial leverage maintained through genuine multi-provider distribution

The Decision Matrix

> Use this matrix in a working session with your cloud, compliance, and finance leads. Score each dimension 1–5 using the guidance above, then apply your own weighting based on which dimensions matter most to your organisation and regulatory context.

Recommended weighting for financial services (DORA-regulated):

DIMENSION	SUGGESTED WEIGHT	YOUR WEIGHT	YOUR SCORE (1–5)	WEIGHTED SCORE
Exit Capability	25%	___%	___	___
Concentration Risk	30%	___%	___	___
Audit Readiness	25%	___%	___	___
Operational Continuity	20%	___%	___	___
Total	**100%**	**100%**		**___**

Recommended weighting for NIS2-regulated entities (non-financial):

DIMENSION	SUGGESTED WEIGHT	YOUR WEIGHT	YOUR SCORE (1–5)	WEIGHTED SCORE
Exit Capability	20%	___%	___	___
Concentration Risk	25%	___%	___	___
Audit Readiness	30%	___%	___	___
Operational Continuity	25%	___%	___	___
Total	**100%**	**100%**		**___**

What Your Weighted Total Means

WEIGHTED TOTAL	ASSESSMENT	RECOMMENDED ACTION
4.0–5.0	**Strong position**	Maintain and document. Ensure periodic review of exit strategies and concentration risk. Your current posture supports regulatory defensibility.
3.0–3.9	**Adequate with gaps**	Address specific weaknesses identified in lowest-scoring dimensions. Prioritise dimensions with regulatory deadlines attached (exit strategies for DORA, audit readiness for upcoming supervisory reviews).
2.0–2.9	**Material risk exposure**	Structured remediation required. Current posture creates regulatory exposure and operational fragility. Develop a 6–12 month roadmap addressing the two lowest-scoring dimensions first.
1.0–1.9	**Critical exposure**	Immediate attention required. Single-provider dependency with inadequate exit capability and compliance evidence creates compounding risk. Escalate to board level with a remediation plan and timeline.

What the Framework Reveals

Organisations that score themselves honestly against these four dimensions almost always arrive at the same conclusion: the risk is not in any single dimension but in the correlation between them. Low exit capability combined with high concentration risk means that the scenarios where you most need to move are the scenarios where you least can. Low audit readiness combined with tightening regulatory requirements means that compliance gaps are discovered at the worst possible time.

The architectural response to this correlated risk is not a wholesale provider migration. It is a distributed, policy-governed operating model that:

> Reduces concentration by distributing workloads across multiple providers — hyperscaler and sovereign — based on regulatory requirements, data sensitivity, and operational criticality

> Builds exit capability by operating across providers continuously, so that migration is a tested, repeatable operation rather than an emergency procedure

> Generates audit evidence from the infrastructure itself, through policy enforcement at deployment time and continuous governance of running workloads

> Ensures continuity by making multi-provider operations the default, not the contingency

This is the model that emma's platform is designed to support. Not as a replacement for your existing cloud providers, but as the governance and orchestration layer that lets you use multiple providers — including hyperscalers, EU-sovereign providers, and on-premises infrastructure — under a single operational model with unified visibility, policy enforcement, and compliance evidence.

Cloud Infrastructure Risk Assessment: Summary for the Board

This page is designed to be extracted and included directly in a board pack.

Context

European regulation now requires organisations to demonstrate that their cloud infrastructure meets specific standards for operational resilience, data sovereignty, and third-party risk management. The Digital Operational Resilience Act (DORA), enforceable since January 2025, requires financial entities to maintain multi-vendor ICT strategies, assess concentration risk, and have tested exit strategies. The NIS2 Directive requires supply chain security assessments for all cloud providers. The GDPR continues to intensify enforcement of data residency and international transfer controls.

Current Risk Assessment

We have assessed our cloud infrastructure against four dimensions: exit capability (can we leave a provider without disruption), concentration risk (what is the impact of single-provider dependency), audit readiness (can we prove compliance from operational data), and operational continuity (can we maintain operations if a provider's posture changes).

Our weighted score is: ___/5.0

Key findings:

1. [Insert 2–3 specific findings from your scoring, e.g., "78% of production workloads on a single provider, creating concentration risk that exceeds our risk tolerance under DORA Article 29"]
2. [Insert finding, e.g., "Exit strategy for primary provider is documented but has not been tested; DORA Article 28(8) requires periodic testing"]
3. [Insert finding, e.g., "Data residency is contractually specified but not enforced at infrastructure level; evidence of actual deployment locations requires manual verification"]

Recommended Approach

Rather than migrating away from our current providers, we recommend adopting a distributed cloud operating model that:

> Reduces concentration risk by distributing workloads across multiple providers, including EU-sovereign infrastructure, based on data sensitivity and regulatory requirements

> Builds tested exit capability by operating across providers continuously, making migration a routine operation rather than a crisis response

> Automates compliance evidence through policy-governed deployment and continuous governance, producing audit-ready proof from operational systems

> Preserves innovation capability by maintaining access to hyperscaler services for workloads that benefit from them, while placing sovereignty-sensitive workloads on appropriate infrastructure

Investment Required

[Insert estimated investment range and timeline]

Risk of Inaction

2%
DORA fines up to 2% of annual worldwide turnover

€10M
NIS2 fines up to €10M or 2% of turnover

€20M
GDPR fines up to €20M or 4% of turnover

Management body liability: both DORA (Article 5) and NIS2 (Article 20) hold management bodies personally accountable for compliance oversight.

Operational fragility: single-provider dependency without tested exit capability creates unmitigated business continuity risk.

Recommended Timeline

QUARTER	ACTION
Q1	Complete four-dimension assessment; document concentration risk per DORA Art. 29; review exit strategy documentation
Q2	Evaluate multi-cloud governance platforms; select secondary provider for pilot workloads; update contractual provisions per Data Act requirements
Q3	Deploy pilot workloads on secondary provider; test failover for critical systems; establish unified monitoring and governance
Q4	Expand multi-provider operations; validate audit readiness with internal compliance review; update board on risk posture improvement

Guidance for Each Audience

For CIOs building board presentations

Use the four-dimension framework to structure your risk assessment. Extract the board-ready summary page and adapt it with your specific scores and findings. The framework translates cloud architecture risk into the same language your board uses for supply chain, financial, and operational risk.

For VPs/Heads of Cloud structuring vendor evaluations

Use the scoring criteria to evaluate current and potential providers against regulatory requirements. The specificity of the scoring guidance — mapped to DORA articles, Data Act provisions, and NIS2 requirements — gives vendor evaluation a compliance-grounded structure rather than a pure feature comparison.

For procurement teams scoring providers

The four dimensions provide weighted scoring criteria that go beyond technical capability and pricing. They assess whether a provider relationship is defensible under the regulatory frameworks that apply to your organisation — a critical but often missing component of procurement evaluation.

For compliance teams preparing for audits

The self-assessment scoring within each dimension identifies the specific gaps that auditors are most likely to probe. A low score in audit readiness, for example, points to the specific evidence gaps (data residency verification, policy enforcement proof, cross-provider audit trails) that will require attention before your next supervisory review.

emma

About emma

The cloud operations platform for distributed sovereign infrastructure

emma is built for organisations running distributed workloads across hybrid and multi-cloud environments — where operational complexity, unpredictable costs, and strict regulations get in the way of building.

It provides a single, policy-driven operating layer that spans hyperscalers, regional European cloud providers, AI-optimized infrastructure, and on-premises environments. From one dashboard, engineering, platform, and finance teams can deploy workloads, enforce compliance policies, and view and govern their entire infrastructure footprint. Sovereignty and compliance are built in through proactive guardrails, not bolted on.

With a vendor-neutral architecture, emma ensures organisations can choose the right infrastructure for cost, performance, and regulatory requirements — without lock-in or operational trade-offs.

Data Residency & Jurisdictional Control

Data stays within defined geographic and legal boundaries, which are enforced at the infrastructure layer across every environment rather than relying on policy documents.

Policy-Driven Workload Placement

Provider eligibility and sovereign constraints are maintained as infrastructure guardrails at deployment time, ensuring workloads run only in approved environments across providers.

Network Boundary Control

Cross-cloud data moves over emma's private networking backbone instead of the public internet. This reduces cross-border public routing exposure within and between jurisdictions.

Continuous Governance & Compliance Evidence

Workloads are continuously evaluated against policies that align with GDPR, NIS2 and DORA. Audit-ready logs mean compliance evidence is generated automatically.

Provider Portability & Exit Readiness

Tested migration paths across providers reduce concentration risk and meet regulatory exit capability requirements before they become urgent.

Encryption & Key Sovereignty

Encryption and key management policies are also enforced at deployment time. Organisations retain control over who holds the keys, regardless of where workloads run.

2021	15+	~90	NO
Founded & HQ in Luxembourg	Cloud providers supported	Cloud engineers at your service	US Cloud Act applicability

CERTIFICATIONS & FRAMEWORKS

emma operates under internationally recognized security and compliance frameworks, including ISO-certified security management and SOC 2 Type II audited controls, with data protection aligned to GDPR and resilience aligned with NIS2 and DORA.

emma

FOR EXECUTIVE LEADERS

See the Platform Built for Distributed Cloud

emma gives CIOs and CTOs a unified operational view across every cloud provider — with governance, compliance, and cost controls built in. Let us show you what that looks like for your organization.

Schedule an Executive Briefing →

Make Cloud Work for You

emma Technologies S.à r.l. · 19-21, route d'Arlon · 8009 Strassen · Luxembourg

emma.ms