cpl.thalesgroup.com

THALES
CYBERSECURITY

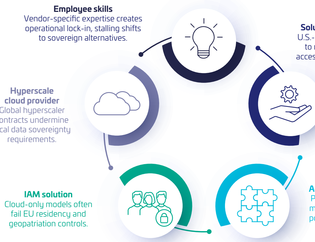
Derisking IAM for Digital Sovereignty

Map risks, explore options, and build resilience with Thales

Your IAM stack's cloud reliance is quietly eroding your autonomy and creating operational dependency - wake up before it's too late. With growing global tensions, derisking empowers you to pivot without panic. This straightforward infographic shows exactly how, step by step.

Step 1
Determine your IAM infrastructure cloud dependency

EU rules like the Data Act are ramping up pressure, and **72%** of EMEA firms already show sovereignty gaps from U.S. cloud lock-in. Don't wait - check your IAM infrastructure across these five critical spots to reveal exactly where you're exposed:



But control and compliance are only part of the risk - if your identity provider becomes unavailable, users cannot authenticate and access breaks down across systems that rely on IAM. Mapping these dependencies is the first step to identifying where fallback options or alternative approaches may be required to maintain business continuity.

Step 2
Evaluate potential alternatives

You spotted the risks - now for each critical spot, ask these questions to uncover viable alternatives. These targeted questions help you dig deeper and see what's feasible right away, turning your assessment into an action plan that reduces dependency risk and improves resilience.

Employee skills
What cross vendor training is currently in place?
Have you adopted open IAM standards like OIDC/SCIM?
Are partner/vendor trainings leveraged for multi-tool skills?

Solution partner or MSP
Do you have a local partner for sovereignty support?
Can internal skills reduce MSP dependency?

Adjacent integrations
Are integrations modern/standards-based (SAML, OIDC, etc)?
Do they allow easy vendor swaps without rework?

IAM solution
Is on-premises deployment realistic? Does a hybrid approach to IAM fit your workflow? Can you deploy a sovereign cloud?
Is geopatriation an option for data control? What is the fallback if the IAM provider becomes unavailable?

Hyperscale cloud provider
Would a sovereign cloud reduce residency risks? Is it possible to use the same provider with a different contracting entity?
Can failover occur across regions or between providers?

Step 3
Plan scenarios based on the EU Cloud Sovereignty Framework

Leverage the EU Cloud Sovereignty Framework as guiding principles for scenario planning - including scenarios where your IAM provider becomes unavailable. It's a solid starting point for auditable, measurable requirements. This framework rates cloud setups across pillars like data control and supply chains, helping you match goals to real-world options. Here's how it works:

1. Rate your IAM scenario/provider against each of the sovereignty objectives. Use evidence like contracts or architecture docs.
2. Pick a target level for each objective based on risk tolerance.
3. Answer the framework's questions per objective found here. Score responses 0-4 reflecting the Sovereignty Effective Assurance Level (SEAL) criteria.
4. Calculate your sovereignty score using the equation. Higher score = stronger sovereignty.

But control and compliance are only part of the risk - if your identity provider becomes unavailable, users cannot authenticate and access breaks down across systems that rely on IAM. Mapping these dependencies is the first step to identifying where fallback options or alternative approaches may be required to maintain business continuity.

What is the EU Cloud Sovereignty Framework?

The EU Cloud Sovereignty Framework is an official European Commission guideline that helps organizations evaluate cloud providers for independence from foreign influence. It defines eight sovereignty pillars and five SEAL assurance levels, letting you score setups for compliance with EU rules like the Data Act - essentially a rubric to ensure your IAM stays under your control, no compromises.

Download Framework

About Thales

As a global leader in cybersecurity, Thales safeguards sensitive data, identities, applications, and software for the most trusted brands in the world. Through advanced encryption, identity access management, application security, and software entitlement, Thales secures cloud environments, defends against cyber threats, ensures compliance, and enables trusted digital experiences.