

— E-BOOK · THE COMPLETE GUIDE

The Sovereignty Handbook.

What data sovereignty actually requires — beyond choosing a region. The layers, the leaks, the evidence, and the frameworks for proving control of your data, your operations, and your jurisdiction.

12 chapters · 3 frameworks · 1 boundary

CONTENTS

What this handbook covers

This guide is written for the people who have to answer for an estate: CIOs, CISOs, compliance leads, and the architects who will implement whatever they commit to. It assumes you already know you need sovereignty. The question it answers is what that actually requires.

01	Why a cloud region is not sovereignty	03	02	The five layers of sovereignty	04
	The difference between location and control			Data, legal, operational, technology, digital	
03	Where residency quietly breaks	05	04	Framework 1 — the artefact test	06
	Backups, logs, admins, keys, and recovery			One rule applied to everything that carries data	
05	Privileged access is the real perimeter	07	06	Key custody decides who can read	08
	Who can log in, from where, under what approval			Separating administration from decryption	
07	Evidence, not assurance	09	08	Framework 2 — the sovereignty maturity model	10
	Turning controls into inspectable records			Five levels from located to provable	
09	Sovereign AI	11	10	Resilience without breaching the boundary	12
	Prompts, embeddings, weights, and bounded agents			Where DR most often undoes sovereignty	
11	Framework 3 — the buyer's evidence checklist	13	12	Choosing an edition, and getting started	14
	Twelve questions that separate claims from controls			Core, multi-cloud, AI-optimized, and HPC	

THREE FRAMEWORKS YOU CAN REUSE

- **The artefact test** — a single rule applied to every object that carries your data.
- **The sovereignty maturity model** — five levels, each defined by what it still cannot prove.
- **The buyer's evidence checklist** — twelve questions that separate claims from controls.

01 CHAPTER ONE

Why a cloud region is not sovereignty

Almost every sovereignty conversation begins in the same place: a provider offers a region in the required country, a box is ticked, and the programme moves on. The audit arrives later and asks a different set of questions.

A region answers one question — where the primary data physically sits. Sovereignty is a compound of at least five, and the other four are rarely settled by geography. Which legal jurisdiction applies to the data and, separately, to the company operating the infrastructure? Who administers the environment, and from which country do they connect? Who holds the encryption keys? And can any of it be demonstrated to a third party who is not inclined to take your word for it?

A region tells you where the data sits. Sovereignty tells you who can reach it, under whose law, and whether you can prove either.

The jurisdiction problem

The subtlety that catches most organisations is that infrastructure location and corporate jurisdiction are independent variables. A data centre inside your borders, operated by a company incorporated elsewhere, may still expose the data it holds to that company's home legal regime. This is not a hypothetical concern for regulated buyers; it is the specific issue that frameworks like GDPR, DORA, NIS2, and national schemes such as BSI C5 and KRITIS were written to address.

Why "secure by design" stopped being enough

Encryption at rest, network isolation, and a strong compliance certification were once sufficient answers. They are no longer, because the questions moved. Regulators and enterprise customers now ask about privileged administrator access, support personnel, key management, data movement, infrastructure ownership, audit logs, operational process, and supply chain. Those are questions about how the environment is run, not how it was built — and a certification describing the latter cannot answer the former.

WHAT THIS CHAPTER MEANS IN PRACTICE

- Treat **location and jurisdiction** as separate questions with separate answers.
- Assume every sovereignty claim will eventually need **evidence**, not assurance.
- The operating model matters as much as the architecture.

02 CHAPTER TWO

The five layers of sovereignty

Sovereignty is not binary. It is layered, and organisations routinely achieve the first layer while assuming they have achieved all five.

Five layers of sovereignty

Data	Where data, backups, logs, metadata, and derived artefacts physically reside
Legal	Which jurisdiction's law applies to the data and to the operator of the infrastructure
Operational	Who may administer the environment, from where, and under whose approval
Technology	Who controls infrastructure, keys, workloads, and the exit path
Digital	Whether critical services remain governable and resilient under your own control

FIGURE 1 — SOVEREIGNTY IS LAYERED, NOT BINARY

Why the layers have to be assessed separately

Each layer can be satisfied or breached independently, and a failure at any one of them undermines the others. Data can sit in-country while the operator is subject to foreign law. The operator can be domestic while administration is performed from abroad. Administration can be local while the provider holds the keys. And every one of those can be true while the organisation still has no inspectable record proving it.

This is why sovereignty programmes that begin with an architecture diagram tend to stall. The architecture addresses the first and fourth layers. The second, third, and fifth are contractual, operational, and evidentiary — and they are usually owned by people who were not in the architecture review.

A FIVE-QUESTION SELF-ASSESSMENT

- **Data:** Can you name every location where a copy of your data, in any form, currently exists?
- **Legal:** Which jurisdiction governs the entity that operates your infrastructure, as distinct from where it sits?
- **Operational:** From which countries were privileged sessions initiated against your estate last month?
- **Technology:** Could your provider decrypt your data without your approval, technically speaking?
- **Digital:** If that provider became unavailable, could you continue to operate and exit?

03 CHAPTER THREE

Where residency quietly breaks

In practice, residency rarely fails at the front door. It fails through the secondary artefacts that follow different rules from the data that generated them.

Where residency quietly breaks

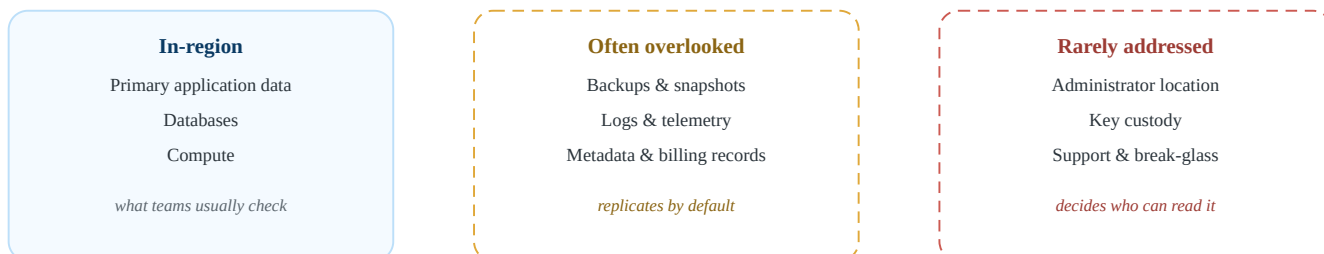


FIGURE 2 — THE THREE TIERS OF RESIDENCY EXPOSURE

The three tiers

The first tier — primary application data, databases, compute — is almost always checked, because it is what the migration plan described. The second tier is where most exposure lives: backups, snapshots, disaster-recovery copies, logs, telemetry, metadata, API activity, monitoring data, and billing records. These replicate by default, often to shared provider services in other regions, and frequently nobody has asked where they land.

The third tier is the one that determines who can actually read the data: where administrators are located, who holds the keys, and how support and emergency access work. An organisation can pass a residency audit on tiers one and two and still have a provider engineer in another jurisdiction able to decrypt a database during an incident.

Primary data is where residency is checked. Backups, logs, and key custody are where it is decided.

ARTEFACTS WORTH LOCATING EXPLICITLY

- Backups, snapshots, and **disaster-recovery copies**
- Application, security, and platform **logs**; monitoring and telemetry
- **Metadata**, API activity records, and billing or usage data
- Encryption keys, key-management services, and **escrow** arrangements
- Support tooling, jump hosts, and **break-glass** paths
- For AI workloads: prompts, embeddings, vector indexes, and **fine-tuned weights**

04 FRAMEWORK ONE

The artefact test

The most useful sovereignty framework is also the simplest. Rather than maintaining separate policies per system, apply one rule to every object that carries your data — and make the default answer "inside the boundary."

THE RULE

- If an artefact contains, describes, or is derived from regulated data, it inherits that data's residency and access rules — without exception, and regardless of which system produced it.

The power of stating it this way is that it removes case-by-case negotiation. A log containing customer identifiers is not "just telemetry." A fine-tuned model derived from patient records is not "just a model artefact." A backup is not a lesser copy. Each one inherits the obligation automatically, and the burden of proof shifts to anyone arguing for an exemption.

ARTEFACT	CONTAINS, DESCRIBES, OR DERIVES FROM DATA?	THEREFORE
Primary database	Contains	In-boundary, customer-keyed, access-controlled
Backup / snapshot / DR copy	Contains	Same rule — including during recovery
Application and security logs	Describes, often contains identifiers	In-boundary retention and monitoring
Metadata and usage records	Describes	In-boundary; frequently overlooked
Embeddings and vector indexes	Derived	In-boundary; treat as regulated data
Fine-tuned model weights	Derived	In-boundary; the most commonly missed artefact
Encryption keys	Controls access to all of the above	Customer-owned and customer-controlled

How to apply it

Run the test as an inventory exercise before selecting a platform, not after. For each artefact, record where it currently lives, who can reach it, under which jurisdiction, and what evidence exists. The gaps that surface are almost always in the same three places — recovery copies, observability data, and key custody — and they are considerably cheaper to design for than to remediate.

05 CHAPTER FIVE

Privileged access is the real perimeter

Once data is in the right country and encrypted, the remaining question is entirely about people: who can log in, from where, and with whose permission.

This is the layer where standard cloud operating models and sovereignty requirements diverge most sharply. Follow-the-sun support is a genuine operational strength — it is also, by construction, a model in which privileged sessions may originate from any jurisdiction the provider staffs. For most workloads that trade is sensible. For sovereign workloads it inverts the entire control model, because an administrator in another country with production access represents a jurisdictional exposure no amount of data residency can offset.

What a sovereign access model constrains

Who

Role-based access control, with administration restricted to authorized regional personnel rather than any available engineer.

From where

Residency-specific controls that constrain the physical location from which privileged sessions may be initiated.

Under what approval

Sensitive actions requiring customer approval, time-bound access, segregation of duties, and documented break-glass.

Break-glass is the test case

Every environment needs emergency access. The difference between a sovereign model and a conventional one is not whether break-glass exists, but whether it is pre-authorised by the provider or approved by the customer, and whether invoking it produces a record the customer holds. A break-glass path that the customer cannot see is functionally a standing exception to every other control on the page.

Residency decides where the data sits. Privileged access decides who can read it. Only one of those is visible on an architecture diagram.

06 CHAPTER SIX

Key custody decides **who can read**

Encryption is universal and therefore no longer differentiating. The question that matters is who holds the keys, and whether infrastructure administration and data decryption are the same privilege or two separate ones.

Under a provider-managed key model, the entity operating your infrastructure can, technically, decrypt your data. Contractual commitments may prohibit it, monitoring may detect it, and reputation may deter it — but the capability exists, and a regulator assessing a control environment will assess capability rather than intent. A customer-controlled key model changes the answer from "they are contractually prohibited" to "they are technically unable without your approval," which is a materially different statement to make to a supervisor.

What customer-controlled custody enables

FIVE CONSEQUENCES WORTH UNDERSTANDING

- **Separation of duties** between infrastructure administration and data access becomes structural rather than procedural.
- **Exceptional access requires your approval**, producing a decision point and a record where previously there was neither.
- **Provider exposure is bounded** — a compromise of provider credentials does not automatically expose plaintext data.
- **Lifecycle and destruction** become controllable, since revoking a key is a customer action with immediate effect.
- **Contractual and regulatory commitments** can be backed by a technical control rather than a policy statement.

The practical caveat

Customer-controlled keys move responsibility as well as control. Key loss becomes data loss, rotation becomes your operational burden, and availability of the key-management service becomes a dependency of every encrypted workload. These are manageable — they are also the reason this model should be designed deliberately rather than enabled casually, with escrow, rotation, and recovery procedures settled before the first workload depends on them.

07 CHAPTER SEVEN

Evidence, not assurance

A control that cannot be demonstrated is, for audit purposes, a control that does not exist. This is the distinction that separates a sovereign estate from a well-intentioned one.

Most cloud compliance models are assurance-based: the provider holds certifications, publishes attestations, and commits contractually, and the customer inherits confidence from that chain. It is an efficient model and it works for a large majority of workloads. It breaks down precisely where sovereignty matters, because the customer is being asked to evidence control over an environment whose operational records belong to someone else.

Assurance is someone telling you the control held. Evidence is you being able to check.

What evidentiary sovereignty requires

QUESTION AN AUDITOR ASKS	EVIDENCE THAT ANSWERS IT
Who accessed this environment, and when?	Real-time access logging retained in-boundary
Was that access authorized?	Role and policy records, with approval trail
Has any record been altered after the fact?	Tamper-evident audit trails
Was emergency access ever invoked?	Break-glass records tied to customer approval
Where did each artefact reside during this period?	Residency records covering backups, logs, metadata
Who could have decrypted the data?	Key custody model and key-use records

The operative requirement in every row is that the record sits inside the boundary and is inspectable by the customer directly — not retrievable from the provider on request. A log you must ask permission to see is an assurance mechanism wearing the clothes of an evidentiary one.

08 FRAMEWORK TWO

The sovereignty maturity model

Each level is defined not by what it has achieved but by what it still cannot prove. Most organisations can place themselves in under a minute.

1	Located	Workloads run in a region within the required country. Cannot prove: where backups, logs, and metadata actually reside.
2	Contained	Every artefact — backups, snapshots, logs, telemetry, metadata — is held to the same residency rule. Cannot prove: who administered the estate, or from where.
3	Governed	Administration restricted by role and residency, MFA enforced, break-glass documented and customer-approved. Cannot prove: that the provider could not decrypt the data.
4	Controlled	Customer-owned keys separate infrastructure administration from decryption; exceptional access requires customer approval. Cannot prove: any of it, independently, to a third party.
5	Provable	Tamper-evident audit trails, residency records, and key-use records retained in-boundary and inspectable by the customer. Cannot prove: nothing material — sovereignty is now evidenced rather than asserted.

How to use it

The levels are sequential for a reason: governing an estate whose artefacts still leave the boundary produces policy that cannot be enforced, and evidencing an estate you do not govern produces records of the wrong things. The common stall is between three and four, because key custody transfers real operational responsibility and is therefore easy to defer. It is also the level at which the claim changes from "they are not supposed to" to "they cannot" — which is the change that regulated buyers and supervisors actually respond to.

09 CHAPTER NINE

Sovereign AI

AI extends the sovereignty question in two directions at once: new artefacts that carry regulated data, and new actors that access systems autonomously.

The artefacts multiply

A conventional workload produces data, backups, and logs. An AI workload adds prompts, retrieved context, embeddings, vector indexes, and fine-tuned weights — every one of which may contain or derive from regulated data. Applying the artefact test from Chapter 4 makes the conclusion immediate: they inherit the same residency and access rules as the records that produced them. In practice this is the single most common gap in AI governance, because a model artefact does not intuitively feel like a copy of the training data.

A fine-tuned model is a derived copy of the data that trained it. Treat it as one.

The actors multiply

Autonomous agents introduce something genuinely new: a component that reasons about which systems to access and takes action without a human in the loop for each step. Sovereignty requirements therefore extend past storage into execution — an agent must operate within enforceable identity, network, and execution boundaries, and those boundaries have to be imposed by a separate deterministic layer rather than by the model's own judgement.

WHAT SOVEREIGN AI REQUIRES IN PRACTICE

- **Compute inside the perimeter** — dedicated GPU clusters so training and inference run where the data already sits.
- **Encryption in transit and during training**, with customer-controlled keys throughout.
- **Derived artefacts governed** — embeddings, indexes, and weights held to the data's residency rule.
- **Bounded agents** — enforceable identity, network, and execution limits applied outside the model.
- **Lineage documentation** — which data trained which model, approved by whom, mapped to applicable regimes such as the EU AI Act.

10 CHAPTER TEN

Resilience without breaching the boundary

Disaster recovery is where sovereignty most often fails, because DR is by definition the act of putting copies somewhere else — and resilience architectures were optimised for distance long before residency became a requirement.

The conventional instinct is sound engineering: place recovery capacity far enough away that a regional event cannot affect both sites. Applied without a residency constraint, that instinct routinely lands recovery copies in another jurisdiction, which means the organisation is sovereign during normal operation and non-compliant during precisely the incident when scrutiny is highest.

Designing for both

REQUIREMENT	CONVENTIONAL APPROACH	SOVEREIGN APPROACH
Geographic separation	Cross-region, often cross-border	Separated sites within the sovereign boundary
Backup storage	Provider-managed, possibly replicated	In-boundary, customer-keyed, immutable where required
Recovery testing	Performed in whichever region has capacity	Performed in-boundary, with records retained
Cyber recovery	Restore from most recent clean copy	Immutable vault inside the boundary
Operational continuity	Follow-the-sun failover operations	In-jurisdiction operations during failover

The requirement is not to abandon resilience for sovereignty. It is to treat the sovereign boundary as a constraint that resilience must be designed within — which is achievable in almost every jurisdiction, but only if it is stated as a requirement before the architecture is drawn rather than discovered during a recovery test.

THE QUESTION TO ASK OF ANY DR DESIGN

- During a full failover, in which jurisdiction does every copy of the data reside — and who is operating the environment at that moment?

11 FRAMEWORK THREE

The buyer's evidence checklist

Whatever platform you evaluate, these twelve questions separate a sovereignty claim from a sovereignty control. The useful signal is not whether a provider answers yes, but whether they can show you.

- | | |
|---|--|
| ☐ Where do backups, snapshots, and DR copies physically reside? | ☐ Where are logs, telemetry, and metadata stored and processed? |
| ☐ Which legal entity operates the infrastructure, and under whose law? | ☐ From which countries may privileged sessions be initiated? |
| ☐ Who holds the master encryption keys — technically, not contractually? | ☐ Can the provider decrypt data without customer approval? |
| ☐ How is break-glass access approved, and who holds the record? | ☐ Are audit trails tamper-evident and retained in-boundary? |
| ☐ Can we inspect access records without a provider request? | ☐ During failover, does every copy stay inside the boundary? |
| ☐ For AI: where do prompts, embeddings, and weights reside? | ☐ What is the exit path, and who controls it? |

How to score the answers

Group the responses into three categories. **Contractual** answers ("we commit not to") establish intent. **Architectural** answers ("the system is configured so that") establish capability. **Evidentiary** answers ("here is the record, and you hold it") establish proof. A credible sovereign platform should produce architectural or evidentiary answers to at least the questions covering key custody, administrator location, audit retention, and recovery residency. Where the answer is contractual only, treat it as a risk to be accepted explicitly rather than a control to be relied upon.

Ask to see the record, not the policy. The gap between the two is the whole subject.

12 CHAPTER TWELVE

Choosing an edition, and getting started

UPC Sovereign is delivered in four editions, each addressing a different starting point. Most organisations begin with Core and add capability as workloads migrate.

EDITION	START HERE WHEN	WHAT IT PROVIDES
Sovereign Core	Regulated workloads need a governed home in a specific jurisdiction	Fully managed private cloud at your chosen location; GDPR, DORA, NIS2, BSI C5 alignment; VMware, KVM, Hyper-V, Canonical; built-in Observability, AIOps, Agentic Orchestration
Secure Multi-Cloud Orchestration	Sovereign and non-sovereign estates must be governed together	Data sovereignty and policy enforcement across clouds; policy-as-code governance with real-time audit visibility; AI-driven placement; one control plane across public, private, and edge
AI-Optimized Sovereign	AI must run on regulated data without exporting it	Dedicated GPU clusters in-perimeter; training and inference pipelines; encryption in transit and during training; EU AI Act mapping and data lineage
HPC Sovereign	Compute-intensive or national-security workloads	Optimized infrastructure for compute-intensive work; high-throughput interconnects in-boundary; dedicated storage tiers; certified for national security and critical infrastructure

A sensible sequence

Run the artefact test first, because it determines scope and usually reveals the gaps that will drive the design. Settle key custody early, since it carries operational responsibility that needs procedures around it. Design resilience against the boundary rather than retrofitting it. And decide who will hold the evidence — the records are only useful if someone is accountable for reviewing them.

THE FIVE THINGS WORTH TAKING AWAY

- **A region is layer one of five.** Location, jurisdiction, operations, technology, and evidence are separate questions.
- **Secondary artefacts carry the exposure.** Backups, logs, metadata, and derived AI artefacts break residency quietly.
- **Privileged access is the real perimeter.** Who can log in, from where, matters as much as where data sits.
- **Key custody converts policy into capability.** "Cannot" is a stronger answer than "will not."
- **Evidence beats assurance.** If you cannot inspect the record yourself, you are relying on someone else's word.

IN CLOSING

The power of cloud, **with sovereignty built in**

Cloud made infrastructure easier to consume. For regulated and mission-critical organisations, convenience cannot come at the cost of control — and increasingly it does not have to.

Data must remain within the right jurisdiction. Administrators must be governed. Encryption keys must remain under customer control. Backups and logs must follow the same residency rules as primary data. AI workloads must operate within enforceable identity, network, and execution boundaries. And every sensitive action must be visible, auditable, and accountable. None of those requirements is exotic; what has changed is that they now have to be demonstrable rather than asserted.

BOTTOM LINE

Modernize with confidence. Operate with control. Keep your data local, and your operations accountable.

Build your sovereign cloud strategy **with UPC.**

Speak with a specialist, or ask us to run an artefact and residency assessment against your current estate.

UPC SOVEREIGN™
UNITEDLAYER.COM



EMAIL
contact@unitedlayer.com



PHONE
[+1-888-853-7733](tel:+1-888-853-7733)



X
x.com/unitedlayer



LINKEDIN
linkedin.com/company/unitedlayer