

FOUNDATION AND DECISION GUIDE · F09

Sovereign and air-gapped AI

A testable model for jurisdiction, data, keys, compute, licences, source, operations, verification, continuity, and exit.

DECISION

SCOPE

EVIDENCE

OWNERSHIP

PROOF

EXIT



A complete guide to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

F09

CONTENTS

From the first question to a defensible decision

This 38-page guide turns 14 owned topics into an explanation, evidence requirement, proof challenge, and closing decision record.

PRIMARY READERS

Sovereignty, security and infrastructure leaders

READING DEPTH

Specialist

DECISION THIS SUPPORTS

Decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

01

Read this first

03–05

Audience, reader decision, canonical boundary, terms, and guide-specific factual spotlight

02

Understand the decision and its language

06–...

A testable definition of sovereignty · Dependency map · Managed Fabric posture · Customer-owned posture · Fully disconnected posture

03

Define the mechanism, controls, and evidence

...

Data and key ownership · Models and component replaceability · Source and modification rights · No-kill-switch and continuity claims · Portable proof and independent verification

04

Prove adoption, operation, continuity, and exit

...–36

Supply-chain and update sovereignty · Exit exercise · Sovereign commercial model · Sovereignty acceptance checklist

05

Sources and next action

37–36

verification records and closing decision package

06

Subject index

37–38

An alphabetical finder for concepts, controls, products, and decisions.

TARGET LENGTH

9,000–13,000 words.. Page count varies with the number and depth of topics rather than forcing every subject into the same shell.

SOURCE DISCIPLINE

Dweve-specific facts are taken directly from the English website text audited 2026-07-20; web-navigation wording is humanised for print. Evaluation guidance is editorial, and scenarios and derived visuals are illustrative. Unsupported synthesis is replaced by canonical copy or omitted.

READ THIS FIRST • READER DECISION

Who should use this guide, and what decision it supports

public authorities, defence, critical infrastructure, regulated enterprises, sovereignty officers, and national/sector procurement teams.

Decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

The worked scenario is a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. It is illustrative and deliberately bounded. Replace it with the organisation's actual workflow, systems, data, sources, policies, roles, infrastructure, commercial conditions and consequences while preserving the evidence discipline.

The guide's concrete output is a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer. Use the chapter explanation pages to align language, the evidence pages to create acceptance records, and any challenge pages to test whether the boundary survives missing assumptions and failure. End in a named decision, not an attractive summary.

JURISDICTION**Entity + law + site**

Current guide lens; verify source and scope.

OPERATION**Local + disconnected**

Current guide lens; verify source and scope.

CONTROL**Keys + licences + source**

Current guide lens; verify source and scope.

EXIT**Export + replace + verify**

Current guide lens; verify source and scope.

PRIMARY RISK

An apparently local deployment can still depend on foreign identity, model APIs, telemetry, licence checks, update infrastructure, keys, build systems, support or closed verification. A contract can also promise continuity without an exercised package and runbook.

READ THIS FIRST • DISCIPLINE

How to read claims, evidence, responsibility, and status

The website is the only factual source for this edition. The guide adds explanation, architecture and proof requirements without inventing current product, regulatory, assurance, commercial, or customer-result facts.

Six evidence layers

A published description states a current proposition. Delivered software and documentation show what is available in a selected version. Customer configuration shows how it is used. An observed run shows one result. Independent assurance has scope, method and date. A written agreement creates commercial commitments and remedies.

Responsibility stays explicit

The relevant owners include sovereignty and programme owner, infrastructure and operations, security/keys/supply chain, data and model/source owners, legal/procurement, records/verifier, continuity, national or sector authority, and Dweve. The supplier can provide product, evidence and commitments; customer owners still decide purpose, source and policy authority, professional or domain judgement, acceptable risk, infrastructure, staffing, affected-person treatment and production reliance.

Status and strong statements

Measured claims stay tied to workload, hardware and method. Research remains research. Alignment is not certification. "Open" is verified per component and licence. Pricing is re-audited at release. Roadmap and availability are not assumed. Conflicts or ambiguity become diligence items.

LAYER	EVIDENCE	CANNOT ESTABLISH ALONE
Website	website copy + captured date	Delivery, fit, contract
Delivery	Manifest + docs + artefacts	Customer result
Configuration	Data/roles/policy/posture	Operating outcome
Run	Raw output + target + packet	General performance
Assurance	Scoped test/report + findings	Universal security/compliance
Agreement	Rights + duties + remedy	Technical behaviour without test

Keep the layers separate in every chapter and decision record.

READING RULE

Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items.

READ THIS FIRST • CANONICAL SPOTLIGHT

Sovereignty decomposed into ten tests

A buyer can evaluate control only after every dependency with stopping, seeing, changing, or verification power is named.

Test the contracting entity and governing jurisdiction; physical and cloud infrastructure; data and metadata paths; cryptographic keys and trust; compute and hardware; models, tools and source packages; licence enforcement; build, signing and update chain; operations and support; evidence, verifiers, export and exit. Add sector or national dimensions explicitly.

For every dependency ask who owns it, which jurisdiction applies, what network path exists, what protected material it sees, whether it can change a result, whether it can stop operation, how it is updated, what happens on expiry or revocation, which evidence survives, and how it is replaced. Observe the answers in the target posture.

The strongest exercise removes the supplier and external network. Local operators restore the estate, authenticate, run a representative workflow, verify an old packet, reject or stage an update, rotate a key, renew or validate the offline licence as contracted, export state, and demonstrate the documented continuation or replacement path.

AREA	CURRENT GUIDE RECORD	VERIFY / DECIDE
Jurisdiction	Entity, law, site, providers	Foreign control and legal path
Data / keys	Bytes, metadata, stores, backups, trust	Visibility and unilateral access
Compute / models	Hardware, runtime, artefacts, tools	External substitution or revocation
Licence / updates	Offline operation, signing, media	Expiry, kill switch, supply chain
Operations	Admins, support, telemetry, recovery	Remote dependency and competence
Evidence / exit	Formats, verifiers, export, source/rights	Independent review and continuation

Current source-edition summary. Recheck publication-sensitive facts and delivered scope at the decision date.

GUIDE-SPECIFIC PROOF

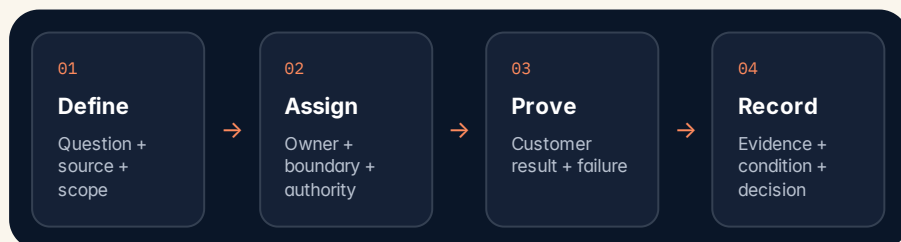
Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights.

01

SOVEREIGN AND AIR-GAPPED AI

Understand the decision and its language

Define the real question, current state, responsibilities, source claims, and the artefact this guide must produce.



The same evidence discipline applies to every chapter in the section.

CHAPTER 01 • EXPLAIN

A testable definition of sovereignty

jurisdiction, data, keys, compute, licences, source, operations, supply chain, evidence, and exit.

This chapter owns a specific part of the reader's decision: jurisdiction, data, keys, compute, licences, source, operations, supply chain, evidence, and exit.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "A testable definition of sovereignty", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

Jurisdiction

Define the exact proposition and current authoritative source.

LENS 2

Data

Name the responsible person, system, dependency, and version.

LENS 3

Keys

Specify the evidence and how an independent reviewer checks it.

LENS 4

Compute

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 01 • APPLY

Turn “A testable definition of sovereignty” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, jurisdiction, data, keys, compute, licences, source, operations, supply chain, evidence, and exit., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant source and version, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for a testable definition of sovereignty; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

CHAPTER 02 • EXPLAIN

Dependency map

identify every outside party or service that could see data, change a result, stop operation, or prevent verification.

This chapter owns a specific part of the reader's decision: identify every outside party or service that could see data, change a result, stop operation, or prevent verification.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "Dependency map", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

Identify every outside party or service that could see data

Define the exact proposition and current authoritative source.

LENS 2

Change a result

Name the responsible person, system, dependency, and version.

LENS 3

Stop operation

Specify the evidence and how an independent reviewer checks it.

LENS 4

Or prevent verification

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 02 • APPLY

Turn “Dependency map” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, identify every outside party or service that could see data, change a result, stop operation, or prevent verification., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant delivered mechanism, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for dependency map; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

CHAPTER 03 • EXPLAIN

Managed Fabric posture

benefits and limits of Dweve-operated Fabric and public-Mesh service operation within the declared processing perimeter.

This chapter owns a specific part of the reader's decision: benefits and limits of Dweve-operated Fabric and public-Mesh service operation within the declared processing perimeter.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "Managed Fabric posture", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

Benefits

Define the exact proposition and current authoritative source.

LENS 2

Limits of Dweve-operated Fabric

Name the responsible person, system, dependency, and version.

LENS 3

Public-Mesh service operation within the declared processing perimeter

Specify the evidence and how an independent reviewer checks it.

LENS 4

Scope and limits

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 03 • APPLY

Turn “Managed Fabric posture” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, benefits and limits of Dweve-operated Fabric and public-Mesh service operation within the declared processing perimeter., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant customer configuration, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for managed fabric posture; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

CHAPTER 04 • EXPLAIN

Customer-owned posture

hardware, network, keys, operations, signed binaries, and rights.

This chapter owns a specific part of the reader's decision: hardware, network, keys, operations, signed binaries, and rights.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "Customer-owned posture", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

Hardware

Define the exact proposition and current authoritative source.

LENS 2

Network

Name the responsible person, system, dependency, and version.

LENS 3

Keys

Specify the evidence and how an independent reviewer checks it.

LENS 4

Operations

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 04 • APPLY

Turn “Customer-owned posture” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, hardware, network, keys, operations, signed binaries, and rights., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant observed operation, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for customer-owned posture; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

CHAPTER 05 • EXPLAIN

Fully disconnected posture

licence file, media shuttle, update verification, local identity, no outbound dependency, and degraded-site continuity.

This chapter owns a specific part of the reader's decision: licence file, media shuttle, update verification, local identity, no outbound dependency, and degraded-site continuity.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "Fully disconnected posture", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

Licence file

Define the exact proposition and current authoritative source.

LENS 2

Media shuttle

Name the responsible person, system, dependency, and version.

LENS 3

Update verification

Specify the evidence and how an independent reviewer checks it.

LENS 4

Local identity

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 05 • APPLY

Turn “Fully disconnected posture” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, licence file, media shuttle, update verification, local identity, no outbound dependency, and degraded-site continuity., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant contract and assurance, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for fully disconnected posture; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

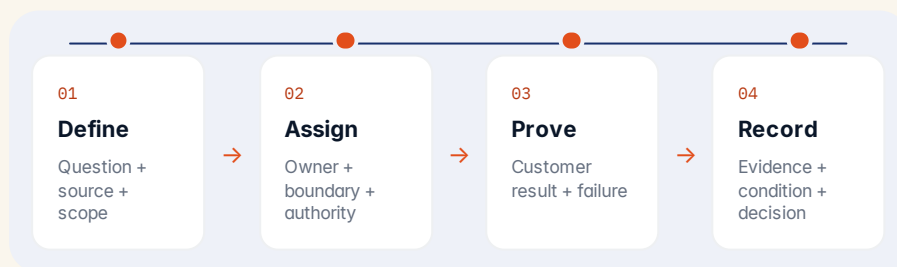
Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

02

SOVEREIGN AND AIR-GAPPED AI

Define the mechanism, controls, and evidence

Turn architecture and policy language into versions, owners, boundaries, tests, records, failures, and explicit limitations.



The same evidence discipline applies to every chapter in the section.

CHAPTER 06 • EXPLAIN

Data and key ownership

paths, stores, backups, encryption boundaries, operator responsibilities, and evidence access.

This chapter owns a specific part of the reader's decision: paths, stores, backups, encryption boundaries, operator responsibilities, and evidence access.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "Data and key ownership", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

Paths

Define the exact proposition and current authoritative source.

LENS 2

Stores

Name the responsible person, system, dependency, and version.

LENS 3

Backups

Specify the evidence and how an independent reviewer checks it.

LENS 4

Encryption boundaries

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 06 • APPLY

Turn “Data and key ownership” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, paths, stores, backups, encryption boundaries, operator responsibilities, and evidence access., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant source and version, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for data and key ownership; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

CHAPTER 07 • EXPLAIN

Models and component replaceability

connectors, open foundations, versioned contracts, and what “swap a layer” requires in practice.

This chapter owns a specific part of the reader’s decision: connectors, open foundations, versioned contracts, and what “swap a layer” requires in practice.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to “Models and component replaceability”, the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website’s jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

Connectors

Define the exact proposition and current authoritative source.

LENS 2

Open foundations

Name the responsible person, system, dependency, and version.

LENS 3

Versioned contracts

Specify the evidence and how an independent reviewer checks it.

LENS 4

And what “swap a layer” requires in practice

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 07 • APPLY

Turn “Models and component replaceability” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, connectors, open foundations, versioned contracts, and what “swap a layer” requires in practice., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant delivered mechanism, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for models and component replaceability; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

CHAPTER 08 • EXPLAIN

Source and modification rights

distinguish public source, source on request, view-only access, full access, and modification rights exactly as current pages state.

This chapter owns a specific part of the reader's decision: distinguish public source, source on request, view-only access, full access, and modification rights exactly as current pages state.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "Source and modification rights", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

Distinguish public source

Define the exact proposition and current authoritative source.

LENS 2

Source on request

Name the responsible person, system, dependency, and version.

LENS 3

View-only access

Specify the evidence and how an independent reviewer checks it.

LENS 4

Full access

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 08 • APPLY

Turn “Source and modification rights” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, distinguish public source, source on request, view-only access, full access, and modification rights exactly as current pages state., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant customer configuration, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for source and modification rights; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

CHAPTER 09 • EXPLAIN

No-kill-switch and continuity claims

state the supported website promise and list the contractual/technical evidence a buyer should verify.

This chapter owns a specific part of the reader's decision: state the supported website promise and list the contractual/technical evidence a buyer should verify.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "No-kill-switch and continuity claims", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

State the supported website promise

Define the exact proposition and current authoritative source.

LENS 2

List the contractual/technical evidence a buyer should verify

Name the responsible person, system, dependency, and version.

LENS 3

Scope and limits

Specify the evidence and how an independent reviewer checks it.

LENS 4

Owner and evidence

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 09 • APPLY

Turn “No-kill-switch and continuity claims” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, state the supported website promise and list the contractual/technical evidence a buyer should verify., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant observed operation, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for no-kill-switch and continuity claims; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

CHAPTER 10 • EXPLAIN

Portable proof and independent verification

how archived evidence remains checkable offline.

This chapter owns a specific part of the reader's decision: how archived evidence remains checkable offline.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "Portable proof and independent verification", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

How archived evidence remains checkable offline

Define the exact proposition and current authoritative source.

LENS 2

Scope and limits

Name the responsible person, system, dependency, and version.

LENS 3

Owner and evidence

Specify the evidence and how an independent reviewer checks it.

LENS 4

Failure and next action

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 10 • APPLY

Turn “Portable proof and independent verification” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, how archived evidence remains checkable offline., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant contract and assurance, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for portable proof and independent verification; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

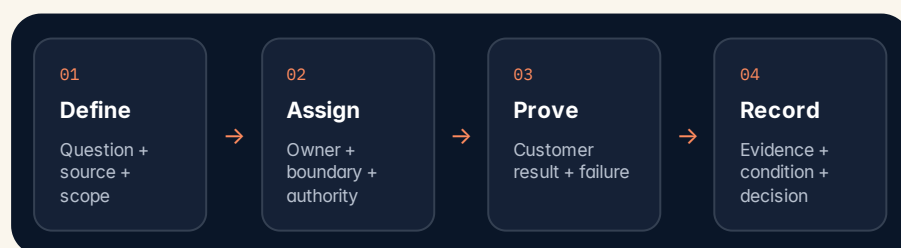
Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

03

SOVEREIGN AND AIR-GAPPED AI

Prove adoption, operation, continuity, and exit

Use customer evidence, challenge, recovery, diligence, commercial terms, and a signed decision before expanding reliance.



The same evidence discipline applies to every chapter in the section.

CHAPTER 11 • EXPLAIN

Supply-chain and update sovereignty

signing, provenance, staging, acceptance, and disconnected distribution.

This chapter owns a specific part of the reader's decision: signing, provenance, staging, acceptance, and disconnected distribution.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "Supply-chain and update sovereignty", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

Signing

Define the exact proposition and current authoritative source.

LENS 2

Provenance

Name the responsible person, system, dependency, and version.

LENS 3

Staging

Specify the evidence and how an independent reviewer checks it.

LENS 4

Acceptance

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 11 • APPLY

Turn “Supply-chain and update sovereignty” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, signing, provenance, staging, acceptance, and disconnected distribution., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant source and version, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for supply-chain and update sovereignty; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

CHAPTER 12 • EXPLAIN

Exit exercise

export data and records, preserve verifiers and keys, pin artefacts, replace services, and prove continued operation.

This chapter owns a specific part of the reader's decision: export data and records, preserve verifiers and keys, pin artefacts, replace services, and prove continued operation.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "Exit exercise", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

Export data

Define the exact proposition and current authoritative source.

LENS 2

Records

Name the responsible person, system, dependency, and version.

LENS 3

Preserve verifiers

Specify the evidence and how an independent reviewer checks it.

LENS 4

Keys

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 12 • APPLY

Turn “Exit exercise” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, export data and records, preserve verifiers and keys, pin artefacts, replace services, and prove continued operation., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant delivered mechanism, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for exit exercise; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

CHAPTER 13 • EXPLAIN

Sovereign commercial model

tiers, reductions, cadence, and scope without confusing price with control.

This chapter owns a specific part of the reader's decision: tiers, reductions, cadence, and scope without confusing price with control.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "Sovereign commercial model", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

Tiers

Define the exact proposition and current authoritative source.

LENS 2

Reductions

Name the responsible person, system, dependency, and version.

LENS 3

Cadence

Specify the evidence and how an independent reviewer checks it.

LENS 4

And scope without confusing price with control

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 13 • APPLY

Turn “Sovereign commercial model” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, tiers, reductions, cadence, and scope without confusing price with control., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant customer configuration, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for sovereign commercial model; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

CHAPTER 14 • EXPLAIN

Sovereignty acceptance checklist

a practical red-team of network, jurisdiction, supplier failure, licence expiry, update refusal, and verifier independence.

This chapter owns a specific part of the reader's decision: a practical red-team of network, jurisdiction, supplier failure, licence expiry, update refusal, and verifier independence.

In this guide, sovereignty is operational control over every dependency able to see protected material, change a result, stop operation, prevent maintenance, withhold evidence, or obstruct replacement and exit. European location is one dimension, not the whole definition. Applied to "Sovereignty acceptance checklist", the practical task is to name the current state, the desired state, the owner of the transition, the material input and dependency, the evidence a reviewer can inspect, and the condition that would make the claim false or the design unsuitable.

The governing boundary is this: Sovereignty requirements are customer-specific and may be legal, security, operational, economic or political. The website's jurisdiction, no-outbound, offline-licence, no-kill-switch, source/right, public-verifier and modification statements become scoped technical and contractual acceptance items. Keep website publication, delivered software, customer configuration, operating result, independent assurance and written contract as separate evidence layers. A strong statement at one layer must not silently become a guarantee at another.

LENS 1

A practical red-team of network

Define the exact proposition and current authoritative source.

LENS 2

Jurisdiction

Name the responsible person, system, dependency, and version.

LENS 3

Supplier failure

Specify the evidence and how an independent reviewer checks it.

LENS 4

Licence expiry

Record scope, failure, unresolved question, and safe next action.

OWNED ARTEFACT

This chapter contributes to a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.

CHAPTER 14 • APPLY

Turn “Sovereignty acceptance checklist” into decision evidence

Move from explanation to a record an accountable owner can use, challenge, update, and carry into proof, procurement, operation, or exit.

Begin with the chapter proposition, a practical red-team of network, jurisdiction, supplier failure, licence expiry, update refusal, and verifier independence., and write it as one or more falsifiable questions. For each question, define scope and time, authoritative website source or customer source, delivered artefact, relevant observed operation, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a public or critical operator disconnects a representative estate, expires external credentials, denies supplier network access, rotates local keys, applies a signed offline update, verifies evidence independently, exports state, and continues under a supplier-failure exercise. Walk it end to end and ask what this chapter changes at request, source, model/tool/rule, human authority, target, evidence, deployment, operation, commercial or exit state. Do not accept a screenshot or summary when the underlying manifest, result, packet, record or contractual term can be inspected.

The proof discipline for this guide is: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights. Preserve negative and unverifiable results. A gap can be remediated, contracted, accepted by the competent owner, or block the decision; it must not disappear behind roadmap language or an average score.

QUESTION	REQUIRED RECORD	OWNER / STOP
What is claimed?	Exact wording, scope, date, source	Guide decision owner
What exists?	Delivered manifest, interface, artefact	Technical/product owner
What is configured?	Customer data, roles, rules, posture	Customer control owner
What happened?	Raw run, target state, packet, metric	Domain/operations owner
What is assured?	Test/report scope, findings, limits	Independent challenger
What is committed?	Offer/agreement, remedy, exit term	Procurement/legal owner

Evidence ladder for sovereignty acceptance checklist; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.

FIND A SUBJECT

Subject index

Page references point to the substantive explanation, worked example, control, boundary, or decision record, not merely to a passing label.

A Acceptance criteria 3-4, 7-16, 18-27, 29-36	A Accountability 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 32, 34, 36	A Adoption 28
A Air-gapped deployment 6, 17, 28	A Appeal and challenge 3, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27-28, 30, 32, 34, 36	A Architecture 4, 17
A Assurance 4, 7, 9, 11, 13, 15-16, 18, 20, 22, 24, 26-27, 29, 31, 33, 35	A Authority 4, 6, 8, 10, 12, 14, 16-17, 19, 21, 23, 25, 27-28, 30, 32, 34, 36	A Availability 4
B Boundaries 3, 6-7, 9, 11, 13, 15, 17-20, 22, 24, 26, 28-29, 31, 33, 35	C Compliance 4	C Configuration 4, 7, 9, 11-13, 15, 18, 20, 22-24, 26, 29, 31, 33-35
C Continuity 3-5, 8, 10, 12, 14-16, 19, 21, 23-25, 27-28, 30, 32, 34, 36	C Contracts 3-4, 7, 9, 11, 13, 15-16, 18, 20, 22, 24, 26-27, 29, 31, 33, 35	C Critical infrastructure 3
D Decision records 4, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 32, 34, 36	D Defence 3	D Dependencies 3, 5, 7-16, 18-27, 29-36
D Deployment 3, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 32, 34, 36	D Due diligence 4, 28	E Evidence 3-36
E Exit 3, 5, 7-16, 18-36	F Fabric 11-12	F Failure 3, 6-36
H Hardware 4-5, 13-14	H Human authority 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 32, 34, 36	I Identity 3, 15-16
I Inputs 7, 9, 11, 13, 15, 18, 20, 22, 24, 26, 29, 31, 33, 35	J Jurisdiction 3-5, 7-16, 18-27, 29-36	K Keys and signing 5, 29-30
L Ledger 3, 7, 9, 11, 13, 15, 18, 20, 22, 24, 26, 29, 31, 33, 35	L Licensing 3-5, 7-16, 18-27, 29-36	L Limits and exclusions 8, 10-12, 14, 16, 19, 21, 23-27, 30, 32, 34, 36
M Manifests 4, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 32, 34, 36	M Mesh 11-12	M Models and solvers 3-4, 7-16, 18-27, 29-36

SUBJECT INDEX CONTINUED

Subject index · O–W

Terms are grouped alphabetically. Consecutive page references are collapsed into ranges.

O Operations 3, 5, 7–16, 18–36	O Outputs 3–4	O Ownership 3–4, 6–36
P Performance 4	P Policies 3–4, 17	P Portability 3, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 32, 34, 36
P Pricing 4, 33–34	P Procurement 3–4, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 32, 34, 36	P Proof 4–5, 8, 10, 12, 14, 16, 19, 21, 23, 25–27, 30, 32, 34, 36
P Provenance 29–30	R Recovery 5, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27–28, 30, 32, 34, 36	R Responsibility 4, 6, 18–19
R Rights 4–5, 8, 10, 12–14, 16, 19, 21–23, 25, 27, 30, 32, 34, 36	R Risk 3–4, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 32, 34, 36	R Rules 4, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 32, 34, 36
S Security 4, 7, 9, 11, 13, 15, 18, 20, 22, 24, 26, 29, 31, 33, 35	S Sources 3–36	S Sovereignty 3–36
S State 3, 5–16, 18–27, 29–36	S Supply chain 4–5, 7–8	T Testing 3–5, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 32, 34, 36
V Verification 3, 5, 8–10, 12, 14–16, 19, 21, 23–27, 30, 32, 34, 36	V Versioning 4, 7–9, 11, 13, 15, 18–20, 22, 24, 26, 29–31, 33, 35	W Workflows 3, 5

CLOSING DECISION RECORD

Close with one evidence-backed, reversible decision

The guide is complete when its reader can decide whether to proceed, narrow, remediate, contract a condition, hold, reject, or exit, and another person can understand why.

Assemble a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer. State the question, scope and exclusions, scenario or workflow, current baseline, canonical source snapshot, delivered manifest, customer configuration, corpus and method, results and failures, owner decisions, risks, operational and commercial conditions, evidence links, remedies, stop/exit and review triggers.

Run the final discipline: Map and observe every dependency, block all egress, remove supplier access, inspect licence behaviour, run with local models/sources/keys, verify signed packages and packets offline, refuse an update, restore from owned material, export and replace one layer, and exercise the written continuity rights.

Have sovereignty and programme owner, infrastructure and operations, security/keys/supply chain, data and model/source owners, legal/procurement, records/verifier, continuity, national or sector authority, and Dweve sign only the boundaries they own. Record pass, conditional pass, gap, fail or unverifiable per proposition. Preserve dissent and raw evidence. A brochure can organise the decision; it cannot make the evidence true or take responsibility from the people who rely on it.

DECISION RECORD	sovereign-air-gapped-ai-decision	
QUESTION	decide whether Dweve's jurisdiction, ownership, offline operation, portability, and supplier-continuity model meets a defined sovereignty requirement.	BOUNDED
SOURCES	website copy + delivered material	CAPTURED
PROOF	corpus + failures + recovery	RUN
OWNERS	domain + technical + assurance	SIGNED
CONDITIONS	gaps + remedies + contract	DATED
DECISION	go / narrow / hold / stop / exit	RECORDED
The closing record remains useful after the presentation, release, team, supplier, or contract changes.		

GUIDE OUTPUT

Produce a sovereignty dependency ledger with owner, jurisdiction, network path, data, keys, licence, source, model/tool, build/update, operational, evidence and exit state for every layer.