

FOUNDATION AND DECISION GUIDE · F08

Deployment and operations handbook

Managed Fabric access, licensed customer operation, and air-gapped operation from topology and sizing through update, recovery, migration, and ownership.

DECISION

SCOPE

EVIDENCE

OWNERSHIP

PROOF

EXIT



A complete guide to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

F08

CONTENTS

From the first question to a defensible decision

This 45-page guide turns 15 owned topics into an explanation, evidence requirement, proof challenge, and closing decision record.

PRIMARY READERS

Platform, infrastructure and operations teams

READING DEPTH

Technical operations

DECISION THIS SUPPORTS

Select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

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–...
Choose a posture by responsibility · What stays the same · Managed Fabric on the public Mesh · Licensed deployment · Air-gapped deployment

03 Define the mechanism, controls, and evidence ...
Reference topology · Packaging and infrastructure modules · Data and trust boundaries · Capacity and hardware planning · Operations model

04 Prove adoption, operation, continuity, and exit ...–43
Release and update management · Failure and continuity · Migration between postures · Operational acceptance plan · Runbook and responsibility matrix

05 Sources and next action 44–43
verification records and closing decision package

06 Subject index 44–45
An alphabetical finder for concepts, controls, products, and decisions.

TARGET LENGTH

11,000–15,000 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

infrastructure, platform engineering, SRE, operations, security architecture, and service ownership teams.

Select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

The worked scenario is a workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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 an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit. 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.

BUSINESS WORKSPACE

Dweve operates

Current guide lens; verify source and scope.

LICENSED

Customer operates

Current guide lens; verify source and scope.

AIR-GAPPED

Closed local estate

Current guide lens; verify source and scope.

INVARIANT

Contracts + packets

Current guide lens; verify source and scope.

PRIMARY RISK

A deployment label can hide outbound dependencies, ambiguous key custody, undersized hardware, unavailable offline models or licences, sensitive telemetry, untested signed-media updates, fragile recovery and an operational responsibility no team owns.

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 service owner, platform/infrastructure engineering, SRE/operations, security and keys, identity, data/storage, application and source owners, evidence/records, support, procurement and continuity. 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

"Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence.

READ THIS FIRST • CANONICAL SPOTLIGHT

One semantic platform, three operating postures

The workload contract and packet can remain portable while responsibility, infrastructure, dependencies and risk move.

With managed Fabric access, Dweve operates the public Mesh capacity and underlying service boundary while the customer owns its use, data, identities, policies and integrations. Managed customers use Fabric surfaces and do not operate Core or the underlying products directly. In a licensed posture, the customer operates delivered products on its infrastructure and holds the local keys. In an air-gapped posture, the complete relied-on path must close without outbound service, licence or telemetry dependency.

Every topology needs ingress, identity, product services, approved source/model/tool packages, runtime/compute, state and queues, evidence storage, keys/trust, observability, administration, backup/restore and target integrations. The exact modules, packaging and Kubernetes support are verified from the delivered edition rather than inferred from the diagram.

Migration proves more than copying data. Export identities, configuration, approved sources/rules/models, product state, queues, packets and verifier dependencies; restore them in the target posture; run new acceptance work and historical verification; reconcile external targets; retain rollback until both operating and accountability state are accepted.

AREA	CURRENT GUIDE RECORD	VERIFY / DECIDE
Business Workspace	Supplier-operated service	Entity, region, paths, keys, subprocessors, exit
Licensed	Customer infrastructure and operation	Hardware, identity, updates, backup, support
Air-gapped	Closed customer estate	Offline packages/licence, time, media, telemetry
Invariant	Semantic contracts and evidence formats	Reproduce in delivered versions
Migration	State and artefact transfer	New work + historical packet + rollback
Acceptance	Install, isolate, load, update, restore	Named operator and raw evidence

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

GUIDE-SPECIFIC PROOF

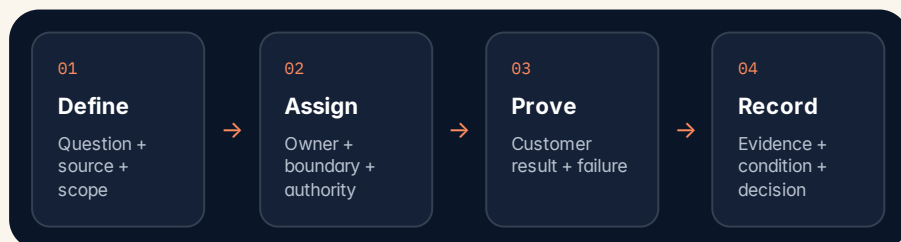
Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity.

01

DEPLOYMENT AND OPERATIONS HANDBOOK

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

Choose a posture by responsibility

decision criteria based on jurisdiction, operations, isolation, latency, modification rights, and continuity.

This chapter owns a specific part of the reader's decision: decision criteria based on jurisdiction, operations, isolation, latency, modification rights, and continuity.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Choose a posture by responsibility", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Decision criteria based on jurisdiction

Define the exact proposition and current authoritative source.

LENS 2

Operations

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

LENS 3

Isolation

Specify the evidence and how an independent reviewer checks it.

LENS 4

Latency

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 01 • APPLY

Turn “Choose a posture by responsibility” 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, decision criteria based on jurisdiction, operations, isolation, latency, modification rights, and 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 source and version, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 choose a posture by responsibility; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 01 • CHALLENGE

Stress-test the boundary behind "Choose a posture by responsibility"

A deep-dive topic earns an additional page for counterexamples, adversarial conditions, missing dependencies, role failure, recovery, and evidence limits.

The principal guide risk is: A deployment label can hide outbound dependencies, ambiguous key custody, undersized hardware, unavailable offline models or licences, sensitive telemetry, untested signed-media updates, fragile recovery and an operational responsibility no team owns.

For this chapter, remove or alter the strongest assumption in "decision criteria based on jurisdiction, operations, isolation, latency, modification rights, and continuity.". Change the source or version, revoke a person or right, replace a delivered dependency, interrupt the selected deployment, introduce incompatible state, withhold a target acknowledgement, tamper with evidence, or make the relied-on contract condition unavailable. Observe whether the boundary refuses, degrades, escalates, reconciles, recovers, or fails silently.

Run the fault from the perspective of service owner, platform/infrastructure engineering, SRE/operations, security and keys, identity, data/storage, application and source owners, evidence/records, support, procurement and continuity. Each owner should see only the authorised information needed to act, understand the current state, and have an explicit safe next step. Restore normal operation, retrieve a pre-change record, and decide whether the chapter proposition still holds, now holds conditionally, requires remediation, or blocks reliance.

STRESS LANE	INJECTION	EXPECTED EVIDENCE
Authority	Role absent, revoked, conflicted or bypassed	Wait/refuse/escalate + receipt
Dependency	Source, service, package, model or key unavailable	Degraded state + manifest + recovery
Integrity	Alter, delete, reorder, substitute	Verification failure + quarantine
Operation	Load, outage, clock, storage or update fault	Alert + safe state + restore
Target	Timeout, duplicate, rejection or conflicting state	Idempotency + reconciliation
Exit	Supplier access removed or contract ends	Export + local verification + continuity result

Select applicable lanes and add topic-specific consequences before the run.

STOP RULE

If a critical assumption fails without a detectable safe state and accountable owner, stop the proof or production lane until the boundary is repaired.

CHAPTER 02 • EXPLAIN

What stays the same

binaries, contracts, trace formats, product boundaries, and artefacts as stated by the website.

This chapter owns a specific part of the reader's decision: binaries, contracts, trace formats, product boundaries, and artefacts as stated by the website.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "What stays the same", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Binaries

Define the exact proposition and current authoritative source.

LENS 2

Contracts

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

LENS 3

Trace formats

Specify the evidence and how an independent reviewer checks it.

LENS 4

Product boundaries

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 02 • APPLY

Turn “What stays the same” 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, binaries, contracts, trace formats, product boundaries, and artefacts as stated by the website., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 what stays the same; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 03 • EXPLAIN

Managed Fabric on the public Mesh

service boundary, customer boundary, processing perimeter, scaling, maintenance, keys, data path, product-access limits, and hand-off points.

This chapter owns a specific part of the reader's decision: service boundary, customer boundary, processing perimeter, scaling, maintenance, keys, data path, product-access limits, and hand-off points.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Managed Fabric on the public Mesh", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Service boundary

Define the exact proposition and current authoritative source.

LENS 2

Customer boundary

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

LENS 3

Processing perimeter

Specify the evidence and how an independent reviewer checks it.

LENS 4

Scaling

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 03 • APPLY

Turn “Managed Fabric on the public Mesh” 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, service boundary, customer boundary, processing perimeter, scaling, maintenance, keys, data path, product-access limits, and hand-off points., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 on the public mesh; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 04 • EXPLAIN

Licensed deployment

customer infrastructure, ownership, keys, signed binaries, unlimited-use boundary, and Dweve/customer responsibilities.

This chapter owns a specific part of the reader's decision: customer infrastructure, ownership, keys, signed binaries, unlimited-use boundary, and Dweve/customer responsibilities.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Licensed deployment", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Customer infrastructure

Define the exact proposition and current authoritative source.

LENS 2

Ownership

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

LENS 3

Keys

Specify the evidence and how an independent reviewer checks it.

LENS 4

Signed binaries

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 04 • APPLY

Turn “Licensed deployment” 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, customer infrastructure, ownership, keys, signed binaries, unlimited-use boundary, and Dweve/customer responsibilities., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 licensed deployment; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 04 • CHALLENGE

Stress-test the boundary behind "Licensed deployment"

A deep-dive topic earns an additional page for counterexamples, adversarial conditions, missing dependencies, role failure, recovery, and evidence limits.

The principal guide risk is: A deployment label can hide outbound dependencies, ambiguous key custody, undersized hardware, unavailable offline models or licences, sensitive telemetry, untested signed-media updates, fragile recovery and an operational responsibility no team owns.

For this chapter, remove or alter the strongest assumption in "customer infrastructure, ownership, keys, signed binaries, unlimited-use boundary, and Dweve/customer responsibilities.". Change the source or version, revoke a person or right, replace a delivered dependency, interrupt the selected deployment, introduce incompatible state, withhold a target acknowledgement, tamper with evidence, or make the relied-on contract condition unavailable. Observe whether the boundary refuses, degrades, escalates, reconciles, recovers, or fails silently.

Run the fault from the perspective of service owner, platform/infrastructure engineering, SRE/operations, security and keys, identity, data/storage, application and source owners, evidence/records, support, procurement and continuity. Each owner should see only the authorised information needed to act, understand the current state, and have an explicit safe next step. Restore normal operation, retrieve a pre-change record, and decide whether the chapter proposition still holds, now holds conditionally, requires remediation, or blocks reliance.

STRESS LANE	INJECTION	EXPECTED EVIDENCE
Authority	Role absent, revoked, conflicted or bypassed	Wait/refuse/escalate + receipt
Dependency	Source, service, package, model or key unavailable	Degraded state + manifest + recovery
Integrity	Alter, delete, reorder, substitute	Verification failure + quarantine
Operation	Load, outage, clock, storage or update fault	Alert + safe state + restore
Target	Timeout, duplicate, rejection or conflicting state	Idempotency + reconciliation
Exit	Supplier access removed or contract ends	Export + local verification + continuity result

Select applicable lanes and add topic-specific consequences before the run.

STOP RULE

If a critical assumption fails without a detectable safe state and accountable owner, stop the proof or production lane until the boundary is repaired.

CHAPTER 05 • EXPLAIN

Air-gapped deployment

no outbound dependency, offline licence, signed-media update path, verification, rollback, and local operations.

This chapter owns a specific part of the reader's decision: no outbound dependency, offline licence, signed-media update path, verification, rollback, and local operations.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Air-gapped deployment", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

No outbound dependency

Define the exact proposition and current authoritative source.

LENS 2

Offline licence

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

LENS 3

Signed-media update path

Specify the evidence and how an independent reviewer checks it.

LENS 4

Verification

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 05 • APPLY

Turn “Air-gapped deployment” 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, no outbound dependency, offline licence, signed-media update path, verification, rollback, and local operations., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 air-gapped deployment; not every question needs every row, but no row may be implied without evidence.

DECISION RECORD

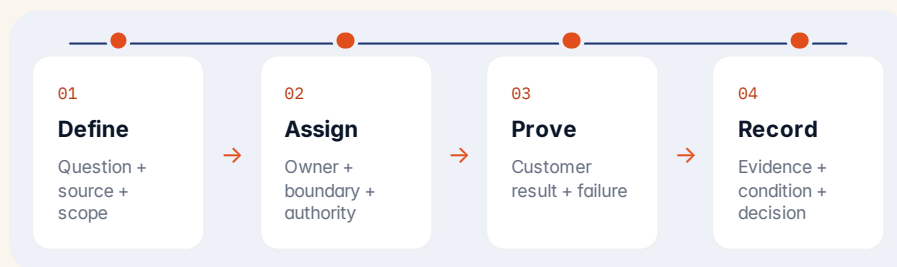
Record pass, conditional pass, gap, fail, or unverifiable; link evidence, owner, remediation, date, residual risk, and effect on select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

02

DEPLOYMENT AND OPERATIONS HANDBOOK

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

Reference topology

compute, storage, identity, API ingress, product services, evidence store, key management, observability, and admin plane.

This chapter owns a specific part of the reader's decision: compute, storage, identity, API ingress, product services, evidence store, key management, observability, and admin plane.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Reference topology", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Compute

Define the exact proposition and current authoritative source.

LENS 2

Storage

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

LENS 3

Identity

Specify the evidence and how an independent reviewer checks it.

LENS 4

API ingress

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 06 • APPLY

Turn “Reference topology” 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, compute, storage, identity, API ingress, product services, evidence store, key management, observability, and admin plane., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 reference topology; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 07 • EXPLAIN

Packaging and infrastructure modules

containers, Kubernetes topology, configuration, environment separation, and website-listed modules.

This chapter owns a specific part of the reader's decision: containers, Kubernetes topology, configuration, environment separation, and website-listed modules.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Packaging and infrastructure modules", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Containers

Define the exact proposition and current authoritative source.

LENS 2

Kubernetes topology

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

LENS 3

Configuration

Specify the evidence and how an independent reviewer checks it.

LENS 4

Environment separation

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 07 • APPLY

Turn “Packaging and infrastructure modules” 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, containers, Kubernetes topology, configuration, environment separation, and website-listed modules., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 packaging and infrastructure modules; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 07 • CHALLENGE

Stress-test the boundary behind "Packaging and infrastructure modules"

A deep-dive topic earns an additional page for counterexamples, adversarial conditions, missing dependencies, role failure, recovery, and evidence limits.

The principal guide risk is: A deployment label can hide outbound dependencies, ambiguous key custody, undersized hardware, unavailable offline models or licences, sensitive telemetry, untested signed-media updates, fragile recovery and an operational responsibility no team owns.

For this chapter, remove or alter the strongest assumption in "containers, Kubernetes topology, configuration, environment separation, and website-listed modules.". Change the source or version, revoke a person or right, replace a delivered dependency, interrupt the selected deployment, introduce incompatible state, withhold a target acknowledgement, tamper with evidence, or make the relied-on contract condition unavailable. Observe whether the boundary refuses, degrades, escalates, reconciles, recovers, or fails silently.

Run the fault from the perspective of service owner, platform/infrastructure engineering, SRE/operations, security and keys, identity, data/storage, application and source owners, evidence/records, support, procurement and continuity. Each owner should see only the authorised information needed to act, understand the current state, and have an explicit safe next step. Restore normal operation, retrieve a pre-change record, and decide whether the chapter proposition still holds, now holds conditionally, requires remediation, or blocks reliance.

STRESS LANE	INJECTION	EXPECTED EVIDENCE
Authority	Role absent, revoked, conflicted or bypassed	Wait/refuse/escalate + receipt
Dependency	Source, service, package, model or key unavailable	Degraded state + manifest + recovery
Integrity	Alter, delete, reorder, substitute	Verification failure + quarantine
Operation	Load, outage, clock, storage or update fault	Alert + safe state + restore
Target	Timeout, duplicate, rejection or conflicting state	Idempotency + reconciliation
Exit	Supplier access removed or contract ends	Export + local verification + continuity result

Select applicable lanes and add topic-specific consequences before the run.

STOP RULE

If a critical assumption fails without a detectable safe state and accountable owner, stop the proof or production lane until the boundary is repaired.

CHAPTER 08 • EXPLAIN

Data and trust boundaries

inbound sources, internal movement, records, optional exports, and prohibited egress.

This chapter owns a specific part of the reader's decision: inbound sources, internal movement, records, optional exports, and prohibited egress.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Data and trust boundaries", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Inbound sources

Define the exact proposition and current authoritative source.

LENS 2

Internal movement

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

LENS 3

Records

Specify the evidence and how an independent reviewer checks it.

LENS 4

Optional exports

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 08 • APPLY

Turn “Data and trust boundaries” 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, inbound sources, internal movement, records, optional exports, and prohibited egress., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 trust boundaries; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 09 • EXPLAIN

Capacity and hardware planning

CPU targets, memory, storage, throughput, evidence retention, and how to use published benchmarks responsibly.

This chapter owns a specific part of the reader's decision: CPU targets, memory, storage, throughput, evidence retention, and how to use published benchmarks responsibly.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Capacity and hardware planning", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

CPU targets

Define the exact proposition and current authoritative source.

LENS 2

Memory

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

LENS 3

Storage

Specify the evidence and how an independent reviewer checks it.

LENS 4

Throughput

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 09 • APPLY

Turn “Capacity and hardware planning” 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, CPU targets, memory, storage, throughput, evidence retention, and how to use published benchmarks responsibly., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 capacity and hardware planning; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 10 • EXPLAIN

Operations model

monitoring, logs versus evidence, health, backups, restore, key rotation, access review, and routine administration.

This chapter owns a specific part of the reader's decision: monitoring, logs versus evidence, health, backups, restore, key rotation, access review, and routine administration.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Operations 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Monitoring

Define the exact proposition and current authoritative source.

LENS 2

Logs versus evidence

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

LENS 3

Health

Specify the evidence and how an independent reviewer checks it.

LENS 4

Backups

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 10 • APPLY

Turn “Operations 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, monitoring, logs versus evidence, health, backups, restore, key rotation, access review, and routine administration., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 operations 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 10 • CHALLENGE

Stress-test the boundary behind "Operations model"

A deep-dive topic earns an additional page for counterexamples, adversarial conditions, missing dependencies, role failure, recovery, and evidence limits.

The principal guide risk is: A deployment label can hide outbound dependencies, ambiguous key custody, undersized hardware, unavailable offline models or licences, sensitive telemetry, untested signed-media updates, fragile recovery and an operational responsibility no team owns.

For this chapter, remove or alter the strongest assumption in "monitoring, logs versus evidence, health, backups, restore, key rotation, access review, and routine administration.". Change the source or version, revoke a person or right, replace a delivered dependency, interrupt the selected deployment, introduce incompatible state, withhold a target acknowledgement, tamper with evidence, or make the relied-on contract condition unavailable. Observe whether the boundary refuses, degrades, escalates, reconciles, recovers, or fails silently.

Run the fault from the perspective of service owner, platform/infrastructure engineering, SRE/operations, security and keys, identity, data/storage, application and source owners, evidence/records, support, procurement and continuity. Each owner should see only the authorised information needed to act, understand the current state, and have an explicit safe next step. Restore normal operation, retrieve a pre-change record, and decide whether the chapter proposition still holds, now holds conditionally, requires remediation, or blocks reliance.

STRESS LANE	INJECTION	EXPECTED EVIDENCE
Authority	Role absent, revoked, conflicted or bypassed	Wait/refuse/escalate + receipt
Dependency	Source, service, package, model or key unavailable	Degraded state + manifest + recovery
Integrity	Alter, delete, reorder, substitute	Verification failure + quarantine
Operation	Load, outage, clock, storage or update fault	Alert + safe state + restore
Target	Timeout, duplicate, rejection or conflicting state	Idempotency + reconciliation
Exit	Supplier access removed or contract ends	Export + local verification + continuity result

Select applicable lanes and add topic-specific consequences before the run.

STOP RULE

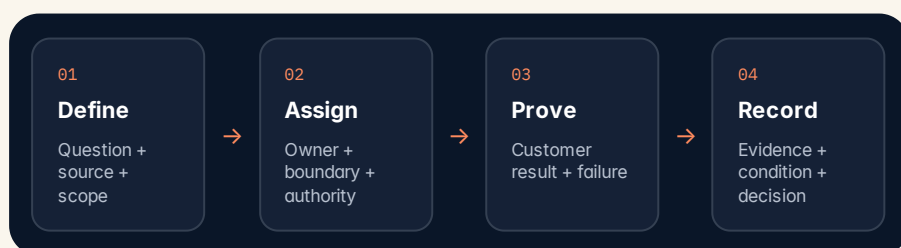
If a critical assumption fails without a detectable safe state and accountable owner, stop the proof or production lane until the boundary is repaired.

03

DEPLOYMENT AND OPERATIONS HANDBOOK

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

Release and update management

signed artefacts, version pinning, staged promotion, acceptance checks, disconnected transfer, and rollback.

This chapter owns a specific part of the reader's decision: signed artefacts, version pinning, staged promotion, acceptance checks, disconnected transfer, and rollback.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Release and update management", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Signed artefacts

Define the exact proposition and current authoritative source.

LENS 2

Version pinning

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

LENS 3

Staged promotion

Specify the evidence and how an independent reviewer checks it.

LENS 4

Acceptance checks

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 11 • APPLY

Turn “Release and update management” 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, signed artefacts, version pinning, staged promotion, acceptance checks, disconnected transfer, and rollback., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 release and update management; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 12 • EXPLAIN

Failure and continuity

degraded dependencies, unavailable model or source, site isolation, failover, replay after recovery, and customer-controlled continuation.

This chapter owns a specific part of the reader's decision: degraded dependencies, unavailable model or source, site isolation, failover, replay after recovery, and customer-controlled continuation.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Failure and continuity", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Degraded dependencies

Define the exact proposition and current authoritative source.

LENS 2

Unavailable model or source

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

LENS 3

Site isolation

Specify the evidence and how an independent reviewer checks it.

LENS 4

Failover

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 12 • APPLY

Turn “Failure and continuity” 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, degraded dependencies, unavailable model or source, site isolation, failover, replay after recovery, and customer-controlled continuation., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 failure and continuity; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 13 • EXPLAIN

Migration between postures

discovery, export, artefact parity, validation, cutover, rollback, and evidence continuity.

This chapter owns a specific part of the reader's decision: discovery, export, artefact parity, validation, cutover, rollback, and evidence continuity.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Migration between postures", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Discovery

Define the exact proposition and current authoritative source.

LENS 2

Export

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

LENS 3

Artefact parity

Specify the evidence and how an independent reviewer checks it.

LENS 4

Validation

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 13 • APPLY

Turn “Migration between postures” 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, discovery, export, artefact parity, validation, cutover, rollback, and evidence 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 customer configuration, named owner, comparison or acceptance rule, raw evidence, known limitation, and decision consequence.

Use the guide-wide scenario: a workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 migration between postures; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 13 • CHALLENGE

Stress-test the boundary behind "Migration between postures"

A deep-dive topic earns an additional page for counterexamples, adversarial conditions, missing dependencies, role failure, recovery, and evidence limits.

The principal guide risk is: A deployment label can hide outbound dependencies, ambiguous key custody, undersized hardware, unavailable offline models or licences, sensitive telemetry, untested signed-media updates, fragile recovery and an operational responsibility no team owns.

For this chapter, remove or alter the strongest assumption in "discovery, export, artefact parity, validation, cutover, rollback, and evidence continuity.". Change the source or version, revoke a person or right, replace a delivered dependency, interrupt the selected deployment, introduce incompatible state, withhold a target acknowledgement, tamper with evidence, or make the relied-on contract condition unavailable. Observe whether the boundary refuses, degrades, escalates, reconciles, recovers, or fails silently.

Run the fault from the perspective of service owner, platform/infrastructure engineering, SRE/operations, security and keys, identity, data/storage, application and source owners, evidence/records, support, procurement and continuity. Each owner should see only the authorised information needed to act, understand the current state, and have an explicit safe next step. Restore normal operation, retrieve a pre-change record, and decide whether the chapter proposition still holds, now holds conditionally, requires remediation, or blocks reliance.

STRESS LANE	INJECTION	EXPECTED EVIDENCE
Authority	Role absent, revoked, conflicted or bypassed	Wait/refuse/escalate + receipt
Dependency	Source, service, package, model or key unavailable	Degraded state + manifest + recovery
Integrity	Alter, delete, reorder, substitute	Verification failure + quarantine
Operation	Load, outage, clock, storage or update fault	Alert + safe state + restore
Target	Timeout, duplicate, rejection or conflicting state	Idempotency + reconciliation
Exit	Supplier access removed or contract ends	Export + local verification + continuity result

Select applicable lanes and add topic-specific consequences before the run.

STOP RULE

If a critical assumption fails without a detectable safe state and accountable owner, stop the proof or production lane until the boundary is repaired.

CHAPTER 14 • EXPLAIN

Operational acceptance plan

installation, security, performance, replay, recovery, isolation, update, and ownership tests.

This chapter owns a specific part of the reader's decision: installation, security, performance, replay, recovery, isolation, update, and ownership tests.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Operational acceptance plan", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

Installation

Define the exact proposition and current authoritative source.

LENS 2

Security

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

LENS 3

Performance

Specify the evidence and how an independent reviewer checks it.

LENS 4

Replay

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

OWNED ARTEFACT

This chapter contributes to an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 14 • APPLY

Turn “Operational acceptance plan” 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, installation, security, performance, replay, recovery, isolation, update, and ownership tests., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 operational acceptance plan; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

CHAPTER 15 • EXPLAIN

Runbook and responsibility matrix

what must be assigned before production and which items require scoped confirmation.

This chapter owns a specific part of the reader's decision: what must be assigned before production and which items require scoped confirmation.

In this guide, deployment is a transfer of operating responsibility around the same semantic products and artefacts. Region, infrastructure, keys, data, identity, packages, observability, updates, backup, recovery, support, licence enforcement and exit must be resolved for the selected posture. Applied to "Runbook and responsibility matrix", 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: "Same platform" can describe contracts and artefacts without implying the same service level, hardware, network, security controls, update cadence or support boundary. Managed, licensed and air-gapped operation require different customer capabilities and evidence. 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

What must be assigned before production

Define the exact proposition and current authoritative source.

LENS 2

Which items require scoped confirmation

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 an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.

CHAPTER 15 • APPLY

Turn “Runbook and responsibility matrix” 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, what must be assigned before production and which items require scoped confirmation., 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 workload moves from a managed Fabric evaluation to licensed customer infrastructure and then a disconnected site while semantic contracts, source/model/policy packages, records and historical verification remain coherent. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity. 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 runbook and responsibility matrix; 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 select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.

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, 5, 8, 11, 13, 15, 18, 21, 23, 26, 28, 30, 33-34, 36, 38, 40-41, 43	A Accountability 5, 8-9, 11, 13, 15-16, 18, 21, 23-24, 26, 28, 30-31, 34, 36, 38-39, 41, 43	A Adoption 32
A Air-gapped deployment 3-5, 7, 10, 12, 14, 17-18, 20, 22, 25, 27, 29, 33, 35, 37, 40, 42	A Appeal and challenge 3, 8-9, 11, 13, 15-16, 18, 21, 23-24, 26, 28, 30-32, 34, 36, 38-39, 41, 43	A Architecture 3-4, 19
A Assurance 4, 7, 10, 12, 14, 17-18, 20, 22, 25, 27, 29-30, 33, 35, 37, 40, 42-43	A Authority 4, 6, 8-9, 11, 13, 15-16, 18-19, 21, 23-24, 26, 28, 30-32, 34, 36, 38-39, 41, 43	A Availability 4
B Boundaries 3-7, 9-17, 19-20, 22, 24-27, 29, 31-33, 35, 37, 39-40, 42	C Capabilities 4, 7, 10, 12, 14, 17, 20, 22, 25, 27, 29, 33, 35, 37, 40, 42	C Compliance 4
C Configuration 4-5, 7, 10, 12-14, 17, 20, 22-27, 29, 33, 35, 37-38, 40, 42	C Continuity 3-5, 7-9, 11, 13, 15-16, 18, 21, 23-24, 26, 28, 30-32, 34-39, 41, 43	C Contracts 4-5, 7, 9-10, 12, 14, 16-18, 20, 22, 24-25, 27, 29-31, 33, 35, 37, 39-40, 42-43
D Decision records 4, 8, 11, 13, 15, 18, 21, 23, 26, 28, 30, 34, 36, 38, 41, 43	D Dependencies 3, 5, 7-18, 20-31, 33-43	D Deployment 3, 6-43
D Due diligence 4, 32	E Evidence 3-43	E Exit 3, 5, 7-18, 20-43
F Fabric 3, 5, 8, 11-13, 15, 18, 21, 23, 26, 28, 30, 34, 36, 38, 41, 43	F Failure 3, 6-7, 9-10, 12, 14, 16-17, 19-20, 22, 24-25, 27, 29, 31-33, 35-37, 39-40, 42	H Hardware 3-5, 7, 9-10, 12, 14, 16-17, 20, 22, 24-25, 27-29, 31, 33, 35, 37, 39-40, 42
H Human authority 8, 11, 13, 15, 18, 21, 23, 26, 28, 30, 34, 36, 38, 41, 43	I Identity 4-5, 7, 9-10, 12, 14, 16-17, 20-22, 24-25, 27, 29, 31, 33, 35, 37, 39-40, 42	I Inputs 7, 10, 12, 14, 17, 20, 22, 25, 27, 29, 33, 35, 37, 40, 42
J Jurisdiction 7-9	K Keys and signing 3, 9, 16, 24, 31, 39	L Licensing 4-5, 7, 10, 12, 14, 17-18, 20, 22, 25, 27, 29, 33, 35, 37, 40, 42
L Limits and exclusions 8-9, 11-13, 15-16, 18, 21, 23-24, 26, 28, 30-31, 34, 36, 38-39, 41-43	M Manifests 3-5, 7-18, 20-31, 33-43	M Mesh 5, 12-13
M Migration 3, 5, 7-8, 10-15, 17-18, 20-23, 25-30, 33-43	M Models and solvers 3, 5, 8-9, 11, 13, 15-16, 18, 21, 23-24, 26, 28-31, 34-36, 38-39, 41, 43	M Monitoring 29-31

SUBJECT INDEX CONTINUED

Subject index · O–W

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

O Operations 4–5, 7–18, 20–43	O Outputs 3–4	O Ownership 3–4, 6–43
P Performance 4, 40–41	P Policies 3–5, 8, 11, 13, 15, 18–19, 21, 23, 26, 28, 30, 34, 36, 38, 41, 43	P Pricing 4
P Procurement 4, 8–9, 11, 13, 15–16, 18, 21, 23–24, 26, 28, 30–31, 34, 36, 38–39, 41, 43	P Proof 4–5, 8–9, 11, 13, 15–16, 18, 21, 23–24, 26, 28, 30–31, 34, 36, 38–39, 41, 43	R Recovery 3, 5, 7–18, 20–43
R Replay 5, 8, 11, 13, 15, 18, 21, 23, 26, 28, 30, 34–36, 38, 40–41, 43	R Reproducibility 5	R Responsibility 3–18, 20–31, 33–43
R Retention 27–28	R Rights 4, 7–9	R Risk 3–5, 8–9, 11, 13, 15–16, 18, 21, 23–24, 26, 28, 30–31, 34, 36, 38–39, 41, 43
R Rules 4, 8–9, 11, 13, 15–16, 18, 21, 23–24, 26, 28, 30–31, 34, 36, 38–39, 41, 43	S Security 3–4, 7, 9–10, 12, 14, 16–17, 20, 22, 24–25, 27, 29, 31, 33, 35, 37, 39–42	S Service levels 4, 7, 10, 12, 14, 17, 20, 22, 25, 27, 29, 33, 35, 37, 40, 42
S Sources 3–43	S Sovereignty 4–5, 7–8, 10–15, 17–18, 20–23, 25–30, 33–38, 40–43	S State 5–18, 20–31, 33–43
T Testing 3–4, 8–9, 11, 13, 15–16, 18, 21, 23–24, 26, 28, 30–31, 34, 36, 38–39, 41, 43	T Trace 10–11	V Validation 37–39
V Verification 3, 5, 7–18, 20–31, 33–43	V Versioning 4, 7–10, 12, 14, 16–17, 20–22, 24–25, 27, 29, 31, 33–35, 37, 39–40, 42	W Workflows 3

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 an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit. 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: Install from the delivered manifest, observe all data and network paths, run workload and load corpus, rotate keys, remove dependencies, update and roll back, isolate the site, restore clean infrastructure, replay history, migrate a case and packet, and execute supplier-independent continuity.

Have service owner, platform/infrastructure engineering, SRE/operations, security and keys, identity, data/storage, application and source owners, evidence/records, support, procurement and continuity 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	deployment-operations-handbook-decision	
QUESTION	select a deployment posture and understand the infrastructure, responsibility, migration, update, observability, recovery, and continuity consequences.	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 an installed topology and responsibility manifest plus runbooks and tested evidence for service health, updates, failure, clean-room recovery, migration, historical verification and exit.