

The Sovereign AI Operator & Trainer module pack

The four foundations, the trainer module, and the two field steps — the same lessons your workspace teaches.

Personal copy for NGARi Corps members · not for redistribution · verify the programme at ngari.ai/corps

Framework v1.0 · 2026-10-02 · ngari.ai/corps/competencies

Progress in this pack is a snapshot. Your record — the thing that counts — lives at ngari.ai/corps/workspace and is the only thing NGARi verifies.

How this pack works

Each module is a short read followed by one hands-on exercise and a set of questions to answer out loud. There is no quiz and no exam: you read it, you do it on your own node, and you click **Mark done** in your workspace. That click writes a timestamped self-declaration into your own record.

What each level means

LEVEL	WHAT IT MEANS
Foundation	Has completed the module and can explain it.
Practitioner	Has done it on hardware they own, and it is in their record.
Verified	NGARi has verified it against the system of record.

Only **Verified** requires NGARi to issue something, and that is deliberate: you cannot mark it for yourself. It is also only reachable on Pathway B, which carries the teaching step.

Who this pack is for

ROLE	REQUIRES
NGARi Node Maintainer	4 competencies at the levels listed on ngari.ai/corps/competencies
Certified Sovereign AI Operator	5 competencies at the levels listed on ngari.ai/corps/competencies · CSAO
Certified Sovereign AI Trainer	6 competencies at the levels listed on ngari.ai/corps/competencies · CSSA
Community Deployment Lead	5 competencies at the levels listed on ngari.ai/corps/competencies

Contents

- | | |
|--|--|
| 1 Module 1 · Sovereign foundations | 5 Module 5 · Teach it |
| 2 Module 2 · Run your own stack | F1 Stand up your first community deployment |
| 3 Module 3 · The data conversation | F2 Enroll your first learner cohort |
| 4 Module 4 · Price and support a local deployment | |

Personal copy for NGARi Corps members · not for redistribution · verify the programme at ngari.ai/corps

MODULE 1

Module 1 · Sovereign foundations

20 minutes to read · Pathway B, Certified Sovereign Systems Architect / Trainer

By the end of this module you can: Explain local-first in your own words, and tell the difference between an air-gapped node and a dedicated tenant.

The three questions that decide sovereignty

Where does the model run, where does the data go, and who can switch it off? Cloud answers all three the same way: somebody else's building, somebody else's terms, somebody else's switch. Local-first changes the first two. The third is a contract question, and you should ask it out loud before you sell anything.

The box you own

NGARi+ appliances are Jetson-class machines that sit on the same desk as the data. The Nano (~\$999) runs one small queue; the Orin (~\$4,999) is the box NGARi itself serves on and the right first node to learn on; the Thor (~\$8,999) is the fleet box for several sites. Every one of them runs the model locally — no API call leaves the room. All three can be reserved in installments at the list price, 0% interest.

Air-gapped node is not the same claim as dedicated tenant

The node has no cloud egress: nothing you type leaves the machine. Separately, a tenant may share the model runtime with other members on that same node, which means a large run by someone else can make you wait. Both facts are on your workspace page, in their own words, because "air-gapped" on its own invites you to assume the stronger of the two.

What “tamper-evident” actually buys you

Each entry in the audit log carries the hash of the entry before it, so a chained action cannot be quietly edited: change one line of an old record and the chain stops matching at exactly that entry. That is the whole trick, and it is enough — you are not claiming nobody can touch the file, you are claiming nobody can touch it unnoticed. Whether a given node is writing that log right now is a fact about that node, not about the design, so check it rather than assert it: the trust surface says which of the two you have.

Do this on your own node

Open the “Tamper-evident audit trail” section on this page — it sits below your pathway, in the Tenant card — and read one entry out loud: what does it prove to a client? If it is empty, run a prompt in the box above first; the run is what writes the entry.

Answer these out loud before you mark it done

1. Where does the model run, and where does the prompt go?
2. What is the difference between “the node is air-gapped” and “this tenant has the box to itself”?
3. If someone edited yesterday's audit line, how would you know?

That is the whole test. When you can answer those, click **Mark done** in your workspace. Nobody grades it and there is no quiz: your click is a timestamped self-declaration in your own record, and you can undo it.

Go deeper: Your audit trail (on this page) ([#w-audit-section](#)) · The three appliances and their prices ([/hardware.html](#)) · Corps programme and FAQ ([/corps/#faq](#))

Personal copy for NGARi Corps members · not for redistribution · verify the programme at [ngari.ai/corps](#) · NGARi Corps competency framework v1.0

MODULE 2

Module 2 · Run your own stack

30 minutes to read · Pathway B, Certified Sovereign Systems Architect / Trainer

By the end of this module you can: Run a prompt on your own tenant, find the audit entry it wrote, and explain what the meter is counting.

A metered, audited call — not a demo

The Run box on this page posts to your own tenant, on this node. It is metered (you have a monthly request allowance, shown under the box) and audited (the call is written to the chain with the model, the timing and a hash of the result). That is the difference between showing someone a chatbot and showing them a system.

Cold load versus resident

The first call after a model has been idle pays a load cost — the weights come off disk into memory. Use Preload before a long prompt or a demo so the first thing your audience sees is not a spinner. The reply footnote tells you which it was: warm, or cold with the load time.

Read the entry, don't trust the claim

After your first run there is a new line in the audit trail. Find it. It records what was asked, which model answered, how long it took and a SHA-256 of the response — not the response itself. That distinction matters: the log proves the work happened without becoming a second copy of the client's data.

Do this on your own node

Click one of the suggested prompts below, run it, then locate its entry in your audit trail and note the model and the hash.

Answer these out loud before you mark it done

1. Which model answered you, and was it warm or a cold load?
2. What does the audit entry store, and what does it deliberately not store?
3. What exactly does one request cost you against your allowance?

That is the whole test. When you can answer those, click **Mark done** in your workspace. Nobody grades it and there is no quiz: your click is a timestamped self-declaration in your own record, and you can undo it.

Go deeper: Your run box (#w-run) · Your audit trail (#w-audit)

Personal copy for NGARi Corps members · not for redistribution · verify the programme at ngari.ai/corps · NGARi Corps competency framework v1.0

MODULE 3

Module 3 · The data conversation

25 minutes to read · Pathway B, Certified Sovereign Systems Architect / Trainer

By the end of this module you can: Answer “we can't put our data in the cloud” with a demonstration instead of a promise — and know what you must not claim.

The objection is usually about one document

Almost nobody means “all data, everywhere”. They mean the client list, the patient notes, the bid, the payroll file. Find the one document in the room that would end the business if it leaked, and design the answer around that. Vague privacy talk loses to a specific file.

Show it, don't say it

Put the box on the table. Type their sentence into it with the network cable out. Then open the audit trail and let them read the entry. You are not asking them to believe a claim about your infrastructure; you are letting them watch a machine do the work with nothing plugged in.

What you must not claim

“Unhackable” is false and one incident ends your credibility. “HIPAA compliant”, “GDPR compliant”, “SOC 2” are legal positions about a specific deployment, not features of a box — do not say them unless the paperwork for that client exists. Claim what you can demonstrate: the data stayed here, and here is the log.

The second-computer objection

Someone will say they already do this by keeping a second computer off the network. That is real, and you should say so. What it is missing is the record: a second computer cannot show a client, an auditor or a funder what was run and that nobody edited it afterwards.

Do this on your own node

Write the four-sentence version of this answer for one named client, then run the “Answer the data-privacy objection” prompt below and compare what you get against yours.

Answer these out loud before you mark it done

1. What is the single document this client actually cares about?
2. What will you put on the table in front of them?
3. Which three words are you never going to say?

That is the whole test. When you can answer those, click **Mark done** in your workspace. Nobody grades it and there is no quiz: your click is a timestamped self-declaration in your own record, and you can undo it.

Go deeper: Corps programme and FAQ (</corps/#faq>)

Personal copy for NGARi Corps members · not for redistribution · verify the programme at ngari.ai/corps · NGARi Corps competency framework v1.0

MODULE 4

Module 4 · Price and support a local deployment

30 minutes to read · Pathway B, Certified Sovereign Systems Architect / Trainer

By the end of this module you can: Scope, price and support a small on-prem deployment without giving the maintenance away.

Discovery questions that decide the price

Who actually uses it, what breaks when it stops, who is on call at 9pm, and what does an hour of downtime cost them? The answers set the support tier. A café that prints a queue ticket is not the same risk as a clinic, and pricing them the same is how you end up carrying someone else's outage.

Three costs, not one

The hardware at list price, your one-off time to install and tune it, and the ongoing maintenance hours. Novices price the first two and discover the third at their own expense. Put a number on the maintenance line even when it is small — a free maintenance promise is a promise you will eventually break.

Anchor against the published ladder

NGARi's own prices are public and you should quote them instead of inventing your own: the appliances at list, the Deliverable Sprint at \$149 for a scoped piece of work, Practitioner at \$49/mo, Extended Support at \$149/mo. Being consistent with the ladder is what makes a regional trainer's pricing credible next to the company that trained them.

What maintenance actually is

Patch the runtime, watch the disk, rotate keys, keep the backups restorable, and answer the phone. Write down the response time and the included hours. Everything past the included hours is billable, and saying that on page one prevents the argument on month three.

Do this on your own node

Price a twelve-month café pilot on one page: hardware, install, monthly support, and one sentence on what is excluded.

Answer these out loud before you mark it done

1. What does an hour of downtime cost this client?
2. How many support hours are included, and what happens after them?
3. Which published NGARi price are you anchoring each line to?

That is the whole test. When you can answer those, click **Mark done** in your workspace. Nobody grades it and there is no quiz: your click is a timestamped self-declaration in your own record, and you can undo it.

Go deeper: The appliances and installment plans (</hardware.html#installments>) · Corps tiers (</corps/#tiers>)

Personal copy for NGARi Corps members · not for redistribution · verify the programme at ngari.ai/corps · NGARi Corps competency framework v1.0

MODULE 5

Module 5 · Teach it

40 minutes to read · Pathway B, Certified Sovereign Systems Architect / Trainer

By the end of this module you can: Turn the four foundations into a cohort you can run, assess and repeat.

Shape before content

Six to eight learners, four sessions, one artifact each. Small enough that everybody touches the hardware every session, large enough that they argue with each other. A cohort that watches a screen is a webinar, and a webinar does not produce operators.

The assessment is already written

The self-check questions at the end of modules 1 to 4 are the assessment. Ask them out loud, one learner at a time, and let the learner answer in their own words. If they can explain the audit chain and the air-gap distinction to you, they can explain it to a client — which is the actual job.

Teach on the metal

Every session runs on a real node with the network cable out at least once. The moment a learner sees the model answer with nothing plugged in is the moment they stop taking your word for it. Budget for the load time; use Preload so the demonstration is not a wait.

The credential is not yours to issue

CSAO and CSSA are issued by NGARi against the system of record once the foundations are complete. You cannot mark that step done for yourself, and neither can a learner. That is deliberate: it is what makes the credential worth something to the third party who is going to read it.

Do this on your own node

Outline your first cohort: dates, who is in it, the artifact each learner ships, and how you will assess them.

Answer these out loud before you mark it done

1. How many learners, how many sessions, and what does each one ship?
2. How will you know a learner can explain the audit chain?
3. Who issues the credential, and what has to be true first?

That is the whole test. When you can answer those, click **Mark done** in your workspace. Nobody grades it and there is no quiz: your click is a timestamped self-declaration in your own record, and you can undo it.

Go deeper: Corps credentials (</corps/#credentials>) · Corps programme (</corps/#program>)

Personal copy for NGARi Corps members · not for redistribution · verify the programme at ngari.ai/corps · NGARi Corps competency framework v1.0

FIELD STEP

Stand up your first community deployment

By the end of this step you can: Stand up one real site on your own hardware.

What counts as done

One named site, on hardware you own, being used by at least one person who is not you. A pilot that only you have touched is a rehearsal, not a deployment.

The install day

Site survey first: power, network, physical space, who signs off. Then flash and configure, join it to your own pool, run the load test, and walk the owner through the audit trail before you leave. Take a backup of the configuration before you drive home.

Do this

Write down the site, the day, and the name of the person who will be using it after you leave.

Before you mark this done

1. Who uses it daily, and do they know how to reach you?
2. Where is the configuration backup, and have you restored one?

Personal copy for NGARi Corps members · not for redistribution · verify the programme at ngari.ai/corps

FIELD STEP

Enroll your first learner cohort

By the end of this step you can: Run your first cohort of the four foundations.

What counts as done

A scheduled cohort that has met at least once, with an assessment plan you have written down. Enrolling is the step; the credential for the learners follows the same NGARi assessment as yours.

Use the modules you already passed

Modules 1 to 4, in order, with the check questions as the assessment. Do not invent new material for the first run — teach the pathway you were trained on, and improve it in the second cohort.

Do this

Put the first session in a calendar and invite the learners.

Before you mark this done

1. When is session one, and who is coming?
2. How will you assess each learner, and against what?

Personal copy for NGARi Corps members · not for redistribution · verify the programme at ngari.ai/corps

Your copy

Personal copy for NGARi Corps members · not for redistribution · verify the programme at ngari.ai/corps

Issued 11 October 2026 from the NGARi Corps competency framework v1.0.

What actually proves your work is not this file. It is your record: the modules you have marked, the metered calls your tenant has run, the appliance you own, and — at Verified — the credential NGARi signs against the system of record.

Open your record at **ngari.ai/corps/workspace**.

Questions or a correction: **corps@ngari.ai**.

Personal copy for NGARi Corps members · not for redistribution · verify the programme at ngari.ai/corps