RENCORE GOVERNANCE · DEPLOYMENT PLAN

The first ninety days

What governing your AI estate involves, phase by phase, including the work on your side. Written for the team that will run it.

DAYS 1 TO 30

You know what exists

A list of every agent, app, and workspace in the estate, each with an owner and what it can reach.

DAYS 31 TO 60

The worst exposure is closed

The highest-risk sharing and ownership problems are fixed, with the first policies enforcing rather than reporting.

DAYS 61 TO 90

It runs without you

Policies run on a schedule, reporting is automated, and audit evidence is produced on demand.

At this stage the question is rarely whether AI governance matters. It is whether this becomes another project the team does not have the people for.

So this document is a plan rather than an argument. Each phase names what you get rather than what happens, and who you need from your side to get it. Nothing here assumes a change freeze, a migration, or a rebuild of your tenant.

The sequence matters more than the dates. Inventory comes first because every control after it applies only to what you can see. Remediation comes second because fixing what you have found is what makes the inventory worth keeping. Continuous governance comes third because by then there is something worth protecting from drift.

The ninety days is a shape, not a commitment. How long each phase takes depends on the size of your tenant and how much governance you are introducing, so the dates are agreed with Customer Success rather than fixed here. If you have already run a Proof of Value in your own tenant, much of the first phase is behind you and the plan starts further in.

Days 1 to 30 Inventory

Connection takes hours rather than weeks, and no Global Admin rights are required. The first scan returns the estate as it actually is, which is usually larger than expected: the agents nobody registered, the sites nobody archived, the licenses nobody reclaimed.

Most teams find their first real surprise in this phase. It is normally an agent built by someone who has since left, still running against the access they had.

WHAT YOU HAVE AT THE END OF IT

OUTPUT	WHAT IT CONTAINS
An agent inventory	Every authored Copilot Studio agent, with its maker, its current owner, its environment, its data connections, and its knowledge sources. SharePoint agents appear at site and approval-status level: which sites hold agents, which are approved, which are not.
An ownerless list	Agents, sites, and workspaces with no active owner, including those built by people who have left the organization.
An exposure report	Where sensitive content is reachable: widely shared and anonymously shared assets, open libraries, guest and external access.
A cost view	Microsoft 365 and Microsoft 365 Copilot licenses that are unassigned or attached to disabled users, alongside agent consumption, in one place.
The declarative picture	Agents defined over Microsoft 365 content rather than authored in Copilot Studio, including Agent Builder agents, are governed through the person who created them and the permissions on the content they sit on. There is no separate per-agent registry for this population today, and the phase ends with that stated rather than discovered later.
A baseline	The numbers above, dated, so the next ninety days can be measured against them rather than described.

> WHAT CHANGES FOR END USERS
>
> Nothing. This phase reads the estate. No permissions change, no content moves, and nobody is notified.

Days 31 to 60 Remediation

The inventory produces more findings than anyone wants to act on at once, so this phase is about order. Fix what carries the most exposure, automate the fixes that repeat, and leave the rest on a list with a date against it.

This is also the phase where policy starts enforcing rather than reporting. The difference matters: a policy that reports gives you a longer list each month, and a policy that enforces gives you a shorter one.

WHAT YOU HAVE AT THE END OF IT

OUTPUT	WHAT IT CONTAINS
Owners assigned	A named, active owner against every agent and workspace that had none, or a decision to retire it.
The highest-risk sharing closed	Anonymous and organization-wide links on sensitive content revoked, with expiry applied to what remains.
The first enforcing policies	Typically three to five, taken from the shipped catalog. For agents those are usually Orphaned Copilot Agent Ownership Gap, Unauthenticated Public Agent Security Risk, Confidential Site Referenced in Copilot Agent, and Unused Agent Cleanup Candidate at 90 days. For the estate, external sharing of labeled content and unassigned licenses.
Licenses reclaimed	Seats recovered from disabled users and unassigned licenses, with the saving stated against the baseline.
A remediation record	What was changed, when, by whom, and on whose approval. This is the first piece of audit evidence the program produces.

WHAT CHANGES FOR END USERS

Some people notice this phase, and it is better to say so. Owners of inactive workspaces get a notification before anything is archived. People holding links to content that is about to be restricted are told before the link stops working. New sites follow a naming standard. Nothing is deleted in this phase.

Days 61 to 90 Continuous

Governance that depends on someone running a report lapses the first busy quarter. The work in this phase is to move everything established so far onto a schedule, so the estate stays governed as it grows rather than being cleaned up again next year.

By the end of it, the question an auditor or a security review asks should be answerable from a dashboard rather than from a project.

WHAT YOU HAVE AT THE END OF IT

OUTPUT	WHAT IT CONTAINS
Scheduled policy monitoring	Policies running on a set frequency with automated remediation where it was agreed, and alerts where a human decision is required.
Recurring access reviews	Guest and external access reviewed on a schedule, with workspace owners confirming or removing access themselves.
An AI system register with an evidence trail	What AI systems exist, what they reach, who owns them, and how that changed over time, across the Microsoft AI estate, produced on demand rather than assembled for each audit. The register is the evidence. Mapping it to your own regulatory obligations stays with your compliance team.
A standing cost view	License and agent consumption tracked against the baseline, by department, so spend is attributed rather than estimated.
A named review owner	One person and one frequency, agreed and in a calendar. The cheapest control in the plan and the one most often missed.

WHAT CHANGES FOR END USERS

Workspace owners take on a recurring access review, which takes minutes rather than hours. Provisioning requests go through a Teams app rather than a ticket, which most teams experience as faster than what they had.

Who you need

The objection at this stage is rarely price. It is people. This is who the plan asks for from your side, and what they are actually doing, so your team can judge it against what they already have on.

PHASE	WHO YOU NEED	WHAT THEY DO
Days 1 to 30, inventory	One Microsoft 365 administrator.	Connects the tenant, then reviews the first set of findings with us. The connection itself uses an ordinary user account. Consent to scan is granted per service by an administrator, which is a short, separate step and can be delegated to the owner of each service.
Days 31 to 60, remediation	The same administrator, plus whoever signs off on policy.	Decides what gets fixed first and what the policies enforce. The work on your side is mostly decisions rather than configuration.
Days 61 to 90, continuous	The administrator and the named review owner. Compliance if regulatory reporting is in scope.	Agrees what runs on a schedule, what escalates to a person, and what evidence has to be producible on demand.
After day 90	The review owner.	Runs the recurring review. Workspace owners confirm or remove access on their own areas, which takes each of them minutes.

What this is not

Worth saying plainly, because governance projects have a reputation that this one does not deserve.

Not a migration

Nothing moves. Content stays where it is, in the tenant you already run.

Not a change freeze

People keep building agents, sites, and flows throughout. The point is to see them, not to stop them.

Not a tenant rebuild

No re-architecture of SharePoint, no new information architecture as a precondition.

Not a replacement for Microsoft's controls

Restricted SharePoint Search, Purview, and the Copilot Control System keep doing their jobs. This is the view across them.

Not a Global Admin handover

The connection uses an ordinary user account. Consent is granted per service, so each service owner approves only their own scope.

Not a compliance guarantee

The plan produces evidence and enforces policy. The compliance position stays yours.

WHAT THIS ASSUMES YOU HAVE

Agent coverage sits in the AI & Agents module, which is an optional add-on alongside Digital Workplace. Policy monitoring and governance automation are included from the Professional tier upward, and they are what phases two and three run on. Worth checking against your own subscription before any dates go into a plan.

Using this as a mutual action plan

The phases above are structured so they can be lifted into a joint plan without rewriting. If that is useful, four things turn this document into one.

1. **Put real dates against the three phases.** Start from the date the connection is scheduled rather than from signature.
2. **Name the people.** One administrator, one policy approver, one review owner on your side. The named review owner is the role most often left blank and most often missed later.
3. **Agree what counts as done for each phase.** The output tables are written to be used as acceptance criteria as they stand.
4. **Agree the baseline date.** Everything after day 30 is measured against the numbers the first scan returns, so the baseline is worth recording formally.