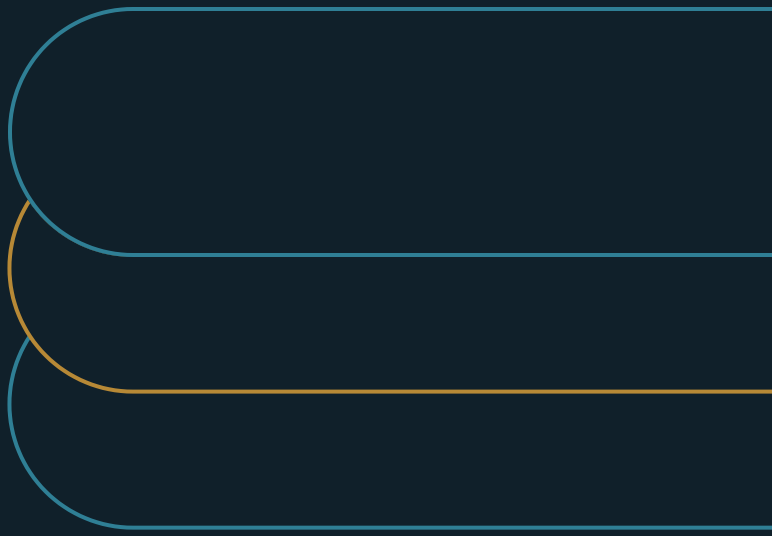
9

WHITE PAPER · PORTFOLIO & AI OPERATING GOVERNANCE

Who Owns Governance?

What the EPMO owns when a big decision crosses several teams



Marco Policani

Enterprise Portfolio · PMO · AI Operating Governance

policani.net · linkedin.com/in/marcpolicani

August 2026

EXECUTIVE SUMMARY

The EPMO owns the framework that ties the decision together: owners, evidence, options, authority, escalation, record, and review triggers.

In a governance meeting, every specialist can sign off within their own domain while the enterprise choice sits undecided. The ownership question gets urgent when those approvals, added up, change the investment. This paper shows how the EPMO owns the framework that ties the decision together, without taking authority from the people who own the standards, the outcome, or the final call.

01 Keep enterprise limits, domain standards, sponsor outcomes, delegated decisions, and independent assurance with their accountable owners.

02 Make the EPMO own the decision framework: who owns what, the required evidence, the portfolio options, the authority, the escalation path, the decision record, and the review triggers.

03 Test governance by whether a skeptical executive can reconstruct the choice and its conditions, not by how many reviews or approvals it collected.

The meeting where everyone says yes

The sponsor asks one question: "Are we approved to proceed?"

Security says yes, as long as the rollout is more tightly controlled. Data governance says yes, but not using customer transcripts the way the plan assumes. Architecture can support the design once one dependency is cleared. Operations can't run the old and new processes side by side for the whole switchover. Finance points out that all of these changes remove the cheaper option and push the payoff date back.

Every team is right about its own area. Add the answers up, though, and you get an investment nobody actually chose. The plan the sponsor walked in with no longer exists. All those approvals put the decision on the table. None of them made it.

That gap is what this paper is about. Every function can do its job well and the enterprise decision can still go ungoverned. Someone has to own the moment where the pieces come together into one choice. In most organizations, no one is clearly assigned to it.

A simple way to picture the missing job

Think about driving. The road authority sets the rules. The car has its limits and safety systems. The driver picks the destination and is responsible for the trip. Navigation pulls the destination, the traffic, the closures, and the possible routes into one view so the driver can choose. It doesn't write the traffic laws, and it doesn't decide where to go. It just makes a responsible choice possible.

That last role is the one missing in the meeting, and it's the one the EPMO should own. It doesn't set the rules. It doesn't own the outcome. It brings the whole picture together so the person with authority can actually decide, and so anyone can see later how the decision was made.

Without that, an organization can finish every review and still leave the real choice ungoverned.

What each team already owns

Start with a plain fact: "governance" is not one job. It is several jobs, held at different levels.

Enterprise leaders set the direction and the limits. They decide how much risk the organization is willing to take in pursuit of value. COSO calls this risk appetite: the types and amount of risk an organization is willing to accept in pursuit of value, then ties that guidance back to real business decisions and measures.[2] Risk appetite doesn't decide any one investment. It draws the boundary a decision has to stay inside.

Domain leaders turn those limits into standards in their own fields. NIST's Cybersecurity Framework, for example, describes the security outcomes to aim for but does not dictate how an organization must achieve them.[3] Security owns its standards and the evidence about controls and risk. Whether the business can live with a leftover risk is usually a separate call, made by someone else under the organization's delegation rules, even when one executive happens to wear both hats.

Portfolio governance does something different again. PMI places portfolio governance in support of the governing body's decisions about investments and priorities.[1] Its job is to help the authorized decision-maker choose what to fund, sequence, change, or stop. The portfolio function needs the domains' evidence, but it doesn't take on their responsibilities.

The IIA's Three Lines Model makes the same point another way. Governing bodies, management, and internal audit each have distinct responsibilities, and their work still has to be coordinated.[5] No company has to copy one org chart. The point is that coordinating the work doesn't merge the ownership.

Put it together and the split is clear. Enterprise leaders set the limits. Domain leaders own their standards and judgments. Sponsors own the outcome. A delegated authority makes the funding and

risk call. Assurance checks that the whole thing works. The open question is what happens when all of these meet around one decision.

The program is green. The approved investment is gone.

Take a familiar case. A sponsor proposes an AI-assisted customer-service platform and wants it live before the next big business cycle. The pitch is good: faster handling, wider coverage, a simpler experience for customers. The money looks available. The delivery plan looks doable.

Then the reviews come back. Security can support it only with a tighter rollout. Data governance says some transcripts can't be used the way the plan assumes. Architecture finds a dependency that changes the order of the work. Operations can't run both the old and new processes across the whole transition. Finance confirms the approved case counted on the cheaper option and the earlier date.

No team failed. Each did its job well. The failure shows up somewhere else: the program keeps reporting these reviews as separate red, amber, and green workstreams while still presenting the original plan as intact. The controls are sound. The architecture call is sound. The funding approval was sound the day it was given. But together, the new conditions describe a different investment, and no one has said so out loud.

Here is where the paper turns. Collecting approvals is not the same as making the decision. The organization doesn't need the EPMO to overrule security, reinterpret the law, waive an architecture standard, or pretend operations has capacity it doesn't. It needs someone to say plainly: the plan we approved no longer works under what we now know.

Once that's on the table, a real decision becomes possible. The sponsor can narrow the goal. The portfolio authority can fund the tighter design, change the order, free up capacity elsewhere, or stop. The right authority might grant a limited, time-boxed exception. Until someone puts the evidence together, none of those choices can be weighed honestly.

NIST's enterprise-risk guidance makes the general case: a common language and shared outcomes let an organization pull risk information together across its units and programs.[4] The EPMO does the same thing for the investment decision. It doesn't add one more expert opinion. It shows the authorized decision-maker how the combined conditions have changed the investment.

Name the decision, then the owner

"Who owns governance?" has no clean answer until the organization names the actual decision. Once the decision is on the table, the ownership sorts itself out.

EXHIBIT 1

Governance ownership separates boundaries, outcomes, and decisions

01	**Boundary owners**	Set the enterprise limits, domain standards, controls, and specialist judgments that apply.
02	**Sponsor**	Owns the intended outcome and the continuing case for the commitment.
03	**Delegated authority**	Chooses within its mandate and changes funding, scope, timing, or risk acceptance.
04	**EPMO decision framework**	Integrates evidence, alternatives, authority, escalation, decision record, and review triggers.

Enterprise leaders own the boundary. They set strategy, risk appetite, capital limits, and the other enterprise conditions. Those limits have to be concrete enough to change a real choice. "Align to strategy" is not a usable boundary. A stated limit on customer-data exposure, capital at risk, or operational disruption is.

Domain leaders own their standards, evidence, and expert judgments. Security decides what control evidence is good enough in its area. Architecture says whether a design meets the standard and what a deviation would cost. Legal reads the obligation. Finance tests the case against the numbers. Operations says what the business can absorb. Their job isn't a generic sign-off. It's to make each condition, and its consequence, clear.

The sponsor owns the outcome and the ongoing case for it. The sponsor is accountable for the result the investment is meant to produce. When new evidence changes the case, the sponsor has to say whether the revised plan is still worth backing. A domain approval can't stand in for that call.

The delegated authority owns the decision within its mandate. That might be a portfolio board, an investment committee, or a product council. In another company it might be an executive team or a single named executive. Whatever the title, it has to be able to change funding or scope, and often timing and residual risk too.

Independent assurance owns its review and challenge. Internal audit, or another assurance function, checks whether governance and controls are designed and working as intended. That's separate from

management's decision, and separate from the EPMO's work to set the decision up.

The EPMO owns the framework that ties the decision together. It names the owners, the evidence required, and the portfolio options on the table. It identifies who decides and who can grant an exception, keeps the escalation path and the decision record, and flags the conditions that would force another look. This is the navigation role: the EPMO makes sure the authorized decision weighs the right evidence and can be reconstructed later. It does not take over the expert judgments or the business outcome.

This split heads off two common failures. In the first, every function can object but no one has to combine the conditions and close the decision. In the second, the sponsor pushes ahead while ownership of an unresolved condition stays fuzzy. A usable framework prevents both by showing who supplies each condition, who owns the outcome, who can authorize the commitment, and who can accept an exception.

The six questions the EPMO answers

The framework can be short. For a decision big enough to cross domains, it has to answer six questions.

EXHIBIT 2

A complete decision connects the outcome to a review trigger

01

Outcome

Name the intended result and the sponsor who owns it.

02

Limits and conditions

Bring the applicable boundaries, current evidence, and consequences into view.

03

Options

Show how each alternative changes the portfolio and the outcome case.

04

Authority

Name the decision authority, exception authority, and escalation process.

05

Review trigger

Record what change, expiry, or failed condition requires another decision.

1. What outcome are we after?

State the outcome and name the sponsor who owns it. Say it in a way that makes the commitment testable. If the outcome depends on a date or a service level, put that in plain view instead of burying it in the business case. Do the same for any operating condition that could sink the case.

2. Which rules and limits apply?

List the enterprise and domain boundaries that could change the choice, and name who owns each one. A link to the full policy library isn't the answer. The record needs the few conditions that actually matter here.

3. What do we know about current conditions?

Ask each domain for decision-relevant evidence in a usable form: the condition, the evidence behind it, and what each option would cost. That keeps an expert review from being flattened into a color or a signature.

4. What options are still open?

Lay out the portfolio choice. What changes if the organization proceeds as planned, narrows the scope, or funds a different design? What follows from a new sequence, a delay, or a stop? This is where the EPMO adds what no single domain can see: the effect on other commitments and on the portfolio as a whole.

5. Who decides, and who can grant an exception?

Name the deciding authority and the escalation path before anyone disagrees. Name the authority that can accept a leftover condition, the evidence it needs, how long the acceptance lasts, and any standing right to stop the work. A meeting that can only review is not the decision point.

6. What would reopen the decision?

Record the decision, its conditions, and what would put it back on the table. New evidence or an expired exception can undo the basis for the call. So can a missed dependency, a big cost change, or lost operating capacity. Governance that can approve a commitment but can't respond when conditions change is only half-built.

Size the framework to the decision. A reversible call inside one domain may need only delegated authority and an ordinary record. A commitment that changes enterprise risk, shared capacity, or the viability of other investments needs the full cross-domain review. The EPMO shouldn't stand up a new committee when an existing forum already has the authority. It should make that forum able to decide.

The real test is whether a skeptical executive can reconstruct the decision. That executive should be able to see the intended outcome, the limits that applied, and what the experts found. Then the record should show the options, who decided, the conditions they accepted, and what would trigger another review. If all the organization can produce is a stack of meetings and status colors, it has activity, not a decision anyone can inspect.

The first conversation to have

A new EPMO leader usually inherits a sentence: "the EPMO owns governance." Push back on it too fast and you sound like you're dodging accountability. Accept it without defining it and you've signed up for decisions you can't competently or lawfully make.

The better opening is to ask questions:

- When you say governance, which decisions do you expect the EPMO to make or prepare?
- Which standards and judgments stay with the specialist domains? Name the functions.
- Who owns the business outcome when those requirements change the case?
- Who can accept an exception or a leftover condition, and under what authority?
- Which forum can change funding, scope, sequence, or timing when the constraints collide?
- What has to be recorded, and what event brings the decision back?

The answers show whether the organization has confused governance with owning controls, with collecting approvals, or with running meetings. They also show where the EPMO can help right away: define the decision framework, surface missing authority, connect domain evidence to portfolio consequences, and make the next decision traceable.

Come back to the sponsor's question: "Are we approved to proceed?" The honest answer isn't a stack of domain approvals. It's the recorded decision an authorized leader made after seeing the conditions and their combined effect on the investment.

The EPMO should own the framework that makes that decision possible. It names the owners and the evidence, frames the options, and names who can decide and who can grant an exception. It keeps the escalation path, the decision record, and the review triggers. It should not claim the domain standards, the sponsor's outcome, or the leader's actual choice. When that line is clear, domain authority gets stronger, the sponsor can't quietly evade accountability, and leaders can inspect and revisit the decisions they make.

That is the part of governance the EPMO owns.

Notes and sources

[1] Project Management Institute, The Standard for Portfolio Management, Third Edition, 2013. https://www.pmi.org/-/media/pmi/documents/public/pdf/certifications/standard-for-portfolio-management-third-edition.pdf?rev=67c367d7cf8f483d8e67f99af78205f7

[2] Frank Martens and Larry Rittenberg, Risk Appetite—Critical to Success, Committee of Sponsoring Organizations of the Treadway Commission, 2020. https://www.coso.org/_files/ugd/3059fc_1607e24e43ad44bf96f725765cb8e78a.pdf

[3] Cherilyn Pascoe, Stephen Quinn, and Karen Scarfone, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, National Institute of Standards and Technology, February 26, 2024. https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20

[4] National Institute of Standards and Technology, NIST Cybersecurity Framework 2.0: Enterprise Risk Management Quick-Start Guide, NIST SP 1303, October 2024. https://csrc.nist.gov/pubs/sp/1303/final

[5] The Institute of Internal Auditors, The IIA's Three Lines Model, July 2020. https://www.theiia.org/globalassets/site/communication/2020/three-lines-model-updated.pdf

About the author

Marco Policani is an enterprise portfolio, PMO, and AI operating-governance leader. He builds portfolio governance systems where AI carries the analytical load and named humans own every decision — an approach documented across case studies, walkthroughs, and working governance guides on his portfolio site.

Portfolio & governance library: policani.net/governance · Full portfolio: policani.net · LinkedIn: linkedin.com/in/marcpolicani