Synechron

WHITEPAPER

From Pressure to Proof: Delivering Measurable Governance Outcomes

A Practical Guide to Outcome-Led IRM Transformation

synechron.com

Authors

Oliver Vistisen

ServiceNow Architect, Synechron

About Synechron:

Synechron is a global technology consulting firm that helps leading organizations accelerate digital transformation through innovation, expertise and agility. With more than 16,500 professionals across around 60 offices in 20 countries, we combine deep industry knowledge with advanced capabilities in such areas as AI, cloud, cybersecurity, and data engineering.

Our regional teams, supported by strategic delivery centers, provide scalable, cost-efficient solutions tailored to local markets. Through our award-winning Synechron FinLabs accelerators and strategic partnerships with AWS, Microsoft, Databricks, Salesforce, and ServiceNow, we enable clients to innovate fast and lead with confidence. For more information on the company, please visit our website or LinkedIn community.

Introduction

There is a pattern that repeats across mature, well-resourced risk and compliance environments: Programs are well funded. Supporting technology is modern. Reporting reaches the board. And yet, when governance is genuinely tested, by a regulator, an auditor or a material incident, the same structural weaknesses surface:

- Ownership is unclear.
- Evidence requires reconstruction.
- Risk, security, and IT tell different stories.
- The response is fast, but the defensibility is fragile.

This paper is not about maturity frameworks or technology roadmaps. It is about a more fundamental question:

Why do organizations with significant investment in governance repeatedly fail to demonstrate defensibility when it matters most?

The answer, in practice, lies not in what organizations have built, but in the principles and sequence in which they have built it, and in the choices (often unspoken) that leadership teams make when governance comes under pressure.

> “Why do organizations with significant investment in governance repeatedly fail to demonstrate defensibility when it matters most?”

1. The Structural Reality

The Confidence That Collapses Under Scrutiny

Most regulated organizations operate with genuine confidence day-to-day.

Risk registers and control libraries are maintained. Both are delegated, owned, assessed and tested. Reporting is regularly produced to a known cycle. Transformation programs are in flight. Continuous improvement is ongoing. If you asked a CRO or CISO whether their function was mature, most would say yes, and by conventional measures, they would not be wrong.

The problem surfaces when that confidence is put to the test.

Not in a controlled workshop or a scheduled audit. Real scrutiny: a regulatory request or material incident, a board challenge during a period of stress. A question that cannot be answered by pointing to the latest report.

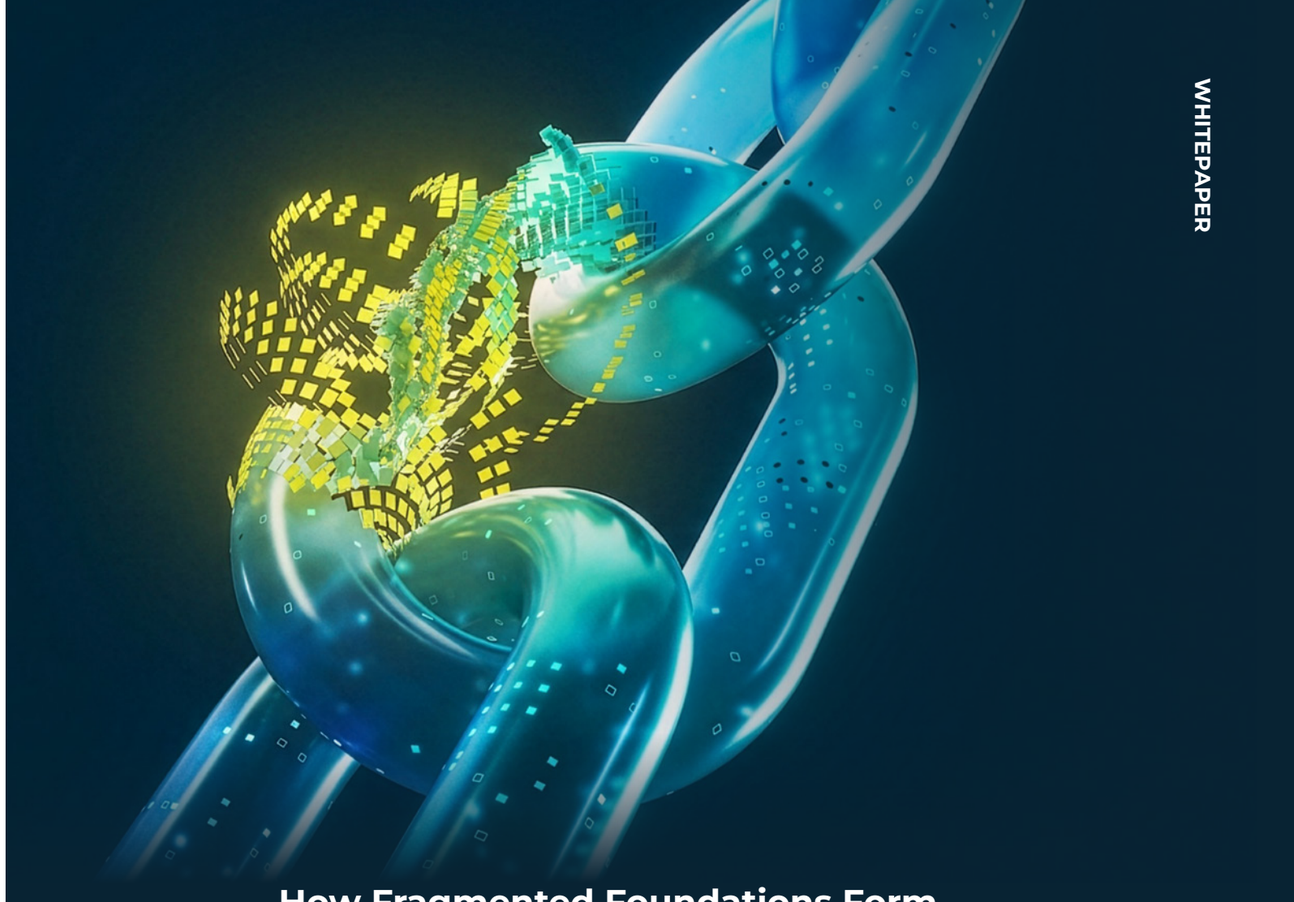
- Can you tell me, right now, who owns this risk end-to-end?
- When was escalation triggered, and was that formally recorded?
- Was risk appetite breached? Was that recognized at the time, not reconstructed afterwards?
- What decision was made, by whom and why?
- How did that influence capital allocation or remediation priority?

These are not unreasonable questions. They are precisely the questions regulators, auditors, and non-executive directors ask when governance is challenged. And the answer, in many organizations that would otherwise describe themselves as mature, requires coordination meetings, narrative alignment and evidence retrieval that can take days rather than minutes.

That gap, between the confidence organizations feel in steady state and the defensibility they can demonstrate under scrutiny, is the central problem this paper addresses.

Being busy is not the same as being defensible and operational maturity is not the same as governance coherence. The distinction matters far more than most transformation programs acknowledge.

> “Can you tell me, right now, who owns this risk end-to-end?”



How Fragmented Foundations Form

Understanding why this gap exists requires going back to how enterprise risk and compliance environments are built.

Most organizations do not set out to create fragmented governance architectures. They evolve into them through entirely rational, locally justified decisions.

A new regulation arrives with a tight implementation deadline or limited scope, so a region stands up its own processes and tooling. An acquisition brings with it a mature but separate control framework and accompanying toolset.
A business unit, frustrated with the pace of the central function or lack of specific functionality, deploys a point solution. An audit team with distinct needs and separate authority selects a different platform. An individual contributor, (once using VBA, now using AI) builds a local workaround that quietly becomes operational infrastructure.

Each decision is defensible in isolation, with each adding capability. Over time the cumulative effect is a control landscape that has expanded horizontally without a unifying architecture underneath.

The result is a risk and assurance environment that functions adequately in steady state but reveals structural inconsistency the moment it needs to speak with one voice.

The most visible symptom is reconciliation. Before an audit, before a regulatory submission, before a board pack, data is exported from multiple systems. Definitions are aligned across teams that have drifted apart. Narratives are negotiated. Risk views are synthesized from sources that do not agree on scope, taxonomy or ownership. Many reading this will have had their own experiences cramming evidence collection immediately prior to annual deadlines.

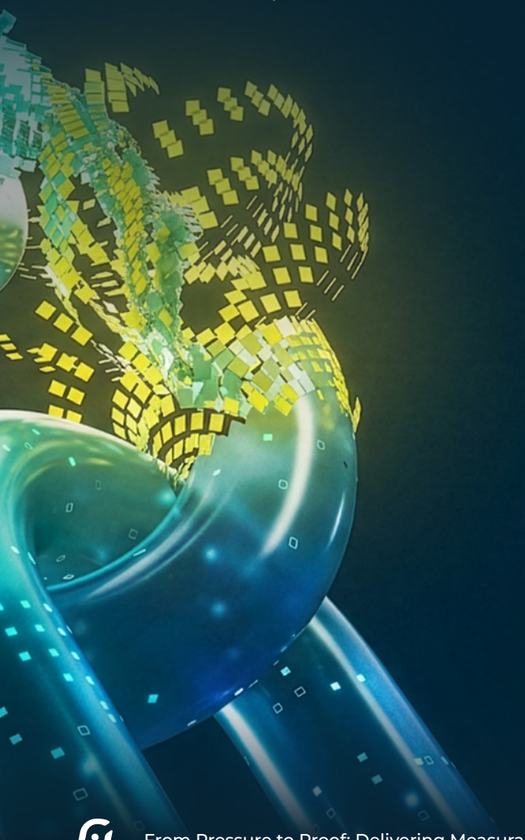
It works. But what it produces is a reconstructed artifact, a single-use, high-effort output that represents what the organization wants to show, rather than an inherent, always-current view of what the organization actually knows.

The difference matters enormously under scrutiny. A foundation that demonstrates inherent consistency behaves differently to one that requires coordination to appear coherent. Auditors recognize this distinction. So do regulators. And increasingly, so do boards.

Repeated audit findings are rarely about the quality of individual controls. They are almost always about structural inconsistency, the same root cause resurfacing because the foundation beneath it has not been addressed.

The real decision organizations face is not whether to improve their documentation or invest in better tooling. It is whether to continue compensating for fragmentation through increasing effort, or to redesign the foundation so that reconciliation becomes unnecessary.

That decision is more consequential than it appears. Because reconciliation effort does not plateau, it compounds. As regulatory scope expands, as business complexity grows, as scrutiny intensifies, the cost of maintaining a fragmented foundation rises year after year. The organizations that address this structurally today are not just improving their audit outcomes, they are preventing a very predictable deterioration in governance confidence over time.



The Latency Problem

The second structural pattern is more insidious, because it hides behind apparent sophistication.

Most mature organizations have no shortage of signals. Security alerts fire continuously. KRI thresholds are breached and reported. Control exceptions are logged. Third-party findings accumulate. Vulnerability backlogs exist, are known and are tracked.

The problem however is the gap between a signal existing and that signal converting into owned, accountable action, preferably before impact, not after.

This gap, call it detection-to-action latency, is where exposure grows quietly.

In many environments, risk indicators are technically live and visible. But escalation still depends on someone interpreting a report, forwarding it to the right person and manually coordinating a response across teams that operate in separate workflows with separate priorities. The signal exists. The pathway from signal to action does not.

The consequence is predictable. Risk sees it. Security detects it. IT owns part of it. No single function owns it end-to-end. And by the time coordination has happened, the issue has escalated. A manageable control failure becomes an incident. An incident becomes a regulatory event.

The uncomfortable question, when that sequence completes, is rarely, “did we detect it?” Rather it is, “why didn’t we act sooner?”

Adding more dashboards and monitoring tools does not solve this. In many cases, it compounds it. More alerts without clearer ownership produces noise, not faster response. Awareness and action are not the same thing, and organizations that invest in improving the former without addressing the latter consistently find that their governance posture under pressure does not improve in proportion to their monitoring capability.

The structural fix requires deliberately designing three things:

1. Ownership clarity at the point where a signal is generated.
2. Threshold logic that triggers escalation without manual interpretation.
3. Workflow integration that connects the signal to the right team with the right authority.

Without all three, latency persists, and under regulatory scrutiny, “we responded to it” is not the same as “we managed it.”

> “Why didn’t we act sooner?”

1. The Structural Reality

Fragmenting Under Pressure

The third structural pattern becomes visible during incidents, and it is the one that most directly undermines executive and regulatory confidence.

Consider a realistic scenario. A significant cyber or operational event occurs. The technical response is strong. Systems are restored quickly. The right teams are mobilized. Containment is achieved within acceptable timeframes.

Then the second phase begins.

Regulators request the decision trail. Second line asks for linkages between the incident, the relevant risks and the controls that should have prevented it. Internal audit asks for evidence. The board asks how the event aligned to risk appetite, and whether appetite was formally breached. Executives ask who made which decisions, and when.

At that point, often within 48–72 hours of an incident that was operationally handled well, the fragmentation between risk, security and IT surfaces.

Security has closed its tickets. IT has documented its recovery activities. Risk is reconstructing the governance narrative from sources that were not connected during the event itself. Assurance is chasing documentation across functions that have already moved on.

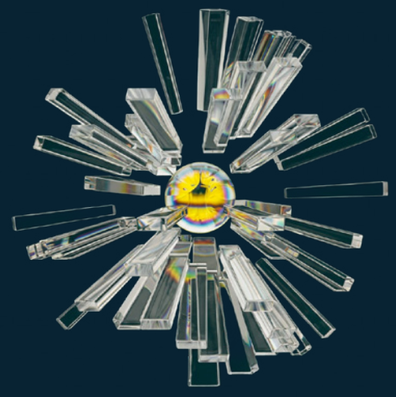
> “Containment is achieved within acceptable timeframes.”

Each team did its job, but they did not do it together. The result is an organization that responded impressively at an operational level, but cannot demonstrate coherent governance of that response after-the-fact.

This is not a problem with those involved. The individuals are typically capable and experienced. It is an operating model problem where risk, security, and IT have optimized their respective functions locally. Integration across those functions was assumed rather than designed. When pressure exposes the seams and reveals that teams still operate in silos, the consequence is not operational failure, it is governance failure. Even enterprise platform-level tooling suffers from this problem, with workflows and records siloed within their respective function despite being on the same system (a subject often covered by Michael Rasmussen himself).

The board’s confidence in how the organization manages risk is not formed during BAU. It is formed during exactly these moments, when something goes wrong and leadership asks: can we account for our decisions? Can we demonstrate, with evidence, that we governed this as we said we would?

If the answer requires a week of reconstruction, that confidence erodes. And once it erodes, it rarely recovers through process documentation or governance committees. It recovers through structural change.



> “The result is an organization that responded impressively at an operational level, but cannot demonstrate coherent governance of that response after-the-fact.”

1. The Structural Reality

The Forced Decision

We’re identified three structural patterns so far:

A.
Fragmented, non-defensible foundations

B.
Delayed detection and response

C.
Disconnected operating models

None of these are new problems. Every CRO, CISO and Head of Audit reading this will recognize at least one of them. Many will recognize all three.

What is interesting, and unfortunately typical, is what usually happens next.

Most organizations do not make a deliberate strategic decision when they encounter these patterns. They optimize around them. More documentation, better dashboards, another reporting layer, an additional governance committee, a new use case for an existing platform. Occasionally, a transformation programme that improves workflow activity without addressing the structural condition underneath.

It feels like progress. Sometimes, it is. But beneath that activity, there is usually an unspoken choice being made, and it is one of the most consequential choices in enterprise governance.

Continue compensating for structural fragmentation through increasing effort or redesign the operating model around defensibility.

> “Here’s the lesson: determinism isn’t binary. You don’t need perfect repeatability for every output.”

These are not the same thing.

The first path adds workload, complexity and cost. It produces better-looking outputs from a foundation that has not fundamentally changed. The second path reduces ambiguity, shortens decision latency and builds governance that behaves coherently under pressure beyond just the steady state.

The distinction between the two paths is rarely framed clearly at the executive level. Instead, transformation is incremental and continuous, and no one says explicitly: we are choosing to tolerate structural reconciliation for the next three years. But, that is often precisely what is happening.

Doing nothing is still a decision. Optimizing locally is still a decision. The question is not whether leadership is making these choices, they are. The question is whether they are making them deliberately, with full visibility of the consequences, or whether those choices are being made by default through accumulated inertia.

The organizations that move beyond this inflection point, that choose structural redesign over continued optimization, share one characteristic: they start with outcomes.

2. The Outcome Commitment Model

Outcome Anchors

There is a question that almost every governance transformation programme asks at the outset: What functionality do we need?

It is a reasonable question. But it is entirely the wrong starting point.

When organisations begin with capability, they make an implicit assumption that more functionality, better tooling, and greater automation will produce better governance. In practice, this assumption fails regularly and expensively.

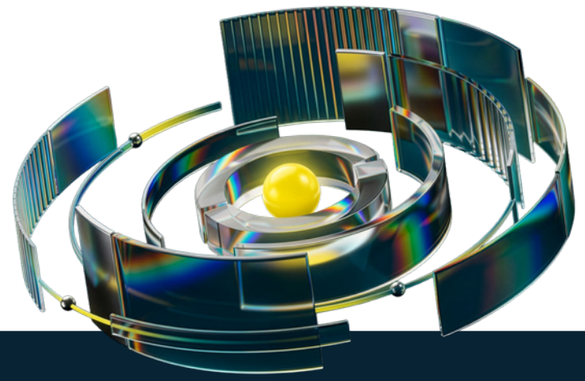
Organisations can have modern, well-configured platforms. Extensive control libraries. Sophisticated analytics. AI-assisted monitoring. And still be unable to answer a clear Board question with confidence, still struggle to demonstrate defensibility under regulatory scrutiny, still find that incidents expose the same governance gaps they have been trying to close for years.

The reason is structural. Capability expansion without outcome definition produces horizontal growth. Platforms extend across more use cases, more domains, more process steps. The system of record gets larger. The data model gets more complex. The reporting surface area grows. But the question of what specific, measurable, executive-level outcomes are being delivered, and whether governance is getting demonstrably better against those outcomes, often goes unanswered.

Technology, in this pattern, becomes documentation and reporting infrastructure. It captures what has happened and surfaces it. It does not change the operating logic underneath.

The shift that makes the critical difference is simple to describe and genuinely difficult to execute.

Define the outcomes first. Not operational KPIs nor system metrics. Executive-level commitments about what governance will demonstrably deliver, expressed in language that regulators, auditors, and boards recognise as meaningful.



In Practice

Outcome commitment is a governance discipline, and it is the organising principle that everything else follows from.

The outcomes that matter most, in the context of the structural patterns described in Act I, can be grouped into four categories:

1.

Decisions without reconstruction – The organisation can answer, at any moment, who owns a given risk, what the current status is, and whether it falls within appetite, without coordination meetings or evidence reconstruction. The time required to produce a defensible account of a decision drops from days to minutes.

2.

Escalation by design, not by negotiation – When a threshold is breached, when a control fails, when an incident occurs, accountability is not negotiated after the fact. It is built into the architecture of how work flows across the first, second, and third lines-of-defence. Escalation is triggered automatically. Governance and operational response happen simultaneously, not sequentially.

3.

Risk stated in capital language – Risk information reaches executives and boards in terms they can act on. Not control percentages or KRI heat maps. Financially meaningful language. Impact on capital, on operational continuity, on regulatory standing. The translation layer between technical risk and strategic decision is removed.

4.

Evidence that exists before it's asked for – The cost, time, and stress involved in responding to regulatory requests falls materially, not because more people are working on it, but because the evidence is always current, always consistent, and always retrievable without reconstruction.

These commitments are specific enough to be measured, honest enough to be challenged, and meaningful enough that the regulator, auditor, or board member hearing them can judge whether they have been delivered.

The discipline of committing to outcomes like these before expanding capability has a significant effect on how architecture decisions get made. If the outcome is "reduce time-to-decision under pressure," then workflow design, escalation logic, and threshold configuration are evaluated against that specific test. If the outcome is "shorten regulatory response cycles to zero," then data architecture, audit trail design, and cross-functional integration are oriented around what that capability actually requires.

Technology becomes enforcement infrastructure, the mechanism through which outcome commitments are made durable and verifiable, rather than a reporting layer over an operating model that has not fundamentally changed.

2. The Outcome Commitment Model

Sequencing

Perhaps the most underestimated element of the outcome commitment model is sequence.

Most governance transformation programmes run in the opposite direction to what is described here. They begin with a platform assessment, or a maturity review, or a business case for a specific technology capability. The outcome (improved governance, better audit results, faster regulatory response) is implied rather than defined. And when those outcomes fail to materialize, the diagnosis is usually, “not enough has been implemented yet,” which produces another phase of expansion.

The outcome commitment model reverses this sequence deliberately.

Outcomes are defined and committed to before any capability decision is made. This is not comfortable. It requires leadership teams to make specific, measurable promises about what governance transformation will deliver, and to be held to those promises.

But the discipline of that commitment changes everything downstream.

It forces clarity about what “better” actually means. It creates a shared definition of success across functions that typically disagree about what governance is for. It allows every capability decision, every platform configuration, every workflow design, every integration, to be evaluated against the question: does this move us toward the committed outcome, or does it move us away from it?

Without that anchor, platforms expand. Complexity increases. Activity rises. Outcomes remain elusive.

With it, governance architecture sharpens. Investment is concentrated where it creates the most measurable impact. The organization builds a coherent capability, not an accumulation of features.

This distinction, between activity maturity and defensibility, is the difference between governance that looks impressive on paper and governance that holds up when it actually matters.

> “These aren’t technical problems but rather governance challenges.”

Technology as Enforcement Architecture

A note on technology, because it is where most organizations start and where most transformation programs falter.

Technology is not neutral in this model. Used correctly, it is the mechanism through which outcome commitments are made verifiable and durable. Used incorrectly, as the starting point rather than the conclusion, it amplifies the structural problems it was intended to solve.

When organizations lead with platform configuration, they are making an implicit bet: that the technology will impose structure and discipline on operating models that have not been deliberately designed. That bet rarely pays off. What happens instead is that the technology inherits the fragmentation of the environment it was deployed into. Data models reflect existing silos. Workflow logic mirrors existing process fragmentation. Reporting surfaces what the data supports, not what leadership actually needs to know.

The platform ends up as an expensive, sophisticated layer on top of an operating model that has not changed.

The alternative is to treat technology as enforcement architecture. This means designing the operating model, ownership, escalation logic, accountability structures and evidence standards before deciding how technology supports and enforces it. The platform is configured against a designed operating model, not in place of one.

This approach produces something qualitatively different: a system in which the commitments made earlier (ownership clarity, decision speed, regulatory defensibility) are built into the architecture of how work happens. Not documented as aspirations, rather enforced as operational reality.

Platforms such as ServiceNow are powerful enablers of this model, but they are just enablers. The strategic logic, the outcome commitments and the operating model design must come first. Technology works when it is applied in support of outcomes. It undermines outcomes when it is treated as the strategy itself.

3. The Implementation Pathway

Four Stages That Compound Over Time

The transition from the structural patterns described in part one to the outcome-led model described in part two does not happen in a single transformation program. It happens in stages, and the most important characteristic of those stages is that they are designed to compound value over time, not to deliver a point-in-time improvement that plateaus.

The pathway has four stages. They are not purely sequential. In practice, organizations run them in parallel across different domains and at different speeds. But the logic of each stage depends on what precedes it.

Stage One: Outcome Definition

Before any capability work begins, leadership commits to a small number of specific, measurable governance outcomes. The criteria for a well-formed outcome commitment are:

1. It must be expressed in language meaningful to regulators, auditors or boards, not in technology or operational terms.
2. It must be measurable, with a baseline and a defined improvement target.
3. It must be honest about the current state: an organization that cannot currently answer a regulatory question in under 48 hours should state that, not obscure it.

This is the hardest stage because the commitment needs to be real, not just a token statement. Most organizations can describe what better governance looks like in the abstract. Fewer are willing to commit publicly to what they will deliver, by when and how they will evidence it.

The organizations that complete this stage well establish a durable foundation for everything that follows. The ones that skip it, or treat it as a planning formality, tend to find that later stages of transformation drift back toward capability expansion without direction.

> “Fewer are willing to commit publicly to what they will deliver, by when and how they will evidence it.”

Stage Two: Decision Mapping

With outcome commitments established, the next stage maps the decision flows that must change in order to deliver them.

This is not a process documentation exercise. It is an architectural exercise. The question at every step is: where does a decision about risk, a control failure, an escalation, where does that decision currently get made? And who owns it? Where should it be made, and by whom, in order to deliver the committed outcome?

This mapping typically reveals three things. It reveals where ownership is genuinely ambiguous, as opposed to where it is merely undocumented. It reveals where the current workflow requires manual coordination that could and should be replaced by automated escalation. And it reveals where the integration between risk, security, and IT is designed versus assumed.

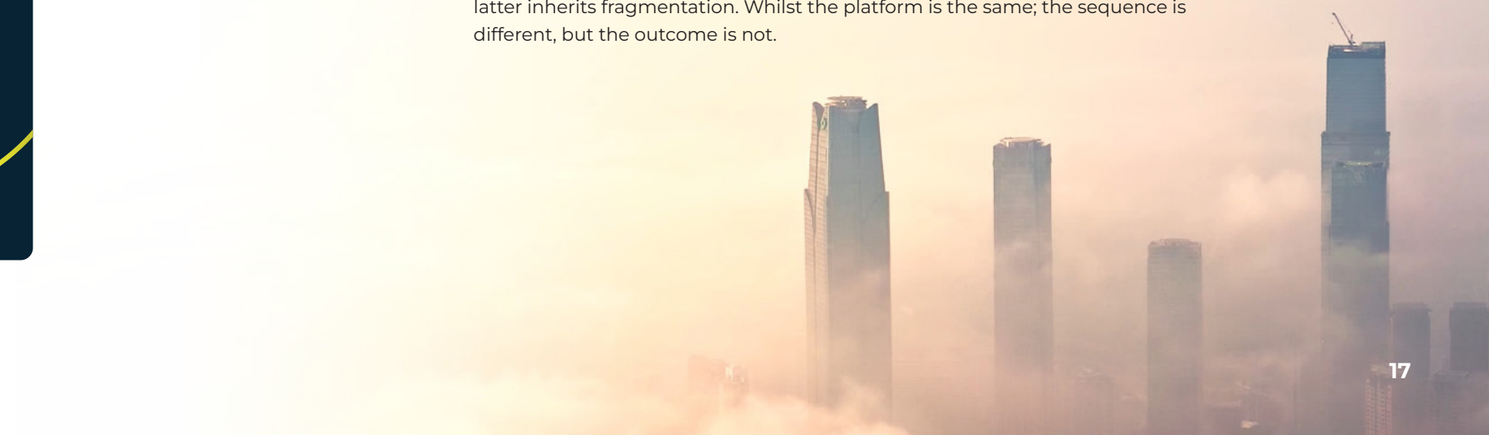
Decision mapping is the design work that precedes architectural alignment. Without it, platform configuration decisions are made in a vacuum.

Stage Three: Architectural Alignment

With decision flows designed, the technology architecture is aligned to support and enforce them.

This stage includes platform configuration, workflow design, data model alignment and integration work across the functions that must operate coherently. The critical discipline at this stage is scope constraint. Architectural alignment work should be prioritized against the outcome commitments established in Stage One. If a capability decision does not demonstrably move the organization toward a committed outcome, it is deferred.

This is where technology platforms, configured correctly against a designed operating model and with defined outcomes, deliver their real value. The distinction the market is increasingly drawing is not between platforms, but between implementation approaches. A platform configured in support of a designed operating model, with outcome commitments already defined and decision flows already mapped, behaves architecturally differently to the same platform deployed as the strategy itself. The former enforces coherence, the latter inherits fragmentation. Whilst the platform is the same; the sequence is different, but the outcome is not.



3. The Implementation Pathway

Stage Four: Instrumented Success

The final stage, and the one most consistently omitted, is the design of the measurement framework that makes outcome delivery verifiable.

Each committed outcome should have a corresponding set of metrics that track progress against it from the point of implementation. These metrics should be distinct from operational activity measures. They should answer the question: is governance getting demonstrably better against what we committed to, and can we evidence that improvement to the regulator, auditor or board?

This stage also produces the artifacts that close the loop with external stakeholders: regulatory responses supported by always-current evidence, audit submissions that do not require reconstruction and board reporting that translates risk into financially meaningful, decision-useful language.

The measurement framework is also what makes the value of transformation defensible in its own right, which matters in environments where governance investment is under pressure and the case for continued commitment needs to be made clearly and regularly.

> “Here’s the lesson: determinism isn’t binary. You don’t need perfect repeatability for every output.”

What Changes, and When

The staged pathway described above does not deliver all its value immediately. Different outcomes mature at different points, and part of the leadership discipline required is understanding what to expect at each stage and communicating that honestly.

In the early stages, the most visible changes are internal. Decision ownership becomes explicit, escalation pathways are documented and tested, workflows begin to operate with less manual coordination and teams that previously operated in silos develop a shared operating rhythm during incidents and regulatory events.

These changes are important but hard to evidence externally. They are the structural improvements that make defensibility possible, but they do not yet produce the measurable, board-level outcomes that were committed to.

In the middle stages, the measurement framework begins to yield data. Time-to-decision under pressure shortens measurably. Response to regulatory requests accelerates. Audit cycle preparation time falls. The reconciliation effort that consumed significant assurance capacity begins to reduce.

These are the changes that make the transformation visible and credible to external stakeholders. They are also the changes that distinguish genuine governance improvement from activity maturity, because they are outcomes, not outputs.

In the mature stages, governance becomes a compounding asset. Foundations that do not require reconciliation. Detection that is genuinely proactive rather than retrospective. An operating model that functions coherently under pressure because it was designed to, not because individuals are compensating for structural gaps.

At this point, the expansion into automation, AI-assisted decisioning and advanced analytics becomes viable, and becomes genuinely value-generating, rather than a capability layer on top of a fragile foundation.

This sequencing is not a limitation. It is the condition under which AI creates real governance value rather than accelerating existing fragmentation. Applied to a coherent foundation, it compounds the outcomes already being delivered. Applied before that foundation exists, it makes a broken operating model faster and more expensive.

The Diagnostic Test

There is a practical test for where an organization currently sits, and it is worth applying before committing to any transformation pathway.

Answer the following questions honestly, as if a regulator asked them today:

- **Who owns this risk, end-to-end?** Not in the abstract, for a specific, material risk that is currently active.
- **When was the last escalation triggered against that risk, and can you show the record of it without retrieving documents from multiple systems?**
- **Was risk appetite breached in the last six months?** If so, when was that formally recognized, at the time, or in retrospect?
- **What decisions were made regarding the risk, its exposure, appetite breach and remedial actions?** Are these clearly recorded with supporting rationale and the decision maker?
- **If your control framework was tested tomorrow by an external auditor, how long would it take to produce a defensible, consistent account of control effectiveness across the first, second and third lines of defense?**
- **If a cyber or operational incident occurred tonight, how long would it take to produce a governance narrative that a regulator could rely on?** Not an operational incident report, but a governance account that traces the decision trail from detection to escalation to resolution.

There are no universally correct answers to these questions. But the amount of coordination, retrieval and reconstruction that each answer requires is an accurate proxy for governance defensibility. The faster, the more immediate, the more inherently consistent the answers are, the closer the organization is to the outcome-led model.

For most organizations, working through these questions honestly produces a clearer picture of the structural work required than any maturity assessment or capability gap analysis. Because they are not questions about what the organisation has. They are questions about what the organisation can demonstrate, which is, ultimately, what governance is for.

> “Who owns this risk, end-to-end? Not in the abstract, for a specific, material risk that is currently active.”

5. Conclusion

This paper can be distilled to a single observation: **Defensibility is demonstrated, not declared.**

Governance is not tested in steady state. It is tested under pressure, by a regulator who wants answers, an auditor who finds inconsistencies and a board that loses confidence during a material event. The organizations that demonstrate defensibility in those moments are not necessarily the ones with the largest programs, the most modern platforms or the most extensive control libraries.

They are the ones who build governance around a clear answer to a simple question: **What will we commit to delivering, and how will we evidence it?**

The three structural patterns described in part one: fragmented foundations, delayed detection and disconnected operating models are not new. They are persistent because the conventional response to them is to add capability, add activity and optimize locally rather than to address the operating logic underneath.

The outcome commitment model described in part two does not require organizations to abandon what they have built. It requires them to sequence what comes next differently, starting with what they will deliver rather than what they will deploy.

And the implementation pathway in part three provides the structure to make that commitment real: defining outcomes before expanding capability, designing decision flows before configuring platforms and measuring what matters rather than what is easy to count.

The organizations that take this path do not just improve their audit results or reduce their regulatory exposure in the near term.

They build:

- Governance that compounds.
- Foundations that grow more coherent over time.
- Detection that becomes more proactive.
- Operating models that function with greater integrity under each successive challenge.

Defensibility is not declared in a governance framework or a board paper. It is demonstrated in the quality of the decisions made under pressure, in the coherence of the evidence available when it is needed and in the confidence of the executives, auditors and regulators who rely on it.

The question is not whether your governance would withstand scrutiny today. Ask whether you are building governance that will demonstrate it reliably, today and in every stress test that follows.

Next Steps

Interested in exploring what outcome commitment looks like applied to your specific governance environment? The conversation starts with three questions:

1. What would you measure publicly? And how would you report it?
2. What would you commit to improving within 12 months? And what does that baseline look like today?
3. What would have to change in your operating model for that commitment to be credible? And are you willing to say so explicitly?

Contact us:

Synechron Limited, 95 Gresham Street,
London - EC2V 7NA, United Kingdom

enquiries@synechron.com

synechron.com