The Decision Architecture Diagnostic

20 Questions That Reveal Whether Your Organisation Actually Decides. Or Just Discusses.

For Board Members, C-Suite Executives, and Senior Risk Leaders who suspect the gap is bigger than the reports suggest.

I once sat in a board risk session where three executives presented the same cyber incident using three completely different risk classifications. One called it operational. One called it reputational. One called it a technology event. They were describing the same breach.

Nobody in the room flagged the contradiction.

That's not a data problem. That's an architecture problem. And it's more common than most board realise.

This diagnostic exists because most organisations assess risk management by measuring process activity. Meeting frequency. Report page count. Register line items. None of that tells you whether your decisions are getting better. This does.

Before You Start

Complete this in one sitting. Forty-five minutes, maximum. Answer for how things actually work, not how the governance documentation says they should. The gap between those two answers is, in itself, important information.

Score each question:

- **0.** Not in place. Hasn't been seriously considered.
- **1.** Partially there. Inconsistently applied across the organisation.
- **2.** Largely in place. Works in most areas, most of the time.
- **3.** Fully embedded. Consistently applied, regularly reviewed.

DIMENSION 1: Risk Taxonomy Clarity

Does your organisation share a common language for risk, or is everyone working from a different map?

Q1. Do all your risk-owning functions: cyber, operational, financial, supply chain, HR, and legal use a single agreed definition of what constitutes a risk versus an issue versus a threat?

Not a definition buried in a policy document. One that people actually use in meetings.

Q2. Is your risk taxonomy documented, version-controlled, and genuinely reflected in board and executive reporting? Or does it live in a framework nobody opens?

Q3. When a new risk category emerges — say, an AI governance exposure or a geopolitical supply chain disruption — does your organisation have a clear, repeatable process for classifying and integrating it? Or does it get wedged into whichever existing category seems closest?

Q4. Can your Board Members articulate your top three risk categories in the same language as your CRO and CISO? Without someone doing translation work before the meeting?

Dimension 1 Total: ___ / 12

DIMENSION 2: Decision Rights and Architecture

Is it clear who decides what, when, and with what information? Or does that depend on who's in the room?

Q5. Does your organisation have an explicit Decision Architecture, a documented map of which risk decisions sit at which level: operational, management, executive, board?

Not implied. Not assumed. Written down and agreed.

Q6. When a risk escalates, is the escalation pathway clear and pre-agreed? Or does it depend on who happens to be reachable, or who feels strongly enough to push it upward?

Q7. Are decision rights reviewed when the organisation restructures, acquires, or enters a new market? Or do outdated decision maps persist long after the organisation they were built for no longer exists?

Q8. Is there a working distinction between decisions that require board approval, decisions that require board awareness, and decisions that sit within management authority? And does that distinction hold in practice, not just on paper?

Q9. When a significant risk decision is made, is the rationale documented in a way that would hold up under regulatory review or a post-incident audit?

Dimension 2 Total: ___ / 15

DIMENSION 3: Decision Infrastructure

Do you have the systems, data, and processes that actually support quality risk decisions? Or are you deciding on incomplete information and calling it governance?

Q10. Does your organisation have a single, trusted source of risk data? Or do your risk, audit, cyber, and operational teams each maintain separate registers that tell different; sometimes contradictory stories?

Q11. Are your risk reports presented to the board in a format that enables decisions? Or are they compliance documents that confirm what's already happened?

Describing the past is not the same as informing the future.

Q12. Does your organisation use leading indicators of risk alongside lagging ones? Do you see the signals before the incident, or only after?

Q13. Is your risk infrastructure connected to your strategic planning cycle? Does risk appetite actively shape where budget goes and which opportunities get pursued?

Q14. Can your organisation model second and third-order consequences of a major risk event? Or is your infrastructure only capable of describing individual risks as if they exist in isolation?

Dimension 3 Total: ___ / 15

DIMENSION 4: Cross-Functional Risk Integration

Are your risk decisions joined up? Or are four functions managing the same risk in four different directions?

Q15. When a cyber risk has supply chain implications, and those supply chain implications carry financial and reputational consequences, is there a mechanism for those risk owners to make a connected decision? Or does each function manage its piece while the full picture remains invisible?

Q16. Does your board receive an integrated view that shows how risks interact and compound? Or does it receive sequential updates from individual functions, each telling their own story?

Q17. Is your internal audit plan built around your risk taxonomy and decision architecture? Or is it shaped more by historical coverage patterns and audit team familiarity?

Q18. When your organisation makes a major strategic move — a merger, a market entry, a digital transformation — does risk taxonomy inform it from day one? Or does the risk assessment arrive as a checklist after the decision has already been made?

Dimension 4 Total: ___ / 12

DIMENSION 5: Board and Leadership Risk Literacy

Can your leadership actually use the architecture you've built? Or is the sophistication running ahead of the capability?

Q19. Could your Board Members distinguish a well-constructed risk assessment from a superficial one? Would they challenge the latter, or would it pass through because it looked professional?

Q20. Has your organisation invested in building genuine risk decision-making capability at board and executive level in the last two years? Not compliance training. Actual decision quality development.

Dimension 5 Total: ___ / 6

Reading Your Score

Total	Where You Are	What It's Telling You
0–15	Fragmented	Risk and decisions live in separate worlds. The gap between what your framework says and what your organisation decides is wide enough to drive a governance failure through.
16–30	Developing	Some foundations exist. But consistency is dependent on individuals, not systems. When the right person is in the room, it works. When they're not, it doesn't.
31–45	Established	A working framework is in place. The integration gaps that remain are costing you in decision speed and board confidence.
46–55	Connected	Risk taxonomy and decision architecture are beginning to function as a system. The focus now is infrastructure sophistication and board-level application.
56–60	Operating	Your organisation treats risk decision-making as a strategic asset, not a governance obligation. You're making decisions your competitors are still discussing.

The More Useful Number

Your total score matters less than your lowest dimension score. That's your constraint. The thing that's quietly limiting every other part of the system.

If Dimension 1 is lowest, your people are working from different maps. Every decision carries translation risk between the people making it and the people accountable for it.

If Dimension 2 is lowest, authority is ambiguous. Risk decisions are being made by default; by whoever feels empowered enough or pressured enough to act. That's not governance. That's improvisation with accountability attached.

If Dimension 3 is lowest, your infrastructure can't support the decisions your leaders are trying to make. Better data and reporting aren't luxuries here. They're prerequisites.

If Dimension 4 is lowest, functional silos are generating blind spots at exactly the intersections where your most serious risks compound. No single function can see the full picture because no single function owns it.

If Dimension 5 is lowest, the architecture may be sound, but the people using it aren't equipped to get the most from it. A sophisticated framework interpreted by underprepared people is still a blunt instrument.

What Comes Next

If your scores revealed gaps you recognise — particularly in how your risk taxonomy connects to actual decision-making — that's the exact problem the Integrated Risk Taxonomy, Decision Architecture, and Decision Infrastructure model addresses.

Not as a framework to be filed. As an operating architecture to be used.

If you want to walk through your results and identify where the gap is costing you most, book a 45-minute Decision Architecture Conversation (https://calendly.com/maman-thedecisionlayer/). No pitch. No proposal. A direct conversation between people who take this seriously.

Maman Ibrahim, Founder of DiamondSoul

ICF Accredited Coach & Mentor
F-IoCR. Fellow of the Institute of Corporate Resilience
F-ISRM. Fellow of the Institute of Strategic Risk Management
ChCSP. Cyber Security Audit and Assurance (Chartered Cyber Security Professional)
CISSP. CISA. CRISC. CDPSE. ISO 27001 Lead Auditor. Microsoft Azure Security Architect

maman@thedecisionlayer.org

https://thedecisionlayer.org