NORTHSEAT

Governance. And Strategy.
That Performs.

Risk Management

ESSENTIAL SNAPSHOT

May 2026

Illustrative governance reference only - not a legal instrument or formal policy document.

Purpose

Risk management is the system a board uses to see material risk early, test management framing, connect risk to strategy, and record how judgement was formed.

A working Risk Management Framework (RMF) should make clear:

- what the Board owns
- what management owns
- how material risks are identified, assessed, escalated and reported
- how risk appetite, risk categories, the risk register and assurance activity fit together
- how risk considerations shape strategy, capital allocation, major initiatives and incidents
- how the Board reviews whether the framework remains effective

An RMF should shape Board papers, risk reporting, executive recommendations, committee work, assurance activity and minutes.

When it sits in the governance pack and rarely appears in decisions, risk management is operating as documentation.

Why this matters now
Boards are facing heavier scrutiny over risk, governance, resilience, cyber, AI, compliance, conduct, funding, transactions and stakeholder trust.

ASX Corporate Governance Principles (4th edition) Principle 7 expects listed entities to establish a sound risk management framework and review at least annually whether it remains sound. APRA-regulated entities face explicit requirements under CPS 220. AICD's H2 2025 Director Sentiment Index identifies legal and regulatory compliance, cyber and data security, AI, and reputation and crisis management among directors' top concerns.

Before you scroll on....

Can your Board point to decisions in the past six months where the RMF changed the Board’s questions, reporting request, escalation path, assurance request, approval condition or minutes?

⚠️ If your Board has an RMF but cannot show how it shaped Board papers, reporting, escalation, assurance requests and records, the framework is giving comfort without discipline.

Where risk discipline breaks down

RMF discipline weakens through repeated habits that look reasonable at the time

1.0 The RMF exists; decisions bypass it 🚧

👉 Directors debate strategy, investment or incidents using instinct or precedent.

⚠️ The result? The Board approves or accepts positions without a visible risk-governance reference.

2.0 Ownership is blurred

👉 Management treats risk as operational detail; directors assume escalation will occur when required.

⚠️ The result? Important matters sit between Board oversight and management execution

3.0 Reporting shows activity rather than judgement

👉 Risk packs show lists, ratings and controls, while appetite position, owner, trend, control confidence and required Board action remain unclear.

⚠️ The result? Directors receive information and still need to infer the governance signal

4.0 Escalation depends on confidence or politics ❌

👉 Risks move upward when someone feels safe or sufficiently worried

⚠️ The result? The Board sees some matters late, some through side channels, and some only after options have narrowed.

⚠️ **The risk category, appetite position, owner, assessment method, escalation route, assurance request, Board decision record and follow-up should form one governance trail. Weakness across several points makes the Board's risk position harder to explain later.**

Common tension points in Risk Management

Every tension point below is a governance signal. Boards with disciplined RMF practice use these moments to reinforce role clarity, escalation discipline, assurance and record integrity.

🔍 These are the most common tension points we see, even in otherwise capable Boards.

Tension point	Questions to ask (but rarely are)
Decision use	🔍Can directors identify recent decisions where the RMF shaped the recommendation, conditions, escalation path, assurance request or Board record?
Board vs management	🔍Does the Board challenge risk, appetite and assurance while management owns execution, or do directors drift into operational treatment?
Reporting	🔍 Do risk reports show appetite position, owner, movement, control confidence and required Board action, or only lists, ratings and commentary?
Escalation discipline	🔍 Can executives raise bad news, control weakness or unwelcome assessments without smoothing or personal cost?
Framework integration	🔍 Does the RMF connect clearly to the Risk Appetite Statement, Risk Register, Delegation of Authority, Board Approval Framework, BCP, CIRP and DRMF where relevant?

⚠️ If these questions feel familiar, RMF discipline should be reviewed before the next audit, insurer question, transaction, incident, strategy cycle, leadership change or Board reset.

Which next step fits your board?

Situation	Best next step
We want to test whether our RMF is visible in Board papers, risk reporting, escalation, assurance and records	Complete the [Risk Management Assessment]
No Board-approved RMF exists, or the current document is informal	Start with the Foundation Edition
An RMF exists but does not shape reporting, escalation, appetite alignment, assurance, framework integration or Board records	Move to the Governance Edition
For organisations operating under the highest levels of accountability	Discuss Institutional design and implementation

Trigger moments

RMF weakness becomes commercially expensive at predictable points. Boards usually act around one of the following:

- audit, assurance, lender, insurer, funder, investor, regulator or adviser question
- new Chair, Audit and Risk Chair, CEO, CFO, CRO, Company Secretary or Head of Risk
- sale, merger, acquisition, PE involvement, capital raise, refinancing, IPO preparation or major grant funding
- incident, near miss, control failure or late escalation
- Board-executive tension over ownership, authority, reporting or escalation
- cyber, AI, data, continuity, outsourcing or operational resilience concern
- risk register review showing unclear categories, ownership, ratings, control confidence or appetite alignment
- annual strategy cycle where risk profile has moved faster than the current framework

Where any of these are visible, the RMF should be formalised before the trigger controls the timetable.

Our frameworks are:
👉 **Board-ready**: informed by the Corporations Act 2001 (Cth) director duty principles, ASX Corporate Governance Principles and Recommendations where relevant, ASIC Corporate Governance Taskforce observations on non-financial risk, APRA CPS 220 for APRA-regulated entities, ASIC RG 104 for AFS licensees where relevant, AICD guidance, AS ISO 31000:2018 and ISO 37000.
👉 **Behavioural governance**: designed for how Boards govern risk when information is incomplete, incentives conflict and directors carry different assumptions
👉**Clear**: gives directors and executives shared language for roles, categories, escalation, appetite connection, assurance and records
👉**Practical**: connects the RMF to Board papers, risk reporting, the Risk Register, Risk Appetite Statement, Delegation of Authority, Board Approval Framework, BCP, CIRP, DRMF and minutes.

Why this gets postponed

Boards can recognise the gap, and still delay closing it.

❌ “We already have an RMF.”
📌 The test is whether it appears in Board papers, risk reporting, escalation decisions, assurance requests, minutes and executive recommendations. A rarely referenced framework creates comfort without discipline.

❌ “Risk is handled by management.”
📌 Management owns day-to-day controls. The Board needs a clear framework for oversight, challenge, escalation, assurance and review.

❌ “We have a risk register.”
📌 A risk register names exposures. The RMF defines how those exposures are governed, escalated, owned, reported, reviewed and connected to appetite and authority.

❌ “This will add more governance work.”
📌 The work already exists. It is being paid through repeated debate, late escalation, unclear owners, risk-pack confusion and post-event reconstruction.

❌ “We can refresh it internally.”
📌 Internal build can work when there is enough time and political permission. The test is whether it covers Board role, management role, three lines, risk categories, risk culture, assessment logic, escalation, assurance, integration and records in a way the Board will use.

Application across contexts

The Foundation and Governance Editions are informed by recognised Australian governance reference points set out on page 5 and are adaptable to a wide range of organisational contexts including private companies, listed companies, not-for-profits and government entities. Each Board must determine the risk management framework most fit-for-purpose for its organisation’s size, complexity, obligations, risk profile, governance maturity and operating context.

Recognised governance practice provides a reference point. Departures should be deliberate, documented and risk-assessed for their effect on decision quality, role clarity, escalation, assurance and accountability.

NorthSeat works with Boards and executive teams across private, listed, NFP and government sectors to improve governance maturity and leadership alignment.

About This Essential Snapshot

This Essential Snapshot is provided by NorthSeat as a free governance resource for board leaders.

You are welcome to:
✅ Share this document with your board, colleagues, or governance networks
✅ Reference insights in board discussions or strategy sessions
✅ Forward the download link to others who might find it valuable
✅ Print or save for personal use

We ask that you:
- Attribute content to NorthSeat when sharing or referencing
- Share the original document (don't alter, rebrand, or misrepresent content)

Not permitted:
❌ Selling or licensing this document
❌ Using this as a commercial training product without permission
❌ Removing NorthSeat branding or attribution
❌ Using this content to create competing products or services

This Essential Snapshot is a starting point. For structured frameworks or board-ready policies, contact us:

📧 liam@northseat.com.au | 🌐 www.northseat.com.au

NORTHSEAT