NORTHSEAT
Governance. And Strategy.
That Performs.

Digital Risk Management

ESSENTIAL SNAPSHOT

Sep 2026

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

Purpose

Digital risk is where strategy, technology, data, vendors, continuity, AI and trust meet.

A working Digital Risk Management Framework should make clear:

- which digital risks require Board visibility
- which digital risks sit with management
- how cyber, privacy, vendor, AI, continuity and transformation risks are escalated
- how digital risk shapes strategic decisions, capital allocation and major technology change
- how the Board receives evidence that controls, recovery capability and management action are working

A DRMF should shape Board papers, risk reporting, digital investment approvals, vendor oversight, incident escalation, assurance activity and minutes.

Where cyber policies, dashboards, continuity plans and committee updates exist separately, the Board may receive digital risk information without governing digital risk.

Why this matters now

In May 2026, ASIC issued an open letter to industry calling cyber resilience a core licensing obligation and a board-level matter. The letter was directed at financial services licensees and market participants, but the direction of regulatory and stakeholder thinking applies more broadly: boards across sectors are expected to govern digital risk through structure, evidence, escalation and review - rather than policy alone.

The practical implication is the same regardless of sector.

Before you scroll on....

Can your Board point to recent decisions where digital risk changed the recommendation, timing, conditions, vendor choice, escalation path or Board record?

⚠️ If your Board receives digital risk reports but cannot show how those reports influence decisions, escalation or oversight, digital risk is probably being monitored more than governed.

Where discipline breaks down

Digital risk governance weakens through repeated habits that look reasonable at the time

1.0 Digital risk sits inside IT reporting 🚧

👉 Directors receive cyber metrics, project updates or dashboards, but the governance signal remains unclear.

⚠️ The result? The Board sees activity without a clear view of decision impact, accountability or escalation.

2.0 Vendor exposure is known inside management

👉 Critical SaaS, cloud, data or outsourced dependencies are understood operationally, but reach the Board only after options narrow.

⚠️ The result? The Board sees consequences after contract, cost, continuity or customer exposure has already increased.

3.0 Incidents and near misses close too quickly

👉 Management explains what happened, but the Board does not test whether reporting, escalation, recovery and decision rights worked.

⚠️ The result? The same weakness can remain hidden until the next incident is larger.

4.0 Digital transformation and AI use outrun governance ❌

👉 New systems, automation, data use and AI tools expand before risk appetite, privacy, continuity, vendor and assurance questions are visible.

⚠️ The result? Strategic momentum builds faster than Board-level control.

⚠️ The reporting signal, risk appetite position, escalation route, Board decision record and follow-up action should form one governance trail. Weakness across several points makes the digital risk position harder to explain later.

Common tension points in a DRMF

Every tension point below is a governance signal. Boards with disciplined digital risk governance use these moments to improve decision quality, escalation, assurance and the integrity of the record.

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

Tension point	Questions to ask (but rarely are)
Board visibility	🔍 Do digital risk papers change the Board's view - or simply update it?
Incident escalation	🔍 Do serious digital events reach directors while choices still exist?
Critical vendors	🔍 Could a critical digital provider fail before the Board understood the dependency?
Director challenge	🔍 When cyber, AI or vendor language gets dense, does silence pass as agreement?

⚠️ If these questions feel familiar, digital risk governance should be reviewed before the next major cyber incident, privacy breach, vendor failure, system outage, AI rollout, transformation program, audit review or transaction.

Which next step fits your board?

Situation	Best next step
We want to test whether digital risk is visible in Board papers, reporting, escalation and records	Complete the Digital Risk Governance Assessment
AI use, automated decisions, vendor AI, foundation models or staff AI use are already live, emerging or unclear	Complete the Artificial Intelligence Governance Assessment
No coherent DRMF exists, or current documents are fragmented across cyber, continuity, vendors and IT	Start with the Foundation Edition
A DRMF exists but does not shape reporting, escalation, vendor oversight, transformation decisions or Board records	Move to the Governance Edition

Trigger moments

Digital risk ambiguity becomes commercially expensive at predictable points. Boards usually act around one of the following:

- cyber incident, privacy breach, SaaS outage, data loss event or serious near miss
- audit, insurer, lender, funder, regulator, investor or customer question
- new Chair, CEO, CFO, CRO, Company Secretary or Audit & Risk Committee Chair
- sale, merger, acquisition, capital raise, IPO preparation or PE involvement
- major digital transformation, AI rollout, vendor transition or system replacement
- Board papers showing digital risk without clear appetite, escalation or decision impact
- annual strategy cycle where digital dependency has outgrown the current framework

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

Our frameworks are:
👉 **Board-ready**: informed by the Corporations Act 2001 (Cth) where relevant, ASX Corporate Governance Principles, ASIC cyber resilience commentary including the May 2026 industry letter, the Privacy Act 1988 (Cth) including the 2024 amendments and automated decision-making provisions, the Notifiable Data Breaches scheme, APRA CPS 230 where relevant, ACSC Essential Eight, ISO 31000, ISO 27001/27002 and ISO 37000.
👉 **Behavioural governance**: designed for how Boards interpret digital risk when reporting is technical, time is short and directors hold different assumptions
👉 **Clear**: gives directors and executives shared language for digital risk, escalation, vendor dependency, continuity and assurance
👉 **Practical**: connects digital risk to Board papers, risk reporting, incident escalation, transformation decisions, assurance and records

Why this gets postponed

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

❌ "We already have a cyber policy, CIRP or BCP."
📌 Those documents may describe controls, response and recovery. A DRMF defines how the Board governs digital risk across reporting, escalation, vendors, continuity, data, transformation and records.

❌ "Cyber is handled by management."
📌 Management runs the controls. The Board needs a clear framework for oversight, challenge, escalation and assurance.

❌ "Our dashboards tell us what we need."
📌 Dashboards show information. A DRMF shows which information changes decisions, who owns the response and when escalation reaches the Board.

❌ "We are too small for this."
📌 Digital dependency can exceed organisational size. SaaS, cloud, outsourced platforms, payment systems and client data can create Board-relevant exposure well below enterprise scale.

❌ "We will wait until the technology program is further along."
📌 Late governance costs more. Once contracts, data migration, vendor design and operating changes are committed, the Board has fewer clean options.

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 digital risk governance framework most fit-for-purpose for its organisation's size, complexity, obligations, digital dependency, data sensitivity, vendor concentration 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, continuity 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

© 2026 NorthSeat ABN 67 690 779 072. All rights reserved.

This document does not constitute legal, governance, or professional advice. Directors should seek independent advice for governance, legal, or compliance matters.

NORTHSEAT