NORTHSEAT
Governance. And Strategy.
That Performs.

Business Continuity

ESSENTIAL SNAPSHOT

May 2026

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

Purpose

Business continuity is the governance structure for keeping critical operations, client obligations, staff safety, supplier reliance, communications and recovery decisions coherent during disruption.

The CEO and executive team run the incident. The board owns oversight of the framework, thresholds, reporting and post-incident follow-up.

A disciplined Business Continuity Plan should make clear:

- which events activate the plan;
- which events require board notification;
- who has authority to classify, escalate and communicate;
- which critical functions are restored first;
- which suppliers, systems and people the organisation depends on;
- what information the board receives during a serious disruption;
- how decisions, communications, recovery actions and lessons are recorded.

This snapshot helps Chairs, Directors, CEOs, CFOs, risk leaders and Company Secretaries identify where continuity governance may be weaker than the existence of a BCP suggests.

Why this matters now

Operational resilience is now a live board, insurer, lender, auditor and regulator question.

APRA CPS 230 has refined board and executive language around critical operations, service providers, tolerance breaches and scenario testing. It applies directly to APRA-regulated entities and influences expectations in adjacent sectors.

Cyber incidents, cloud outages, supplier failures, workforce disruption and public-trust failures have also made continuity a board-level evidence issue

Before you scroll on....

⚠️ Could your current BCP explain who classifies the event, who notifies the board, who speaks externally, which functions recover first, and what record is created afterwards?

Where continuity governance breaks down

Continuity weakness usually develops through repeated habits that look harmless before an incident.

1.0 The BCP is noted without being exercised 🚧

👉 The board receives the document annually.
👉 Management confirms it has been reviewed.
👉 No one has walked through a serious scenario with current people, systems and suppliers.

⚠️ Consequence: the board has a document, but limited evidence that the plan can be used.

2.0 Activation criteria are vague

👉 "Material disruption" is understood differently by the CEO, Chair, risk team and operational leaders.
👉 Board notification depends on judgement rather than agreed thresholds.

⚠️ Consequence: escalation becomes late, uneven or personality-dependent.

3.0 The board receives updates without role boundaries

👉 Directors want visibility.
👉 Executives need room to manage the response.
👉 The plan does not define what the board receives, when, and for what purpose.

⚠️ Consequence: directors can drift into operations, or receive too little to discharge oversight properly.

4.0 Supplier, cyber and financial assumptions sit outside the plan ❌

👉 Critical services depend on cloud platforms, IT providers, payment systems, insurers, contractors or key people.
👉 Their continuity evidence may be stale, incomplete or self-certified.

⚠️ Consequence: the recovery plan depends on assumptions no one has verified.

⚠️ The plan, activation criteria, board reporting, authorised voice, recovery priorities and post-incident review form one connected continuity record. Weakness across several points makes the response harder to explain later.

Common tension points in continuity planning

Every tension point below is a governance signal. Boards with disciplined continuity practice use these moments to clarify authority, escalation, reporting and the integrity of the record.

🔍 These are the most common tension points we see, including in otherwise well-managed organisations.

Tension point	Questions to ask (but rarely are)
Existing BCP as comfort	🔍 Has the Board seen this plan operate anywhere beyond being approved?
Board notification thresholds	🔍 Is it clear which disruptions the Board must hear about - and which it would not?
CEO authority during disruption	🔍 If disruption struck tomorrow, would the CEO clearly hold authority - or would it move around the room?
Single voice communications	🔍 If clients, staff or media needed answers, would one authorised voice be obvious - or would several people speak?
Post-incident record	🔍 After a serious disruption, could the Board show how it governed the event - not just that it happened?

⚠️ If these questions feel familiar, continuity governance should be reviewed before the next audit, renewal, funding, insurer, cyber or board review cycle.

Which next step fits your board?

Situation	Best next step
We want to see whether our current BCP has governance gaps	Complete the Business Continuity Governance Assessment
No Board-approved BCP exists, or the current document is informal	Start with the Foundation Edition
We have a BCP, but it does not shape testing, escalation, board reporting, supplier reliance, communications or post-incident review	Move to the Governance Edition
For organisations operating under the highest levels of accountability	Discuss Institutional design and implementation

Trigger moments

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

- cyber incident, IT outage or supplier failure;
- insurer, lender, auditor, funder or regulator question;
- new Chair, CEO, CFO, risk leader or Company Secretary;
- M&A, sale, PE investment, refinancing or due diligence;
- critical supplier concentration or cloud-platform reliance;
- board concern after a tabletop exercise or incident debrief;
- public-trust, client-service or workforce disruption.

If any of these are visible on your horizon, continuity governance should be formalised before the next external question controls the timetable.

Our frameworks are:
👉 **Board-ready**: informed by ISO 22301, ISO 37000, Corporations Act director and officer duty principles, ASX Corporate Governance Principles where relevant, and APRA CPS 230 for APRA-regulated entities or operational-resilience reference points.
👉 **Behavioural governance**: designed for how boards and executives make decisions when facts are incomplete, systems are unavailable, leaders are tired, and informal authority can distort escalation.
👉 **Clear**: gives Directors, Chairs, CEOs, CFOs, Company Secretaries, crisis leaders, legal, communications, IT and risk teams shared language for activation, board notification, authorised voice, recovery priorities and review.
👉 **Practical**: connects the BCP to the Risk Appetite Statement, Risk Management Framework, Cyber Incident Response Plan, vendor register, insurance assumptions, liquidity planning, board reporting and minutes.

Why this gets postponed

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

❌ "We already have a BCP."
📌 The test is use. Has it shaped scenario testing, board notification, CEO authority, supplier evidence, critical function recovery, client communication, insurer contact and post-incident review?

❌ "This belongs with management."
📌 Management runs the response. The board owns the governance frame: risk appetite, escalation thresholds, reporting expectations, authority boundaries and follow-up.

❌ "This will create more governance work."
📌 Clear continuity governance reduces repeated debate during disruption. It gives management authority to act and gives directors the information they need at the right level.

❌ "We can update this during the annual review."
📌 Audit, insurer, lender, regulator, cyber and supplier questions rarely wait for the policy calendar. A stale BCP creates work at the moment the organisation has the least spare capacity.

❌ "Our executives know what to do."
📌 Strong executives still need agreed authority, fallback contacts, communication channels, supplier escalation, recovery priorities and board reporting rules before the event starts.

Application across contexts

The Foundation and Governance Editions are informed by recognised governance and continuity reference points, including ISO 22301, ISO 37000, Corporations Act director and officer duty principles, ASX Corporate Governance Principles where relevant, and APRA CPS 230 where applicable. Each board must adapt its continuity framework to the organisation's size, structure, risk appetite, regulatory exposure, supplier reliance, client obligations and operating model.

Recognised governance practice provides a reference point. Departures should be deliberate, documented and risk-assessed for their effect on role clarity, escalation, recovery priorities, board reporting and post-incident review.

The Foundation and Governance Editions are adaptable to a wide range of organisational contexts including private companies, listed companies, not-for-profits and government entities.

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

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

NORTHSEAT