Insync Boards framework series

From cyber risk to digital resilience

Applying the **SECURE framework** to strengthen board oversight of cyber risk.

STRENGTHENING BOARD-LEVEL
CYBER GOVERNANCE

Cyber risk now sits firmly at board level. It affects strategy, operational resilience, regulatory exposure, reputation and stakeholder confidence.

Boards are not expected to understand technical architecture. They are expected to exercise informed judgement, ensure disciplined oversight and maintain confidence that the organisation is prepared to withstand and recover from cyber disruption.

The SECURE framework provides boards with a structured approach to assessing and strengthening cyber governance oversight.

When boards begin to question their cyber oversight

Cyber governance reviews are rarely triggered by breach alone. More often, they begin with uncertainty.

Directors may receive detailed cyber reports yet still feel unclear about the organisation's true exposure. Metrics are presented and dashboards reviewed — but the conversation lacks forward-looking insight.

A new digital strategy may have expanded technology reliance, yet board oversight structures have not evolved at the same pace.

A near miss or industry incident may prompt reflection — not simply about operational controls, but about whether the board had clear visibility of escalating risk. Risk appetite statements may reference cyber exposure, yet it is not always evident how they shape investment decisions, prioritisation or strategic trade-offs.

Committees may be active and management diligent, but directors remain unsure whether cyber oversight is proportionate to the organisation's complexity and threat environment. None of these necessarily indicate weakness. They often reflect growth, digitisation and rising regulatory expectations.

But they do raise important questions.
Is cyber risk being governed strategically at board level?
Are we confident in our visibility, preparedness and resilience?

Cyber risk is a governance responsibility

Cyber risk is no longer simply a technology issue. It is a core governance discipline.

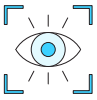
Boards are not responsible for managing cyber risk day to day. They are responsible for governing it. That means ensuring cyber risk is integrated into strategy, clearly aligned with risk appetite, and overseen through disciplined reporting and accountability structures.

Effective cyber governance ensures the board understands the organisation's exposure, challenges management constructively and has confidence in preparedness, response capability and recovery resilience.

Cyber governance is not about technical detail. It is about structured oversight and confident stewardship.

When cyber governance is disciplined and proactive, boards benefit from:

Clearer visibility of cyber exposure and emerging threats



Greater confidence in reporting and oversight

Stronger integration of cyber risk into strategic decisions

Better preparedness for responding to cyber incidents

© Copyright 2026

Introducing the SECURE Framework

A board cyber governance review is built on the SECURE framework, a governance-focused model that defines what effective cyber oversight looks like at board level.

The framework examines six interrelated domains of cyber governance maturity.

S

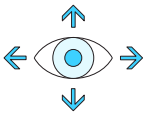
Strategy integration
How clearly cyber risk is integrated into organisational strategy, risk appetite discussions, and broader decision-making processes across the business.

E

Enterprise risk and compliance
How effectively cyber oversight is integrated into enterprise risk management processes, with clear reporting lines, defined accountabilities, and regular board visibility.

C

Culture and capability
How the board oversees and actively models cyber awareness, accountability, and the development of internal capability across the organisation.



U

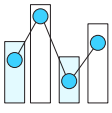
Understanding cyber risk
Evaluates how well the organisation understands the evolving threat landscape, identifies critical asset exposures, and anticipates emerging cyber and technology risks.

R

Response and resilience
Board oversight of organisational preparedness, incident response capability, and recovery planning in the event of a cyber incident.

E

Evaluation and metrics
How the board uses meaningful, forward-looking indicators to monitor cyber performance, track risk trends, and assess effectiveness over time.



Together these domains provide a disciplined framework for assessing whether cyber governance is structured, aligned and proportionate to organisational exposure.

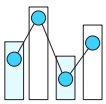
© Copyright 2026

What a cyber governance review is — and is not

A SECURE Cyber Governance Review provides an independent, structured assessment of how effectively cyber risk is governed at board or committee level.

It evaluates whether:

Oversight structures are clear and proportionate



Reporting supports informed challenge and decision-making

Risk appetite meaningfully shapes strategic decisions

Accountability is embedded across governance layers

Preparedness and resilience are understood and tested

The review does not assess operational cyber controls in detail. It is not a technical cyber audit.

Instead, it evaluates whether governance disciplines, oversight behaviours and decision frameworks enable the board to govern cyber risk with confidence.

Rather than producing extensive action lists, the review focuses on a small number of practical recommendations that materially strengthen cyber governance maturity.

Key questions for directors

Boards do not need to be cyber experts, but they do need confidence that cyber risk is being governed effectively.

Directors may wish to consider:

Do we have a clear view of our most material cyber risks and how they are evolving?

Is cyber risk explicitly integrated into strategy and risk appetite discussions?

Does reporting provide forward-looking insight or mainly historical updates?

Are governance responsibilities clear across the board, committees and executive leadership?

Are incident response and recovery capabilities well understood and tested?

If these questions prompt uncertainty or debate, a structured governance review can help clarify whether oversight arrangements remain fit for purpose.

© Copyright 2026

How we work

Our approach is structured, proportionate and tailored to the organisation's complexity and digital exposure. A review typically includes a confidential board or committee assessment aligned to the SECURE framework, supported where appropriate by interviews. Independent analysis is undertaken and findings are synthesised into clear, practical insight.

We are experienced governance advisers with the appropriate gravitas to work at board level and to handle sensitive and confidential matters with discretion.

Our particular strength lies in synthesising diverse perspectives and information into a small number of practical recommendations that, taken together, deliver the greatest improvement in governance effectiveness. Reviews may be conducted at full board level or at committee level where cyber oversight responsibilities are delegated.

Many organisations undertake cyber governance reviews as a focused standalone assessment. Where appropriate, they can also be aligned with broader board effectiveness or risk governance reviews.

Part of the Insync Boards governance architecture

Cyber governance does not sit in isolation. Board effectiveness is strengthened when oversight disciplines are aligned across the board, its committees, the CEO and the executive team.

Insync Boards supports organisations through a structured governance architecture built on proprietary, evidence-based frameworks developed through many hundreds of governance engagements.

These include:

WhatWhoHowDo - Board effectiveness
DRIVE - Director effectiveness
SCOPE - CEO performance
SOLID - Executive effectiveness (individual contribution)
ALIGN - Executive forum effectiveness
THRIVE - Risk governance maturity
SECURE - Board cyber governance
CLEAR - Clinical governance committee effectiveness

Together these frameworks provide disciplined insight across every layer of governance.

Governing cyber with confidence

Strong organisations do not wait for crisis to test their governance. They periodically step back to assess whether oversight remains aligned with strategy, organisational complexity and digital dependency.

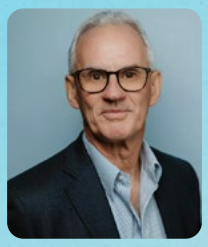
A structured cyber governance review provides boards with clarity about their oversight effectiveness, visibility of potential blind spots and confidence that governance arrangements remain fit for purpose.

If your board would value a disciplined, independent perspective on its cyber governance maturity, we would welcome a confidential discussion.

© Copyright 2026

Independent governance reviews and advisory.

Gill Collins
Principal Consultant
0414 486 188
gcollins@insyncboards.com
insyncboards.com



Nicholas Barnett
Executive Chair
0407 175 551
nbarnett@insyncboards.com

insyncboards.com
Governance. Elevated.

insync BOARDS