FUJITSU

AICD Cyber Security Governance Principles Reporting

Clear insights into board-level cyber governance alignment

Independent assessment and reporting against the AICD Cyber Security Governance Principles to help boards understand their current position, identify gaps, and strengthen assurance over cyber security risk.

What we do

We conduct a short-term, one-off assessment against the AICD Cyber Security Governance Principles to evaluate how effectively cyber security is governed, overseen and assured at the board and executive level.

The risks we help uncover

- Limited visibility of boards into cyber security governance effectiveness.
- Gaps between cyber strategy, risk oversight and board assurance.
- Unclear accountability for cyber security at executive and board levels.
- Difficulty demonstrating governance maturity against recognised principles.

Clear alignment view
A concise assessment of how current government aligns to the AICD Cyber Security Governance Principles.

Identified gaps and priorities
Clear identification of governance gaps and priority uplift actions.

Improved board assurance
Greater confidence that the board is appropriately overseeing cyber security risk.

Structured path forward
A practical foundation to support governance uplift and ongoing tracking.

Our approach is pragmatic, independent and designed specifically for board and executive audiences.

Principle-based assessment

- Focused on governance effectiveness rather than technical control testing.

Board-ready reporting

- Clear, concise output suitable for board discussion and assurance.

Targeted engagement

- Short-term assessment designed to minimise disruption while delivering clarity.

Foundation for ongoing assurance

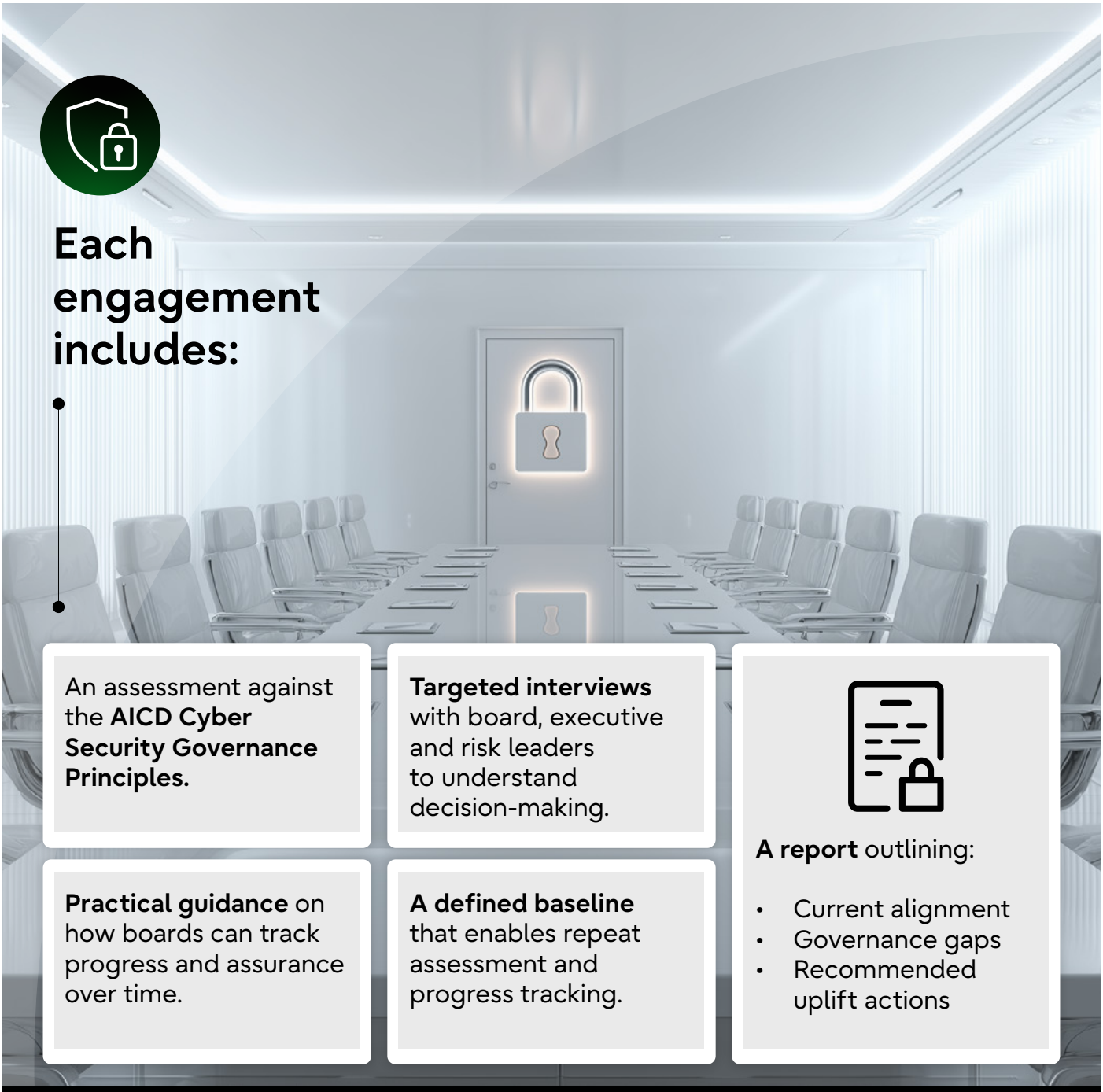
- Designed to integrate seamlessly with ongoing board advisory or assurance services, where required.

When to use this service

- After a cyber incident or “near miss”.
- New board members / new CISO / major leadership change.
- Major transformation (cloud migration, M&A, outsourcing).
- Before insurance renewal, assurance review, or regulator engagement.
- When cyber reporting feels “busy but not decision-useful”.

What are the AICD Cyber Security Governance Principles?

- Set clear roles, responsibilities and accountabilities.
- Oversee the development and evolution of cyber security strategy.
- Embed cyber security into enterprise risk management.
- Ensure organisation capability and cyber resilience.
- Prepare for and respond to significant cyber incidents.



Each engagement includes:

An assessment against the **AICD Cyber Security Governance Principles.**

Targeted interviews with board, executive and risk leaders to understand decision-making.

Practical guidance on how boards can track progress and assurance over time.

A defined baseline that enables repeat assessment and progress tracking.

A report outlining:

- Current alignment
- Governance gaps
- Recommended uplift actions

Why choose us?

Deep understanding of Australian cyber governance expectations and frameworks.

Independent, objective advice focused on board-level assurance.

Trusted delivery backed by Fujitsu's scale, credibility and experience across regulated environments.

Contact us today to discuss how we can strengthen your board oversight, assurance and confidence in cyber security governance.