
# The National Cyber Security Strategy can be delivered yet risk reduction remains unproven

**An FOI-released ministerial briefing shows the issue:**

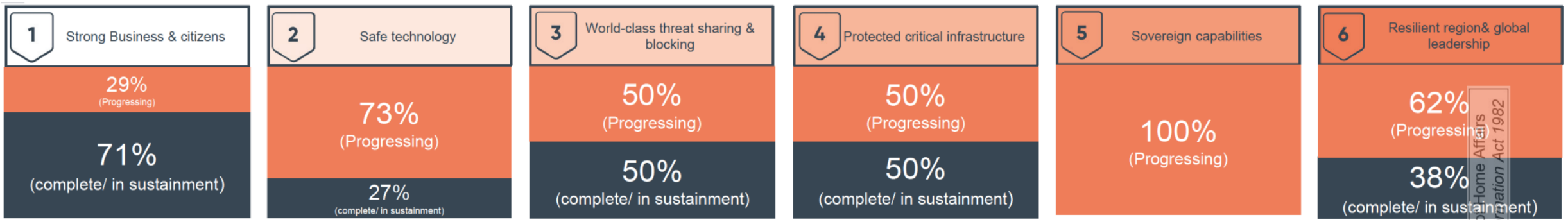
Current reporting shows the Minister for Cyber which initiatives have been delivered across the six Shields, but not whether those initiatives are reducing priority national cyber risks. This is a reporting gap—not evidence that the initiatives are ineffective.

Prepared by Benjamin Mossé for the Hon. Tony Burke MP | 26 August 2026

# A ministerial briefing released under FOI reports delivery progress across the six shields, not the effect on national cyber risk

1. Progress is reported as delivered, sustained, progressing, or on track

2. Success is reported through initiative and delivery status across the six shields




Source: Home Affairs FOI FA 26/06/01087, a targeted FOI request into how Strategy progress and success are reported at ministerial level.

**<u>This means:</u> The Minister for Cyber Security may be receiving assurance on program delivery while lacking evidence of whether Australia's priority risks are within tolerance.**

# Sooner or later, the Strategy's $586.9 million of funding will be judged on whether it made Australia safer

**A national cyber crisis**
*Did the strategy reduce this risk?*

**An inquiry or audit**
*Can we show that Australia became safer?*

**More funding requested**
*What did the previous investment achieve?*

**Without this assurance, funding decisions could direct hundreds of millions to the wrong priorities while essential services remain exposed**

# The UK Strategy shows this can be done:

## ask not only “What did we deliver?” but “Which risks did we reduce?”

**Use risk to decide where to act:**

“Progress towards [the strategy’s aim] will be driven by an **understanding of risk**. This means **identifying areas of particular risk** and **prioritising the most impactful interventions** to ensure that government can rapidly improve its cyber resilience.”

**Measure real outcomes:**

“KPIs will not be pursued at the expense of genuine cyber security outcomes. **KPIs will demonstrate genuine impacts and benefits.**”

The UK is not a like-for-like comparison with Australia, but it shows that a national cyber strategy can measure risk and value



Source: UK Government Cyber Security Strategy: 2022 to 2030

# A National Cyber Risk Assurance Model would help the Government assess whether the Strategy is reducing priority cyber risks

**Prioritised risks**

The risks the Strategy must reduce

**Clear ownership**

Who is accountable for each risk

**Evidence of impact**

Evidence of whether risk is reducing

**Funding rationale**

What to fund, change, or stop — and why

**Risk-based reporting would give decision-makers a consistent way to assess whether initiatives, grants and investments are aligned to priority risks, whether the evidence indicates those risks are reducing, and where funding should be adjusted.**

# Decide whether to
# add risk assurance to Strategy reporting

1. Map each existing Shield to the priority risks it is intended to reduce
2. Name someone accountable for each priority risk
3. Commission a prototype ministerial report for one priority risk

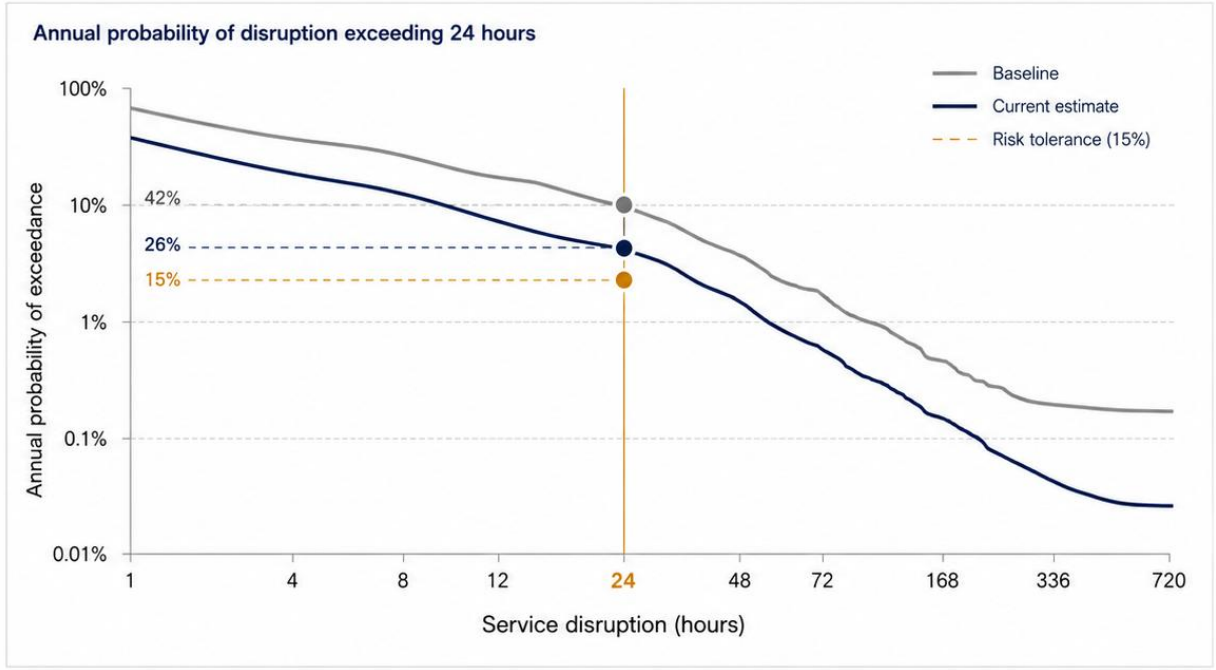
**See Appendices A–C for illustrative examples of how ministerial reporting could look under a National Cyber Risk Assurance Model**

# Appendix A: Illustrative National Cyber Risk Assurance Model - from the Strategy's Shields to ministerial assurance and decisions

# Appendix B:
# Illustrative priority risk scenario reporting

**Material cyber disruption to essential services is less likely, but remains above tolerance.**

Risk scenario: a cyber incident causes more than 24 hours of disruption to an essential service.




Baseline: 42%

Current estimate: 26%

Risk tolerance: 15%

90% uncertainty range: 18%–35%

Model inputs: incident data, exercise results, independent resilience assessments.

**Ministerial decision**

**Scale resilience investment in the highest-risk sectors; reassess in Q4.**

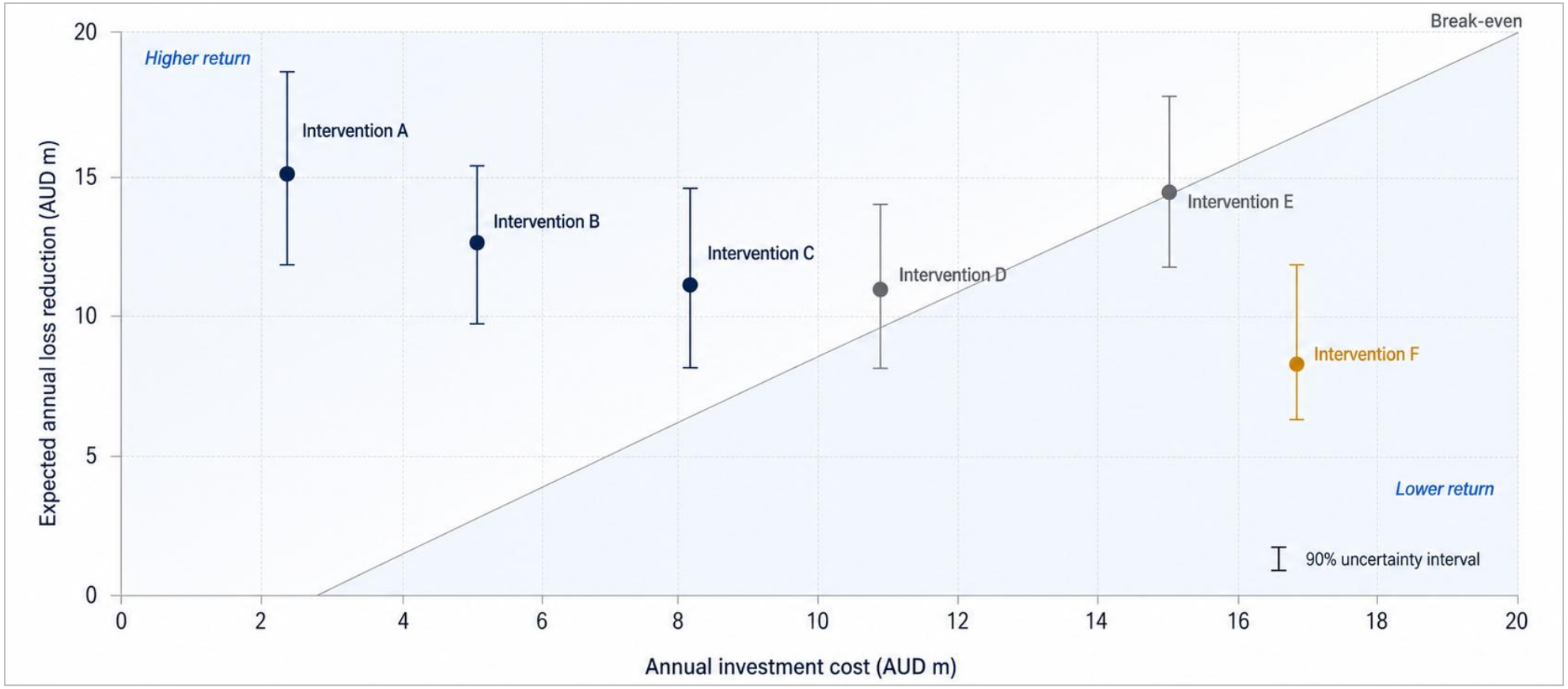
**Illustrative cost of inaction:**

"At the current estimate, this risk remains 11 percentage points above tolerance: a 26% annual chance of disruption exceeding 24 hours, against a tolerance of 15%

Without further risk reduction, Government continues to carry that excess exposure into the next reporting period."

Illustrative example—not a current risk estimate or investment recommendation.

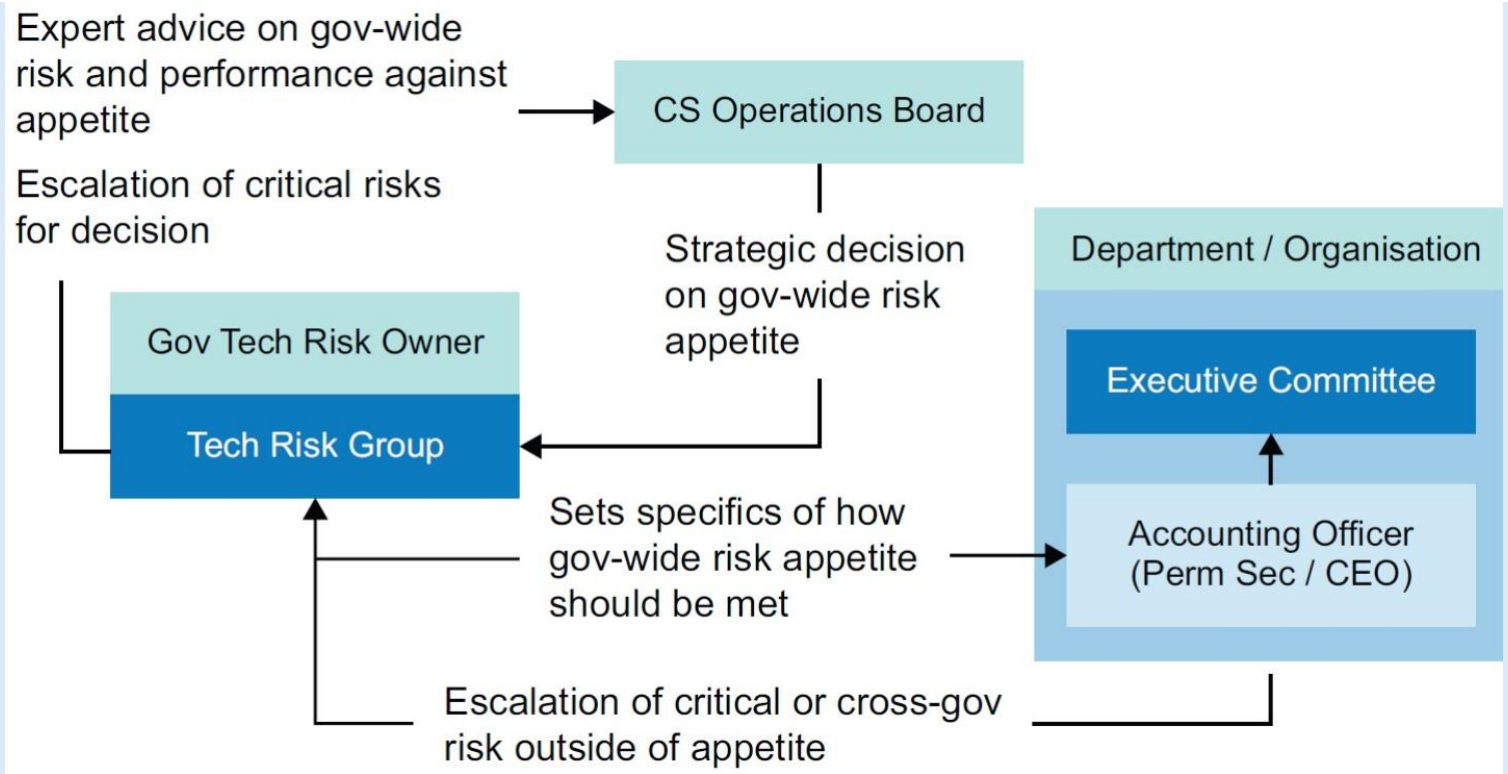
# Appendix C: Illustrative return-on-security-investment (ROSI) reporting




Compare investment options by expected loss reduction and uncertainty.

# Appendix D: Features Australia would need to make risk reporting actionable

**Illustrative governance features for consideration:**




- **Clear risk ownership**
- **Senior accountability**
- **Agreed level of risk**
- **Escalation of serious risks**
- **Government-wide oversight**

Source: UK Government Cyber Security Strategy: 2022 to 2030