**FORTE/CYBERx**
AI decision support for tech leaders

# Cyber Security Board Report Template

*Australian Edition - aligned to APRA CPS 234, SOCI Act, ACSC Essential Eight, ISO/IEC 27001:2022 and the Cyber Security Act 2024.*

## Purpose

A defensible, board-grade reporting template for Australian CISOs, CIOs and Heads of Risk. Use it to translate operational cyber posture into the language an Australian board expects - risk posture, framework alignment, regulatory status, scenarios, incident readiness and decision requests.

## Who should use it

CISOs, CIOs, Heads of Information Security, Audit & Risk Committee secretaries, fractional CISOs, and consultants preparing quarterly or annual cyber updates for boards of ASX-listed entities, APRA-regulated entities, SOCI-covered critical infrastructure, government bodies and Australian SMEs.

## How to use

Complete each section in order. Replace every bracketed placeholder with your data. Keep the executive summary to a single page. The board should be able to read it in under five minutes and arrive at the decision request with full context.

| | |
|---|---|
| **Reporting entity** | [Insert entity name] |
| **Reporting period** | [Quarter / FY] |
| **Prepared by** | [CISO / CIO / Head of Risk] |
| **Date presented to board** | [DD Month YYYY] |
| **Document classification** | Board confidential |

# 1. Executive Summary (One Page)

State the headline in business terms, not technical terms. The board should be able to make the decision from this page alone.

| | |
|---|---|
| **Current cyber risk posture** | [Low / Moderate / Elevated / High] - anchored to ACSC Essential Eight maturity and ISO/IEC 27001 control family coverage. |
| **Change since last report** | [Improved / Stable / Deteriorated] - quantified against last quarter, with the drivers. |
| **Top three material risks** | 1. [Scenario]<br>2. [Scenario]<br>3. [Scenario] |
| **Regulatory status** | APRA CPS 234: [Status] - SOCI: [Status] - OAIC NDB: [Status] - Privacy Act reform: [Status] - Cyber Security Act 2024 ransomware reporting: [Status] |
| **Material incidents this period** | [Number] notifiable, [Number] non-notifiable, MTTR: [hours]. |
| **Investment position** | FY spend: $[X], approved budget: $[Y], variance: [%], outstanding capex: $[Z]. |
| **Decision requested** | [Specific decision the board must make this meeting - risk appetite, investment, accountability, or third-party threshold.] |

# 2. Risk Posture by Domain

Score inherent risk and control maturity 1-5 for each domain. Residual risk is inherent minus maturity. Use this table to anchor the board's view of where capability is strong, where it is weak, and where investment needs to land.

| Risk Domain | Inherent (1-5) | Maturity (1-5) | Residual | Commentary |
|---|---|---|---|---|
| Identity & Access | [ ] | [ ] | [ ] | [Insert] |
| Endpoint & Devices | [ ] | [ ] | [ ] | [Insert] |
| Cloud & SaaS | [ ] | [ ] | [ ] | [Insert] |
| Data Protection & Privacy | [ ] | [ ] | [ ] | [Insert] |
| Third-Party / Supply Chain | [ ] | [ ] | [ ] | [Insert] |
| Application Security | [ ] | [ ] | [ ] | [Insert] |
| Operational Technology | [ ] | [ ] | [ ] | [Insert] |
| Incident Response & Recovery | [ ] | [ ] | [ ] | [Insert] |

Heat-map alternative: replace 1-5 with Low/Moderate/High if the board prefers a qualitative view. Always quantify the underlying evidence in the appendix.

# 3. Top Three Material Scenarios

Boards expect three scenarios, not thirty. Pick the scenarios with the largest potential business impact and present them as scored exposure.

| Scenario | Likelihood (1-5) | Impact ($AUD) | Current Controls | Treatment & Owne |
|---|---|---|---|---|
| Ransomware: production systems offline 72+ hrs | [ ] | [$ ] | [List] | [Plan / Owner] |
| Major data breach: customer PII exfiltration (OAIC notifiable) | [ ] | [$ ] | [List] | [Plan / Owner] |
| Critical third-party / supply-chain compromise | [ ] | [$ ] | [List] | [Plan / Owner] |

# 4. Framework & Regulatory Alignment

Australian boards expect cyber posture to be anchored against the recognised baselines. Present current status against target, with one-line gap commentary.

| Framework / Obligation | Target | Current | Gap Commentary |
|---|---|---|---|
| ACSC Essential Eight - Maturity Level | ML2 | [ML0/1/2/3] | [Insert] |
| ISO/IEC 27001:2022 - Annex A coverage | 95% | [%] | [Insert] |
| APRA CPS 234 - Information Security capability | Compliant | [Status] | [Insert] |
| SOCI Act - Risk Management Program | Approved | [Status] | [Insert] |
| OAIC Notifiable Data Breach readiness | Tested | [Status] | [Insert] |
| Cyber Security Act 2024 - Ransomware reporting | Ready | [Status] | [Insert] |
| NIST CSF 2.0 - Function maturity (avg) | Tier 3 | [Tier] | [Insert] |
| ISO/IEC 42001 - AI Management System | Defined | [Status] | [Insert] |

# 5. Incident Readiness & Recovery

Boards want assurance that the entity can detect, respond and recover. Report the inputs that prove readiness, not the volume of alerts handled.

| | |
|---|---|
| **Last tabletop exercise** | [DD/MM/YYYY] - Scenario: [Ransomware / Data Breach / Supply Chain] |
| **Last material incident** | [None / Date - outcome] |
| **Mean Time To Detect (MTTD)** | [hours] |
| **Mean Time To Recover (MTTR)** | [hours] |
| **Critical systems with tested backups** | [count / total] |
| **Crisis communications plan** | [Approved / In progress / Gap] |
| **Cyber insurance coverage** | $[X]m - Renewal: [Date] |
| **External IR retainer** | [Provider / Status] |

# 6. Decisions Requested

A cyber board paper without decisions is a status update. End every report with the decisions the board must make, the options considered, and the recommendation with owner.

| Decision | Options Presented | Recommendation | Owner |
|---|---|---|---|
| [Insert] | [Insert] | [Insert] | [Insert] |
| [Insert] | [Insert] | [Insert] | [Insert] |
| [Insert] | [Insert] | [Insert] | [Insert] |
| [Insert] | [Insert] | [Insert] | [Insert] |

## Appendix - Suggested supporting evidence

Control attestations, audit findings, third-party assurance status, penetration test summaries, vulnerability trend, training completion rates, and any open regulator correspondence.