Information Pack
Tier 1 – Baseline Setup

Provided by Ingest services

Ingest services 2025 Tier 1 – Baseline Setup

Contents

Purpose 2

Why This Matters 2

Context: National Direction 3

The Government's Action Plan includes initiatives such as: 3

Ingest services' Tier 1 supports these objectives by: 3

What Tier 1 Provides 3

These measures align with recognised frameworks: 3

Why Boards Should Care 4

Limitations 4

Alignment with the Australian Cyber Security Strategy 4

Important distinction: 4

Board Actions 5

Engagement Model 5

About the Consultant 5

FAQ – Straight Answers for Boards 6

Closing Note 6

Purpose

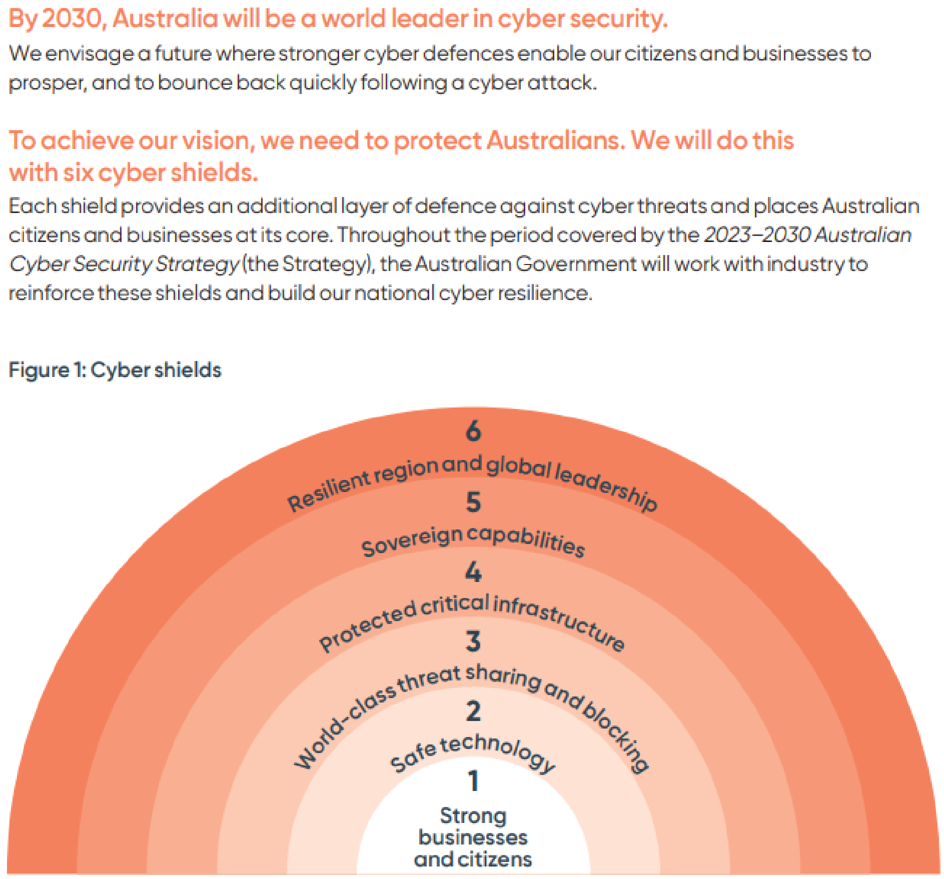
This document provides directors and senior leaders with a clear understanding of what Tier 1 – Baseline Setup achieves, why it matters, and how it relates to Australia’s national cyber security direction. It is intended to support informed governance decisions.

Why This Matters

Cyber security is now a governance issue. Boards are expected to demonstrate that reasonable steps have been taken to protect systems and data.

The **Australian Cyber Security Strategy 2023–2030** and its **Action Plan** set out a national vision for making Australia a world leader in cyber security by 2030. This includes **uplifting the security of small and medium businesses** through practical measures and clear guidance.

While these initiatives are government-led, **businesses remain responsible for their own systems and risk posture**. Tier 1 – Baseline Setup provided by Ingest services, does not implement the government strategy. Instead, it **helps organisations prepare and align with its intent** by addressing common weaknesses in Microsoft 365 environments.



By 2030, Australia will be a world leader in cyber security.

We envisage a future where stronger cyber defences enable our citizens and businesses to prosper, and to bounce back quickly following a cyber attack.

To achieve our vision, we need to protect Australians. We will do this with six cyber shields.

Each shield provides an additional layer of defence against cyber threats and places Australian citizens and businesses at its core. Throughout the period covered by the *2023–2030 Australian Cyber Security Strategy* (the Strategy), the Australian Government will work with industry to reinforce these shields and build our national cyber resilience.

Figure 1: Cyber shields

6
Resilient region and global leadership
5
Sovereign capabilities
4
Protected critical infrastructure
3
World-class threat sharing and blocking
2
Safe technology
1
Strong businesses and citizens

Insert from: 2023–2030 Australian Cyber Security Strategy pg. 6

Context: National Direction

The Strategy identifies six “cyber shields” to make Australia a harder target. The first shield: **Strong Businesses and Citizens** - focuses on improving the resilience of businesses through foundational security measures.

The Government’s Action Plan includes initiatives such as:

- Providing **clear cyber guidance for businesses**.
- Offering **health checks and resilience services** for SMBs.
- Encouraging boards to adopt **better cyber governance practices**.

Ingest services’ Tier 1 supports these objectives by:

- Establishing **basic security hygiene** (multi-factor authentication, email authentication, and audit logging).
- Creating **evidence of due diligence** for insurers, regulators, and stakeholders.
- Preparing organisations for more advanced protections without costly rework.

What Tier 1 Provides

- **Identity Security:** Multi-factor authentication for users and administrators; removal of legacy sign-in methods.
- **Email Trust:** SPF, DKIM, and DMARC to reduce spoofing and phishing risk.
- **Device Readiness:** Basic configuration for secure onboarding and recovery (e.g., BitLocker key escrow).
- **Governance:** Audit logging, role-based access, and documented configurations for accountability.

These measures align with recognised frameworks:

Ingest services bases its Tier packages on two recognised security frameworks, the Essential 8 provided by the ASD (Australian Signals Directorate) and CIS (Centre of Information Security) benchmarks. This approach ensures that recommendations are transparent, evidence-based, and free from bias, within tier 1 these include:

- **ASD Essential Eight (Maturity Levels 1–2)**
  Developed by the **Australian Signals Directorate (ASD)** to help organisations, including SMBs and SMEs, implement practical cyber resilience measures.

- **CIS Microsoft 365 Foundations Benchmark (Level 1)**
  Published by the **Center for Internet Security (CIS)**, a global non-profit that develops consensus-based best practices for securing IT systems.

Why Boards Should Care

- **Risk Reduction:** Addresses common attack vectors that lead to breaches.
- **Regulatory and Insurance Readiness:** Demonstrates reasonable steps and improves responses to due diligence questionnaires.
- **Future-Proofing:** Creates a foundation for advanced security without disruption.

Limitations

Tier 1 is a **starting point**, not a complete solution. It does not include:

- Conditional Access policies
- Endpoint detection and response
- Data loss prevention or insider risk controls
- Continuous monitoring or incident response

These are addressed in later tiers. Boards should **acknowledge residual risk** and plan for progression.

Alignment with the Australian Cyber Security Strategy

Tier 1 contributes to the national effort by:

- Supporting **Shield 1 – Strong Businesses and Citizens** through practical, foundational controls.
- Aligning with **Horizon 1 – Strengthen Foundations**, which calls for improved cyber maturity across entire economy.
- Providing a structured, evidence-based approach that complements, not replaces, government initiatives.

Important distinction:

- The **government sets the policy and provides guidance**.

- **Your organisation remains responsible for its own systems and compliance obligations**.
- Our role is to **help you prepare and demonstrate reasonable steps**, not to implement government programs.

Board Actions

1. **Approve** Tier 1 as the minimum Microsoft 365 setup baseline.
2. **Acknowledge residual risk** and determine whether to progress to higher tiers.
3. **Ensure oversight** of implementation and review of assurance artefacts.

Engagement Model

Tier 1 is delivered under a **Services Contract** with a scoped **Statement of Work (SoW)**.

Engagement process:

1. **Contract Approval –** governance and confidentiality terms.
2. **Pre-Audit Checklist –** capture of current state.
3. **Readiness Items –** access, DNS, branding assets.
4. **Implementation –** staged rollout and validation.
5. **Handover & Support –** documentation, knowledge transfer, and short support window.

This structured approach ensures changes are controlled, auditable, and aligned with organisational governance.

About the Consultant

Jordan Albaladejo

Implementation-focused security and systems engineer, founder of **Ingest services** in Brisbane, Australia.

- Specialist in Microsoft 365 security and compliance projects for SMBs and SMEs.
- Background in MSSP operations, SIEM engineering, and structured hardening engagements.
- Certified in multiple IT and cyber security products and practices.

- Approach: **CIS-aligned, blue team defensive mindset**, ensuring practical, defensible security outcomes.

FAQ – Straight Answers for Boards

Isn't Microsoft 365 secure by default?
No. Defaults prioritise compatibility, not security. MFA, email authentication, and logging are not fully enforced.

Does this make us "fully secure"?
No. Tier 1 is the foundation. It addresses common risks but not advanced threats or monitoring.

How do we know it worked?
You receive a configuration report, Secure Score improvement, and framework mapping.

What's next after Tier 1?
Tier 2 introduces Conditional Access and threat protection. Tier 3 adds data protection, privileged access, and monitoring.

How long does Tier 1 take?
Typically one week, depending on access and approvals.

How soon after signing can work start?
Within a few business days once access and DNS are confirmed.

Can work be done outside business hours?
Yes. Critical changes can be scheduled after hours to minimise disruption.

What if something breaks?
The rollout is staged and tested. Any issues are resolved immediately during the included support window.

Closing Note

Tier 1 is about **readiness and resilience**. It positions your organisation to meet rising expectations from regulators, insurers, and customers, while supporting the broader national objective of making Australia a harder target for cybercrime.