# IT & Cyber Capability Assessment Report

Maturity Benchmarking Across Five Capability Pillars

| | |
|---|---|
| **Organisation:** | **Assessment Preview** |
| **Assessment Date:** | 19 November 2025 |
| **Prepared For:** | Direct Download |
| **Overall Maturity:** | **32%** Developing |

## Assessment Overview

This assessment evaluates organisational maturity across five critical capability areas: ITSM & Service Management, Cyber Security Readiness (Essential 8/ISO/SMB1001), Business Process & Automation, Operational Excellence & Intelligent Automation, and Technical Capability Foundations.

The report identifies strengths, gaps, and priority improvement actions based on responses to 35 validated maturity questions.

# Executive Summary

**Overall Assessment: 32% (Developing)**

*Some structure exists, but consistency, depth, or enforcement is still developing.*

## Capability Pillar Scores

| Capability Pillar | Score | Maturity | Performance |
|---|---|---|---|
| **Operational Excellence & Intelligent Automation** | **14%** | **Initial** | 14% |
| **Technical Capability Foundations** | **29%** | **Initial** | 29% |
| **Business Process & Automation** | **31%** | **Developing** | 31% |
| **ITSM & Service Management Maturity** | **37%** | **Developing** | 37% |
| Cyber Readiness (Essential 8 / ISO / SMB1001) | **49%** | **Developing** | 49% |

### Immediate Priorities

**Operational Excellence & Intelligent Automation** and **Technical Capability Foundations** and **Business Process & Automation** and **ITSM & Service Management Maturity** are the weakest pillars and represent the greatest risk. These areas should be prioritised over the next 90 days to establish foundational controls and reduce organisational exposure.

## Top Recommended Actions

The following actions are derived from your lowest-scoring areas and represent the highest-value improvements:

→ Knowledge documentation is outdated, incomplete, or not used in daily operations. *(ITSM & Service Management Maturity)*

→ Service performance is not tracked meaningfully, limiting the ability to improve service delivery. *(ITSM & Service Management Maturity)*

→ Logging, monitoring, and alerting are incomplete or inconsistent, creating blind spots in threat detection. *(Cyber Readiness (Essential 8 / ISO / SMB1001))*

→ Documentation is outdated or inaccessible, creating inconsistent process execution. *(Business Process & Automation)*

→ Manual execution of routine tasks leads to inefficiency and risk of human error. *(Operational Excellence & Intelligent Automation)*

# Priority Pillar Analysis

## Operational Excellence & Intelligent Automation

**14%** Initial

*Operational practices are mostly reactive with limited monitoring, automation, or governance.*

**Strengths Identified**

Limited strengths identified in this area.

**Priority Improvements**

- ⚠ Manual execution of routine tasks leads to inefficiency and risk of human error.
- ⚠ Intelligent automation opportunities remain unimplemented, leading to preventable manual work.
- ⚠ Root cause analysis is inconsistent or absent, causing repetitive incidents.

## Technical Capability Foundations

**29%** Initial

*Technical foundations such as identity, device management, networks, and DR require significant uplift.*

**Strengths Identified**

- ✓ Cloud adoption or readiness planning is well-defined and progressing.

**Priority Improvements**

- ⚠ Identity controls are fragmented, manual, or inconsistent.
- ⚠ Network segmentation is limited or outdated, increasing lateral movement risk.
- ⚠ Backup or DR architecture cannot meet required recovery objectives.

# Secondary Priority Pillars

## Cyber Readiness (Essential 8 / ISO / SMB1001)

**49%** Developing

*Some cyber controls exist, but enforcement is uneven or incomplete. Key areas such as MFA, patching, logging, or backup testing require improvement to meet Essential 8 and SMB1001 expectations.*

**Strengths**

- ✓ Cyber controls are well aligned with Essential 8, ISO 27001, or SMB1001 requirements.
- ✓ MFA is fully enforced for all staff and administrator accounts.

**Priority Improvements**

- ⚠ Logging, monitoring, and alerting are incomplete or inconsistent, creating blind spots in threat detection.
- ⚠ Backups are unreliable or untested, creating high risk of data loss during incidents.

# Established Capability Pillars

## Improvement Roadmap

Based on your maturity assessment, the following phased approach will systematically address your capability gaps:

## Phase 1 – Foundations

*Address foundational capability gaps that affect stability, risk, and predictability.*

### **ITSM & Service Management Maturity** (Developing)

ITSM processes exist but lack consistency or maturity. Improvements are needed in documentation, governance, and service quality measurement.

- Strengthen governance around change and escalation processes.
- Expand your knowledge base with up-to-date, searchable documentation.
- Improve SLA tracking and introduce regular service performance reviews.

### **Cyber Readiness (Essential 8 / ISO / SMB1001)** (Developing)

Some cyber controls exist, but enforcement is uneven or incomplete. Key areas such as MFA, patching, logging, or backup testing require improvement to meet Essential 8 and SMB1001 expectations.

- Fully enforce MFA for all privileged accounts.
- Expand endpoint protection enforcement to any uncovered devices.
- Increase the frequency and reliability of backup testing.

### **Business Process & Automation** (Developing)

Processes show structure but lack maturity, with inconsistent automation or unclear integration.

- Expand automation to multi-step workflows and common approvals.
- Improve data flow between systems by aligning integration points.
- Update training materials to reflect new processes.

### **Operational Excellence & Intelligent Automation** (Initial)

Operational practices are mostly reactive with limited monitoring, automation, or governance.

- Establish core monitoring and alerting for critical systems.
- Document basic operating procedures for routine tasks.
- Identify high-frequency manual tasks suitable for automation.

### **Technical Capability Foundations** (Initial)

Technical foundations such as identity, device management, networks, and DR require significant uplift.

- Introduce strong identity lifecycle management with enforced access controls.
- Deploy central device management and enforce security baselines.
- Document network segmentation strategy and begin implementing modern controls.

# Framework Recommendations

The following framework recommendations are based on your assessment scores and reflect realistic readiness for each certification pathway.

### **Essential 8** (Score-based recommendation)

**Posture:** Developing - Strengthen Level 1 and Plan for Level 2

Your cyber security controls show partial maturity. Strengthen existing Essential 8 Level 1 controls to ensure consistent enforcement, then begin planning your path to Level 2 maturity.

**Timeline:** Level 1 completion within 3-6 months, Level 2 within 12-18 months.

**Next Steps:**

- Complete Essential 8 Level 1 gaps and ensure consistent enforcement
- Begin collecting evidence for compliance validation
- Develop roadmap for Level 2 maturity uplift

### **SMB1001** (Score-based recommendation)

**Posture:** Too Early for Formal Certification

Current maturity across cyber, process, and operations is not yet sufficient for SMB1001 certification. Use SMB1001 as a practical roadmap to guide your security uplift, focusing on foundational controls first.

**Timeline:** Build foundations for 6-12 months before pursuing Bronze certification.

**Next Steps:**

- Use SMB1001 Bronze requirements as a practical improvement checklist
- Focus on MFA, backups, patching, and incident response basics
- Revisit certification once foundational controls are established

## How Integralis Can Help

**Based on your assessment results, the area where we can provide quickest impact is Operational Excellence & Intelligent Automation.**

We can help establish operational excellence & intelligent automation controls and begin framework alignment within 30-60 days.

**Our services include:**

- Cyber security gap assessments and Essential 8/SMB1001 implementation
- ITSM design, implementation, and maturity uplift (ServiceNow, FreshService)
- Technical infrastructure assessment and modernisation
- Business process automation and workflow integration
- Managed security services and ongoing operational support

## Contact Information

**Email:** contact@integralis.com.au
**Website:** www.integralis.com.au
**Response Time:** We typically respond within 24 hours

---

**Thank you for completing the IT & Cyber Capability Assessment**
Report generated 19 November 2025 for Assessment Preview