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:	**27%** 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: 27% (Developing)

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

Capability Pillar Scores

Capability Pillar	Score	Maturity	Performance
ITSM & Service Management Maturity	23%	Foundational	23%
Business Process & Automation	23%	Foundational	23%
Operational Excellence & Intelligent Automation	29%	Developing	29%
Cyber Readiness (Essential 8 / ISO / SMB1001)	31%	Developing	31%
Technical Capability Foundations	31%	Developing	31%

Immediate Priorities

ITSM & Service Management Maturity and **Business Process & Automation** and **Operational Excellence & Intelligent Automation** and **Cyber Readiness (Essential 8 / ISO / SMB1001)** and **Technical Capability Foundations** 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:

→ Service desk processes are inconsistent or undocumented, leading to variable service quality. *(ITSM & Service Management Maturity)*

→ Knowledge documentation is outdated, incomplete, or not used in daily operations.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

→ Endpoint protection is missing or inconsistently deployed across devices, creating significant detection gaps. *(Cyber Readiness (Essential 8 / ISO / SMB1001))*

→ Business processes are inconsistent or undocumented, creating operational variability. *(Business Process & Automation)*

→ Documentation is outdated or inaccessible, creating inconsistent process execution.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

Priority Pillar Analysis

ITSM & Service Management Maturity

23% **Foundational**

ITSM processes are inconsistent or informal. Core practices such as incident, change, and service catalog management require structured definition and adoption.

Strengths Identified

Limited strengths identified in this area.

Priority Improvements

- ⚠ Service desk processes are inconsistent or undocumented, leading to variable service quality.
- ⚠ Knowledge documentation is outdated, incomplete, or not used in daily operations.
- ⚠ Change management is informal or incomplete, increasing the risk of outages and service disruption.

Business Process & Automation

23% **Foundational**

Business processes are informal or inconsistent, with limited documentation and minimal automation.

Strengths Identified

Limited strengths identified in this area.

Priority Improvements

- ⚠ Business processes are inconsistent or undocumented, creating operational variability.
- ⚠ Documentation is outdated or inaccessible, creating inconsistent process execution.
- ⚠ Manual processes remain unidentified or unaddressed, limiting efficiency gains.

Established Capability Pillars

90-Day Improvement Roadmap

Focus on your two weakest pillars (ITSM & Service Management Maturity and Business Process & Automation and Operational Excellence & Intelligent Automation and Cyber Readiness (Essential 8 / ISO / SMB1001) and Technical Capability Foundations) to achieve measurable risk reduction within 90 days:

Phase 1: Days 0-30 (Stabilise)

- Document core ITSM processes for incident, request, change, and escalation.
- Create a foundational service catalog and publish it for users.
- Introduce basic SLAs and begin tracking performance.
- Document core business processes and standard operating procedures.
- Identify manual processes with the highest time impact.
- Introduce foundational workflow tools for simple automation.

Phase 2: Days 30-90 (Improve)

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: Foundational - Establish Level 1 Baseline

Your cyber security maturity is foundational. Focus on establishing Essential 8 Maturity Level 1 controls across all eight mitigation strategies. Prioritise MFA, patching, and application control as immediate actions.

Timeline: Level 1 achievable within 6-9 months with focused effort.

Next Steps:

- Conduct Essential 8 gap assessment against Level 1 requirements
- Prioritise MFA enforcement and patch management
- Document current state and create uplift roadmap

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 ITSM & Service Management Maturity.

We can help establish itsm & service management maturity 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