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:	**58%** Established

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: 58% (Established)

Most capabilities are in good shape, with opportunities to refine and automate.

Capability Pillar Scores

Capability Pillar	Score	Maturity	Performance
ITSM & Service Management Maturity	**14%**	**Initial**	14%
Business Process & Automation	**51%**	**Established**	51%
Cyber Readiness	**57%**	**Established**	57%
Technical Capability Foundations	**80%**	**Managed**	80%
Operational Excellence	**89%**	**Managed**	89%

Immediate Priorities

ITSM & Service Management Maturity is the weakest pillar and represents the greatest risk. This area 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:

→ Change management is informal or incomplete, increasing the risk of outages and service disruption. *(ITSM & Service Management Maturity)*

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

Priority Pillar Analysis

ITSM & Service Management Maturity

14% **Initial**

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

- ⚠ Change management is informal or incomplete, increasing the risk of outages and service disruption.
- ⚠ Service performance is not tracked meaningfully, limiting the ability to improve service delivery.
- ⚠ Service desk processes are inconsistent or undocumented, leading to variable service quality.

Secondary Priority Pillars

Business Process & Automation

51% **Established**

Processes are well-documented and increasingly automated, with reliable workflow consistency.

Strengths

- ✓ Business processes are clearly documented and consistently followed.

Priority Improvements

- ⚠ Documentation is outdated or inaccessible, creating inconsistent process execution.
- ⚠ Apps and systems have poor integration or inconsistent data flow, creating manual work and errors.

Established Capability Pillars

Technical Capability Foundations

80% **Managed**

Technical capabilities are robust, automated, and aligned with leading engineering and platform practices.

Strengths Identified

- ✓ Identity lifecycle is centralised with strong joiner/mover/leaver controls.
- ✓ Devices are centrally managed with enforced baselines and compliance reporting.
- ✓ Network segmentation and security controls follow strong modern best practices.

Improvement Opportunities

- ⚠ Introduce engineering automation for platform updates and compliance checks.
- ⚠ Deploy advanced telemetry and predictive performance analytics.
- ⚠ Integrate technical metrics into business reporting dashboards.

Operational Excellence

89% **Managed**

Operational excellence is proactive and data-driven with automation and intelligent tooling embedded across workflows.

Strengths Identified

- ✓ Monitoring and alerting provide strong visibility across systems with proactive issue detection.
- ✓ Routine operational tasks are automated, improving efficiency and consistency.
- ✓ Intelligent or rules-based tools successfully support decision-making and reduce manual effort.

Improvement Opportunities

- ⚠ Introduce predictive analytics for outage prevention.
- ⚠ Implement fully automated remediation scripts for common issues.
- ⚠ Align operational excellence KPIs with strategic business outcomes.

Improvement Roadmap

Based on your maturity assessment, focus on these priority areas:

Immediate Priorities (Next 30 Days)

Focus on your weakest areas to achieve quick wins and reduce risk.

ITSM & Service Management Maturity (Initial)

- 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.

Business Process & Automation (Established)

- Introduce advanced workflow automation across departments.
- Implement monitoring dashboards to track process performance.
- Standardise integration patterns across business applications.

Secondary Focus (Days 30-90)

Build on initial improvements with these enhancements.

Cyber Readiness (Established)

- Align cyber controls with SMB1001 and Essential 8 Level 2 requirements.
- Develop formal evidence collections for audits and client assurance.
- Expand monitoring and logging to full coverage for all critical systems.

Ongoing Optimization

Maintain and enhance your stronger capabilities.

- Conduct quarterly capability reviews
- Establish continuous improvement processes
- Monitor performance metrics and KPIs
- Plan strategic technology investments

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: Bronze Tier Feasible with Focused Uplift

Your organisation demonstrates sufficient maturity to pursue SMB1001 Bronze certification with focused effort. Bronze provides a practical, achievable baseline that strengthens cyber resilience for small to medium organisations.

Timeline: Bronze certification achievable within 6-9 months.

Next Steps:

- Conduct SMB1001 Bronze gap assessment
- Address priority gaps in cyber, process, and operational controls
- Engage SMB1001 assessor once Bronze readiness is achieved

ISO 27001 (Score-based recommendation)

Posture: Begin Alignment - Certification is a Medium-Term Goal

Your organisation demonstrates sufficient maturity to begin ISO 27001 alignment activities. Certification is achievable as a medium-term goal (12-18 months) with structured ISMS development and gap remediation.

Timeline: ISO 27001 certification achievable within 12-18 months.

Next Steps:

- Conduct ISO 27001 gap assessment against Annex A controls
- Establish ISMS framework and document management system
- Address priority gaps and build toward Stage 1 audit readiness

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