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:	**47%** 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: 47% (Developing)

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

Capability Pillar Scores

Capability Pillar	Score	Maturity	Performance
ITSM & Service Management Maturity	**14%**	**Initial**	14%
Business Process & Automation	**31%**	**Developing**	31%
Cyber Readiness (Essential 8 / ISO / SMB1001)	**60%**	**Established**	60%
Technical Capability Foundations	**63%**	**Established**	63%
Operational Excellence & Intelligent Automation	**69%**	**Established**	69%

Immediate Priorities

ITSM & Service Management Maturity and **Business Process & Automation** 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:

→ Incidents are handled inconsistently, causing delays and repeat issues. *(ITSM & Service Management Maturity)*

→ Knowledge documentation is outdated, incomplete, or not used in daily operations.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

→ Service catalog or self-service functions are unclear or underused, increasing manual workload. *(ITSM & Service Management Maturity)*

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

→ Manual processes remain unidentified or unaddressed, limiting efficiency gains. *(Business Process & Automation)*

Priority Pillar Analysis

ITSM & Service Management Maturity

14% Initial

undefined

Strengths Identified

Limited strengths identified in this area.

Priority Improvements

- ⚠ Incidents are handled inconsistently, causing delays and repeat issues.
- ⚠ Knowledge documentation is outdated, incomplete, or not used in daily operations.
- ⚠ Service catalog or self-service functions are unclear or underused, increasing manual workload.

Business Process & Automation

31% Developing

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

Strengths Identified

- ✓ Cross-team workflows are structured, reducing handoff delays and errors.

Priority Improvements

- ⚠ Business processes are inconsistent or undocumented, creating operational variability.
- ⚠ Manual processes remain unidentified or unaddressed, limiting efficiency gains.
- ⚠ Apps and systems have poor integration or inconsistent data flow, creating manual work and errors.

Secondary Priority Pillars

Cyber Readiness (Essential 8 / ISO / SMB1001)

60% Established

Core cyber controls are generally strong, with good coverage across identity, endpoints, access, and recovery. Remaining work focuses on consistency, automation, and deeper alignment with SMB1001 and ISO.

Strengths

- ✓ Patching and vulnerability remediation are consistently performed following a defined schedule.
- ✓ Cyber controls are well aligned with Essential 8, ISO 27001, or SMB1001 requirements.

Priority Improvements

- ⚠ MFA is not consistently enforced for staff or administrators, leaving accounts exposed to credential-based attacks.
- ⚠ Backups are unreliable or untested, creating high risk of data loss during incidents.

Established Capability Pillars

Operational Excellence & Intelligent Automation 69% Established

Operational practices are consistent, automated, and regularly reviewed.

Strengths Identified

- ✓ Monitoring and alerting provide strong visibility across systems with proactive issue detection.
- ✓ Operations follow clearly documented standard procedures.
- ✓ Event correlation and RCA processes effectively identify recurring issues.

Improvement Opportunities

- ⚠ Capacity and availability issues are detected late, increasing the risk of outages.

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 (Initial)

undefined

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.

Phase 2 – Stabilisation

Tighten processes, improve visibility, and lift consistency across operations.

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

Core cyber controls are generally strong, with good coverage across identity, endpoints, access, and recovery. Remaining work focuses on consistency, automation, and deeper alignment with SMB1001 and ISO.

- 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.

Operational Excellence & Intelligent Automation (Established)

Operational practices are consistent, automated, and regularly reviewed.

- Implement event correlation and automated RCA insights.

- Optimise automation coverage and remove remaining manual steps.
- Enhance governance cadence with measurable outcomes.

Technical Capability Foundations (Established)

Technical foundations are strong with sound identity, device, network, and platform governance.

- Expand observability and telemetry across all core systems.
- Optimise network segmentation and strengthen micro-segmentation.
- Formalise governance processes for cross-platform lifecycle activities.

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

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