IT & Cyber Capability Assessment Report

Maturity Benchmarking Across Five Capability Pillars

Organisation:	**Integralis**
Assessment Date:	19 November 2025
Prepared For:	Kelly Pellas
Overall Maturity:	**38%** 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: 38% (Developing)

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

Capability Pillar Scores

Capability Pillar	Score	Maturity	Performance
Operational Excellence	**29%**	**Initial**	**29%**
Business Process & Automation	**31%**	**Developing**	**31%**
ITSM & Service Management Maturity	**34%**	**Developing**	**34%**
Technical Capability Foundations	**40%**	**Developing**	**40%**
Cyber Readiness	**54%**	**Established**	**54%**

Immediate Priorities

Operational Excellence and **Business Process & Automation** and **ITSM & Service Management Maturity** 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)*

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

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

→ Approvals are manual or email-driven, causing delays and inconsistent outcomes. *(Business Process & Automation)*

→ Process outcomes are not measured, limiting insight into performance and bottlenecks. *(Business Process & Automation)*

Priority Pillar Analysis

Operational Excellence

29% Initial

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

Strengths Identified

- ✓ Capacity and availability are routinely monitored with proactive mitigation.

Priority Improvements

- ⚠ Monitoring is limited or reactive, leading to delayed issue detection.
- ⚠ Intelligent automation opportunities remain unimplemented, leading to preventable manual work.
- ⚠ Manual execution of routine tasks leads to inefficiency and risk of human error.

Business Process & Automation

31% Developing

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

Strengths Identified

- ✓ Training materials and process documentation are updated, accessible, and widely used.

Priority Improvements

- ⚠ Approvals are manual or email-driven, causing delays and inconsistent outcomes.
- ⚠ Process outcomes are not measured, limiting insight into performance and bottlenecks.
- ⚠ Business processes are inconsistent or undocumented, creating operational variability.

Secondary Priority Pillars

Cyber Readiness

54% 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

- ✓ All devices have endpoint protection deployed and actively reporting.
- ✓ Cyber controls are well aligned with Essential 8, ISO 27001, or SMB1001 requirements.

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, focus on these priority areas:

Immediate Priorities (Next 30 Days)

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

Operational Excellence (Initial)

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

Business Process & Automation (Developing)

- 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.

Secondary Focus (Days 30-90)

Build on initial improvements with these enhancements.

ITSM & Service Management Maturity (Developing)

- 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.

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: 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.

We can help establish operational excellence 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 Integralis