INTEGRALIS

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:	**30%** Initial

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: 30% (Initial)

undefined

Capability Pillar Scores

Capability Pillar	Score	Maturity	Performance
Cyber Readiness (Essential 8 / ISO / SMB1001)	**20%**	**Initial**	20%
Technical Capability Foundations	**23%**	**Initial**	23%
ITSM & Service Management Maturity	**31%**	**Developing**	31%
Operational Excellence & Intelligent Automation	**31%**	**Developing**	31%
Business Process & Automation	**46%**	**Developing**	46%

Immediate Priorities

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

→ 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)*

→ MFA is not consistently enforced for staff or administrators, leaving accounts exposed to credential-based attacks. *(Cyber Readiness (Essential 8 / ISO / SMB1001))*

→ Admin rights are poorly controlled or excessive, increasing the risk of privilege-based attacks. *(Cyber Readiness (Essential 8 / ISO / SMB1001))*

→ Cyber controls are not aligned with Essential 8, ISO 27001, or SMB1001 requirements, creating compliance and audit risks. *(Cyber Readiness (Essential 8 / ISO / SMB1001))*

Priority Pillar Analysis

Cyber Readiness (Essential 8 / ISO / SMB1001)

20% Initial

Cyber controls are inconsistent or missing across identity, devices, access, and recovery. The environment is highly vulnerable to common attacks, and several Essential 8 baseline requirements are not met.

Strengths Identified

Limited strengths identified in this area.

Priority Improvements

- ⚠ MFA is not consistently enforced for staff or administrators, leaving accounts exposed to credential-based attacks.
- ⚠ Admin rights are poorly controlled or excessive, increasing the risk of privilege-based attacks.
- ⚠ Cyber controls are not aligned with Essential 8, ISO 27001, or SMB1001 requirements, creating compliance and audit risks.

Technical Capability Foundations

23% Initial

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

Strengths Identified

Limited strengths identified in this area.

Priority Improvements

- ⚠ Identity controls are fragmented, manual, or inconsistent.
- ⚠ Network segmentation is limited or outdated, increasing lateral movement risk.
- ⚠ Platform governance is inconsistent or undefined, creating unmanaged risks.

Secondary Priority Pillars

Business Process & Automation

46% Developing

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

Strengths

- ✓ Manual processes have been identified, prioritised, and some are already automated.

Priority Improvements

- ⚠ Approvals are manual or email-driven, causing delays and inconsistent outcomes.
- ⚠ Process outcomes are not measured, limiting insight into performance and bottlenecks.

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.

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

- Implement MFA for all staff and administrators and enforce it consistently.
- Deploy endpoint protection across all devices, including laptops, servers, and workstations.
- Establish reliable, secure backups and test recovery regularly.

Technical Capability Foundations (Initial)

- 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.

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 Cyber Readiness (Essential 8 / ISO / SMB1001).

We can help establish cyber readiness (essential 8 / iso / smb1001) 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