IT & Cyber Capability Assessment

Test Organisation

51%

Established

Prepared for: Test User

19 November 2025

Executive Summary

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

This assessment evaluates your organisation's maturity across five critical capability pillars, providing a comprehensive view of your IT and cyber readiness.

Capability Assessment by Pillar

ITSM & Service Management Maturity

69%

Established

ITSM practices are mature and well-governed. Opportunities remain in automation, optimisation, and proactive service management.

Cyber Readiness (Essential 8 / ISO / SMB1001)

40%

Developing

Some cyber controls exist, but enforcement is uneven or incomplete. Key areas such as MFA, patching, logging, or backup testing require improvement to meet Essential 8 and SMB1001 expectations.

Business Process & Automation

63%

Established

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

Operational Excellence & Intelligent Automation

31%

Developing

Some operational structure is emerging, but automation and consistency need improvement.

Technical Capability Foundations

54%

Established

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

Key Strengths

Your organisation demonstrates strong capability in these areas:

ITSM & Service Management Maturity: Service Desk Process Consistency
Service desk processes are well-documented and followed consistently across the organisation.

ITSM & Service Management Maturity: SLAs & Performance Visibility
SLAs and KPIs are actively tracked, reviewed, and used to drive improvements.

Business Process & Automation: Process Documentation
Business processes are clearly documented and consistently followed.

Business Process & Automation: Integration & Data Flow
Applications are well-integrated with reliable data flow and minimal duplication.

Technical Capability Foundations: Device Management
Devices are centrally managed with enforced baselines and compliance reporting.

Priority Improvement Areas

These areas require immediate attention to improve your overall capability:

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

Cyber Readiness (Essential 8 / ISO / SMB1001): Patching and vulnerability remediation
Patching and vulnerability remediation are irregular or reactive, increasing exposure to known threats.

Operational Excellence & Intelligent Automation: Event Correlation & Root Cause Analysis
Root cause analysis is inconsistent or absent, causing repetitive incidents.

Operational Excellence & Intelligent Automation: Operational Governance
Operational governance is irregular, reducing visibility and improvement traction.

Technical Capability Foundations: Tooling & Platform Governance
Platform governance is inconsistent or undefined, creating unmanaged risks.

Framework Alignment & Recommendations

Essential 8

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

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

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

Prioritised Action Plan

Based on your assessment, focus on these priority actions:

High **Operational Excellence & Intelligent Automation**

Expand monitoring coverage and establish performance baselines.

High **Operational Excellence & Intelligent Automation**

Automate multi-step operational tasks such as provisioning and checks.

High **Operational Excellence & Intelligent Automation**

Introduce intelligent rules or lightweight AI features to reduce manual workload.

Medium **Cyber Readiness (Essential 8 / ISO / SMB1001)**

Fully enforce MFA for all privileged accounts.

Medium **Cyber Readiness (Essential 8 / ISO / SMB1001)**

Expand endpoint protection enforcement to any uncovered devices.

Medium **Cyber Readiness (Essential 8 / ISO / SMB1001)**

Increase the frequency and reliability of backup testing.

Medium **Technical Capability Foundations**

Expand observability and telemetry across all core systems.

Medium **Technical Capability Foundations**

Optimise network segmentation and strengthen micro-segmentation.

Medium **Technical Capability Foundations**

Formalise governance processes for cross-platform lifecycle activities.

Low **ITSM & Service Management Maturity**

Automate routine workflows in ITSM tooling (assignments, approvals, categorisation).

Next Steps with Integralis

To transform these insights into action:

- **Schedule a consultation:** Review your assessment results with our experts
- **Develop a roadmap:** Create a tailored improvement plan aligned to your business goals
- **Access expertise:** Leverage Integralis' deep experience in IT transformation and cyber security
- **Track progress:** Establish metrics and milestones for continuous improvement

Contact us at **assessment@integralis.com.au** to discuss your results and next steps.

Integralis
www.integralis.com.au
This report is confidential and prepared specifically for Test Organisation