INTEGRALIS

IT & Cyber Capability Assessment Report

Maturity Benchmarking Across Five Capability Pillars

Organisation:	**Test Company Pty Ltd**
Assessment Date:	19 November 2025
Prepared For:	John Smith
Overall Maturity:	**0%** **Foundational**

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

Core practices are largely ad hoc or missing, with significant room for improvement.

Maturity Scores by Capability Pillar

Capability Pillar	Score	Maturity Level
ITSM & Service Management Maturity	0%	Foundational
Cyber Readiness (Essential 8 / ISO / SMB1001)	0%	Foundational
Business Process & Automation	0%	Foundational
Operational Excellence & Intelligent Automation	0%	Foundational
Technical Capability Foundations	0%	Foundational

Key Strengths

Priority Improvement Areas

ITSM & Service Management Maturity

Current Maturity

0% Foundational

ITSM processes are inconsistent or informal. Core practices such as incident, change, and service catalog management require structured definition and adoption.

Assessment Results

Capability Area	Score
Service Desk Process Consistency	**undefined%**
Incident Management Maturity	**undefined%**
Change Management Control	**undefined%**
Knowledge Management	**undefined%**
Service Catalog & Self-Service	**undefined%**
SLAs & Performance Visibility	**undefined%**
Continual Service Improvement	**undefined%**

Cyber Readiness (Essential 8 / ISO / SMB1001)

Current Maturity

0% **Foundational**

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.

Assessment Results

Capability Area	Score
MFA and identity protections	**undefined%**
Endpoint protection (EDR/XDR)	**undefined%**
Patching and vulnerability remediation	**undefined%**
Backup reliability and testing	**undefined%**
Admin rights and least privilege	**undefined%**
Logging and monitoring	**undefined%**
Framework alignment (E8/ISO/SMB1001)	**undefined%**

Business Process & Automation

Current Maturity

0% Foundational

Business processes are informal or inconsistent, with limited documentation and minimal automation.

Assessment Results

Capability Area	Score
Process Documentation	**undefined%**
Workflow Automation Adoption	**undefined%**
Integration & Data Flow	**undefined%**
Approval Workflow Automation	**undefined%**
Documentation & Training	**undefined%**
Process Metrics	**undefined%**
Cross-team Workflows	**undefined%**

Operational Excellence & Intelligent Automation

Current Maturity

0% Foundational

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

Assessment Results

Capability Area	Score
Monitoring & Alerting	**undefined%**
Standardised Operating Procedures	**undefined%**
Automation of Routine Tasks	**undefined%**
Intelligent Tools (AI-Assisted)	**undefined%**
Capacity & Availability Management	**undefined%**
Event Correlation & Root Cause Analysis	**undefined%**
Operational Governance	**undefined%**

Technical Capability Foundations

Current Maturity

0% Foundational

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

Assessment Results

Capability Area	Score
Identity & Access Management	**undefined%**
Device Management	**undefined%**
Network Segmentation & Security	**undefined%**
Backup & DR Architecture	**undefined%**
Cloud Readiness	**undefined%**
Tooling & Platform Governance	**undefined%**
Observability & Engineering Practices	**undefined%**

Framework Alignment & Recommendations

Based on your maturity assessment, the following frameworks and standards are recommended to guide your improvement journey:

Essential 8 (Foundational - Establish Level 1 Baseline)

Your cyber security maturity is foundational. Focus on establishing Essential 8 Maturity Level 1 controls across all eight mitigation strategies. Prioritise MFA, patching, and application control as immediate actions.

→ Conduct Essential 8 gap assessment against Level 1 requirements

→ Prioritise MFA enforcement and patch management

→ Document current state and create uplift roadmap

SMB1001 (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.

→ 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

Next Steps

1. Review detailed findings with your leadership team
2. Prioritise improvement initiatives based on business impact and risk
3. Develop a roadmap aligned with recommended frameworks
4. Establish metrics and regular assessment cycles to track progress
5. Consider engaging specialist support for critical capability gaps