IT & Cyber Capability Assessment Report

Maturity Benchmarking Across Five Capability Pillars

Organisation:	**Test Company Ltd**
Assessment Date:	19 November 2025
Prepared For:	Jane 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

Priority Pillar Analysis

ITSM & Service Management Maturity

0% Foundational

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

Strengths Identified

Limited strengths identified in this area

Priority Improvements

⚠ Continue monitoring and optimisation

Cyber Readiness (Essential 8 / ISO / SMB1001)

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.

Strengths Identified

Limited strengths identified in this area

Priority Improvements

⚠ Continue monitoring and optimisation

Secondary Priority Pillars

Business Process & Automation

0% Foundational

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

Strengths

Building foundations

Priority Improvements

⚠ Continue current progress

Established Capability Pillars

Operational Excellence & Intelligent Automation

0% Foundational

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

Strengths Identified

- ✓ Consistent performance maintained

Optimisation Opportunities

- → Establish core monitoring and alerting for critical systems.
- → Document basic operating procedures for routine tasks.

Technical Capability Foundations

0% Foundational

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

Strengths Identified

- ✓ Consistent performance maintained

Optimisation Opportunities

- → Introduce strong identity lifecycle management with enforced access controls.
- → Deploy central device management and enforce security baselines.

90-Day Improvement Roadmap

Focus on your two weakest pillars (ITSM & Service Management Maturity and Cyber Readiness (Essential 8 / ISO / SMB1001)) to achieve measurable risk reduction within 90 days:

Phase 1: Days 0-30 (Stabilise)

- Document core ITSM processes for incident, request, change, and escalation.
- Create a foundational service catalog and publish it for users.
- Introduce basic SLAs and begin tracking performance.
- 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.

Phase 2: Days 30-60 (Strengthen)

- Document core business processes and standard operating procedures.
- Identify manual processes with the highest time impact.

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