INTEGRALIS

IT & Cyber Capability Assessment Report

Organisation	Test Company
Prepared For	John Smith
Assessment Date	19 November 2025
Overall Maturity	**Foundational** (0/100)

This report provides a comprehensive assessment of your organisation's IT and cyber capabilities, identifying strengths, gaps, and providing actionable recommendations for improvement.

Executive Summary

Overall Assessment

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

Capability Scores by Pillar

Capability Pillar	Score	Maturity Level
ITSM & Service Management Maturity	0/100	Foundational
Cyber Readiness (Essential 8 / ISO / SMB1001)	0/100	Foundational
Business Process & Automation	0/100	Foundational
Operational Excellence & Intelligent Automation	0/100	Foundational
Technical Capability Foundations	0/100	Foundational

ITSM & Service Management Maturity

Overall Score: 0/100	**Maturity Level:** Foundational

Current State Assessment

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

Individual Components

Component	Score	Status
Service Desk Process Consistency	0	⚠ Gap
Incident Management Maturity	0	⚠ Gap
Change Management Control	0	⚠ Gap
Knowledge Management	0	⚠ Gap
Service Catalog & Self-Service	0	⚠ Gap
SLAs & Performance Visibility	0	⚠ Gap
Continual Service Improvement	0	⚠ Gap

Priority Improvements

- **Service Desk Process Consistency:** Service desk processes are inconsistent or undocumented, leading to variable service quality.
- **Incident Management Maturity:** Incidents are handled inconsistently, causing delays and repeat issues.
- **Change Management Control:** Change management is informal or incomplete, increasing the risk of outages and service disruption.
- **Knowledge Management:** Knowledge documentation is outdated, incomplete, or not used in daily operations.

- **Service Catalog & Self-Service:** Service catalog or self-service functions are unclear or underused, increasing manual workload.
- **SLAs & Performance Visibility:** Service performance is not tracked meaningfully, limiting the ability to improve service delivery.
- **Continual Service Improvement:** Continuous improvement is ad hoc or absent, limiting long-term service enhancement.

Recommended Actions

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

Cyber Readiness (Essential 8 / ISO / SMB1001)

Overall Score: 0/100	**Maturity Level:** Foundational

Current State Assessment

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.

Individual Components

Component	Score	Status
MFA and identity protections	0	⚠ Gap
Endpoint protection (EDR/XDR)	0	⚠ Gap
Patching and vulnerability remediation	0	⚠ Gap
Backup reliability and testing	0	⚠ Gap
Admin rights and least privilege	0	⚠ Gap
Logging and monitoring	0	⚠ Gap
Framework alignment (E8/ISO/SMB1001)	0	⚠ Gap

Priority Improvements

- **MFA and identity protections:** MFA is not consistently enforced for staff or administrators, leaving accounts exposed to credential-based attacks.
- **Endpoint protection (EDR/XDR):** Endpoint protection is missing or inconsistently deployed across devices, creating significant detection gaps.
- **Patching and vulnerability remediation:** Patching and vulnerability remediation are irregular or reactive, increasing exposure to known threats.
- **Backup reliability and testing:** Backups are unreliable or untested, creating high risk of data loss during incidents.

- **Admin rights and least privilege:** Admin rights are poorly controlled or excessive, increasing the risk of privilege-based attacks.
- **Logging and monitoring:** Logging, monitoring, and alerting are incomplete or inconsistent, creating blind spots in threat detection.
- **Framework alignment (E8/ISO/SMB1001):** Cyber controls are not aligned with Essential 8, ISO 27001, or SMB1001 requirements, creating compliance and audit risks.

Recommended Actions

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

Business Process & Automation

Overall Score: 0/100	**Maturity Level:** Foundational

Current State Assessment

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

Individual Components

Component	Score	Status
Process Documentation	0	⚠ Gap
Workflow Automation Adoption	0	⚠ Gap
Integration & Data Flow	0	⚠ Gap
Approval Workflow Automation	0	⚠ Gap
Documentation & Training	0	⚠ Gap
Process Metrics	0	⚠ Gap
Cross-team Workflows	0	⚠ Gap

Priority Improvements

- **Process Documentation:** Business processes are inconsistent or undocumented, creating operational variability.
- **Workflow Automation Adoption:** Manual processes remain unidentified or unaddressed, limiting efficiency gains.
- **Integration & Data Flow:** Apps and systems have poor integration or inconsistent data flow, creating manual work and errors.
- **Approval Workflow Automation:** Approvals are manual or email-driven, causing delays and inconsistent outcomes.

- **Documentation & Training:** Documentation is outdated or inaccessible, creating inconsistent process execution.
- **Process Metrics:** Process outcomes are not measured, limiting insight into performance and bottlenecks.
- **Cross-team Workflows:** Cross-team workflows lack clarity, causing delays and inconsistent outcomes.

Recommended Actions

1. Document core business processes and standard operating procedures.
2. Identify manual processes with the highest time impact.
3. Introduce foundational workflow tools for simple automation.

Operational Excellence & Intelligent Automation

Overall Score: 0/100	**Maturity Level:** Foundational

Current State Assessment

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

Individual Components

Component	Score	Status
Monitoring & Alerting	0	⚠ Gap
Standardised Operating Procedures	0	⚠ Gap
Automation of Routine Tasks	0	⚠ Gap
Intelligent Tools (AI-Assisted)	0	⚠ Gap
Capacity & Availability Management	0	⚠ Gap
Event Correlation & Root Cause Analysis	0	⚠ Gap
Operational Governance	0	⚠ Gap

Priority Improvements

- **Monitoring & Alerting:** Monitoring is limited or reactive, leading to delayed issue detection.
- **Standardised Operating Procedures:** Operational procedures are inconsistent or outdated, creating variability in outcomes.
- **Automation of Routine Tasks:** Manual execution of routine tasks leads to inefficiency and risk of human error.
- **Intelligent Tools (AI-Assisted):** Intelligent automation opportunities remain unimplemented, leading to preventable manual work.

- **Capacity & Availability Management:** Capacity and availability issues are detected late, increasing the risk of outages.
- **Event Correlation & Root Cause Analysis:** Root cause analysis is inconsistent or absent, causing repetitive incidents.
- **Operational Governance:** Operational governance is irregular, reducing visibility and improvement traction.

Recommended Actions

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

Technical Capability Foundations

Overall Score: 0/100	**Maturity Level:** Foundational

Current State Assessment

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

Individual Components

Component	Score	Status
Identity & Access Management	0	⚠ Gap
Device Management	0	⚠ Gap
Network Segmentation & Security	0	⚠ Gap
Backup & DR Architecture	0	⚠ Gap
Cloud Readiness	0	⚠ Gap
Tooling & Platform Governance	0	⚠ Gap
Observability & Engineering Practices	0	⚠ Gap

Priority Improvements

- **Identity & Access Management:** Identity controls are fragmented, manual, or inconsistent.
- **Device Management:** Devices lack centralised management or consistent baseline enforcement.
- **Network Segmentation & Security:** Network segmentation is limited or outdated, increasing lateral movement risk.
- **Backup & DR Architecture:** Backup or DR architecture cannot meet required recovery objectives.

- **Cloud Readiness:** Cloud readiness is unclear or unplanned, limiting flexibility and scalability.
- **Tooling & Platform Governance:** Platform governance is inconsistent or undefined, creating unmanaged risks.
- **Observability & Engineering Practices:** Observability is limited, reducing visibility into system performance and failures.

Recommended Actions

1. Introduce strong identity lifecycle management with enforced access controls.
2. Deploy central device management and enforce security baselines.
3. Document network segmentation strategy and begin implementing modern controls.

Framework Alignment & Recommendations

Essential 8

Recommended Posture: 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.

Implementation Timeline: Level 1 achievable within 6-9 months with focused effort.

Next Steps:

- Conduct Essential 8 gap assessment against Level 1 requirements
- Prioritise MFA enforcement and patch management
- Document current state and create uplift roadmap

SMB1001

Recommended 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.

Implementation 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

Prioritised Action Plan

Based on your assessment results, we recommend focusing on the following actions to improve your IT and cyber capabilities:

Priority	Capability Area	Recommended Action
High	ITSM & Service Management Maturity	Document core ITSM processes for incident, request, change, and escalation.
High	ITSM & Service Management Maturity	Create a foundational service catalog and publish it for users.
High	ITSM & Service Management Maturity	Introduce basic SLAs and begin tracking performance.
High	Cyber Readiness (Essential 8 / ISO / SMB1001)	Implement MFA for all staff and administrators and enforce it consistently.
High	Cyber Readiness (Essential 8 / ISO / SMB1001)	Deploy endpoint protection across all devices, including laptops, servers, and workstations.
High	Cyber Readiness (Essential 8 / ISO / SMB1001)	Establish reliable, secure backups and test recovery regularly.
High	Business Process & Automation	Document core business processes and standard operating procedures.
High	Business Process & Automation	Identify manual processes with the highest time impact.
High	Business Process & Automation	Introduce foundational workflow tools for simple automation.

Priority	Capability Area	Recommended Action
High	Operational Excellence & Intelligent Automation	Establish core monitoring and alerting for critical systems.