INTEGRALIS

IT & Cyber Capability Assessment Report

Organisation	Assessment Preview
Prepared For	Direct Download
Assessment Date	19 November 2025
Overall Maturity	**Foundational** (25/100)

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	37/100	Developing
Cyber Readiness (Essential 8 / ISO / SMB1001)	26/100	Developing
Business Process & Automation	20/100	Foundational
Operational Excellence & Intelligent Automation	23/100	Foundational
Technical Capability Foundations	17/100	Foundational

Key Organisational Strengths

- **Service Catalog & Self-Service** (ITSM & Service Management Maturity): A well-structured service catalog and self-service portal provide users with clear pathways for support.

Priority Improvement Areas

- **Change Management Control** (ITSM & Service Management Maturity): Change management is informal or incomplete, increasing the risk of outages and service disruption.
- **MFA and identity protections** (Cyber Readiness (Essential 8 / ISO / SMB1001)): MFA is not consistently enforced for staff or administrators, leaving accounts exposed to credential-based attacks.
- **Backup reliability and testing** (Cyber Readiness (Essential 8 / ISO / SMB1001)): Backups are unreliable or untested, creating high risk of data loss during incidents.

- **Workflow Automation Adoption** (Business Process & Automation): Manual processes remain unidentified or unaddressed, limiting efficiency gains.
- **Integration & Data Flow** (Business Process & Automation): Apps and systems have poor integration or inconsistent data flow, creating manual work and errors.

ITSM & Service Management Maturity

Overall Score: 37/100	**Maturity Level:** Developing

Current State Assessment

ITSM processes exist but lack consistency or maturity. Improvements are needed in documentation, governance, and service quality measurement.

Individual Components

Component	Score	Status
Service Desk Process Consistency	20	⚠ Gap
Incident Management Maturity	60	→ Developing
Change Management Control	0	⚠ Gap
Knowledge Management	40	⚠ Gap
Service Catalog & Self-Service	80	✓ Strong
SLAs & Performance Visibility	20	⚠ Gap
Continual Service Improvement	40	⚠ Gap

Key Strengths

- **Service Catalog & Self-Service:** A well-structured service catalog and self-service portal provide users with clear pathways for support.

Priority Improvements

- **Service Desk Process Consistency:** Service desk processes are inconsistent or undocumented, leading to variable service quality.
- **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.
- **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. Strengthen governance around change and escalation processes.
2. Expand your knowledge base with up-to-date, searchable documentation.
3. Improve SLA tracking and introduce regular service performance reviews.

Cyber Readiness (Essential 8 / ISO / SMB1001)

Overall Score: 26/100	**Maturity Level:** Developing

Current State Assessment

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.

Individual Components

Component	Score	Status
MFA and identity protections	0	⚠ Gap
Endpoint protection (EDR/XDR)	20	⚠ Gap
Patching and vulnerability remediation	40	⚠ Gap
Backup reliability and testing	0	⚠ Gap
Admin rights and least privilege	40	⚠ Gap
Logging and monitoring	20	⚠ Gap
Framework alignment (E8/ISO/SMB1001)	60	→ Developing

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.

Recommended Actions

1. Fully enforce MFA for all privileged accounts.
2. Expand endpoint protection enforcement to any uncovered devices.
3. Increase the frequency and reliability of backup testing.

Business Process & Automation

Overall Score: 20/100	**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	60	→ Developing
Workflow Automation Adoption	0	⚠ Gap
Integration & Data Flow	0	⚠ Gap
Approval Workflow Automation	40	⚠ Gap
Documentation & Training	0	⚠ Gap
Process Metrics	20	⚠ Gap
Cross-team Workflows	20	⚠ Gap

Priority Improvements

- **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: 23/100	**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	60	→ Developing
Automation of Routine Tasks	60	→ Developing
Intelligent Tools (AI-Assisted)	20	⚠ Gap
Capacity & Availability Management	0	⚠ Gap
Event Correlation & Root Cause Analysis	20	⚠ Gap
Operational Governance	0	⚠ Gap

Priority Improvements

- **Monitoring & Alerting:** Monitoring is limited or reactive, leading to delayed issue detection.
- **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: 17/100	**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	40	⚠ Gap
Device Management	0	⚠ Gap
Network Segmentation & Security	20	⚠ Gap
Backup & DR Architecture	40	⚠ Gap
Cloud Readiness	0	⚠ Gap
Tooling & Platform Governance	20	⚠ 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	Strengthen governance around change and escalation processes.
High	ITSM & Service Management Maturity	Expand your knowledge base with up-to-date, searchable documentation.
High	ITSM & Service Management Maturity	Improve SLA tracking and introduce regular service performance reviews.
High	Cyber Readiness (Essential 8 / ISO / SMB1001)	Fully enforce MFA for all privileged accounts.
High	Cyber Readiness (Essential 8 / ISO / SMB1001)	Expand endpoint protection enforcement to any uncovered devices.
High	Cyber Readiness (Essential 8 / ISO / SMB1001)	Increase the frequency and reliability of backup testing.
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.
High	Operational Excellence & Intelligent Automation	Establish core monitoring and alerting for critical systems.

INTEGRALIS

Building Better IT Capabilities for Australian Businesses

www.integralis.com.au | assessment@integralis.com.au