EXAMPLE Essential Eights /Cyber Security Assessment Report

Organisation:	InnovateTech Pty Ltd
Date:	6 November 2025
Assessor:	CyberSecure Consulting
Assessment Scope:	Stage 1 Assessment
Maturity Assessment:	Level 1

Executive Summary

InnovateTech engaged CyberSecure Consulting to assess the current cybersecurity posture against the Australian Cyber Security Centre (ACSC) Essential Eight Maturity Level 1.
The assessment determined that while several controls are well-implemented, the organisation **does not yet fully meet Maturity Level 1 requirements**. Three key areas require urgent attention to manage immediate cyber risks: Multi-Factor Authentication (MFA) for privileged access, complete Application Control coverage, and timely backup testing.

- **Key Strengths:** Strong Operating System patching process and effective user application hardening.
- **Major Weaknesses:** Gaps in MFA implementation and backup restoration testing frequency.
- **Overall Risk:** The current posture leaves the organisation vulnerable to common attack vectors, particularly those involving credential theft and system compromise.

Assessment Overview

The Essential Eight framework comprises eight critical mitigation strategies designed to make it much harder for adversaries to compromise systems. Maturity Level 1 represents a foundational level of cyber hygiene.
The scope of this assessment covered all corporate workstations, key servers, and internet-facing services within the InnovateTech environment.

Detailed Findings and Status

The table below provides a high-level status for each of the eight strategies at Maturity Level 1.

Mitigation Strategy	Status	Key Finding
1. Application Control	Partial	Solution implemented, but does not block execution in temporary internet file locations.
2. Patch Applications	Partial	Most applications patched, but the critical CRM internet-facing application missed the 2-week deadline.
3. Patch Operating Systems	Met	All servers and workstations patched within the required one-month timeframe via automated system.

4. Multi-factor Authentication	Partial	Used for VPN access, but not for internal administrative/privileged logons.
5. Restrict Admin Privileges	Met	Principle of least privilege is enforced; admin access is logged and accounts are limited
6. Restrict Microsoft Office Macros	Partial	GPOs block most macros, but several sales staff have approved exceptions that lack sufficient security justification
7. User Application Hardening	Met	All applications are vendor-supported; web browsers are configured to block Java and Flash from the internet
8. Regular Backups	Partial	Daily backups are run, but the last restoration test was 6 months ago (ML1 requires quarterly testing)

Priority Recommendations

The following actions are recommended to achieve full Maturity Level 1 alignment and uplift the organisation's cyber resilience.

Priority	Recommendation	Business Impact
HIGH	Implement Multi-Factor Authentication for *all* privileged user accounts (local and domain)	Prevents attackers from using stolen credentials to gain administrative control
HIGH	Update Application Control rules to cover all temporary execution paths (e.g., temporary internet files)	Stops malware from running in common download locations
MEDIUM	Ensure all internet-facing service patches are applied within *two weeks* of release	Protects public-facing systems from known critical vulnerabilities
MEDIUM	Update the Disaster Recovery plant to included mandatory quarterly backup restoration testing	Ensures data can be recovered reliably in case of a ransomware attack or system failure
LOW	Review and remove unnecessary Microsoft Office macro exceptions for sales staff	Reduces the attack surface for email-based phishing attacks