Deploy IQ

Sample Essential Eight Assessment Report

Illustrative Only — Not a real customer report

Prepared for: ExampleCo Pty Ltd
Status: SAMPLE
Report date: 09 Feb 2026

Document details

Assessment

Assessment Details	
Essential Eight version	Feb 2026
System security classification	OFFICIAL: Sensitive
Report template alignment	Aligned to ACSC Essential Eight Assessment Report Template

Prepared by

Organisation	Deploy IQ Pty Ltd
Assessor name	Sample Assessor
Contact email	info@deployiq.co
Address	Sydney, NSW, Australia

Prepared for

Entity name	ExampleCo Pty Ltd
Contact name	Alex Example (fictional)
Contact email	alex@exampleco.example
Address	Australia (example)

Revision history

Version	Date	Description	Author
0.1	09 Feb 2026	Initial sample report for website preview	Deploy IQ
1.0	09 Feb 2026	Public sample (sanitised)	Deploy IQ

Disclaimer: This sample is provided for illustrative purposes only and does not represent a completed assessment for any real organisation.

Executive summary

This sample Essential Eight assessment report demonstrates the format and depth of reporting customers receive from Deploy IQ. All entity details, findings, and evidence in this document are fictional and included only to illustrate typical reporting outputs.

Assessment snapshot

System under assessment	ExampleCo M365 tenant, endpoints, and core line-of-business applications (example)
Target maturity level	Maturity Level 2 (example)
Overall maturity outcome	Mixed: 3/8 strategies at ML2, 4/8 at ML1, 1/8 below ML1 (example)
Top risk themes	Patch currency; admin privilege sprawl; macro controls; backup recoverability (example)
Priority next steps	Close critical gaps, then standardise ML2 across all eight strategies (example)

Key positive findings (examples)

• Multi-factor authentication is enforced for privileged access and remote access pathways (example).

• Centralised endpoint protection and logging is in place for most managed devices (example).

Key risks and gaps (examples)

• Inconsistent patching of internet-facing applications increases exposure to rapid exploitation (example).

• Administrative privileges are not consistently restricted to privileged access workstations (example).

• Backup testing is irregular, and immutable backup protections are not consistently applied (example).

Recommendations overview (examples)

1. Implement a risk-based patch SLA for internet-facing and high-value applications (example).

2. Reduce admin privilege sprawl and enforce just-in-time access for privileged roles (example).

3. Harden Office macro execution and enforce signed macros only (example).

4. Implement immutable backups and quarterly restore tests for critical systems (example).

Introduction

Background

The Essential Eight is a set of eight prioritised mitigation strategies designed to reduce the likelihood and impact of common cyber attacks. This sample report illustrates how Deploy IQ documents maturity outcomes, evidence, and prioritised recommendations.

Scope

In-scope (example):

- Microsoft 365 tenant configuration (Entra ID, Exchange Online, SharePoint Online)
- Managed Windows endpoints for corporate users
- Backup solution for critical business data

Out-of-scope (example):

- Operational technology (OT) environments
- Unmanaged personal devices

Approach

This sample assumes a mixed-method assessment approach (example):

- Configuration review against Essential Eight requirements
- Sampling of endpoints and user accounts
- Evidence collection from management portals and logs

Limitations

This sample report does not include real evidence or screenshots. In a live engagement, limitations are documented here (e.g., access constraints, sampling exclusions).

Detailed findings

Note: For website readability, this sample includes two fully worked examples and summarises the remaining strategies.

Patch applications

Findings (example)

Outcome: Partially effective at target maturity. Patch deployment is inconsistent for some internet-facing applications (example).

Requirement	Implementation status	Test type	Assessment justification
Internet-facing applications are patched within defined SLA (example)	Not Effective	Config review + vulnerability scan sample	Several exposed services exceeded patch SLA (example).
Automated patch reporting is implemented (example)	Effective	Portal evidence review	Central reporting exists for managed assets (example).
Emergency patch process for critical vulnerabilities (example)	Not Implemented	Interview + process review	No documented process for expedited remediation (example).

Recommendations (example)

• Define and enforce patch SLAs by application criticality and exposure (example).

• Establish an emergency change pathway for critical CVEs (example).

Multi-factor authentication

Findings (example)

Outcome: Effective at target maturity for privileged accounts; gaps remain for legacy authentication pathways (example).

Requirement	Implementation status	Test type	Assessment justification
MFA enforced for all privileged accounts (example)	Effective	Tenant configuration review	Conditional Access covers privileged roles (example).
MFA enforced for all remote access (example)	Effective	Config review	VPN and cloud access require MFA (example).

Legacy authentication blocked (example)	Not Effective	Sign-in logs review	Legacy protocols detected for small subset (example).

Recommendations (example)

• Disable legacy authentication and remediate dependent applications (example).

• Extend MFA coverage to service accounts using modern auth patterns (example).

Summary of remaining strategies (example)

• Patch operating systems: Mostly ML1; inconsistent reboot cadence (example).

• Restrict administrative privileges: Below target; excessive standing admin rights (example).

• Application control: Mixed; allowlisting not consistently enforced (example).

• Restrict Microsoft Office macros: Below target; policy exceptions exist (example).

• User application hardening: Mostly ML2; some legacy browser features enabled (example).

• Regular backups: ML1; restore testing not consistent (example).

Summary of recommendations

1. Implement risk-based patch SLAs for internet-facing applications and document emergency patch procedures. (example).

2. Reduce standing privileged access and adopt just-in-time access for administrative tasks. (example).

3. Harden Microsoft Office macro settings and enforce signed macros only. (example).

4. Implement immutable backups and schedule quarterly restore tests for critical workloads. (example).

5. Standardise maturity level targets across all eight strategies to reduce weak-link exposure. (example).

Appendix A — Assessment evidence (sample)

In a live engagement, this appendix includes supporting evidence (e.g., screenshots, exports, scan summaries). This public sample lists example evidence types only.

- Conditional Access policy export (example)
- Endpoint patch compliance summary (example)
- Backup job configuration and restore test records (example)

Attribution: Assessment structure aligned to the ACSC Essential Eight Assessment Report Template (November 2023).