WHITE PAPER

USEZER
Essential Eight Cybersecurity Framework

Assessment | Maturity Uplift | Implementation Services

About USEZER – USEZER Pty Ltd, an Australian-owned company headquartered in Sydney, extends its operations to regional offices in Sri Lanka, New Zealand and Singapore. We prioritize customer satisfaction by providing innovative and flexible IT services that enhance business productivity. Distinguished as a Technology Services Company, we offer simple, customer-focused solutions on a fixed-fee basis. Founded in mid-2018, USEZER Pty Ltd was born from the vision of key individuals determined to overcome the inefficiencies faced by traditional IT systems integrators.

Introduction

In today's threat landscape, cyberattacks are not only more frequent—they are more sophisticated, targeted, and disruptive. Australian organizations, especially those operating in critical industries, are expected to adopt proactive cybersecurity strategies that go beyond basic protection. The Australian Cyber Security Centre (ACSC)'s Essential Eight (E8) framework is a proven baseline for minimizing cyber risk.

The Essential Eight outlines eight mitigation strategies that, when implemented effectively, can prevent over 85% of common cyber threats. However, understanding your current maturity level, identifying gaps, and implementing these strategies effectively can be complex.

USEZER helps organizations address this challenge through a practical and outcome-driven approach to Essential Eight compliance. Whether you're starting from scratch or aiming to uplift from Maturity Level 1 to Level 2 or beyond, our assessment and implementation services provide clear guidance, expert remediation, and tailored cybersecurity outcomes.

Our methodology is aligned with ACSC guidelines, the Information Security Manual (ISM), and government frameworks like the Protective Security Policy Framework (PSPF). With a strong presence in regulated sectors—including financial services, city councils, and infrastructure—USEZER brings technical expertise, operational experience, and strategic clarity to your cyber uplift journey.

Objective of this Document

This whitepaper provides a structured overview of how **USEZER** delivers Essential Eight (E8) assessment, implementation, and uplift services aligned with the Australian Cyber Security Centre's framework.
It outlines:

- The approach used to assess current maturity across the eight mitigation strategies
- How maturity gaps are identified and prioritized
- The delivery of actionable, remediation-focused roadmaps
- The tools, automation, and methods applied during and after implementation
- USEZER's alignment to recognised frameworks, including the Information Security Manual (ISM) and Protective Security Policy Framework (PSPF)

This document is intended for organisations seeking to enhance their cybersecurity posture, meet regulatory requirements, or engage a specialist partner for Essential Eight compliance. It is suitable for both cloud-based and on-premises environments across the public and private sectors.

About USEZER

USEZER is a cybersecurity and infrastructure services provider supporting organisations across public, private, and regulated sectors in the Asia-Pacific region. We deliver tailored security programs that improve cyber maturity, align with compliance standards, and enhance operational resilience.
Our work spans across cloud, hybrid, and on-premises environments, helping clients meet the requirements of frameworks such as the ACSC Essential Eight, Information Security Manual (ISM), and ISO 27001. We support both advisory-led assessments and hands-on implementation, ensuring outcomes are not just documented but delivered.

Our Cybersecurity Services

Cybersecurity Frameworks & Maturity

- Essential Eight assessments, gap analysis, and uplift programs
- Security control reviews aligned with ISM and ISO 27001
- Compliance readiness and advisory for audits and frameworks

Threat Detection & Response

- Managed Detection & Response (MDR)
- SIEM and 24/7 SOC Operations.
- Incident response planning and readiness assessments

Identity, Access & Application Security

- Identity and access control design (IAM, PAM)
- Application control implementation and policy enforcement
- Multi-factor authentication and privileged access hardening

Endpoint, Network & Cloud Security

- Endpoint protection and integration
- Managed firewall and network security services
- Secure Access Service Edge (SASE) enablement
- Cloud security posture assessment and remediation

Vulnerability & Data Protection

- Vulnerability management and patch automation
- Email threat protection and phishing defence
- Data loss prevention (DLP) and backup strategy advisory

The Essentials Eight Explained

The Essential Eight is a set of baseline cybersecurity mitigation strategies published by the Australian Cyber Security Centre (ACSC). It is designed to help organisations prevent, limit, and recover from cybersecurity incidents by focusing on the most common and impactful threats.

The framework provides a practical and structured approach to improving security posture across endpoint devices, applications, user behaviour, and data protection. It is particularly relevant for organisations operating in regulated environments, or those seeking alignment with the Information Security Manual (ISM) and Protective Security Policy Framework (PSPF).

Each of the eight strategies is explored in the following pages, including their purpose, maturity levels, and how USEZER supports implementation and uplift.

1 . Application Control

Purpose

Prevent the execution of unapproved or malicious software, including executables, scripts, installers, and control panel applets.

Why It Matters

Application control reduces the attack surface by ensuring only trusted applications can run. This stops malware and unauthorised tools from being executed, especially via email, external devices, or compromised websites.

Implementation Focus

- Maintain a central allowlist of approved applications
- Block execution from temporary folders and user profiles
- Apply rules to workstations and internet-facing servers
- Monitor and log all allowed and blocked executions
- Periodically review and validate control rulesets

Threats Prevented

- Ransomware and malware delivered via phishing or drive-by attacks
- Unauthorised remote tools and scripting utilities
- Lateral movement through unmanaged software.

How USEZER Helps

USEZER implements application control by defining and enforcing allowlisting policies across endpoints and servers. We help design baseline application profiles, block unauthorised or risky executables, and monitor execution attempts. Our service includes ruleset validation, logging enablement, and guidance for achieving and sustaining maturity alignment.

Maturity Level	Tool Support & USEZER Services
Level 1	Allowlisting on workstations, execution logging
Level 2	Server enforcement, driver block rules, annual validation
Level 3	Event log protection, real-time monitoring, integration with SIEM

2. Application Patching

Purpose

Ensure that third-party applications and business-critical software are regularly patched to mitigate known vulnerabilities and prevent exploitation.

Why It Matters

Outdated applications are among the most common paths to compromise. Timely, automated patching of third-party software significantly reduces the likelihood of successful malware delivery or privilege escalation.

Implementation Focus

- Conduct regular vulnerability scans on all applications
- Identify and prioritise missing patches based on severity and exploitability
- Apply vendor patches and mitigation updates within defined timeframes
- Remove unsupported or legacy applications that can't be secured
- Maintain audit-ready records of patching activity

Threats Prevented

- Exploitation of known software vulnerabilities
- Malware delivery through compromised applications
- Initial access and lateral movement using unpatched third-party tools

How USEZER Helps

USEZER conducts patch management assessments and implements application update processes aligned with maturity-level targets. This includes setting patching schedules, enabling centralised update control, performing regular vulnerability scans, and ensuring timely remediation. We support clients in applying risk-based prioritisation and maintaining compliance with patching SLAs.

Maturity Level	Tool Support & USEZER Services
Level 1	Acronis vulnerability scanning and automated patching of apps; daily scans on internet-facing assets
Level 2	Fortnightly scans and patching for office apps, email clients, browsers; risk-prioritised patching
Level 3	Critical patches deployed within 48 hours; unsupported apps removed; continuous posture validation

3. Restrict Microsoft Office Macros

Purpose
Prevent the execution of potentially malicious macros embedded in Microsoft Office documents, particularly those originating from external or untrusted sources.

Why It Matters
Macros are commonly used in phishing attacks to deliver malware or initiate lateral movement. Blocking or tightly controlling macro execution significantly reduces this risk.

Implementation Focus
- Block macros from Office files originating from the internet
- Prevent users from enabling or modifying macro settings
- Allow only signed macros from trusted publishers or verified locations
- Enable macro scanning through endpoint protection tools
- Monitor macro-related events and enforce centralised policies

Threats Prevented
- Initial compromise via phishing attachments with embedded scripts
- Malware execution triggered through macro automation
- Persistence or privilege escalation via macro-based attacks

How USEZER Helps

USEZER restricts macro execution by applying centrally managed policies and securing macro-enabled environments. We block untrusted sources, enforce macro scanning, and support allowlisting for signed or trusted macros where business requirements apply. This ensures organisations minimise macro-based attack vectors while preserving user productivity.

Maturity Level	Tool Support & USEZER Services
Level 1	Macros blocked from internet sources; macro settings locked via Intune/GPO
Level 2	Logging of macro execution events; Office configured to block Win32 API calls
Level 3	Only signed macros in trusted locations allowed; logging monitored via Airlock/SIEM

4. User Application Hardening

Purpose
Harden commonly used applications such as web browsers, Office suites, and PDF readers to reduce exploitable functionality and enforce secure configurations.

Why It Matters
Exploits often leverage features like Java, macros, or scripting in everyday applications. Disabling or restricting these features closes off common attack vectors and reduces the risk of compromise.

Implementation Focus
- Remove deprecated or insecure applications (e.g. IE11, Flash, Java)
- Harden browser, Office, and PDF settings using vendor and ASD guidance
- Block risky application behaviors (e.g. macros spawning processes, code injection)
- Enforce centrally managed settings that users cannot override
- Enable secure scripting configurations and centralised event logging

Threats Prevented
- Browser-based and malvertising attacks
- Document-based code injection (e.g. VBA, OLE, PDF exploits)
- Unmonitored script execution or process spawning
- Lateral movement or persistence through user-level tools

How USEZER Helps

USEZER hardens user-facing applications by disabling high-risk features, aligning browser and Office configurations to vendor and ASD guidance, and locking down scripting functionality where applicable. We help organisations prevent code injection, script abuse, and ad-based attacks by securing applications and restricting changes to user settings.

Maturity Level	Tool Support & USEZER Services
Level 1	Browser Java/ads disabled; OLE and Office process controls applied
Level 2	PDF and Office hardened using ASD/vendor guidance; PowerShell logging enabled
Level 3	Event logs centrally monitored; script execution tightly restricted; security settings protected

5. Restrict Admin Privileges

Purpose
Limit administrative access to systems, applications, and infrastructure to only those who require it, and only when it is needed.

Why It Matters
Administrative accounts are prime targets for attackers. Restricting and monitoring privileged access reduces the risk of lateral movement, persistence, and full-environment compromise.

Implementation Focus
- Apply least privilege principles across all user roles
- Use separate accounts for administrative and standard activities
- Prevent admin accounts from accessing email, internet, and web services
- Enforce just-in-time (JIT) or time-bound access for elevated privileges
- Audit, log, and regularly review all privilege assignments

Threats Prevented
- Credential theft and misuse of admin accounts
- Lateral movement via privileged sessions
- Persistent access to critical systems or infrastructure
- Use of privilege escalation tools post-compromise

How USEZER Helps

USEZER reviews administrative access across systems and environments to enforce least privilege. We implement role-based access models, enforce separation of duties, establish privileged account workflows, and introduce time-bound or just-in-time access. We also support logging and regular review of privileged activities in alignment with maturity requirements.

Maturity Level	Tool Support & USEZER Services
Level 1	Admin accounts restricted from internet/email; separate admin/user accounts enforced
Level 2	JIT access implemented; inactive access auto-revoked; credentials managed centrally
Level 3	Privilege access logs monitored; Credential Guard enabled; full SIEM integration for audit trail

6. Multi-Factor Authentication

Purpose
Require users to verify their identity using two or more authentication factors before accessing critical systems or data.

Why It Matters
Passwords alone are no longer sufficient protection. MFA significantly reduces the risk of credential theft, phishing attacks, and unauthorised access—even when login details are compromised.

Implementation Focus
- Enforce MFA for all internet-facing services
- Apply MFA to privileged, administrative, and remote access accounts
- Require MFA for third-party and cloud-based services handling sensitive data
- Use phishing-resistant MFA methods where possible
- Monitor and log authentication events centrally

Threats Prevented
- Credential compromise through phishing or brute force
- Unauthorised access to business systems or cloud services
- Account misuse following leaked or reused passwords

How USEZER Helps

USEZER assists with MFA implementation across cloud, on-prem, and third-party services. We assess current coverage, define policies for privileged and high-risk access, and deploy phishing-resistant MFA where required. Our process ensures alignment with maturity expectations and integration with identity and access management processes.

Maturity Level	Tool Support & USEZER Services
Level 1	MFA enabled for users accessing internet-facing services
Level 2	MFA enforced for privileged and high-risk users; phishing-resistant MFA introduced
Level 3	Phishing-resistant MFA extended organisation-wide; authentication logs centrally monitored

7. Regular Backups

Purpose
Ensure that critical data, applications, and configurations are backed up regularly and securely, enabling recovery in the event of data loss or a cyber incident.

Why It Matters
Backups are the final layer of defence against ransomware, accidental deletion, and system corruption. Without secured and tested backups, organisations may face significant downtime or permanent data loss.

Implementation Focus
- Perform scheduled backups of important systems and data
- Store backups in a secure, resilient location—isolated from production
- Restrict access to backups (even for privileged users)
- Test backup restoration as part of disaster recovery exercises
- Protect backups from unauthorised modification or deletion

Threats Prevented
- Data loss due to ransomware, system failure, or human error
- Inability to restore services after a cyber incident
- Backup tampering or destruction by threat actors

How USEZER Helps

USEZER develops and maintains backup strategies tailored to business continuity requirements. We configure secure backup storage, enforce access controls, support immutable retention policies, and test recovery as part of DR planning. Our service includes role-based restrictions and monitoring to ensure backup integrity and maturity compliance.

Maturity Level	Tool Support & USEZER Services
Level 1	Backups configured and retained per recovery needs
Level 2	Secure storage; non-admin access blocked; recovery tested
Level 3	Immutable backups enforced; admin tamper protection; backup logs monitored

8. Patch Operating Systems

Purpose

Ensure that operating systems across servers, endpoints, and network devices are kept up to date with the latest vendor patches to protect against known vulnerabilities.

Why It Matters

Operating systems are a primary target for attackers. Unpatched systems create opportunities for privilege escalation, remote code execution, and malware deployment. Regular and timely patching significantly reduces these risks.

Implementation Focus

- Regularly scan for missing OS patches
- Apply updates within timeframes defined by risk (e.g. 48 hours if exploited)
- Remove unsupported or end-of-life operating systems
- Automate patch deployment where possible
- Maintain audit logs for patch status and completion

Threats Prevented

- Exploitation of OS vulnerabilities (e.g. RDP flaws, privilege escalation bugs)
- Malware or ransomware installation on unpatched hosts
- Network compromise through outdated or misconfigured systems

How USEZER Helps

USEZER configures and manages operating system patching for servers and endpoints across cloud and hybrid environments. We help establish patching baselines, enforce required timelines, remove unsupported systems, and integrate reporting and compliance tracking into operational routines.

Maturity Level	Tool Support & USEZER Services
Level 1	Internet-facing systems are patched within two weeks; daily vulnerability scanning is performed
Level 2	Workstations and servers are patched within one month; vulnerability scanning conducted fortnightly
Level 3	Critical patches are applied within 48 hours; unsupported operating systems are removed; patch logs are centrally monitored

USEZER's Tooling Strategy for E8

Airlock Digital

Overview

Airlock Digital provides allowlisting-based application control and script execution restriction, enabling strict enforcement of what can run on endpoints and servers. It offers high-confidence execution control and visibility for security and compliance teams.

Supports the Following E8 Controls

- Application Control – Enforces allowlists, logs executions, supports rule validation
- User Application Hardening – Blocks PowerShell misuse and scripting-based attacks
- Restrict Microsoft Office Macros – Prevents macro-enabled content from launching executables
- Restrict Administrative Privileges – Supports script control on privileged accounts

How It Supports Maturity

Airlock Digital enables organisations to meet higher E8 maturity levels by enforcing allowlisting at the OS level, monitoring execution events, and blocking unauthorised applications and scripts. This level of control helps meet Maturity Level 2 and 3 outcomes, with strong visibility and audit support for execution policies.

Integration with USEZER Services

USEZER delivers Airlock Digital as either a one-time implementation or as part of an ongoing managed service. Our team handles full platform onboarding including allowlist policy design, environment profiling, deployment to endpoints and servers, and ruleset tuning.
We also offer ongoing policy validation, exception handling, log review, and execution monitoring as a managed service — ensuring the platform remains aligned with operational changes and E8 maturity goals over time.

Acronis Cyber Protect

Acronis Cyber Protect

Overview

Acronis Cyber Protect combines vulnerability scanning, patch management, and backup into a single agent platform designed for hybrid infrastructure and endpoint protection.

Supports the Following E8 Controls

- Patch Applications – Automates patching of third-party applications
- Patch Operating Systems – Supports timely patching across OS workloads
- Regular Backups – Backs up endpoints and Microsoft 365 workloads with access controls and immutability
- User Application Hardening – Monitors and blocks malicious application behaviour

How It Supports Maturity

Acronis helps organisations achieve Maturity Level 2 and above by consolidating patching and backup tasks with central management, access controls, and scheduled recovery testing. It enables faster vulnerability remediation and improves resilience against ransomware and data loss.

Integration with USEZER Services

USEZER delivers Acronis as a fully configured solution for endpoint protection, patch automation, vulnerability scanning, and Microsoft 365 backup. We handle one-time deployment across hybrid infrastructure and assist in configuring retention, recovery policies, and reporting.

We also offer a managed service for continuous patch coverage, backup health monitoring, restore testing, and alert triage, ensuring alignment with maturity-level timelines and recovery readiness

Microsoft

Entra, Intune, Azure, Defender

Overview

Microsoft's security stack provides policy enforcement, identity protection, system hardening, and backup capabilities across cloud and on-premises environments.

Supports the Following E8 Controls

- Patch Applications – Manages application update policies
- Patch Operating Systems – Applies OS updates using update rings and automation
- Restrict Microsoft Office Macros – Enforces macro policies using Intune or GPO
- User Application Hardening – Applies attack surface reduction rules and baseline configurations
- Restrict Administrative Privileges – Enforces role-based access and just-in-time elevation
- Multi-Factor Authentication – Provides native MFA and Conditional Access
- Regular Backups – Supports backup of Azure-hosted workloads

How It Supports Maturity

Microsoft's tools enable broad E8 control coverage for organisations with Microsoft-based infrastructure. These tools support structured patching, user access enforcement, application configuration, and data protection — all aligned with Maturity Levels 1–3 depending on implementation depth.

Integration with USEZER Services

USEZER configures Microsoft-native tools to enforce patching, macro policies, hardening baselines, access control, and backup across Microsoft 365 and Azure environments. One-off engagements typically include baseline deployment, configuration reviews, and policy enforcement tailored to E8 controls.
Ongoing management services include policy monitoring, compliance drift remediation, patch tracking, and reporting. These are designed to help organisations maintain maturity-level alignment and prepare for compliance assessments.

SentinelOne

Overview

SentinelOne is an integrated EDR and SIEM platform that provides real-time threat detection, response automation, and centralised security event logging. It enables continuous visibility across endpoints while collecting and correlating events to support incident detection and response.

Supports the Following E8 Controls

- User Application Hardening – Provides behavioural detection and real-time blocking of script-based and in-memory exploits that bypass static controls
- Restrict Microsoft Office Macros – Detects macro-driven attack chains including child process spawning and suspicious Office behaviours
- Restrict Administrative Privileges – Monitors live abuse of administrative tools (e.g. PSExec, cmd) and triggers alerts or automated response
- SIEM Functionality – Acts as the central log ingestion and analysis platform for correlating events across all E8 control areas

How It Supports Maturity

SentinelOne helps organisations achieve Maturity Levels 2 and 3 by detecting and stopping sophisticated threats that bypass preventive controls. It enhances visibility into macro behaviour, application misuse, and privilege abuse, while feeding events into a SIEM for monitoring and response. This supports ACSC expectations for log monitoring, alerting, and incident detection tied to multiple E8 strategies.

Integration with USEZER Services

USEZER provides SentinelOne as part of its managed SOC offering, covering deployment, configuration, log monitoring, threat detection, and response support. Our team manages the platform continuously to ensure effective detection, alerting, and incident coordination aligned with Essential Eight maturity objectives.

Okta and Duo

Overview

Okta and Duo provide adaptive and phishing-resistant multi-factor authentication for modern IT environments. They help enforce strong identity protection across cloud, on-premises, VPNs, and third-party platforms.

Supports the Following E8 Controls

- Multi-Factor Authentication – Provides flexible, risk-based MFA across diverse systems
- Restrict Administrative Privileges – Enforces MFA for privilege escalation and remote access sessions

How It Supports Maturity

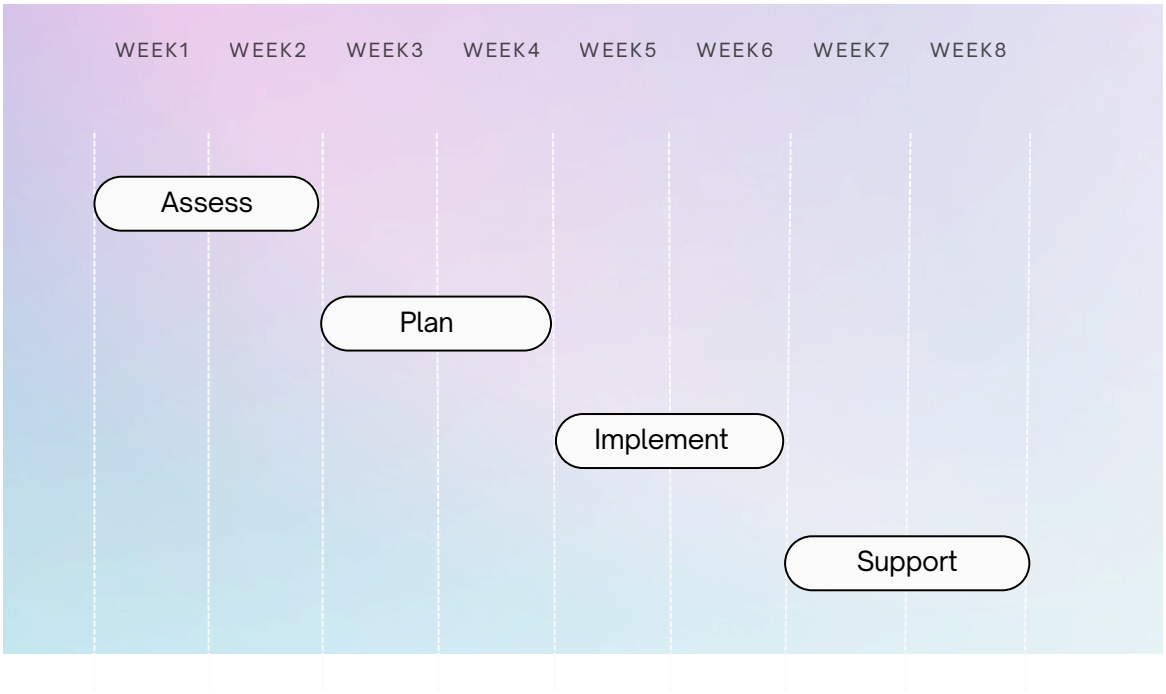
Duo and Okta support E8 maturity uplift by enabling consistent and phishing-resistant MFA aligned to Maturity Levels 2 and 3. These platforms allow secure access enforcement across identity systems, reducing exposure to credential theft and lateral movement.
They are particularly valuable in scenarios where Azure Entra ID (formerly Azure AD) does not natively support phishing-resistant MFA or lacks integration with non-Microsoft systems such as VPNs, legacy applications, or third-party SaaS platforms.

Integration with USEZER Services

USEZER configures Okta or Duo based on the client's identity stack, access requirements, and target maturity level. We support one-off deployments that include MFA policy design, integration with cloud and on-prem services, user onboarding, and enforcement configuration.

USEZER's E8 Delivery Approach

USEZER follows a structured, outcomes-focused delivery model that supports organisations at any maturity level. Whether the goal is a point-in-time assessment, uplift to Level 2 compliance, or a fully managed security framework, our process is designed to deliver clarity, control, and measurable improvements.



Phase 1 - Assess

We begin by auditing the current environment to determine each control's maturity level. This includes technical validation, stakeholder input, and mapping against the ACSC model.

- Conduct E8 maturity assessment and baseline audit
- Identify coverage gaps and exceptions
- Map existing tools, processes, and risks
- Deliver a maturity heatmap, risk register, and assessment report

Phase 2 - Plan

With gaps identified, we build a tailored roadmap to reach the target maturity level. The plan is risk-aligned, standards-aware, and implementation-ready.

- Define target maturity level (typically Level 2)
- Develop a remediation roadmap by control area
- Prioritise activities based on criticality and compliance impact

Phase 3 - Implement
We configure, deploy, and enforce the required security controls. This stage is hands-on and outcome-driven, focused on delivering measurable improvement.

- Implement and/or tune security controls
- Apply policies, allowlists, and configuration baselines
- Enable monitoring, alerting, and response workflows
- Optionally re-audit post-implementation to confirm maturity uplift with Evidence collection.

Phase 4- Support
Support is optional. For clients who need ongoing assistance, USEZER provides managed services to maintain maturity alignment and operational oversight.

Key Deliverables

USEZER provides a focused set of deliverables to support Essential Eight assessment and uplift engagements:

Essential Eight Assessment Report

Includes control-by-control maturity ratings, gap analysis, and a visual heatmap aligned to the ACSC model.

Remediation Roadmap

Actionable plan to address maturity gaps, prioritised by risk and aligned to the target maturity level.

Risk Register

Documents identified weaknesses, associated risks, and suggested mitigation strategies for tracking and resolution.

Proof of Execution Pack (optional)
A package of evidence showing implemented controls, useful for audits or internal compliance validation.

Why Partner with USEZER?

USEZER combines practical delivery experience with deep technical capability to help organisations achieve Essential Eight maturity efficiently and effectively.

We've supported public and private sector clients across regulated, hybrid, and cloud-first environments—aligning security outcomes with ACSC, ISM, ISO 27001, and PSPF frameworks. As an ISO 27001 certified organisation, we embed security and governance into every engagement.

CERTIFIED ISO 27001

Our Partnerships

Get in Touch!

Ready to assess or uplift your cybersecurity maturity?
Our team can provide a tailored proposal based on your environment, target maturity level, and tooling preferences.

Nuwan Fernando
nfernando@usezer.com.au
0414 764 949

Grace Waldemar
gwaldemar@usezer.com.au
0414 442 485

Boniface Fernando
bfernando@usezer.com.au
0414 442 485