# Security Architecture Review — Essential 8 Focused

## Introduction & Purpose

This Security Architecture Review (SAR) evaluates your Microsoft 365 and endpoint environment against the **Australian Cyber Security Centre’s Essential 8 (E8)** maturity model.

The **goal** is to help you understand your current security posture, prioritise actions that improve resilience, and create a practical roadmap to higher E8 maturity.  
We will also highlight how your existing or recommended controls map to **NIST Cybersecurity Framework** and **Zero Trust** principles, but these will be positioned as complementary, not the primary focus.

## Rules of Engagement

### Keep in mind the Engage Squared charter

We want customers to be knowledgeable, confident, and supported in building (and betting) their businesses on Microsoft 365.

This means: - Addressing generic cloud concerns early (security, integration, reliability, compliance, etc.) - Framing security discussions to help the business make informed, strategic decisions — not overwhelming them with technical minutiae

### Take a solution-centric approach

Focus the conversation on: - **Business requirements, goals, and objectives** - **Non-functional requirements** — SLAs, RTO/RPO, cost of downtime - **Availability, uptime, business continuity**, geographic distribution (single vs. multi-region) - **Purpose of the solution** — what it does and why it is needed - **Why this review now?** — proactive planning or response to an incident? - **User profile** — total number, concurrent activity, geographic spread - **Internal policies, legal, or compliance requirements** - **High-level technical design** — major components, internal vs. 3rd party, dependency maps

### Strategic discussion principles

* Reference **publicly documented best practices and design principles**
* Work **top-down**: start with the big picture, move into relevant technical detail only when needed
* Keep the conversation tied to **customer-defined priorities**
* Use a “parking lot” for deep-dive questions suited to a follow-on engagement

### Avoid

* Low-level technical requirements unless they directly support the business context
* Tactical debates that don’t serve the agreed priorities
* Making assumptions — confirm any vague customer statements
* Detailed design or configuration specifics

### Red flags

* If customer-initiated questions go into deep technical design or specific configuration:  
  ➜ Identify if another engagement type is more appropriate

## Steps

### Step 1 — Define Goals & Objectives

* Capture the **vision for the end state**
* Clearly define problems, goals, and high-level approaches to solving them
* Ensure a common vision and agreement among all stakeholders

### Step 2 — Identify Business Goals (Non-Functional Requirements)

* Vision driven by:
  + High-level requirements and business goals
  + Cost drivers — reduce TCO, maximise ROI
  + Design goals — high availability, robust security, scalability, consolidation, fault avoidance
* Gather requirements through:
  + **Use cases** — high-level interactions between users and the system
  + **Usage scenarios** — tasks and sequences that form business processes

### Step 3 — High-Level Technical Design (Dependency Map)

* Outline the **solution concept**
  + High-level approach for all system components
  + Include internal and 3rd party dependencies
* Assess technology choices based on:
  + Business needs
  + Technical feasibility
  + Time and budget constraints

### Step 4 — Solution-Specific Questions

* **Application** — migration vs. modernisation, interoperability, location
* **Database** — special features, shared services
* **Infrastructure** — compute, storage, networking, identity
* **Abilities needed** — availability, scalability, manageability, security
* **Users** — who they are, how they consume services

## Applying the Essential 8

When walking through the architecture, map each relevant component and control to the E8 strategies:

1. Application Control
2. Patch Applications
3. Configure MS Office Macros
4. User Application Hardening
5. Restrict Admin Privileges
6. Patch Operating Systems
7. Multi-Factor Authentication
8. Regular Backups

For each: - Record current maturity level (ASD Level 0–3) - Identify quick wins - Note dependencies for strategic uplift

## Engagement Output

* Stay **high-level** - no customised low-level design documents or specific configurations
* Provide:
  + Annotated **E8–M365 Mind Map**
  + Maturity score table (current vs. target)
  + Prioritised recommendations and roadmap
* Reference public documentation for detailed implementation steps
* Advise on readiness for deployment/migration:
  + Has the customer tested at current and future load?
  + Does the architecture align to their business growth plans?

## Deliverables

* Executive summary deck
* Annotated E8–M365 Mind Map
* Maturity scoring table
* Risk and recommendation register
* Roadmap with owners and timelines

## References & Talking Notes

### Microsoft & Essential 8

🔗 [Microsoft 365 & Essential Eight Overview](https://learn.microsoft.com/en-us/compliance/anz/e8-overview)  
Shows Microsoft’s mapping to the E8 framework and the components “under the hood.” Useful for connecting M365 capabilities directly to ACSC requirements.

**Talking note:** This can help customers see where Microsoft tools already contribute to E8 maturity, but still emphasise that maturity is about correct configuration and operational discipline - not just tool availability.

### Microsoft Cybersecurity Reference Architecture (MCRA)

🔗 [MCRA Overview](https://learn.microsoft.com/en-us/security/adoption/mcra)  
Visualises Microsoft’s full security stack and integrations.

**Talking note:** This shows Microsoft’s significant investment in security, but also reveals a “world according to Microsoft” approach in defaults. You can enable all tools and still have gaps if they’re not tailored to the business context.

### Microsoft Security Adoption

🔗 [Security Adoption Overview](https://learn.microsoft.com/en-us/security/adoption/adoption)  
High-level, business-focused guidance for executives.

**Talking note:** Good for framing security in business terms, but not detailed enough for technical implementation. Ideal for leadership buy-in conversations.

### ACSC Essential 8 Maturity Model

🔗 [ACSC E8 Maturity Model](https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight/essential-eight-maturity-model)  
Vendor-neutral, detailed description of each maturity level.

**Talking note:** This is an important reminder that E8 (and other frameworks like Zero Trust, ISO 27001) can be implemented with or without Microsoft tools. Whether you use Microsoft, Linux, AWS, CyberArk, or other tech, you can still achieve compliance and maturity.  
Also: none of these frameworks are “set and forget.” New users, new apps, and new operating models mean you must continually reassess.