# Essential 8 Delivery

## Introduction & Purpose

The Australian Cyber Security Centre’s **Essential 8 (E8)** is the most practical way for Australian organisations to improve their security maturity. It reduces the risk of common attacks, sets clear priorities, and provides a framework for uplift that is easy to communicate.

This session will help you understand:  
- Where your organisation stands today against the Essential 8  
- What actions you can take immediately to improve maturity  
- How Microsoft 365 and your existing tools map to E8  
- How E8 aligns with broader frameworks like NIST and Zero Trust

## Rules of Engagement

* **Stay business focused**: Protect the ability to operate, not just tick boxes.
* **Use plain language**: Keep the discussion accessible for all stakeholders.
* **Visual first**: Use the E8–M365 mind map during discovery.
* **Quick wins and future steps**: Identify both short-term and long-term improvements.
* **No deep dives**: Capture technical questions in a parking lot for follow-up.
* **Framework agnostic**: E8 can be achieved with Microsoft, AWS, Linux, or other tools. Microsoft is an enabler, not the only path.

## Agenda

1. **Kickoff & Context**
   * Explain why E8 matters for Australian organisations
   * Clarify the purpose: measure, prioritise, and plan
2. **Walkthrough of the Essential 8**
   * Application Control
   * Patch Applications
   * Configure MS Office Macros
   * User Application Hardening
   * Restrict Admin Privileges
   * Patch Operating Systems
   * Multi-Factor Authentication
   * Regular Backups
3. **Maturity Assessment**
   * Record current maturity (Level 0–3) for each category
   * Capture strengths, weaknesses, and quick wins
4. **Mapping to Microsoft 365**
   * Show how Microsoft 365 security tools map to each E8 strategy
   * Call out where existing tools already contribute
5. **Recommendations & Roadmap**
   * Prioritised actions by E8 category
   * Highlight immediate uplift vs. strategic projects
6. **Wrap Up & Next Steps**
   * Confirm understanding of current state and agreed roadmap
   * Provide reference material

## Example Customer Discussion Prompts

**Application Control**  
- How do you prevent unauthorised applications from running?  
- Do you use Microsoft Defender Application Control or AppLocker?

**Patch Applications**  
- How quickly are updates applied to third-party applications?  
- Do you use Microsoft Endpoint Manager for patching?

**Restrict Admin Privileges**  
- How many admins are in your environment today?  
- Do you use Privileged Identity Management for just-in-time access?

**Multi-Factor Authentication**  
- Is MFA enforced for all users or only admins?  
- Do you use Conditional Access policies with Microsoft Authenticator?

## Quick Wins vs. Strategic Goals

**Quick Wins**  
- Enforce MFA for all accounts  
- Disable macros from the internet in Office apps  
- Enable cloud backups for critical data  
- Apply baseline Attack Surface Reduction rules

**Strategic Goals**  
- Implement Microsoft Defender Application Control  
- Mature patch management processes with Endpoint Manager and Windows Update for Business  
- Deploy role-based access control with Privileged Identity Management  
- Regularly test backup restores

## Engagement Output

* Annotated E8–M365 mind map with customer inputs
* Current vs. target maturity score table
* List of quick wins with owners
* Strategic roadmap aligned to E8 categories
* Links to learning and reference material

## References to Share

* [Microsoft 365 & Essential Eight Overview](https://learn.microsoft.com/en-us/compliance/anz/e8-overview)
* [Microsoft Cybersecurity Reference Architecture (MCRA)](https://learn.microsoft.com/en-us/security/adoption/mcra)
* [Microsoft Security Adoption](https://learn.microsoft.com/en-us/security/adoption/adoption)
* [ACSC Essential 8 Maturity Model](https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight/essential-eight-maturity-model)

## Closing Facilitator Script

The Essential 8 is not a checklist you do once and move on.  
It is a maturity model that adapts as your business, people, and applications evolve.  
The goal is to keep improving your security posture in a way that makes sense for your business context.  
Today we identified where you are, what you can do immediately, and how to plan for the next stage of your maturity journey.