# Essential 8 Maturity Score Table

This table is used to capture the organisation’s current and target maturity levels against the **ACSC Essential 8** strategies.  
Use ASD’s maturity model levels (0–3):  
- **Level 0**: Not implemented  
- **Level 1**: Partially implemented, basic coverage  
- **Level 2**: Mostly implemented, consistent but with some gaps  
- **Level 3**: Fully implemented, comprehensive and effective

## Maturity Assessment

| Essential 8 Strategy | Current Level | Target Level | Key Risks / Observations | Recommended Actions (Quick Wins & Strategic) |
| --- | --- | --- | --- | --- |
| Application Control |  |  |  |  |
| Patch Applications |  |  |  |  |
| Configure MS Office Macros |  |  |  |  |
| User Application Hardening |  |  |  |  |
| Restrict Admin Privileges |  |  |  |  |
| Patch Operating Systems |  |  |  |  |
| Multi-Factor Authentication |  |  |  |  |
| Regular Backups |  |  |  |  |

## Summary View

The Essential 8 strategies don’t line up perfectly one-to-one with the CIA Triad, but they do reinforce its principles.  
This table helps show the relationship so customers can see *why* each E8 category matters in terms of security outcomes.

| CIA Principle | Relevant Essential 8 Strategies | Examples | Current Average | Target Average | Overall Gap |
| --- | --- | --- | --- | --- | --- |
| **Confidentiality** | - Multi-Factor Authentication- Restrict Admin Privileges- Application Control- Office Macro Controls | Ensures only the right people can access data and prevents attackers from escalating privileges. |  |  |  |
| **Integrity** | - Patch Applications- Patch Operating Systems- Application Control- User Application Hardening | Keeps systems and data accurate by reducing vulnerabilities and stopping unauthorised changes. |  |  |  |
| **Availability** | - Regular Backups- Patch Operating Systems- User Application Hardening | Ensures systems and data are available when needed, and can be recovered after an incident. |  |  |  |

## Notes on the Mapping

* Some strategies contribute to more than one CIA principle (for example, patching helps both **Integrity** and **Availability**).
* This mapping is designed to help explain the “why” of the Essential 8, not to create a rigid audit framework.
* When capturing scores, average the maturity levels of the mapped strategies to give a quick view of how the organisation is tracking in each CIA category.
* Use this as a storytelling tool to connect E8 maturity to business outcomes like protecting confidentiality of sensitive data, ensuring system integrity, and maintaining service availability.

## Notes

* **Quick wins** should be achievable within 30 days (e.g. enforcing MFA, disabling macros, enabling backups).
* **Strategic actions** may require projects, budget approval, or organisational change.
* Always record **context** (e.g. “backups exist but are not tested”) rather than just the level.