**Audience:** Risk and procurement teams asking how baseline cyber mitigations are **operated**, not only documented.

## Why this matters

The Australian Cyber Security Centre Essential Eight describes mitigation strategies organisations should consider. Procurement success often depends on naming which party **runs** each control day to day and how evidence is produced for audits and insurers.

## Mitigation snapshot (high level)

| Mitigation | Operational question for your reviewer |
|---|---|
| Application control | Who maintains allow lists, exceptions, and expiry for elevated apps? |
| Patch applications | Who drives vendor patch cadence for line-of-business and security tools? |
| Configure MS Office macro settings | Who enforces macro policy and handles business exceptions with risk acceptance? |
| User application hardening | Who configures and audits browser and Office hardening baselines? |
| Restrict administrative privileges | Who provisions PAM, reviews standing admin rights, and revokes access? |
| Patch operating systems | Who owns OS patch windows and validation for critical systems? |
| Multi-factor authentication | Who enforces MFA rollout, recovery, and break-glass procedures? |
| Regular backups | Who verifies immutability, retention, restore tests, and ransomware runbooks? |

## Trucell's role

When you engage Trucell managed IT, security, and backup lines, mitigations are mapped to accountable services on the Essential Eight readiness solution page. Maturity tiers and official ACSC assessment approaches are your organisation's to apply; Trucell supplies the **operational** linkage and evidence streams for the services in contract.

## Deeper diligence

Use the separate **Essential Eight diligence checklist** (`essential-eight-diligence-checklist.pdf`) for question sets during RFP and shortlisting.

## Reference

Official ACSC publications remain the authoritative source for strategy definitions and assessment methodology.