Audience: Information security, risk, and procurement reviewers.

Operating principles

- **Defined ownership** — Security-relevant run-state (patching discipline, endpoint posture, backup immutability where Trucell operates backups, identity alignment where in scope) is tied to named services and escalation paths, not implicit “best effort.”
- **Integrated response** — Incidents involving identity, malware, network, or data availability are handled with tooling and processes that connect service desk, security operations, and recovery context when those lines are under Trucell management.
- **Governed change** — Changes affecting security posture flow through controlled workflows so production drift is visible and reversible.

Alignment to baseline controls

Trucell aligns delivery to recognised Australian baseline guidance (ACSC Essential Eight) when customers engage the relevant managed lines. Mapping of mitigations to services appears on the Essential Eight readiness solution page and in diligence materials. Assessment methodology and ACSC framing remain the authority; Trucell helps operationalise controls in your environment under contract.

Government and regulated buyers

Public sector references include NSW Government Accredited Supplier status, IRAP-assessed capabilities, and alignment to ISM PROTECTED-appropriate operations for suitable engagements. Defence-aligned export control context (US ITAR Australian Authorised User, AUKUS registration) applies where relevant to controlled technology discussions; evidence packs are scoped per enquiry.

Assurance limits

This summary supports evaluation. It does not constitute an independent audit opinion, penetration test report, or customer-specific control attestation. Formal assurance artefacts are issued under engagement terms and confidentiality as applicable.