A2g Cyber

# Service Definition

# Entra ID Security Review and Remediation Support (Lot 3 – Cloud Support)

## 1. What the service is

An independent, evidence-based review of your Microsoft Entra ID configuration, identity security controls and operational practices. We identify security risks, prioritise remediation actions, and (optionally) help you implement agreed improvements with knowledge transfer so your team can sustain the changes.

Typical use cases include: tenant security posture reviews, Conditional Access optimisation, privileged access (PIM) hardening, authentication improvements (MFA/passwordless/passkeys), and app/service principal permission reviews.

## 2. What's included

Assessment activities (as applicable to scope):

- Identity and access architecture review
- Conditional Access policy review (coverage, exclusions, enforcement)
- Authentication methods and registration posture review
- Privileged access review (roles, PIM configuration, admin separation)
- Guest/external access controls review
- Application registrations, service principals, and permissions review
- Logging/monitoring review (sign-in/audit visibility and investigation readiness)
- Workshops/interviews with stakeholders (technical and operational)

### Deliverables:

- Executive summary of key findings and priorities
- Detailed findings and risk explanations
- Prioritised remediation plan (quick wins / medium-term / strategic)
- Implementation support plan (if requested)
- Knowledge transfer session(s) and handover notes/runbooks (where applicable)

## 3. Data backup/restore and disaster recovery

This is a consultancy service and **does not provide hosting, data backup, or disaster recovery** for your tenant. Where we make configuration changes with you, we follow your



© A2g Cyber Limited 2026

change control and rollback approach (for example: documenting pre-change state, staged rollouts, pilot groups, and rollback steps).

## 4. Onboarding and offboarding

Onboarding:

- Kick-off to confirm objectives, scope, stakeholders, and timelines
- Access method agreed (least privilege)
- Data sources confirmed (e.g. sign-in/audit log availability and retention)

Offboarding / exit:

- Final report and deliverables supplied in agreed formats
- Access removed (accounts revoked, guest access removed if used)
- Working files handled per data retention section below

## 5. Service constraints

- Delivered **remotely by default** (onsite by agreement).
- Findings depend on **access granted** and **log retention**. Limited access/retention may reduce assurance depth.
- Implementation support requires buyer approvals, change windows, and testing availability.
- Scope is limited to the **agreed tenant(s)** and agreed systems; additional tenants/systems are out of scope unless added.

## 6. Service levels and support hours

- Support/engagement hours: **Mon–Fri 09:00–17:00 UK**
- Channels: Email, Microsoft Teams, phone (as agreed)
- Target response to questions during business hours: **within 8 working hours**
- No enhanced/out-of-hours support unless explicitly agreed in a call-off.

## 7. After-sales support

We can provide follow-up advisory sessions, remediation check-ins, and validation reviews after the main engagement. All time is delivered and charged in line with the **Lot 3 rate card** for the relevant role.

## 8. Technical requirements

Buyer provides:

- A named technical contact and decision-maker for approvals



© A2g Cyber Limited 2026

- Appropriate tenant access (preferably read-only for assessment; elevated only when implementing)
- Access to relevant logs where required (sign-in logs, audit logs, Entra ID configuration)
- Workspace for collaboration (Teams and document sharing)

## 9. Outage and maintenance management

We do not operate any buyer production service. Where changes are implemented, we plan changes within your maintenance windows and change control process and support testing, pilot rollout and rollback steps.

## 10. Hosting options and locations

No hosting is provided. Delivery is remote. Any documentation produced is shared using buyer-approved tooling and locations (e.g. buyer SharePoint/Teams or agreed secure transfer).

## 11. Access to data on exit

All outputs (reports, plans, runbooks) are provided to the buyer. On request, we will return or securely delete any buyer data we hold as working material, per agreed retention.

## 12. Security

- Least-privilege access
- Buyer-controlled accounts and approval for changes
- Secure handling of information (encrypted storage where used; controlled sharing)
- No credential harvesting; no intrusive testing unless explicitly in scope
- Data minimisation: we only request/access what is needed for the engagement
- Compliance with buyer security policies and reasonable assurance requirements

## 13. Commercials (high level)

The service is delivered on a time-and-materials basis and charged at the relevant **hourly rates listed on the Lot 3 rate card**, aligned to the role(s) provided. We provide an estimate for the basis of a purchase order, and provide regular burn-down information against that.



© A2g Cyber Limited 2026