



AI Security, Privacy, and Assurance Support – Service Definition

G-Cloud 15 Lot 3 – Cloud Support Services (Additional Services)

Document control

Service name: AI Security, Privacy, and Assurance Support

Supplier name: Lean Tree Ltd

Version: v1.0

Date: 23 January 2026

Status: Final

1. Service overview

Outcome: Security and assurance support service to help buyers design, document, and implement controls for artificial intelligence (AI) services operated in cloud environments, including risk assessment inputs, assurance artefacts, and operational readiness guidance.

How: Delivered through workshops and artefact review, producing control mappings, assurance approach, decision logs and remediation recommendations.

Boundary: Delivery is limited to the activities described in this service definition and agreed at call-off; any additional delivery/build activities or managed operations beyond the agreed scope are out of scope unless separately commissioned. The buyer retains control of their cloud accounts, data and access approvals.

Who it is for: Cloud and platform teams, Delivery and programme teams, Security and risk teams, Operations and service management teams

Buyer needs met: Assurance and validation for change; Performance and resilience confidence; Ongoing operational support and incident assistance where agreed

Service type: Professional services.

How this service supports transition to cloud services: Supports safe transition and ongoing operation by producing decision-ready plans, governance, patterns, and evidence packs that buyers and delivery teams can implement and operate within buyer-controlled cloud environments.

2. What this service covers (Lot 3 scope) and exclusions

Included activities and responsibilities:



- Threat modelling for AI services and data flows
- Control mapping to buyer policies and assurance needs
- Data Protection Impact Assessment (DPIA) and privacy evidence structuring support
- Logging and monitoring requirements for auditability
- Guidance on prompt-injection and data leakage mitigation
- Secure configuration recommendations and secrets controls
- Incident readiness playbooks for AI-specific risks
- Outputs are evidence-led. Where applicable, Lean Tree produces an evidence pack (assurance hooks) containing agreed validation artefacts.
- Roles, responsibilities and decision points are agreed at call-off and documented using a Responsible, Accountable, Consulted, and Informed (RACI) matrix.
- Delivery is performed within buyer-controlled tenancy/accounts and buyer-approved tooling, unless explicitly agreed otherwise at call-off.

Outputs produced:

- Test strategy/plan and scenarios
- Scripts/harnesses where agreed
- Test execution report and results analysis
- Evidence pack for assurance and sign-off inputs

Explicit exclusions:

- No bespoke design or development of business applications.
- No procurement or resale of cloud subscriptions, licences, or hardware unless explicitly stated in the Call-Off.
- No formal certification or accreditation decisions on behalf of the buyer.
- No 24x7 monitoring or on-call service unless explicitly agreed at call-off.

Buyer responsibilities:

- Provide nominated service/product owners and decision-makers for scope and sign-off.
- Provide access to relevant environments, artefacts, and data required for delivery, using buyer-approved methods.
- Approve priorities, risk appetite, and change windows where applicable.
- Operate the agreed governance model and accept deliverables per the agreed acceptance approach.

3. Deliverables and outputs

Deliverables list and format:

- Test strategy/plan and scenarios



- Scripts/harnesses where agreed
- Test execution report and results analysis
- Evidence pack for assurance and sign-off inputs

Acceptance approach: Deliverables are reviewed at agreed checkpoints. Acceptance criteria and sign-off roles are agreed at call-off and recorded in the delivery plan.

Knowledge transfer outputs: Knowledge transfer includes walkthrough sessions, handover notes, and Q&A. Recordings are provided where agreed at call-off.

4. Service delivery model

Delivery approach: Discovery and evidence capture, then design/plan, then delivery of agreed outputs, then transition and handover to Business as Usual (BAU). Delivery phases and sequencing are agreed at call-off.

Engagement options: Time and materials (rate card), fixed deliverables, or retained/managed support where applicable, agreed at call-off.

Governance and reporting cadence: Cadence is agreed at call-off and typically includes regular check-ins, Risks, Assumptions, Issues, and Dependencies (RAID) management, and formal reviews at key decision points.

Roles and responsibilities: Roles, responsibilities and decision points are agreed at call-off and documented using a RACI matrix.

Tools and ways of working: Buyer-mandated ticketing, collaboration, and change control processes are used where provided. Tooling and ways of working are confirmed at call-off and captured in the delivery plan.

5. Support hours, service levels, and incident management

Support channels and hours:

Service Level Agreement (SLA) not applicable as not a managed service. Engagement support is provided via Email/ticketing, Phone escalation within the service hours agreed at call-off. Standard: 09:00–17:30 UK time, Mon–Fri (excluding Bank Holidays), email/ticketing and scheduled workshops.

Enhanced: Option for extended hours during high-impact releases.

Escalation path: Escalation routes and named roles are agreed at call-off and documented in the delivery plan.

Incident management: SLA not applicable as not a managed service. Any incidents relating to buyer services are managed by the buyer. Lean Tree supports investigation and reporting for in-scope work where agreed.



Planned maintenance and change notices: Not applicable unless the Call-Off includes a managed service element. Change windows and notice periods are agreed at call-off and align to the buyer's change process.

Service reporting: Progress reporting, RAID updates, and recommendations are provided to the cadence agreed at call-off.

6. Onboarding and mobilisation

How onboarding starts: Onboarding starts with a kick-off to confirm scope, outcomes, constraints, governance, and delivery plan.

Information required from the buyer: Scope and priorities, relevant service and platform context, constraints and risk appetite, and nominated sign-off roles.

Access requirements: Access requirements are limited to what is needed for delivery and are provided via buyer-approved methods in buyer-controlled environments.

Typical mobilisation timeline: Mobilisation timeline and dependencies are agreed at call-off based on scope and buyer readiness.

7. Service constraints and assumptions

Assumptions: Delivery is performed within buyer-controlled tenancy/accounts and buyer-approved tooling, unless explicitly agreed otherwise at call-off.

Constraints: Constraints (for example working hours, on-site requirements, clearance needs, and tooling constraints) are confirmed at call-off and documented in the delivery plan.

8. Security and data protection

8.1 Data protection between buyer and supplier

Protection between networks: Information is exchanged using buyer-approved secure channels. Where Lean Tree accesses buyer environments, access uses buyer-approved methods and is limited to what is required for delivery.

Protection within supplier network: By default, Lean Tree works within buyer-provided repositories and tools. Where Lean Tree needs to hold working documents, buyer information is stored only on a secure internal SharePoint site (UK), with access restricted to senior operational staff. The underlying platform provides encryption in transit and at rest.



8.2 Data storage and processing

Data storage locations: By default, information is stored within buyer-provided repositories and tools. Where Lean Tree needs to hold working documents, storage is on a secure internal SharePoint site (UK).

Data processing locations: Processing occurs within buyer-approved tooling and Lean Tree's UK SharePoint tenant where working documents are held.

Sub-processors: Any sub-processors and/or third-party tools used are confirmed at call-off and documented for buyer approval where required.

Data retention: Data is retained for up to 6 years, with retention schedules varied where required to meet buyer needs.

8.3 Encryption and key management

Encryption in transit: Encryption in transit is provided by the underlying platforms used for delivery (buyer-approved tooling and Microsoft 365).

Encryption at rest: Encryption at rest is provided by the underlying platforms used for delivery (buyer-approved tooling and Microsoft 365).

Key management model: Key management is provided by the underlying platforms. Any buyer-specific key management requirements are agreed at call-off.

8.4 Vulnerability, testing, and assurance

Vulnerability management: Lean Tree maintains vulnerability management for its corporate endpoints and collaboration environment. For buyer environments, vulnerability management remains the buyer's responsibility unless explicitly agreed at call-off.

Penetration testing: Not applicable to advisory outputs. Where assurance of supplier-held tooling is required, evidence is provided on request and agreed at call-off.

Remediation: Remediation actions are tracked and closed using the agreed action log and governance cadence.

8.5 Identity and access management

Authentication for any tools provided: Not applicable for most engagements as Lean Tree delivers within buyer-provided tools. Where Lean Tree provides access to supplier-held repositories for working documents, access is restricted to named individuals.

Privileged/admin access controls: Administrative access is restricted to authorised individuals using least privilege, and removed at offboarding.



Access reviews: Access reviews are performed at intervals agreed at call-off and on material change.

8.6 Audit and logging

Buyer user action audit: Buyer user action audit is provided by buyer tooling where applicable. Lean Tree provides engagement reporting and change logs as agreed.

Supplier admin action audit: Supplier administrative actions are recorded through engagement reporting and the audit capabilities of the tools used.

Log retention and access: Log retention and access are determined by the underlying platforms and buyer requirements. Where Lean Tree holds working documents, retention follows the agreed schedule (up to 6 years).

8.7 Security incident management

Security incident response process: Lean Tree as an organisation follows a documented security incident response process covering triage, containment, eradication, recovery, and post-incident review.

Buyer notifications: Notification and reporting timescales are agreed at call-off based on the buyer's incident-management process and reporting needs.

Post-incident review: Post-incident reviews capture lessons learned and corrective actions, with actions tracked to closure where applicable.

8.8 Personnel security

Personnel screening: Lean Tree will perform staff screening which conforms to BS7858:2019

Government security clearance: Lean Tree are willing to obtain clearance for relevant individuals up to Developed Vetting (DV).

Staff access restriction: Staff access is restricted to named individuals who require access to deliver the service. Subcontractor access, where used, is controlled and approved at call-off.

8.9 Data sanitisation and disposal

Secure disposal approach: Buyer information held by Lean Tree is securely deleted/disposed of in line with the agreed retention schedule.

Deletion confirmation: Deletion confirmation is provided on request and follows the timelines and evidence approach agreed at call-off.



9. Pricing model summary

Charging basis: Charged using the Lean Tree Lot 3 rate card. The minimum chargeable unit is half a day (0.5 day).

What is included and what is chargeable: Included and chargeable items (for example travel, on-site time, and any out-of-hours working) are confirmed at call-off and reflected in the agreed pricing schedule.

Invoicing approach: Invoicing arrangements are agreed at call-off (including purchase order (PO) requirements, frequency, and required format).

10. Quality and service management

Quality management: Lean Tree is implementing ISO 9001 (planned audit April 2026). Lean Tree does not have ISO 9001 certification at this time.

Service management: Lean Tree holds an Information Technology Infrastructure Library (ITIL) Maturity Level 2 certification. Lean Tree does not have ISO/IEC 20000-1 certification.

Information security: Lean Tree holds IASME Cyber Essentials and IASME Cyber Assurance. Lean Tree is implementing ISO 27001 (planned audit April 2026) and does not claim ISO 27001 certification at this time.

Delivery assurance: Assurance is provided through peer review, agreed quality gates, and evidence-led deliverables (assurance hooks), aligned to the buyer's governance.

Continuous improvement: Continuous improvement is delivered through retrospectives and service reviews, with actions tracked and agreed at call-off.

11. Exit, handover, and knowledge transfer

Handover approach: Handover includes delivery of agreed artefacts (for example runbooks, plans, and decision logs) and knowledge transfer sessions as agreed at call-off.

End-of-engagement deliverables: Deliverables are stored in buyer repositories by default. Where supplier-held working documents are used, copies are provided to the buyer in agreed formats.

Data return/deletion: Data is retained for up to 6 years, with retention schedules varied where required to meet buyer needs. Buyer information is securely deleted/disposed of in line with the agreed retention schedule.



Timescales and buyer responsibilities: Exit timescales and buyer responsibilities are agreed at call-off and captured in the delivery plan.

12. Dependencies

Buyer-owned subscriptions/accounts: Buyer provides required cloud subscriptions/accounts, licences, and buyer-mandated tooling to enable delivery. Specific dependencies are confirmed at call-off.

Identity, networking, and security dependencies: Identity, networking, and security dependencies are confirmed at call-off and align to buyer standards and approval processes.

Third-party vendors: Third-party vendors and any required supplier coordination are confirmed at call-off.

13. How buyers engage and order

Buyers can directly award a Call-Off Contract via G-Cloud in line with the Call-Off Procedure.

Ordering steps:

- 1) Call-off and assurance context: confirm policies, risk appetite, data sensitivity and governance route.
- 2) Threat and risk modelling: map AI data flows, threats and failure modes relevant to the service.
- 3) Control mapping: map required controls to practical implementation and evidence outputs.
- 4) Privacy support: structure DPIA inputs and data handling decisions with traceability.
- 5) Operational playbooks: define incident response, escalation and exception handling for AI risks.
- 6) Evidence pack: produce audit-ready evidence templates, logs and decision records for approval.
- 7) Stakeholder review: run governance playback and adjust controls based on feedback.
- 8) Handover: deliver the assurance pack, playbooks and ownership model.

Implementation timescales: Implementation timescales are dependent on buyer readiness and confirmed at call-off.