Cloud Security Platform Implementation and Operations Support (Wiz) – Service Definition

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

Document control

Service name: Cloud Security Platform Implementation and Operations Support (Wiz)
Supplier name: Lean Tree Ltd
Version: v1.0
Date: 28 January 2026
Status: Final

1. Service overview

Outcome: A configured and operational cloud security platform capability with clear triage, reporting and governance routines to support remediation coordination.

How: Lean Tree configures the buyer's Wiz tenant (within a buyer-procured subscription), onboards agreed cloud accounts, sets policies and alerting, and establishes operating runbooks, reporting and integrations with buyer tooling where available.

Boundary: The Wiz licence is procured by the buyer; Lean Tree does not resell Wiz. Lean Tree does not customise the underlying Wiz product. Remediation changes in cloud accounts are buyer-owned and are only delivered if explicitly agreed at call-off.

Who it is for: Cloud and platform teams, Security operations teams, Delivery and programme teams

Buyer needs met: Cloud security tooling implementation and operational support

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:

- Onboard agreed cloud accounts/subscriptions into Wiz
- Configure policies, alerting routes and prioritisation approach

- Define triage workflow, ownership mapping and escalation routes
- Set up dashboards and a reporting pack for governance forums
- Configure integrations with buyer ticketing and SIEM (Security Information and Event Management) where available
- Initial tuning to reduce noise and agree operational thresholds
- Create operating runbooks, Responsible, Accountable, Consulted, and Informed (RACI) (Responsible, Accountable, Consulted, Informed) and handover materials
- Backlog shaping and remediation coordination support (implementation excluded unless agreed)
- 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 RACI matrix.
- Delivery is performed within buyer-controlled tenancy/accounts and buyer-approved tooling, unless explicitly agreed otherwise at call-off.

Outputs produced:

- Wiz onboarding and configuration baseline (tenant, accounts, policies and roles)
- Triage and governance operating model (workflow, RACI, runbooks)
- Reporting pack and dashboard setup notes
- Integration configuration notes (ticketing/SIEM where applicable)
- Tuning log and a prioritised improvement backlog
- Handover pack and knowledge transfer sessions

Explicit exclusions:

- No procurement or resale of Wiz licences or subscriptions.
- No bespoke development or modification of the Wiz product.
- No remediation implementation in cloud accounts unless explicitly agreed at 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.
- No bespoke design or development of business applications.

Buyer responsibilities:

- Provide a Wiz subscription/tenant and nominate administrators and product owners.
- Provide access to in-scope cloud accounts/subscriptions and required approvals.
- Provide buyer tooling access for integrations (for example ticketing and SIEM) where required.
- Approve prioritisation, risk appetite, alerting thresholds and change windows.

- Operate the agreed governance model and accept deliverables per the agreed acceptance approach.

3. Deliverables and outputs

Deliverables list and format:

- Wiz onboarding and configuration baseline (tenant, accounts, policies and roles)
- Triage and governance operating model (workflow, RACI, runbooks)
- Reporting pack and dashboard setup notes
- Integration configuration notes (ticketing/SIEM where applicable)
- Tuning log and a prioritised improvement backlog
- Handover pack and knowledge transfer sessions

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 onboarding readiness, then configuration and integration, then tuning and reporting setup, then handover to Business as Usual (BAU) (business as usual). Delivery phases and sequencing are agreed at call-off.

Engagement options: Time and materials (rate card), fixed deliverables, or retained support for agreed activities, confirmed 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) (Risks, Assumptions, Issues, Dependencies) 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 unless explicitly agreed at call-off. Engagement support is provided

via Email/ticketing, with Phone escalation within the service hours agreed at call-off. Standard: 09:00–17:30 UK time, Mon–Fri (excluding Bank Holidays).

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

Incident management: Operational issues and urgent findings are logged and triaged using buyer tooling (for example ticketing and/or SIEM). During agreed cutover or change windows, Lean Tree can provide time-bound hypercare and escalation support if included at call-off.

Planned maintenance and change notices: Not applicable unless the Call-Off includes a retained/managed support 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 the delivery plan.

Information required from the buyer: In-scope cloud accounts/subscriptions, identity and Single Sign-On (SSO) (single sign-on) approach where applicable, integration targets (ticketing/SIEM), operating model preferences, reporting needs, and nominated sign-off roles.

Access requirements: Requires an active buyer Wiz subscription/tenant and administrator access. Access to in-scope cloud accounts/subscriptions is provided via buyer-approved methods and aligned to least privilege. Integration access is provided for agreed buyer tools.

Typical mobilisation timeline: Mobilisation timeline and dependencies are agreed at call-off based on scope, access readiness, and integration complexity.

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: Requires an active buyer Wiz subscription/tenant and timely access to nominated stakeholders, in-scope cloud accounts, and buyer tooling for integrations. Constraints (for example 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: Wiz service data is stored and processed under the buyer's contract with the vendor. Lean Tree does not host Wiz. By default, engagement artefacts are stored within buyer repositories; where supplier-held working documents are required, storage is on Lean Tree's UK SharePoint tenant.

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 and Wiz, vulnerability management remains the buyer's and vendor'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, configuration notes, reporting packs, 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 the Wiz subscription/tenant, cloud subscriptions/accounts, and buyer-mandated tooling to enable delivery. Specific dependencies are confirmed at call-off.

Identity, networking, and security dependencies: Identity (including SSO where used), networking, and security approvals are confirmed at call-off and align to buyer standards and approval processes.

Third-party vendors: Wiz and any buyer-selected tools integrated as part of the agreed scope.

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 scope: confirm in-scope cloud accounts, stakeholders, and reporting needs.
2) Access readiness: confirm Wiz tenant/admin access, cloud connectors, and any identity requirements.
3) Baseline configuration: onboard accounts, set policy baselines, and configure roles and ownership.
4) Workflow setup: define triage, escalation and governance routines; align to buyer change control.
5) Integrations (if in scope): configure ticketing and SIEM integrations where available.

6) Tuning and reporting: reduce noise, confirm thresholds, and publish the reporting pack.
7) Handover: deliver runbooks and configuration notes; complete knowledge transfer.

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