Microsoft Azure Support Services

G-Cloud 15 — Lot 3 (Cloud Support)

Supplier: Inetum Digital Services UK Ltd

1. Services Overview

Managed Azure support that monitors, operates and optimises your cloud 24×7. We provide incident, request and change management; platform governance and policy-as-code; backup/DR and security baselines; FinOps cost control; and proactive Site Reliability Engineering (SRE) improvements. Delivery is by dedicated customer teams with SLAs and service reviews, aligned to Microsoft CAF and Well-Architected.

2. Service scope and activities

- Monitoring & Alerting: Azure Monitor, Log Analytics, Alerts, dashboards (24×7 optional).
- Incident/Request/Change: ITIL-aligned process with runbooks, approvals and peer review.
- Governance: Azure Policy/Initiatives, RBAC/PIM, configuration baselines and compliance reporting.
- Security Operations: hardening, patch cadence, vuln findings triage, backup/restore checks.
- Business Continuity: tested restore procedures and DR plans using Azure Backup/ASR.
- FinOps: tagging, budgets, rightsizing, reservations/savings plans, usage reviews.
- SRE: reliability engineering backlog (automation, resilience, performance, capacity).
- DevOps enablement: Infrastructure-as-Code (Bicep/Terraform) for repeatable changes.
- Service Management: TAM/Platform Manager, service meetings, KPIs and continual improvement.

3. Data backup, restore and disaster recovery

We design and operate Azure-native protection per workload RPO/RTO: Azure Backup (VMs, SQL, Files), Recovery Services Vaults with immutability options, and Azure Site Recovery for failover. Runbooks document restore steps, testing cadence, evidence capture and DR exercise reporting.

4. Onboarding and offboarding

- Onboarding: kick-off, RACI, access and change controls, tooling integration (ticketing/CMDB), discovery and baselining.
- Offboarding: artefact handover (as-built, runbooks, IaC/pipelines), KT sessions, access revocation and exit report.

5. Service constraints

- Changes to production follow agreed maintenance windows and change control.
- Azure consumption and third-party licensing remain buyer costs unless stated in Call-Off.
- Customer SMEs, timely decisions and environment access are required to meet targets.

6. Service levels (performance, availability, support hours)

Coverage: Business Hours (UK) as standard, with optional 24×7 for P1/P2. Typical SLAs (tailored at Call-Off):

- P1 — response 30 minutes; engineering engagement within 2 hours.
- P2 — response 30 minutes; engineering engagement within 4 hours.
- P3/P4 — triaged same business day.
- Change window adherence, deployment success rate and restore test cadence reported monthly.

7. Support channels and ticketing

Incidents/requests raised via the agreed online ticketing portal (ServiceNow or Jira Service Management), email, and—where enabled—web chat/Virtual Agent. Priority, status and SLAs are visible to the buyer; Major Incident comms use conference bridge and stakeholder updates.

8. Technical requirements

- Buyer-owned Azure subscriptions/tenants and identity (Microsoft Entra ID).
- Connectivity as applicable (VPN/ExpressRoute) and firewall rules for agents/pipelines.
- Repository and pipeline platform (Azure DevOps or GitHub) for IaC and automation.
- Access to buyer CMDB/ticketing for integration and asset/change traceability.

9. Outage and maintenance management

Planned changes follow change control with documented risk/rollback. Emergency changes follow an expedited process with immediate post-implementation review. Microsoft advisories are assessed and actions coordinated.

10. Hosting options and locations

Services operate on Microsoft Azure regions selected by the Buyer (e.g., UK South/UK West or EU). Designs consider residency and sovereignty; Availability Zones/multi-region patterns are used for resilience as required.

11. Access to data (upon exit)

The Buyer retains ownership of data and subscriptions. We provide export guidance for Azure services (Storage, SQL, Key Vault, Logs). IaC/pipelines and configurations are delivered to buyer repositories; Inetum access is removed with evidencing.

12. Security

- Zero-Trust: least privilege (RBAC/PIM), MFA, network segmentation, JIT access.
- Policy-as-code: Azure Policy/Initiatives with dashboards and auto-remediation where enabled.
- Monitoring: Azure Monitor/Log Analytics/Sentinel; vulnerability/patch management integrated with DevOps.
- Encryption at rest/in transit; secrets in Key Vault; immutable backup options where supported.
- Personnel: BPSS-aligned screening baseline; higher HMG vetting via buyer route when required. Cyber Essentials maintained.

13. Roles, responsibilities and pricing reference

Roles: L1 (triage/admin), L2 (engineering), L3 (architecture/SRE) and a named TAM/Platform Manager. Pricing: see separate G-Cloud Pricing document (SFIA-mapped rate card) or agreed fixed monthly bundle in the Call-Off.

14. Service reporting and continual improvement

Monthly/quarterly reviews cover SLAs, incidents, change success, reliability items, security posture and FinOps actions. A tracked improvement backlog drives automation and resilience outcomes.

15. Accessibility

Buyer-facing artefacts can be provided in accessible formats. Our portals and documents follow WCAG 2.1 AA guidance where applicable.

16. Assumptions and dependencies

- Timely buyer decisions and SME availability.
- Access to environments and necessary approvals are granted on schedule.
- Non-functional requirements (security, DR, performance) agreed per workload and reviewed annually.

17. Contact and ordering

Ordering is via the G-Cloud Call-Off process. For queries, contact your Inetum account manager or the assigned Platform Manager at onboarding.