



Service Definition Document

G Cloud 15 Lot 3



Overview

Lot 3 – Cloud Support

GP Strategies Cloud Support (Lot 3) delivers professional services that help public sector buyers plan, configure, migrate, assure, train and support their cloud-hosted platforms.

We are technology-agnostic and operate within buyer- or third-party-hosted environments, with specialist experience across learning and web technologies (for example Moodle, Mahara, Learning Locker, OpenSearch, Laravel, Django, Alfresco) and a Defence-experienced team familiar with MODCLOUD.

What the service includes

- Planning & Design: Consulting workshops and a structured Health check across people, process, technology and content; options appraisal and a pragmatic roadmap.
- Setup & configuration: Best-practice configuration and optimisation of buyer- or third-party-hosted environments, roles/permissions and integrations.
- Migration support: Current-state audit, migration plan and cutover runbook; rehearsal and controlled transition support with buyer approval gates.
- Quality assurance & performance testing: Test planning, functional and non-functional test execution support (including performance), defect triage and reporting.

- Training & knowledge transfer: Role-based enablement for administrators and support staff; creation of FAQs and knowledge articles.
- Ongoing support: ITIL-aligned incident, request and problem management across 1st/2nd/3rd line, with service reporting and continuous improvement.

Service features at a glance

- Channels: Direct phone lines (no automated menus) and email/ticketing.
- Service levels: 09:00–17:30 (UK); target 4-hour initial response; target 5-day fix/closure (priority-based).

- Control & transparency: Buyers manage ticket status and priority; receive monthly reports and trend insights.
- Training: Tailored, role-based training delivered online or on-site, typically in two stages (early enablement, then deeper admin training).
- Security & personnel: Staff screening in line with BS7858:2019; ability to field personnel with clearances up to BPSS/SC/DV where roles require.
- Public-sector fit: Defence-experienced team; accessible documentation and ways of working suited to government environments.

Onboarding

Onboarding establishes how our service will operate in the buyer's environment and reduces delivery risk before steady state.

Our focus is on confirming objectives, roles and access, setting up ticketing and communications, and making sure the right knowledge and controls are in place from day one. The steps here explain how we structure that work and the specific outputs a buyer should expect as evidence of readiness.

Steps and deliverables:

Discovery workshops	Transition plan	Service desk set up	Knowledge capture	Early life support
People, process, technology, content	Covering environments, access, integrations, ticketing, comms, and governance.	Queues, priorities, templates, buyer visibility of status/priority.	Known issues, FAQs, service catalogue items.	Heightened monitoring; rapid defect triage.
Deliverable: Discovery summary & recommendations	Deliverable: Onboarding plan & RACI	Deliverable: Onboarding checklist	Deliverable: Initial data set	Deliverable: Handover to BAU



Service scope

Here we define the operational scope of support and the services available to call off. It sets expectations for what each support tier handles, how users and administrators access help, and which add-on modules can be engaged.

Service desk tier	Description
1st line (end user)	Triage, FAQs, “how to” guidance, simple admin tasks
2nd line (administrator)	Configuration assistance, role/permission management, non-code integrations, data and reporting support
3rd line (specialist)	Complex diagnostics, interoperability and data issues, advisory on releases and best practice
Channels	Description
Phone support and email/ticketing	During standard hours
Ticketing tool	Buyers can manage ticket status and priority
Standard Inclusions	Description
Monthly issue reports and trend analysis	Reduce repeat incidents
ITIL-aligned workflows	Incident, request and problem workflows
Direct phone lines	No automated menus
FAQ creation and knowledge base curation	
Optional Modules (call-off)	Description
Migration assistance	Planning, rehearsal, cutover support
QA & performance test support	Plan, execute, report
Administrator training and role-based enablement	
Accessibility readiness support	Content/admin good practice

Service levels

This section outlines the coverage hours, response times, and resolution targets, as well as the practical application of prioritization. To be clear, these targets pertain specifically to the Cloud Support service; service-level agreements from platform providers are distinct and managed in coordination rather than being incorporated by default.

Hours of service

- **Standard:** 9 to 5 (UK time), 7 days a week

Targets (incident/request)

- Initial response: Target within 4 business hours.
- Target fix/closure: Within 5 business days, prioritised by impact/urgency and complexity.
- Buyer control: Buyers can view and manage ticket status and priority.

Note: These are targets for the Cloud Support service; where 3rd-party SaaS/PaaS/IaaS are involved, their contractual SLAs remain with the buyer and/or that provider. We coordinate and escalate on the buyer's behalf as part of support.

Reporting & reviews

- Monthly service report: ticket volumes, SLA/target attainment, aged incidents, root-cause summaries, trends.
- Quarterly service review (or as agreed): roadmap, improvements, risk/issues, and capacity planning.





Incident and problem management

Our ITIL-aligned workflows manage the reception, triage, advancement, and resolution of issues.

The goal is to guarantee consistent processing, clear communication, and thorough knowledge documentation, leading to a reduction in recurring problems over time. Buyers maintain visibility and can monitor status and priority throughout the entire process.

Incident lifecycle

- Log & classify (normalise, assign priority/severity)
- Initial response and customer update
- Diagnosis & workaround (engage 2nd/3rd line as needed)
- Resolution & validation (customer confirmation)
- Closure and knowledge capture

Problem management

- Proactive trend analysis; problem record with root cause hypothesis.
- Corrective actions tracked to closure; updates reflected in KB/FAQs.

Requests & standard changes

- Fulfilled through the service catalogue with defined approvals and lead times.

Quality Assurance & Performance Testing

Assurance and testing services help buyers validate changes before they affect users. The emphasis is on practical risk reduction: planning appropriate test coverage, executing functional and non-functional tests where requested, and turning findings into clear actions:

- Test planning: Scope, data, environments, acceptance criteria.
- Functional testing: Regression, integration and user acceptance support.
- Non-functional testing: Performance/load test design and execution support; results analysis and recommendations.
- Accessibility support: Guidance aligned to public sector accessibility expectations (for admin journeys and content workflows).
- Defect management: Triage, prioritisation, retest, and readiness to deploy.

Security, Data Protection & Vetting

Security activities in Cloud Support focus on secure ways of working, proportionate handling of data in support processes, and deploying appropriately vetted personnel. We coordinate with buyer policies and platform providers rather than supplant them. Here we set out what buyers can expect from our staff screening, data handling, and incident coordination practices:

- Personnel: Staff are screened; where a role requires it, we can deploy personnel with BPSS/SC/DV clearances.
- Secure working: Need-to-know access, encrypted channels, secure device standards, and buyer-approved tooling.
- Data handling: We minimise personal data in tickets, use role-based access, and follow buyer guidance for sensitive information.
- Security services (advisory): Strategy, risk management, design, consultancy, security testing coordination, incident management support, and audit support where requested.
- Incident coordination: If a security incident is suspected, we follow the buyer's process, support triage and evidence capture, and coordinate with platform vendors.

We act as a supporting service in security matters—owning our support processes and coordination while respecting the buyer's and platform providers' security responsibilities.

Training and knowledge transfer

We provide tailored training so buyer teams can operate confidently:

- Two-stage enablement is typical: early fundamentals during initial setup, then deeper administrator training nearer go-live/steady state.
- Topics may include user and role administration, permissions and policies, integrations and data flows, reporting/analytics, best practice for content and configuration, and support workflows.
- Training is online or on-site (as called off), complemented by FAQs and handover artefacts.

Service constraints

The following service constraints apply

- Remote-first delivery unless otherwise agreed.
- Availability of some activities (e.g., test execution windows) may depend on buyer/platform provider change freezes and maintenance windows.
- Access to environments, logs and vendor support portals must be provided to meet target response/fix times.

Offboarding / Termination

In the event that the client wishes to terminate this agreement, a 90-day written notice of intent to terminate must be delivered by the client to GP.

In the event that GP wishes to terminate this agreement, a 90-day written notice of intent to terminate must be delivered by GP to the client.

In the event of site misuse, GP reserves the right to terminate this agreement immediately.

- Exit planning: We prepare a handover plan including knowledge transfer, configuration documentation, and open issue status.
- Data access on exit: We provide an export of ticket data and knowledge artefacts in commonly used, non-proprietary formats.
- Third-party coordination: We support introductions and knowledge handover to your incoming supplier or internal team.

Pricing, ordering and invoicing

Pricing

Pricing follows G-Cloud conventions and is detailed in the Pricing Document and SFIA Rate Card:

- Support service tiers (e.g., defined ticket volumes or instance coverage) — fixed monthly charge per agreed scope.
- Consulting & specialist support (planning, migration, QA/testing, training) — T&M or fixed-price work packages as called off.
- Optional extensions (e.g., extended hours cover, additional reporting, on-site presence) — priced per option

Ordering and invoicing

- Ordering: Via the G-Cloud framework call-off.
- Invoicing: For support, monthly in arrears unless otherwise stated in the Pricing Document; for defined work packages, invoicing per agreed milestones.
- Payment terms: In line with framework standard terms.



Thank you

© 2026 GP Strategies Corporation. All rights reserved.
GP Strategies and GP Strategies with logo design are
registered trademarks of GP Strategies Corporation.

All other trademarks are trademarks or registered
trademarks of their respective owners. Proprietary to
GP Strategies Corporation.