SERVICE DEFINITION

G-Cloud 15
Framework reference: RM1557.15

Push

Leave IT to us

Cloud Support & Service Management

Introduction **4**
Company Overview 4
Leave IT to us 4
Tried and tested familiarity 4
Complete flexibility 4
Service Introduction 5

Service Detail **5**
Support Tiers 5
Tier comparison (Core vs Enhanced) 6
Service Features 6
Service Benefits 7
Supported Cloud Estate 7

Getting Started **9**
Trial Consultation 9
On-Boarding Overview 9
Kick-off and Mobilisation 10
Discovery and Environment Baseline 10
Assurance, Security and Access Requirements 11
Tooling, Monitoring and Service Management Setup 11
Documentation, Runbooks and Knowledge Transfer 11
Go-Live and Service Acceptance 12
Onboarding Checklist 12

Steady-State Service Management **13**
Raising Requests and Incidents 13
Service Management 14
Off-boarding and Service Exit 15
After-sales Account Management 15

Provision of the service **15**
Customer Responsibilities 15
Our Responsibilities 16
Technical Requirements and Customer-Side Requirements 16
Service Constraints 17

Pricing Overview 17

Data Protection 18

Information Assurance 18

Security 19

Data Backup and Restoration 20

Business Continuity and Disaster Recovery 20

Privacy by Design 21

Social Value 21

Kickstart Economic Growth 21

Make Britain a Clean Energy Superpower 22

Break Down Barriers to Opportunity 22

Working to public-sector standards (including NHS, local government and policing contexts) 22

Measurement & Reporting 22

Appendix A - Service Request Catalogue 24

Appendix B – Monthly Service Report Example 25

Report details (example) 25

Executive summary (example) 25

SLA summary (example) 25

SLA summary (example) 26

Planned work next period (example) 26

Contact Details 27

Introduction

Company Overview

Since 2004, we have been focused on providing cloud support and service management, supporting public sector organisations and suppliers to the public sector, using clear scope, predictable delivery and a no lock-in approach. A solutions orientated company, we pride ourselves on providing expert resources to ensure to safe, secure and continued operational integrity of your cloud solutions; initially developing a clear understanding of your needs to provide a strategic and sustainable support solution to enhance your businesses performance. The technology we provide gives a strong and flexible foundation that supports your business 365 days a year.

Leave IT to us

Push IT provide IT support that removes the confusion, wasted time and loss of productivity experienced by many public sector organisations when it comes to their IT systems. Our experts deliver robust, peace-of-mind solutions to improve efficiency, increase productivity and support business growth.

Tried and tested familiarity

IT solutions evolve but as an IT user, familiarity and easy functionality are essential to get the job done. Support from Push IT modernises and standardises your systems without compromising the structure and features you've become accustomed to.

Complete flexibility

Robust IT infrastructure improves efficiencies, increases productivity and realises financial savings. Investing in the right systems will enable business scalability, process continuity and high-level security. Remote access and wireless capabilities support a mobilised workforce and around the clock communication.

Working hand in hand with our security partner ECSC, Push IT your organisation secure

We are an official Cisco partner

As a Gamma partner, we offer voice, connectivity and mobile services to keep organisations at the forefront

As a Microsoft Gold Partner, Push IT are equipped to serve your modern, Microsoft suite needs

Service Introduction

Our Cloud Support & Service Management offering provides ongoing operational support for cloud services and the components that connect to them (such as identity, security configuration and connectivity). We operate as an extension of your internal IT function, helping you keep services secure, reliable and supportable.

Public sector organisations (and their delivery partners) that need structured, standards-based cloud operations without building a large in-house run function. This is particularly relevant where customers must work to public sector expectations for governance, security and auditability.

We also provide public sector support to move from legacy on-premise systems to the cloud, listed under our separate G-Cloud Cloud Deployment & Migration Service.

Service Detail

Push IT's experts deliver robust, peace-of-mind support service to maintain operations, improve efficiency, increase productivity and support business growth by providing:

- IT system upgrades that are fit for the future
- IT solutions that are tailored to your business
- Contingency planning and disaster recovery
- Responsive support and proactive maintenance
- Data protection and security

Support Tiers

Core Support
Delivered during business hours: Monday–Friday, 09:00–17:00 UK time, excluding public holidays, for day-to-day incidents, service requests and operational maintenance

Enhanced Support
Including 24x7 cover for Priority 1 (critical) incidents where required, and/or extended hours by agreement.

Response and resolution targets are defined in the SLA Schedule and tailored to the chosen support option.

Tier comparison (Core vs Enhanced)

Attribute	Core	Enhanced
Support hours	Mon–Fri 09:00–17:00 UK (excluding public holidays).	Core hours plus 24x7 on-call for Priority 1 incidents (where contracted).
Incidents	P1–P4 handled in Core hours. P1 response within 1 business hour.	P1 response within 15 minutes (24x7). P2–P4 handled in Core hours unless otherwise agreed.
Priority 1 target (summary)	Response: 1 business hour. Restore/workaround: 8 business hours (Core).	Response: 15 minutes. Restore/workaround: 4 hours (Enhanced 24x7 P1).
Service requests	Acknowledge within 1 business day; fulfil within 5 business days (Core hours).	Same targets (Core hours) unless otherwise agreed.
Channels	Email/phone and/or customer ITSM tool (as agreed in onboarding).	Same, plus on-call escalation route for P1 incidents.
Reporting & governance	Service reporting (typically monthly) and service reviews (typically monthly or quarterly).	As Core; cadence can be increased by agreement.
Pricing (from)	£2,500 per month per supported cloud estate (see Pricing Document).	£3,750 per month per supported cloud estate (see Pricing Document).
Included (typical)	Incidents and service requests; monitoring and alerting; routine maintenance; reporting and service reviews; onboarding and clean exit (as agreed in scope).	As Core, plus Priority 1 on-call escalation and response outside Core hours (where contracted).
Excluded (typical)	Major migrations, new service introduction, large remediation work, or improvement projects (priced separately using SFIA day rates or fixed price).	Same exclusions; Enhanced provides 24x7 cover for Priority 1 only (not Priority 2–4) unless otherwise agreed.

Service Features

- Business-hours Core; optional 24x7 Priority 1 on-call.
- ITIL-aligned service desk: incident, request, change, problem.

- Proactive monitoring and alerting for in-scope services.
- Security controls aligned to ISO/IEC 27001:2022; Cyber Essentials and Cyber Essentials Plus (certification documentation pending).
- Regular service reporting and reviews with improvement actions.
- Vendor coordination with cloud/SaaS and connectivity suppliers.
- Defined supported cloud estate boundary and shared responsibility model.
- Service request catalogue for standard changes and out-of-scope work.
- FinOps cost optimisation observations and recommendations, by agreement.
- Onboarding and clean exit with documentation and knowledge transfer.

Service Benefits

- Reduced downtime through proactive monitoring and incident response.
- Clear scope and priorities reduce operational friction and risk.
- Predictable SLAs and escalation routes support critical services.
- Faster resolution via direct access to senior engineers.
- Less burden on internal teams; we run operations.
- Optional 24x7 P1 cover reduces critical incident impact.
- Assurance-ready controls support ISO 27001 and audits.
- Better visibility through regular reporting and service reviews.
- Improved cost control with FinOps insights and right-sizing.
- No supplier lock-in through clean exit and documentation.

Supported Cloud Estate

We fully support all cloud platform operations, maintaining operations and providing a Service Desk support function including 24/7/365 cover where needed, across all major cloud platforms:

Microsoft Azure

Amazon Web Services (AWS)

Google Cloud Platform (GCP)

In this service, a supported cloud estate means the agreed set of in-scope cloud services and supporting components managed as one operational unit. It typically aligns to one organisation-level cloud boundary (for example a Microsoft or Google tenant and its associated subscriptions/projects) and one production environment (plus up to one non-production environment) as agreed. Where the customer requires support across multiple tenants or materially separate environments, we agree the appropriate banding and pricing in the Order Form.

In addition, we support organisations to maintain the surrounding infrastructure and connectivity, providing:

- Identity and access management support for cloud services (e.g. user access requests, privileged access processes, multi-factor authentication support).
- Security configuration management for cloud resources (firewalls/security groups, policies, logging and alerting configuration).
- Operational support for connectivity used to access cloud services (e.g. VPN, SD-WAN or secure internet access) where included in scope.
- Liaison with third-party vendors (cloud providers, software suppliers, connectivity providers) where the customer authorises us to do so.

Case Study – UK Electrical Contractor (SME)

This customer is a long-established UK electrical contractor supporting critical infrastructure programmes, often within regulated supply chains and on behalf of public sector customers. Their office team and field engineers rely on secure, dependable access across devices to information and collaboration tools so work can be planned, dispatched and evidenced efficiently.

We provide ongoing support for Microsoft cloud services and connectivity components within scope, providing an ITIL-aligned incident, service request, change and problem processes with clear records. We've setup monitoring and alerting mechanisms, aligned to service criticality and agreed thresholds. Identity and access management support is also provided, including least privilege and access review support. Our team deliver routine maintenance and patch coordination within agreed windows and approvals, and provide runbooks and service documentation for repeatable operational tasks and handover. Regular reporting and service reviews, with an improvement backlog and prioritisation are consistent deliverables, alongside assurance evidence support where required for regulated supply chains (where applicable).

Our service provides predictable operations and clearer priorities during incidents and requests, with responsive support and direct access to senior engineers where needed.

> *"We get clear updates, and the service is structured and reliable."*

Public sector programme stakeholder, UK electrical contractor

Getting Started

Trial Consultation

We offer a free initial consultation call to prospective customers. In that session, we discuss your goals and can provide a high-level review or demo of how we would approach your cloud support, effectively serving as a ‘taster’ of our expertise and introduction to our team and capabilities.

We support a clean exit and avoid supplier lock-in. During onboarding we agree what documentation, runbooks and configuration records are required for handover. On exit we provide knowledge transfer sessions as required and confirm access removal and secure handling of buyer data in line with the Call-Off Contract.

On-Boarding Overview

We run a structured onboarding to confirm the service scope, support option (tier), service levels, contacts, access, assurance requirements, ways of working and any agreed exclusions.. This section will describe how Push IT transitions a new buyer into steady-state Cloud Support & Service Management. The objective is to agree scope, establish secure access, configure monitoring and ways of working, and ensure both parties have clear responsibilities and governance from day one.

Key onboarding outputs typically include:

- Confirmed scope and in-scope service inventory (cloud services, supporting components and dependencies).
- Agreed support option and service hours (Core: Mon–Fri 09:00–17:00 UK, excluding public holidays; optional Enhanced: 24x7 on-call for Priority 1 incidents where contracted).
- Named contacts, escalation matrix, and agreed communication / ticketing channels (including the buyer’s ITSM tool where access is provided).
- Agreed access model (named accounts, multi-factor authentication (MFA), least privilege, privileged access approval and audit logging).
- Monitoring and alerting configuration aligned to service criticality, including agreed thresholds and maintenance windows.
- Runbooks / service handbook covering incident, request and change processes and any buyer-specific requirements.
- Reporting cadence and service review schedule, including a continuous improvement backlog (and financial operations (FinOps) reporting where requested).
- Clean exit readiness: documentation and handover approach agreed up-front to avoid lock-in.

Our structured onboarding includes the following phases:

- Kick-off and Mobilisation
- Discovery and Environment Baseline
- Assurance, Security and Access Requirements
- Tooling, Monitoring and Service Management Setup
- Documentation, Runbooks and Knowledge Transfer
- Go-Live and Service Acceptance

Kick-off and Mobilisation

We begin with a kick-off to confirm scope, priorities and how the service will operate in practice.

- Confirm buyer sponsor / service owner and technical contacts.
- Confirm scope boundaries, assumptions and exclusions (including third-party responsibilities).
- Confirm support option and hours (Core 09:00–17:00; optional Enhanced 24x7 on-call for P1 incidents, if required).
- Confirm incident priority definitions, response/resolution targets, and escalation paths (as per our Terms and Conditions).
- Agree communication channels and ticket logging approach (buyer ITSM tool where access is provided, or agreed alternatives).
- Agree onboarding timetable and acceptance criteria for go-live.

Discovery and Environment Baseline

We establish a shared understanding of the environment, service criticality and operational constraints so support can be delivered safely and predictably.

- Capture in-scope cloud accounts/subscriptions/projects, key workloads and dependencies.
- Confirm service criticality, operational constraints and any planned change freezes.
- Review existing monitoring, backup/recovery arrangements and known risks (where in scope).
- Identify immediate stabilisation actions required for safe support handover (if any).

Assurance, Security and Access Requirements

We confirm security and assurance requirements and agree a secure access model before operational work begins.

- Confirm applicable data protection requirements (UK GDPR and Data Protection Act 2018).
- Confirm any public sector assurance requirements (e.g. Security Policy Framework and National Cyber Security Centre (NCSC) Cloud Security Principles).
- Confirm any sector-specific expectations “where applicable” (e.g. NHS DSP Toolkit expectations, PSN/HSCN connectivity constraints).
- Confirm security clearance requirements: SC available, as required to meet project requirements.
- Agree access controls: named accounts, MFA, least privilege, privileged access approval, and audit logging.
- Agree secure credential handling and joiner/mover/leaver processes for support accounts.

Tooling, Monitoring and Service Management Setup

We configure monitoring and establish ITIL-aligned operational processes so incidents and changes are handled consistently.

- Configure monitoring and alerting to agreed thresholds and priorities (P1–P4), including maintenance windows.
- Agree incident management workflow (acknowledgement, updates, escalation, and incident reporting for P1 where required).
- Agree service request workflow and expected request information (to reduce resolution time).
- Agree change management workflow (approvals, scheduling, rollback planning, and record keeping).
- Agree problem management approach (root cause, preventative actions, and tracking recurring issues).

Documentation, Runbooks and Knowledge Transfer

We produce buyer-specific documentation so the service remains understandable, auditable and transferable.

- Create or update runbooks for common incidents, changes and operational tasks.
- Document the in-scope service inventory, contacts, escalation matrix and support processes (service handbook).
- Document known issues, risks and improvement actions in a shared register/backlog.
- Provide buyer briefing/training on how to engage support and what to expect.

Go-Live and Service Acceptance

We validate the onboarding outputs and confirm readiness to move into steady-state support.

- Validate access model and monitoring/alerting configuration (including test alert where appropriate).
- Validate incident logging and escalation path (including Enhanced 24x7 P1 on-call where contracted).
- Confirm reporting cadence and dates for initial service review.
- Agree acceptance sign-off and any immediate improvement actions for the first service period.

Onboarding Checklist

Use this checklist to track onboarding completion. The final set of items will be tailored to the buyer environment and agreed scope.

Contacts and Governance

- Buyer sponsor, service owner and technical contacts confirmed.
- Push IT service team named (service manager and technical lead).
- Escalation matrix agreed (including out-of-hours on-call contacts where contracted).
- Reporting cadence and service review schedule agreed.

Scope and Inventory

- In-scope cloud accounts/subscriptions/projects confirmed.
- In-scope workloads/services and dependencies documented.
- Out-of-scope items and third-party responsibilities documented.
- Critical business periods and change freezes confirmed.

Assurance, Security and Access

- Applicable requirements confirmed (UK GDPR, Data Protection Act 2018; Security Policy Framework and NCSC Cloud Security Principles where applicable).
- Data location requirements confirmed (UK-only) and any third-party tooling agreed.
- Any sector-specific expectations confirmed (e.g. NHS DSP Toolkit expectations, PSN/HSCN constraints where applicable).
- Access model agreed (named accounts, MFA, least privilege, privileged access approval, audit logging).
- Support account joiner/mover/leaver process agreed.

- **Service Management Setup**
  - Support option and hours confirmed (Core 09:00–17:00; optional Enhanced 24x7 P1 on-call where contracted).
  - Incident logging channels agreed (buyer ITSM tool where access provided, or agreed alternatives).
  - Incident priority and SLA targets agreed (P1–P4).
  - Change approval process and scheduling approach agreed.
  - Problem management and root cause reporting expectations agreed.

- **Monitoring, Alerts and Runbooks**
  - Monitoring and alert thresholds agreed and configured.
  - Maintenance windows agreed and documented.
  - Initial runbooks created/updated for common incident and change scenarios.
  - Backup/recovery responsibilities confirmed (where in scope).

- **Go-Live and Acceptance**
  - Access validated and monitoring/alerting test completed where appropriate.
  - Escalation path validated (including Enhanced 24x7 P1 on-call where contracted).
  - First reporting cycle confirmed and date for initial service review agreed.
  - Buyer acceptance sign-off completed and initial improvement actions captured.

Steady-State Service Management

Once onboarding is complete, we deliver Cloud Support & Service Management in line with the agreed scope and the SLA Schedule. We have provided a Service Request Catalogue in Appendix A to illustrate some typical, day-to-day support services and examples.

We provide regular reporting (typically monthly) and service review meetings at an agreed cadence (monthly or quarterly depending on buyer preference and support option). Continuous improvement actions are tracked and agreed through service reviews.

Raising Requests and Incidents

We agree the channels during onboarding. This can include email, phone and webchat if requested, and (where provided) logging and tracking in the buyer's IT service management (ITSM) tool. We prioritise and manage requests using an ITIL-aligned approach.

Ticket Logged (incident or service request)	Triage and Prioritise (ITIL-aligned)	Investigate and Resolve / Fulfil	Post-incident Review and Problem Management (as needed)	Change Control and Implementation (as agreed)	Reporting and Service Review Cadence

This process flow is illustrative only as each process will be tailored and agreed with the customer.

Service Management

Reporting and governance: We provide service reporting at an agreed cadence (typically monthly) and hold service review meetings (typically monthly or quarterly depending on tier and buyer preference). Reporting covers incidents and trends, service request volumes, change activity, risks and improvement actions. Where requested, we also include cost optimisation/FinOps observations. We have provided an example, anonymised monthly service report within Appendix B of this Service Definition.

We have a broad and highly experienced team of experts spanning all SFIA roles, all of whom are fully onboarded to our internal processes and align with industry recognised quality and security standards.

Case Study – Engineering Consultancy

This customer is an architecture, engineering and consultancy organisation with distributed teams and time-sensitive work. They depend on secure access to cloud-hosted applications and data, and work alongside an in-house IT function and established standards.

We provide ongoing operational support focused on secure access, connectivity and the “cloud edges”. Our standard incident triage process and routine, audit controlled maintenance delivers routing, resilience and updated security configurations. We also work with Cisco-based connectivity components in a way that complements existing designs.

> *“They communicate clearly, follow good operational discipline and keep services supportable.”*
>
> *IT stakeholder, engineering consultancy*

Off-boarding and Service Exit

Off-boarding in the context of a service ceasing means wrapping up the monitoring mechanisms and ensuring a clean handover, with no lock-in. On exit we provide handover documentation, knowledge transfer sessions as required, and confirm access removal and secure handling of buyer data in line with the Call-Off Contract.

After-sales Account Management

Push IT's philosophy is to build long-term partnerships. After a contract has ended, we do not disappear. We provide after-care and account management to ensure the customer is satisfied and to assist with any follow-up needs if required.

- **Account Manager:** We will assign an ongoing Account Manager who will remain your point of contact at Push IT moving forward. They will check in at intervals (for example, a month after project end, then quarterly for a year) to see how things are going in the new environment.
- **Ad-hoc support:** the Account Manager can arrange ad-hoc support or advice if needed via our support desk on a T&M basis, or guide you through raising a small G-Cloud call-off for any minor follow-up work. We won't leave you hanging if you have a few questions after the project, we'll happily help as part of good customer service, typically without immediate charge unless it becomes substantial work.
- **Feedback:** We'll conduct a post-engagement review meeting or survey to capture your feedback on how the service went. We use this to improve, and also it often surfaces small opportunities to fine-tune things for you that we can address right away.
- **Long-term relationship:** The Account Manager can keep you informed on relevant new services or updates. For example, if six months later AWS releases a new feature that could save you money, we'd reach out to tell you about it. We're not just looking for the next sale; we want the solution we implemented to continue delivering value, so we maintain a vested interest.

Provision of the service

Customer Responsibilities

Customer responsibilities typically include:

- Provide timely access to relevant systems and environments, including authorising the agreed support accounts.
- Provide escalation contacts and decision-makers for approvals (especially for changes that impact cost, risk or availability).

- Maintain contracts with third parties (cloud providers, SaaS vendors, telecoms/connectivity providers) unless explicitly included.
- Inform Push IT of planned changes and constraints that may affect service delivery.

Our Responsibilities

- Deliver support and service management in line with the agreed scope and SLA targets.
- Operate controlled change processes and maintain service records for incidents, changes and requests.
- Provide clear communications and progress updates during incidents and planned work.
- Maintain relevant certifications (ISO/IEC 27001:2022; Cyber Essentials and Cyber Essentials Plus (certification documentation pending)) and follow secure operational practices.
- Support continuous improvement through recommendations and agreed improvement backlog.

Service levels: Response and resolution targets are defined in the SLA Schedule and tailored to the support option. Where 24x7 cover is required, this is provided as an optional Enhanced Support arrangement for Priority 1 incidents only and is confirmed in the Order Form.

Technical Requirements and Customer-Side Requirements

On the technical side, there are some requirements for the client's setup to enable the migration.

- **Network Connectivity:** There should be reliable IP network connectivity between the source environment (on-premises data centre or hosting) and the target cloud. This could be via internet VPN or a dedicated link (like Azure ExpressRoute or AWS Direct Connect, if already in place). If none exists, we'll use encrypted internet connections. The requirement is: appropriate firewall rules opened to allow our migration tools to connect (e.g., allowing our migration VM in Azure to talk to your on-prem SQL on port 1433, etc.). The client's network team might need to configure these. If data is extremely large, we might require the client to facilitate use of physical transfer devices or shipping drives – we will discuss if needed.
- **Test Environment:** If the client has a staging or test environment where we can do a trial migration, that's ideal. It's not strictly required, but highly recommended. The client should be willing to let us use such non-prod systems to test procedures. If only production exists, we will take extra care, but this is a constraint to note.
- **Client Infrastructure During Migration:** The source servers ideally should be stable and have resources to support the migration processes (for example, enough free disk space to create an export). If some servers are very constrained, the client might need to provision temporary space or increase resources for the migration duration.

Similarly, if there are legacy OS versions (Windows 2003, for instance), the client should inform us; we may require enabling certain services on them (like installing an agent or enabling RDP/SSH) to extract data. The client's security team must allow those temporary measures.

- **Licensing:** The client should have proper licenses for the software being run in the cloud. Many server OS licenses can be brought to cloud under BYOL or converted to cloud's pay-as-you-go. We'll advise, but the client must ensure they possess any necessary licenses e.g., Windows Server licences with Software Assurance if using Azure Hybrid Benefit, or SQL licenses. If they don't, they may need to use the cloud provider's licensing which will incur cost. We highlight this as a requirement: the client's procurement of licenses or acceptance of cloud licensing costs.
- **Data Compliance Requirements:** If there are specific compliance requirements (like data must remain in UK, or particular encryption standards), the client should communicate those up front. Technically, we can accommodate most (Azure/AWS UK regions, KMS with customer-managed keys, etc.), but it's a requirement to know them to design correctly. Also, if any data or system has regulatory constraints (e.g., might need regulatory approval before moving), the client must handle those approvals.
- **Client Participation in Testing:** We need client-provided test cases or at least guidance on how to verify each application. That is effectively a requirement: someone on the client side who knows what "good" looks like for each system, so we can know the migration succeeded. Without that, we can test basics (ping, login), but only client users know the nuances of their applications.

Service Constraints

Unless explicitly included within the order form, the following services fall out of scope of our support service:

- Major application re-development or new feature development (we can support enabling work and handover to development teams).
- Customer end-user device support unless explicitly included (for example, device management is only included where agreed).
- Guaranteed service availability/uptime for customer systems (availability depends on architecture and third-party services); we focus on response and restoration targets, prevention and resilience improvements.
- Backup/recovery and disaster recovery (DR) design/implementation are the customer's responsibility unless explicitly included; Push IT can support and coordinate by agreement (see Pricing Document add-ons).
- Optional specialist security activities (for example, penetration testing or independent assurance) can be coordinated by Push IT by agreement, where required by the customer.

Pricing Overview

We typically provide a monthly managed support subscription for steady-state operations

(Core or Enhanced), with G-Cloud day rates used for project work, major change and improvement activity. Details are provided in the Pricing Schedule.

Our fees for any consultancy services falling outside of the subscription fee will be based on the rates submitted within our G-Cloud listing and Pricing Schedule, typically structured as a fixed price or time-and-materials with a capped limit (depending on what is most suitable and giving you confidence in cost control). For fixed price engagements, payment milestones are defined in the Order Form i.e.,

- 20% on project kick-off
- 50% on completion of migration execution
- 30% on final acceptance (for example).

For time-and-materials, we invoice monthly in arrears for days expended, up to any agreed cap. In all cases, invoicing is done against work delivered. We invoice either at milestones or monthly, as per the contract, with Net 30-day payment terms (30 days from receipt of invoice). We use electronic invoicing (PDF via email) unless you require another method.

All prices are exclusive of VAT. If any travel or subsistence expenses are necessary (e.g., for on-site work), these will be agreed in advance and billed at cost in line with the Framework terms (though in practice, most work can be done remotely, and we endeavour to minimise expenses). There are no additional setup fees beyond what is quoted for the service itself, the price includes all preparatory work.

Data Protection

Information Assurance

Push IT delivers services using an information security management system (ISMS) aligned to ISO/IEC 27001:2022 and operates to Cyber Essentials and Cyber Essentials Plus requirements (certification documentation pending). We apply security-by-design and least privilege access as standard, and we agree access methods and approvals with the customer during onboarding.

Project staff are briefed on engagement-specific security requirements and operate under confidentiality obligations. We apply least-privilege access, secure handling of any extracts/backups, encryption in transit and at rest, and audit logging appropriate to the customer’s environment.

Where customers require alignment to specific government or sector requirements (for example the Security Policy Framework, NCSC guidance, or NHS DSP Toolkit expectations), we confirm requirements and evidence during discovery and implement appropriate controls within the solution and ways of working. Security-cleared (SC) personnel are available where required.

We apply security-by-design and least privilege access as standard, and we agree access methods and approvals with the customer during onboarding, implementing secure configurations aligned with CIS Benchmarks or Centre for Internet Security guidelines for cloud, enabling audit logging (and routing logs to secure storage or customer SIEM), and configuring identity controls (integrating with the customer's Single Sign-On if desired, or setting strong multi-factor authentication for cloud console access).

We support customers to meet their obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Where we process personal data on behalf of a customer, the Call-Off Contract and any data processing terms set out the roles and responsibilities.

Customer cloud data remains within customer -owned tenants/subscriptions/projects. Push IT stores minimal service management data (for example ticket metadata, runbooks and service reports) in UK-hosted systems. Push IT does not transfer customer personal data outside the UK without written agreement.

We also provide service records and documentation in common, widely supported formats (for example PDF/CSV as agreed) to support governance, reporting and clean exit. Tooling and integrations are agreed with the buyer and designed to avoid lock-in.

Security

Public sector security expectations (where applicable):

- NCSC (National Cyber Security Centre) Cloud Security Principles: we support designs and operations that align to these principles.
- Security Policy Framework (SPF): we can work to buyer security policies and assurance requirements where relevant.
- NHS DSP Toolkit expectations "where applicable": we can support assurance evidence gathering and operational controls that assist compliance where required by the buyer or their environment.
- Security clearance: SC available, as required to meet project requirements.

We agree and document the access model (named accounts, multi-factor authentication, privileged access approval, audit logging) and we maintain an asset and access register for in-scope components. We record incidents and changes and provide evidence suitable for audit and service reviews.

Data Backup and Restoration

As part of migration planning, we will review and support Customers to optimise existing backup measures and rollback plans for each cutover: if something goes wrong, how to restore the original setup quickly. That way, the business isn't left without a working system beyond the planned window. Before moving any system, we confirm there are up-to-date backups or system images in place (either existing ones or we take fresh backups). For example, if migrating a database, we will take a final backup or snapshot before cutover, which can be restored if anything goes wrong.

We would support cloud-native backup services for any new environments: e.g., enabling VM snapshot schedules, database point-in-time restore, etc., as per the customer's retention requirements.

We review backup policies with customers during our initial discovery discussions, surfacing data retention periods and data storage location preferences. Our standard is to implement at least daily backups (or more frequent for critical data) with a retention that meets business needs (often 30 days by default, adjustable).

We also perform test restores of a sample backup to validate that the backups are usable. In summary, data is safe: we mitigate risk by having backups at every stage and ensuring the target environment has an appropriate backup regime from day one.

Business Continuity and Disaster Recovery

We incorporate business continuity considerations in our service delivery. That means we plan for how the business can continue operating during the migration (e.g., staging changes to avoid critical periods, back-out plans if issues occur). More broadly, as part of designing the cloud architecture, we can, if in scope, set up Disaster Recovery (DR) capabilities. For example, we might configure cross-region replication or secondary site for key systems. If DR is not in the initial scope, we at least ensure the design is DR-ready and discuss options with the customer for future DR enhancements. We produce a high-level Business Continuity/DR plan for the new cloud service as one of the deliverables if requested, which outlines how the organisation could recover from scenarios like region-wide cloud outage or major incident. It will cover RTO/RPO (Recovery Time and Point Objectives) for each major system, agreed with the customer. Our own operations are also resilient: because we're a cloud-centric provider, if any of our offices faced an outage, our engineers can continue work remotely using cloud-based tools, so our support to the customer during the project won't be interrupted.

We maintain an internal Business Continuity Plan (BCP) aligned to ISO27001 A.5.29/5.30 controls; in essence, we're prepared to handle incidents on our side without impacting customer work. If during the project any severe incident happens (e.g. a critical system goes down unexpectedly), our team will invoke contingency steps documented in the migration plan to either recover quickly or roll back to the pre-migration state to restore service. A more detailed continuity or DR plan for the specific service can be provided to the customer on request. This ensures all parties know how to maintain or restore operations in worst-case scenarios.

Privacy by Design

GDPR and citizen privacy are fundamental considerations. From the outset of our service, we apply privacy by design principles. We minimise the personal data we handle. If access to data is needed, we discuss and get necessary Data Processing Agreements in place with customer stakeholders. We ensure any personal data we do process is strictly for the purposes of delivering support and is protected (encrypted storage, least-access). When monitoring the cloud solution, we factor in data privacy: e.g., ensuring sensitive data is stored in UK regions to comply with data residency requirements, enabling encryption at rest for all databases and storage (often using cloud provider encryption with keys managed either by the provider or customer-managed keys depending on compliance needs). We also advise on and implement access controls such that personal data in the cloud is only accessible to authorised roles within the customer organisation i.e., setting up separate environments or data stores for production vs test to prevent unnecessary exposure.

We work in line with UK GDPR principles and can support alignment to NHS DSP Toolkit expectations where relevant. If required, we can conduct a Data Protection Impact Assessment (DPIA) in collaboration with the customer's Data Protection Officer for the setup and delivery of the support service, identifying and mitigating any privacy risks. Our team is aware of privacy regulations, and we embed those considerations at every step, so the migrated solution is not only technically sound but also legally and ethically compliant regarding personal data.

Social Value

Push IT supports social value outcomes in line with UK government priorities (PPN 06/20 and the Social Value Model). We agree proportionate, measurable commitments at call-off and report progress as part of project governance.

Kickstart Economic Growth

As an SME based in the South West, we contribute to local skills and economic growth through local employment, training, and use of local partners/suppliers where

appropriate. We prioritise knowledge transfer to customer teams so capability stays in-house after the engagement for a more sustainable service.

Make Britain a Clean Energy Superpower

We minimise environmental impact by defaulting to remote delivery to reduce travel, and by designing cloud environments that avoid waste (for example right-sizing, scheduling non-production resources, and using managed services appropriately). We can support customers to evidence efficiency and cost optimisation improvements as part of the migration outcomes.

Break Down Barriers to Opportunity

We aim to provide fair access to opportunities through inclusive recruitment and development, and by supporting staff training and certification. In delivery, we design with usability and accessibility in mind and support customers to adopt secure, modern ways of working.

Working to public-sector standards (including NHS, local government and policing contexts)

We have supported customers within public-sector supply chains and regulated environments where strong governance, assurance and documentation are required. While we may not always contract directly with a local authority, policing organisation or NHS body, we are familiar with the standards and working practices typically expected. Where relevant, we agree the specific assurance requirements in discovery (for example data handling, access controls, audit logging, change control, and documentation) and deliver accordingly.

Measurement & Reporting

Push IT will track social value outcomes for each contract. For instance, we will report on jobs created (with details if any target groups hired), environmental metrics (e.g., estimated CO_2 savings from cloud optimisation), and any community initiatives undertaken. We assign a Social Value Officer internally who oversees these initiatives and will provide data to customers on request or at contract review meetings. We align our reporting to the Social Value Model criteria, ensuring transparency and accountability for delivering these commitments.

Case Study – DNA Global Testing Customer

This customer conducts DNA testing and research for domestic, legal/judicial, and commercial use cases. Accuracy, confidentiality and trust are central to their service, with dependable access to cloud platforms and supporting security tooling.

We provide day-to-day cloud operations and service management across a combination of Microsoft and Google cloud services. We monitor the secure access controls supported (least privilege) with disciplined handling of operational data and provide regular reporting covering tickets, maintenance activity and improvement actions; aligned to ISO/IEC 27001 control expectations.

Our service helps to reduce the operational burden on internal stakeholders and provides confidence that services are supported securely and consistently.

> *"The reporting and standards-based approach gives us confidence we're operating in a controlled way."*
>
> *Operations stakeholder, DNA Global Testing Customer*

Appendix A - Service Request Catalogue

This catalogue is illustrative and helps clarify what is typically treated as day-to-day support (included within the monthly subscription and included capacity) versus work that is planned and priced separately. Classification is agreed during onboarding and depends on risk, complexity, dependencies and required approvals.

Request category	Typical Examples	Typical Commercial Treatment
Incident (break/fix)	Service outage; degraded performance; access failures; monitoring alert triage; security-related operational incidents (as agreed in scope).	Included (in scope). Response and resolution targets are defined in the SLA Schedule. Enhanced provides optional 24x7 on-call for Priority 1 incidents only where contracted.
Service request	How-to and admin requests; access changes; small configuration tasks; reporting queries; routine operational requests within scope.	Included within the monthly subscription (within included capacity). Targets: acknowledge within 1 business day; fulfil within 5 business days (typical), subject to approvals and third-party dependencies.
Standard change (repeatable, low risk)	Routine maintenance; certificate renewals; patch scheduling; minor configuration updates; monitoring threshold tuning; backup policy adjustments (within scope).	Included where it fits within agreed scope and included capacity. Planned through a controlled change process with buyer approvals as required.
Minor improvement (small backlog item)	Runbook and documentation improvements; minor automation; small optimisation actions agreed in service reviews.	May be included if small and within included capacity; otherwise agreed and priced separately using SFIA day rates or fixed price.
Major change / project work (out of scope by default)	New service introduction; major remediation; platform redesign; large security uplift programme; DR implementation; migrations and transformation work.	Typically out of scope for the monthly subscription and priced separately using SFIA day rates or fixed price (see Pricing Document).

Where request volumes or complexity exceed the selected band, we agree additional capacity using our published day rates (or a fixed price based on day rates where deliverables are clearly defined).

Appendix B – Monthly Service Report Example

This is an illustrative layout only. All figures and content below are sample data (not customer data) and are agreed with each customer in practice.

Report details (example)

Headline	Details
Report period	Example: November 2025
Customer	Anonymised public sector organisation
Service	Push IT Cloud Support & Service Management
Support option	Core / Enhanced (as ordered)
Prepared by	Push IT Services Ltd
Version/date	v1.0 / Example: 05 December 2025

Executive summary (example)

Area	Status	Summary
Availability	Green	No unplanned outage reported for in-scope services during the period.
Incidents	Amber	1x P2 incident affecting a subset of users; resolved within target; follow-up action tracked.
Requests/backlog	Green	Service requests acknowledged within 1 business day; typical fulfilment within 5 business days.
Changes	Green	Planned changes delivered via agreed change process; no adverse impact reported.
Security/compliance	Green	Routine access review completed; patching/updates managed in line with agreed plan.

SLA summary (example)

Metric	Target	Result	Notes
P1 response	Per SLA Schedule	Met	N/A (no P1 incidents logged)
P2 response	Per SLA Schedule	Met	1 incident responded within target
P2 resolution	Per SLA Schedule	Met	Resolved within 1 business day
Service request	Within 1 business	Met	Acknowledged via agreed

acknowledgement	day		channels
Service request fulfilment	Within 5 business days (typical)	Met	Complex requests may be planned as project works

SLA summary (example)

Type	P1	P2	P3	P4	TOTAL
Incidents	0	1	4	3	8
Service requests	0	0	10	6	16
Changes	0	0	3	0	3
TOTAL	0	1	17	9	27

Planned work next period (example)

- Confirm agreed improvement backlog and prioritisation.
- Complete any planned changes and maintenance windows.
- Provide monthly service review and updated risk log.

Contact Details

Framework Manager
Robert Shorland

Telephone
0117 244 5550

Email
bid@pushit.co.uk

Website
https://pushit.co.uk/