

G-Cloud 15

Service Definition

Secure Cloud Migration, Security,
Compliance and Managed Support
Services

Lot 3 Cloud Support Services (Additional
Services)

Contents

1. Introduction	2
Company Overview	2
Value Proposition	2
What the Service Provides	2
Social Value	3
Overview of the G-Cloud Service	4
Associated Services	5
2. Data Protection	6
Information Assurance	6
Data Back-Up and Restoration	6
Business continuity statement/plan	7
Privacy by Design	8
3. Using the service	9
On-Boarding, Off-Boarding, Service Migration, Scope etc.	10
Implementation Plan	12
Service Management	13
Service Constraints.....	14
Service Levels	15
Outage and Maintenance Management.....	16
Financial Recompense Model for not Meeting Service Levels	17
4. Provision of the service	17
Customer Responsibilities.....	17
Technical Requirements and Client-Side Requirements	18
Outcomes/Deliverables.....	19
After-sales Account Management	19
Termination Process.....	20
5. Our experience.....	21
6. Clients.....	24
7. Contact Details	24

1. Introduction

Company Overview

Base3 Solutions Limited is a UK-based technology and consultancy company specialising in delivering innovative IT services and solutions to public and private sector organisations. Founded in 2021, the company is headquartered in Cheltenham and operates across the UK. Our core capabilities include cloud migration and optimisation, data engineering, software development, and IT service management. We work closely with clients to design and implement secure, scalable, and cost-effective technology solutions that support operational objectives and compliance requirements.

Base3 Solutions has experience delivering projects for a range of industries, including government, healthcare, finance, and education. We place a strong emphasis on understanding client needs, ensuring that our work aligns with business goals, technical standards, and regulatory frameworks, including ISO27001, Cyber Essentials, and IASME Cyber Assurance.

Our approach combines technical expertise with a focus on collaboration, transparency, and measurable outcomes. We maintain robust delivery processes, quality assurance practices, and security protocols to ensure that projects meet agreed timelines and budgets without compromising quality or compliance.

Value Proposition

Public sector organisations face increasing pressure to deliver efficient, secure, and user-centred services while operating within tight budgets and rapidly evolving technology landscapes. Initiatives such as the Government Digital Service (GDS) Digital, Data and Technology (DDaT) strategy and the “Cloud First” policy have driven a need for scalable, interoperable, and secure digital solutions. However, many organisations continue to struggle with legacy systems, complex procurement landscapes, and the resources required to deliver transformative change.

Base3 Solutions addresses these challenges by providing expertise in cloud adoption, systems integration, and secure digital service delivery. We help public bodies modernise legacy applications, optimise cloud infrastructure, and implement solutions that improve user outcomes while meeting government security and compliance standards, such as Cyber Essentials and Cyber Assurance.

Our approach goes beyond technical delivery — we work collaboratively with internal teams to transfer skills, reduce long-term vendor lock-in, and ensure that solutions are sustainable, cost-effective, and designed with end-users in mind. This approach directly supports the public sector’s drive for efficiency, resilience, and improved citizen digital experiences.

What the Service Provides

This service provides end-to-end support for public sector organisations adopting, optimising, or managing cloud-based and digital solutions. We deliver projects such as cloud migration, application modernisation, systems integration, and ongoing digital service management. Buyers can expect practical support from initial discovery and planning through design, implementation, and optimisation, with an emphasis on security, compliance, cost efficiency, and skills transfer to in-house teams.

Social Value

1. Kickstart Economic Growth

We actively contribute to economic growth by supporting digital innovation and creating skilled employment in the UK's technology sector.

Our initiatives include:

- Skills and apprenticeships: Providing opportunities for technology apprenticeships or paid internships each year to individuals from a range of backgrounds.
- Prompt payment: Ensuring all suppliers are paid within 30 days, supporting SME liquidity and resilience.
- Innovation enablement: Helping clients modernise legacy systems through cloud transformation, reducing costs and boosting productivity across public sector services.

2. Make Britain a Clean Energy Superpower

As a cloud-first business, we contribute to the UK's transition towards a sustainable, low-carbon economy.

Our initiatives include:

- Net-zero operations: Operating a digital-first, remote-enabled model that minimises business travel and office energy use.
- Sustainable hosting: Partnering exclusively with cloud providers committed to 100% renewable energy and net-zero targets, such as AWS and Microsoft Azure.
- Sustainable procurement: Replacing hardware on an energy-efficiency basis and recycling end-of-life equipment through certified UK e-waste partners.

3. Break Down Barriers to Opportunity

We are committed to inclusion, accessibility, and fair opportunity within our organisation and in the services we deliver.

Our initiatives include:

- Inclusive recruitment: We ensure all recruitment decisions are based solely on skills, experience, and aptitude, without consideration of any protected characteristic, in line with the Equality Act 2010.
- STEM outreach: Supporting local groups (e.g. Code Clubs, Scouts) to inspire digital skills in communities.
- Accessible workplaces: Providing flexible working patterns, assistive technology, and reasonable adjustments for all staff.

4. Build an NHS Fit for the Future

We actively support healthcare and public-sector clients in delivering secure, efficient, and resilient digital services.

Our initiatives include:

- Secure healthcare innovation: Delivering cloud architectures that meet NHS DSPT and Cyber Essentials Plus standards.

- Resilient systems: Enabling clients to adopt cloud technologies that improve data accessibility, reduce downtime, and enhance patient care.
- Staff wellbeing: Promoting flexible working and mental-health support to sustain healthy, motivated teams delivering public-sector outcomes.

Governance & Accountability

Social Value delivery is overseen by the Base3 Solutions Board, who meet monthly.

Outcomes are recorded and reviewed annually to ensure continued alignment with PPN 002 and G-Cloud 15 objectives.

Overview of the G-Cloud Service

Service Scope

This service provides cloud support and delivery capabilities to enable public sector organisations to implement, migrate, optimise, and manage digital services in cloud environments. Activities cover the entire service lifecycle including:

- Discovery and assessment of existing systems and infrastructure
- Cloud strategy development aligned to organisational objectives
- Design and architecture of cloud-based solutions
- Migration planning and execution for applications, data, and workloads
- Integration of cloud services with existing systems
- Performance optimisation and cost management
- Security, compliance, and risk management aligned to NCSC Cloud Security Principles
- Ongoing service management and support, including proactive monitoring, incident resolution, change management, and regular service reviews to ensure secure, reliable and cost-effective cloud operations

Key Service Capabilities

- Cloud-native solutions - leveraging serverless architectures, containerisation (e.g., Docker, Kubernetes), and managed service offerings
- Application modernisation - re-platforming, re-hosting, and refactoring of legacy systems for cloud optimisation
- Infrastructure as Code (IaC) - automated deployment and configuration using tools such as Cloud Formation
- Security and compliance - IASME Cyber Essentials and Cyber Assurance aligned processes, secure configuration, encryption standards, and governance frameworks
- Service monitoring and performance tuning - proactive monitoring, fault management, service health reporting

Cloud Characteristics Delivered (aligned to the NIST model)

- On-demand self-service - service provisioning and scaling without manual intervention, supporting rapid mobilisation
- Broad network access - secure access over standard networks from a range of devices and locations

- Resource pooling - use of shared infrastructure to achieve cost efficiencies while maintaining data segregation for secure workloads
- Rapid elasticity - ability to automatically scale resources to meet changing demand
- Measured service - cloud resource usage monitored and optimised, with cost transparency provided to the buyer

Service Benefits to Public Sector Buyers

- Minimises downtime through phased migration and contingency planning
- Reduces business risk through readiness assessments and gap analysis
- Improves security by embedding compliance into every stage
- Protects sensitive data through encryption and strict access controls
- Increases efficiency with optimised cloud deployment and support processes
- Enhances resilience with proactive monitoring
- Maintains security and performance with regular updates and patching
- Enables scalability to meet future organisational growth needs
- Informs strategic decisions with actionable data-driven insights
- Ensures compliance through continuous governance and risk management
- Delivery Approach:
 - Discovery & Planning - assess current systems, dependencies, and readiness for cloud adoption
 - Design - create an architectural blueprint and migration plan tailored to buyer needs
 - Implementation - execute the build, migration, and integration activities with minimal disruption to live services
 - Transition & Handover - deliver documentation, training, and capability uplift to in-house teams
 - Operate & Optimise - provide ongoing management, monitoring, and service improvement

Associated Services

The following services are available and are priced by the rate card in our pricing document:

- Cloud Readiness/Discovery Assessments
- Solutions Design and Architecture for cloud environments
- Migration of applications, workloads, and data to AWS, Azure, GCP, or hybrid environments
- Integration of cloud services via APIs and secure connectivity
- Service configuration, optimisation, and cost management
- Security controls implementation aligned to NCSC Cloud Security Principles
- Knowledge transfer and training for in house teams
- Service performance monitoring and reporting

- Enhanced data analytics and business intelligence services
- Specialist security accreditation support (e.g. Cyber Essentials, Cyber Assurance)

2. Data Protection

Information Assurance

As an IASME Certification body we are required to meet and be assessed on a number of Information Assurance certifications. Policies and processes are reviewed at least once a year and monthly director meetings take place where we can review organisational risk and detect any policy drift as soon as possible.

Certifications our organisation currently hold and maintain include:

- Cyber Essentials and Cyber Essentials Plus
- Cyber Assurance Level 1 and Cyber Assurance Level 2
- IASME Quality Principles
- ISO 9001 (In Progress)

Data Back-Up and Restoration

All service-related email, documentation, and collaboration data for this service is managed and stored in Microsoft 365 - specifically Outlook (Exchange Online), SharePoint Online, and OneDrive for Business - which provide built-in redundancy, retention, and restoration capabilities.

Backup and Resilience in Microsoft 365

- Exchange Online (Outlook): Emails are protected through Microsoft's data centres, with deleted items retained for a default of 30 days and recoverable items retained for up to 14 days (configurable as required). Data held in Exchange is backed up every 10 minutes and kept for 1 year.
- SharePoint Online: Document libraries have version history enabled by default, allowing rollback to previous versions of files. Deleted files are retained in the recycle bin for 93 days. Data held in SharePoint is backed up every 10 minutes and kept for 14 days. After 14 days we keep 1 backup a week for 1 year.
- OneDrive for Business: Files include version history and recycle bin retention for 93 days. Data held in OneDrive is backed up every 10 minutes and kept for 14 days. After 14 days we keep 1 backup a week for 1 year.
- All data is mirrored across multiple Microsoft data centres for high availability.

Additional Retention and Protection

- Base3 Solutions can configure extended retention policies through Microsoft Purview / Security & Compliance Centre, including litigation hold or preservation policies for email and documents where compliance requires longer retention.
- If required, we can implement third-party backup solutions (e.g. Veeam Backup for Microsoft 365) to provide additional point-in-time recovery options beyond Microsoft's 365 backup service.

Restoration Process

- Restoration requests (e.g., recovering deleted mailboxes, restoring document versions, or OneDrive files) are logged via the Base3 Solutions Service Desk.
- Most restores from version history or recycle bin can be completed within minutes; larger-scale restores (e.g. entire mailbox recovery) may take longer depending on data volumes.
- For enhanced backup solutions, Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) can be agreed per contract.

Process Review and Testing

- Backup and restoration processes are reviewed annually, or following material changes to Microsoft 365 features, and updated as necessary.
- Restoration procedures (including both native M365 and optional third-party backups) are periodically tested to validate integrity and timeliness.

Customer Options

- Buyers can agree alternative retention settings (shorter or longer) to meet governance requirements - these will be documented in the G-Cloud Call-Off Contract or Statement of Work before service commencement.

Business continuity statement/plan

Scope

This plan covers all activities and resources required to deliver and support the Base3 Solutions cloud support service, including:

- Customer relationship management and communications
- Service delivery and technical support functions
- Hosting, data management, and security controls
- Internal corporate functions critical to service provision (e.g., finance, HR, supplier management)

Key Business Areas and Critical Functions

- Service Delivery Management - Oversight of live contracts and ongoing communication with buyers
- Technical Operations - System configuration, monitoring, maintenance, and incident resolution
- Customer Data Management - Protection, backup, and restoration of service-related data (primarily stored in Microsoft 365)
- Supplier/Platform Dependency Management - Engagement with third-party providers (e.g., Microsoft, AWS, Azure, GCP) to ensure continuity of hosted services
- Administration & Governance - Contract, billing, and compliance management

Dependencies

- Availability and performance of underlying cloud platforms and associated SLAs from suppliers

- Connectivity between Base3 Solutions' support network and buyer or platform systems
- Microsoft 365 for communications, documentation management, and collaboration
- Key personnel availability and secure access to necessary systems

Acceptable Downtime for Critical Functions (typical targets — contract-specific values may vary)

- Customer communications (email, service desk) - less than 24 hours
- Critical incident response - Immediate acknowledgment within agreed SLA; service restoration within agreed RTO (often less than 4-8 hours for Severity 1)
- Core cloud platform availability - As per the underlying provider's SLA (e.g. 99.9% monthly uptime)
- Access to documentation and service records - less than 8 hours

Outline Continuity Plan

- Maintain geo-redundant, high-availability cloud environments where applicable
- Keep redundant connectivity options and secure remote-working capabilities for all key staff
- Implement and regularly test data backup/restore procedures for service data stored in Microsoft 365. As per IASME Cyber Assurance requirements this occurs on a monthly basis
- Use proactive monitoring to detect potential service degradation before it becomes customer-impacting
- Maintain clear supplier escalation channels to cloud vendors for rapid resolution of platform issues
- Yearly scenario testing and process reviews to improve recovery measures

A more detailed plan can be provided to the buyer on request.

Privacy by Design

Base3 Solutions incorporates Privacy by Design principles into every stage of service design, delivery, and ongoing management, in compliance with the UK GDPR and Data Protection Act 2018.

Proactive Privacy Measures

- Data Minimisation: Services are engineered to collect and process only the personal data necessary for the specified purpose, reducing privacy risks by design.
- Purpose Limitation: Personal data is used strictly for the delivery of contracted services and not for unrelated purposes.
- Role-Based Access Control (RBAC): Access to personal data is restricted to authorised personnel on a need-to-know basis, and enforced through least-privilege principles.
- Pseudonymisation/Anonymisation: Where feasible, personal data is anonymised or pseudonymised to reduce identifiability in live and test environments.

Integration in the Design Phase

- Privacy impact considerations are addressed during the discovery and requirements stage of all engagements.
- Data Protection Impact Assessments (DPIAs) are conducted where processing is likely to result in high risk to individuals' rights and freedoms.
- Security and privacy controls are embedded from the start — including encryption in transit and at rest, secure API design, and logging for accountability.

Adherence to GDPR Principles

The service and supporting processes are designed to meet the following GDPR principles:

- Lawfulness, fairness, and transparency - Processing is carried out with explicit contractual basis and in full transparency with the customer.
- Purpose limitation - Data is collected for specific, explicit, and legitimate purposes.
- Data minimisation - Only relevant and limited data is processed.
- Accuracy - Data is kept accurate and up to date where the supplier is the data processor.
- Storage limitation - Retention schedules are agreed and enforced, with secure disposal after the period ends.
- Integrity and confidentiality - Appropriate technical and organisational measures are implemented to protect data.
- Accountability - Compliance can be demonstrated through documented policies, controls, and audit logs.

Customer Options and Transparency

- Privacy configurations (e.g. retention periods, access controls, and audit requirements) can be agreed with the buyer and documented in the Call-Off Contract.
- Buyers receive full visibility into where data is stored and processed, with adherence to UK sovereignty requirements unless otherwise agreed.

3. Using the service

Ordering the Service

To discuss your requirements in more detail and place an order, please contact:

Email: sales@base3.co.uk

When contacting us, please include:

- Your organisation name and contact details
- The G-Cloud service name and Lot reference
- A brief description of your requirements, objectives, and any relevant technical context
- Desired start date and any key project deadlines
- Any specific compliance or security considerations

Order Process

- Initial Discussion: We will arrange a meeting to clarify requirements, scope, and timelines.
- Statement of Work (SoW): A detailed SoW will be prepared, setting out pricing, deliverables, milestones, and acceptance criteria.
- Call-Off Contract: We will collaborate with the buyer to complete the G-Cloud Call-Off Contract and Order Form, ensuring all service details, deliverables, pricing, and terms are accurately captured and aligned with the agreed Statement of Work.
- Contract Award: Once signed by both parties, delivery will begin in accordance with the agreed schedule.

Invoicing and Payment Terms

Unless otherwise agreed in the Call-Off Contract, fees are invoiced upon delivery and buyer acceptance of each fixed-price deliverable.

Alternative invoicing arrangements (e.g. milestone-based or periodic invoicing) can be agreed as part of the Call-Off Contract to meet buyer requirements.

Standard payment terms are 30 days after the date of invoice, consistent with UK Government prompt payment policy.

Invoices are issued electronically in PDF format and may be submitted via the buyer's e-invoicing portal if required.

All fees are exclusive of VAT, which is charged at the prevailing rate.

Availability of Trial Service

No service trials are available.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

On-Boarding Process

When a buyer awards a Call-Off Contract for this service, Base3 Solutions follows a structured on-boarding process to ensure a smooth start:

1. Kick-Off Meeting - Within 5 working days of contract signature, we host a session with buyer stakeholders to confirm scope, success criteria, roles, and timelines.
2. Dedicated Point of Contact - A named Delivery Manager is assigned as the primary contact for all communications and coordination.
3. Discovery & Readiness Assessment - Review existing systems, dependencies, and infrastructure to plan the migration path or service set-up.
4. On-Board Plan - A tailored on-board plan is agreed, outlining migration tasks, key dates, risk mitigation, and responsibilities.
5. Technical Set-Up - Configuration of cloud environments, connectivity, security controls, and monitoring in alignment with the agreed solution design.
6. Knowledge Transfer & Documentation - Provide service documentation, architecture diagrams, and operational guides. Where applicable, deliver skills transfer sessions or training workshops.

7. Service Commencement - Handover to live delivery/operational state, with initial performance reporting and buyer sign-off.

Note: On-boarding support can be included within the scope of the Call-Off Contract. Additional on-site or extended transition activities beyond the agreed plan can be purchased as optional professional services. These will be charged at the relevant day rate captured in our pricing document.

Service Migration to Base3 Solutions

Where a buyer is migrating from an existing supplier or system:

- A migration impact assessment is conducted
- Dependencies, integrations, and risks are documented
- Data migration/mapping plans are created, tested, and signed-off prior to execution
- Migration activities are scheduled to minimise service disruption, with fallback and rollback procedures in place
- Performance validation and buyer sign-off are completed before legacy services are decommissioned

Off-Boarding Process

At the end of a contract term or upon termination, Base3 Solutions will:

1. Notice Period - We will observe the notice period specified in the Call-Off Contract by providing written confirmation of termination, agreeing an exit plan with the client, and maintaining service continuity throughout the notice period.
2. Exit Planning Meeting - Engage with the buyer to agree an off-boarding plan, including key activities, resource requirements, and timelines.
3. Data Extraction - Provide all buyer data in an agreed open and portable format (e.g. CSV, JSON, XML), along with relevant configuration documentation.
4. Service Decommissioning - Arrange removal of access credentials, secure deletion of buyer data from our systems in accordance with GDPR and contractual requirements.
5. Handover Support - Support buyer staff or an incoming supplier with understanding the solution and its integrations.

Optional Exit Services: Customisable migration planning and extended off-boarding support (e.g. parallel run environments or complex re-architecture as part of migration away) are available at additional cost and can be defined in the Call-Off Contract. The rates for the additional services can be found in the pricing document.

Scope

Included: Activities explicitly set out in the Statement of Work agreed under the Call-Off Contract, plus standard on-boarding, knowledge transfer, and reasonable co-operation during exit.

Not Included: Major redesigns, unrelated technology workstreams, or extended/tailored off-boarding activities not covered in the agreed SoW (these can be purchased separately if required, using the rates in the pricing document).

Training

Included Training

As part of the standard on-boarding process for this service, Base3 Solutions provides:

- An introductory orientation session (online) with key stakeholders to explain service scope, capabilities, and operational processes
- A walkthrough of documentation including user guides, system architecture, and support processes
- Role-specific training for designated buyer personnel responsible for day-to-day service interaction (e.g. admins, technical contacts)
- Knowledge transfer sessions embedded into the delivery phase to ensure buyer teams have the skills to operate and maintain the solution beyond the contract

Training Delivery Methods

- Live online sessions using secure conferencing platforms, recorded where possible for future reference
- On-site workshops available where necessary (subject to the agreed Statement of Work)
- Written reference materials supplied in PDF and/or HTML format
- Access to knowledge repositories or FAQs maintained by Base3 Solutions for the duration of the Call-Off Contract

Additional / Optional Training

- Extended or customised training programmes, including advanced technical training or “train-the-trainer” sessions, can be provided at additional cost based on our day rates and agreed in the Call-Off Contract
- Refresher training for ongoing contracts or after significant service enhancements

Ongoing Support

- Buyers have access to online help, guidance notes, and technical support channels for the life of the contract
- Questions or clarification requests can be submitted via the designated support contact or Service Desk

Implementation Plan

Base3 Solutions follows a structured and proven approach to service implementation, tailored to the specific requirements, scale, and complexity of each buyer engagement.

Implementation activities include:

- Discovery & Requirements Confirmation - Validate scope, objectives, and constraints; identify dependencies and risks
- Design & Planning - Produce solution architecture, migration approach, and detailed task schedules
- Environment Preparation - Configure cloud environments, connectivity, access controls, and monitoring

- Build & Migration - Implement required services, migrate workloads or applications, and conduct integration activities
- Testing & Validation - Perform functional, performance, and security testing; remedy any defects or gaps
- Transition to Live Service - Go-live with change management controls in place; ensure minimal disruption to operations
- Post-Implementation Review - Assess performance against objectives, gather feedback, and apply service optimisations

A detailed implementation plan can be provided to the buyer on request.

Service Management

Base3 Solutions delivers the cloud support service within a structured IT service management (ITSM) framework, combining qualified personnel, defined processes, and appropriate tools to meet agreed service levels and continually improve outcomes.

Governance and Standards

- Service delivery is aligned to ITIL v4 best practices for the full service lifecycle: strategy, design, transition, operation, and continual improvement.
- Information security and data handling processes align to IASME Cyber Essentials and Cyber Assurance standards.
- Project and delivery management approach uses PRINCE2 and Agile methods, depending on buyer requirements.
- Compliance with NCSC Cloud Security Principles is embedded across our service operations.

People

- A dedicated Delivery Manager is assigned to each contract, acting as the single point of contact for the buyer.
- Specialist consultant teams (Cloud Architects, Developers, Security Engineers) are coordinated and managed by the SDM or a designated Technical Lead.
- Support Analysts and engineering staff operate under defined roles and escalation paths.
- All staff involved in delivery undergo security clearance appropriate to the engagement.

Processes

- Onboarding - Managed transition into service using documented plans and customer sign-off at each key stage.
- Incident Management - All incidents logged via the Service Desk; critical incidents prioritised for immediate triage; root cause analysis conducted and corrective actions implemented.
- Change Management - Formal change control process for service modifications, with risk and impact assessment.
- Request Fulfilment - Defined workflows for common service requests and provisioning tasks.

- Service Reporting - Agreed Key Performance Indicators (KPIs) and progress reports shared at defined intervals (e.g. weekly or monthly).
- Continual Improvement - Regular service reviews with the buyer to identify opportunities for optimisation, efficiency, and cost savings.

Technology

- Cloud-hosted service desk tool for request, incident, and change management, with buyer access available if required.
- Monitoring tools for real-time system performance, availability, and capacity metrics.
- Secure collaboration platforms for communication, document sharing, and status tracking.

Service Desk

- Single point of contact (SPOC) via email, phone, or web portal during contracted service hours.
- Defined Service Level Targets (SLTs) for response and resolution based on priority/severity level.
- Ticket tracking and status updates provided to the buyer for all open issues using HaloITSM.

Constraints Management

- Service constraints, dependencies, and planned maintenance windows are recorded and communicated in advance to minimise business impact.
- Emergency changes follow expedited change procedures with buyer authorisation where appropriate.

Service Constraints

The cloud support service operates within the following fixed parameters unless varied by written agreement in the Call-Off Contract:

Maintenance Windows

- Planned maintenance will be scheduled outside of core UK business hours wherever possible, with a minimum of 5 working days' notice.
- Emergency maintenance may be carried out at short notice to resolve security or stability risks. If the situation allows, we aim to provide at least 24 hours notice.

Level of Customisation

- Customisation is limited to the configurations and features supported by the agreed cloud platform(s) and the service scope defined in the Statement of Work.
- Functionality outside supported configurations will be subject to separate scoping, risk assessment, and commercial agreement. Pricing for any customisation will be charged as a day rate using the pricing document rate card.

Feature Updates and Deprecation

- Functionality delivered via third-party cloud platforms is subject to their published product roadmaps and depreciation schedules.

- Where possible, Base3 Solutions will provide advance notice of changes that could impact service, along with recommended remediation or migration options.

Buyer Responsibilities

- Providing required access, approvals, and technical information in a timely manner.
- Ensuring suitable connectivity, authentication, and compliance within the buyer's environment.

Service Levels

Service levels are discussed and agreed with the buyer prior to contract award and recorded in the G-Cloud Call-Off Contract or Statement of Work.

These may include, but are not limited to:

Performance and Availability Targets

- System availability percentage (e.g. 99.9% monthly uptime) as measured at the service delivery boundary.
- Performance benchmarks such as transaction response times or throughput.
- Availability targets are subject to the underlying SLAs of the buyer's chosen cloud provider (e.g. AWS, Azure, GCP).

Support Hours

- Standard hours: Monday to Friday, 08:00-16:00 UK time, excluding UK public holidays.
- Out-of-hours or 24/7 support available by prior arrangement and may incur additional cost, the details of which can be found in the pricing document.

Incident Severity Definitions (example for discussion)

- Severity 1 (Critical) - Complete loss of service or major incident affecting multiple users
- Severity 2 (High) - Significant degradation of service impacting critical functions
- Severity 3 (Medium) - Partial loss or degradation with a workaround available
- Severity 4 (Low) - Minor issues with little or no operational impact

Typical Response / Resolution Targets (to be finalised per contract)

- Severity 1: Response within 1 business hour, resolution target 4 hours or as agreed
- Severity 2: Response within 4 business hours, resolution target next business day
- Severity 3: Response within 1 business day, resolution target within 5 business days
- Severity 4: Response within 2 business days, resolution target by mutual agreement

Review and Reporting

- Regular service review meetings to monitor performance against agreed SLAs and address any improvement opportunities.
- Monthly or quarterly reporting based on KPIs agreed with the buyer.

Outage and Maintenance Management

Base3 Solutions applies a proactive approach to service continuity, combining preventative measures, ongoing monitoring, and robust maintenance procedures to minimise the risk of technical issues impacting buyer operations.

Outage Avoidance

- Redundant Architecture: Where applicable, services are deployed with high-availability configurations (e.g. multi-AZ, load balancing, failover mechanisms) supported by the underlying cloud provider.
- Proactive Monitoring: Real-time monitoring of system health, performance, and error logs, with automated alerts for threshold breaches.
- Preventative Maintenance: Regular patching, updates, and configuration optimisations to maintain platform stability and security.
- Change Control: All changes follow controlled change management processes with risk and impact assessments prior to implementation.

Service Performance Planning

- Capacity Management: Continuous review of resource usage and trends to ensure adequate capacity for current and forecasted demand.
- Scalability: Use of auto-scaling and elastic infrastructure where supported by the cloud provider to handle load variation without service degradation.
- Performance Benchmarks: Agreed thresholds for latency, throughput, and resource utilisation monitored against service levels.

Downtime Measurement and Reporting

- Availability Monitoring: Automated uptime measurement from multiple locations to verify end-user availability.
- Incident Logging: Any outage or degradation incidents recorded in the service desk tool with root cause analysis and resolution steps documented.
- Reporting: Monthly reporting of availability metrics provided to the buyer, or more frequently where contractually required.

Maintenance Management

- Planned Maintenance: Scheduled outside of agreed core business hours wherever possible, with at least 5 working days' notice.
- Emergency Maintenance: Undertaken only when necessary to address urgent security or stability issues; the buyer is notified at the earliest opportunity.
- Rollback Procedures: All planned changes have tested rollback options to restore service if unforeseen issues occur.

Preparation for Ad-Hoc Service Needs

- Rapid Provisioning: Processes in place to allocate additional resources or onboard supplementary support capacity on short notice.
- Incident Response: Escalation matrix to ensure the right technical expertise is engaged immediately for unplanned service issues.
- Disaster Recovery (DR): Where in scope, DR plans tested with agreed RTO and RPO.

Financial Recompense Model for not Meeting Service Levels

Where service levels are contractually agreed in the G-Cloud Call-Off Contract or Statement of Work, Base3 Solutions can provide financial recompense in the form of service credits if the agreed targets are not met.

Service credits are calculated as a percentage of the monthly service charges for the affected service component.

The percentage credit applied will depend on the degree to which the measured service level falls short of the agreed target, as defined in the Call-Off Contract.

Service credits, if applicable, are applied to the next billing cycle or offset against future invoices.

Service credits are the sole and exclusive remedy for failure to meet service level commitments, unless otherwise agreed in writing in the Call-Off Contract.

Any service credits will be capped at a maximum agreed percentage (e.g. 10% of the monthly charge for the affected service component).

The precise SLA targets, thresholds, calculation method, and maximum credit cap will be confirmed and agreed with the buyer prior to contract award, and documented in the Order Form / Statement of Work.

4. Provision of the service

Customer Responsibilities

To enable Base3 Solutions to deliver the service effectively and within agreed timeframes, the customer will be required to fulfil the following responsibilities, unless otherwise agreed in the Call-Off Contract:

Access and Information

- Provide timely access to relevant systems, networks, and facilities as required for delivery.
- Ensure Base3 Solutions' personnel are granted appropriate user accounts, credentials, and permissions (including privileged access if needed) to perform agreed tasks.
- Supply accurate and complete information on existing systems, configurations, dependencies, and relevant policies.

Personnel and Decision-Making

- Make key stakeholders and subject matter experts available for workshops, interviews, and approvals as per the agreed schedule.
- Nominate a single point of contact to coordinate with the Base3 Solutions Delivery Manager on day-to-day matters.
- Provide prompt decisions and sign-offs to avoid delivery delays.

Environment and Infrastructure

- Ensure that customer-provided infrastructure, environments, and connectivity are operational and meet agreed technical requirements.

- Maintain relevant licences for any third-party software or services not provided under this contract but required for service delivery.

Security and Compliance

- Follow any agreed security, authentication, and change control procedures.
- Ensure compliance with applicable laws and regulations in relation to the use of the service, including data protection obligations.

General Co-operation

- Notify Base3 Solutions promptly of any events, changes, or issues that may impact service delivery.
- Take reasonable steps to resolve any customer-side issues that may prevent or delay Base3 Solutions from meeting agreed deliverables or service levels.

Technical Requirements and Client-Side Requirements

Certain technical and organisational prerequisites must be in place for this service to operate effectively. These will be discussed, confirmed, and documented in the Order Form or Statement of Work prior to contract award.

System and Infrastructure Requirements

- Suitable internet connectivity with sufficient bandwidth and latency to support the agreed service performance.
- Supported web browsers, operating systems, or client software for access to cloud platforms/services (specific versions to be agreed).
- Compatible networking and security configurations (e.g. firewall rules, VPN access, IP allow-listing) to enable secure connectivity to cloud environments.
- Existing infrastructure and devices must meet the minimum specifications documented in the agreed Statement of Work.

Licensing and Third-Party Services

- Any required third-party software or service licences not provided under this contract (e.g. existing productivity suite, database engine, security software) must be valid and in place before delivery starts.
- The customer may need to procure licences for cloud services or APIs selected as part of the agreed solution, unless otherwise stated in the Call-Off Contract.

Access and Security Requirements

- Provision of user accounts and appropriate access permissions for Base3 Solutions staff to relevant systems and environments.
- Compliance with any agreed authentication, encryption, and security controls (e.g. MFA, VPN usage).
- Where applicable, permissions for Base3 Solutions to create, modify, or decommission cloud resources in the buyer's subscription or tenancy.

Organisational and Resource Requirements

- Allocation of buyer personnel with the necessary expertise, authority, and availability to participate in workshops, approvals, and testing.

- Timely provision of required documentation, architectural diagrams, policies, and configuration data relevant to the service.
- Agreement of maintenance windows or access periods where service changes can be implemented without impacting critical operations.

Outcomes/Deliverables

This service will deliver:

- Current state assessment - Identification and documentation of the customer's existing systems, applications, integrations, dependencies, and readiness for cloud adoption.
- Cloud architecture design - A documented and agreed target state architecture meeting the buyer's technical, operational, and compliance requirements.
- Migration plan - A detailed, step-by-step plan for migrating workloads, applications, or services to the target cloud environment.
- Implementation or configuration of agreed cloud services - Delivered to scope, tested, and signed-off by the buyer.
- Security and compliance controls - Configured in line with relevant policies, NCSC Cloud Security Principles, and agreed accreditation standards.
- Knowledge transfer / training sessions - To ensure the buyer's internal teams can manage, operate, and support the solution post-delivery.
- Documentation pack - Including system configuration details, architectural diagrams, operational instructions, and user or admin guides.
- Service performance reporting - Where applicable, reporting on system performance, availability, and cost metrics.
- Handover or exit plan - At the end of delivery or contract term, enabling smooth transition to buyer management or an alternate supplier.

After-sales Account Management

Base3 Solutions provides ongoing account management to maintain strong working relationships and ensure continued alignment between the service delivered and the customer's evolving requirements.

Relationship Management

- A named Delivery Manager is assigned to each customer as the main point of contact throughout the contract term.
- This role is responsible for managing day-to-day communications, coordinating activities, and acting as the escalation point for any contractual or service-related matters.

Structured Communication

- Regular review meetings (frequency agreed in the Call-Off Contract) to monitor performance, discuss upcoming requirements, and address any service improvements.

- Ongoing updates on relevant platform changes, industry developments, or potential optimisation opportunities.
- Formal reporting on agreed KPIs, SLAs, and service outcomes.

Customer Satisfaction

- Feedback gathered through review meetings and/or formal surveys to identify and implement improvements.
- Feedback is requested on all submitted tickets.
- Proactive engagement to resolve issues before they impact service quality or delivery timelines.
- All feedback is reviewed by the management team and translated to actionable improvements, with outcomes tracked and discussed at subsequent client reviews to ensure continuous customer satisfaction.

Partnership Development

- Support in identifying opportunities to optimise existing cloud investments and introduce efficiencies.
- Input into long-term digital or cloud strategy discussions, where invited, to ensure future requirements are considered in service plans.

Continuity of Service

- Retention of delivery and configuration knowledge within the assigned team wherever possible to provide consistent support over time.
- Documenting all service history, key decisions, and configurations in a shared service knowledge base.
- Conduct structured knowledge transfer to client teams or new delivery staff to maintain seamless continuity of service.

Termination Process

General Approach

The termination process is governed by the termination clauses in the G-Cloud Call-Off Contract and the specific terms agreed in the Order Form / Statement of Work. Both parties will act reasonably and in good faith to ensure a smooth and secure termination of the service.

Customer-Initiated Termination

- The customer may terminate the service by providing the contractual notice period defined in the Order Form or Statement of Work.
- Early termination within a Minimum Period or Renewal Term may incur charges, including (but not limited to) recovery of costs for committed resources, third-party licences, and any agreed fixed-price deliverables commenced but not yet invoiced.
- The customer acknowledges that it has purchased the Services for the Minimum Period and any Renewal Term(s), as defined in the Certificate or Order Summary.

Supplier-Initiated Termination

- Base3 Solutions may terminate the service in accordance with the Call-Off Contract provisions, for example where there is material breach, non-payment, or cessation of required cooperation or access.
- Where practical, Base3 Solutions will provide the agreed notice and will work with the customer to minimise disruption.

Early Termination Costs

Any early termination costs will be agreed and documented in the Order Form prior to contract award. These may include non-refundable third-party charges or work already performed but not yet billed.

Obligations on Termination

Base3 Solutions will:

- Provide the customer with all relevant data in a mutually agreed portable format (e.g. CSV, JSON, XML) within the agreed timeframes.
- Securely delete customer data from our systems in accordance with GDPR and contractual requirements.
- Provide reasonable co-operation and handover to the customer or their nominated successor, subject to any agreed exit assistance charges.

The Customer will:

- Pay all outstanding invoices up to the termination date, including any applicable early termination costs.
- Provide access and cooperation necessary for Base3 Solutions to carry out secure data extraction and service shutdown procedures.

Process Summary

- Written notice received from the terminating party in accordance with contractual notice periods.
- Exit planning meeting to agree a termination plan, including data extraction, access removal and final deliverables.
- Execution of the agreed termination plan with progress updates.
- Completion of termination activities, confirmation of data return/destruction, and closure of any remaining service tickets.

5. Our experience

Case Studies

Deployment of a Private Large Language Model (LLM) for Financial Process queries in a Public Sector Agency

Customer Context

A large public sector agency responsible for managing complex finance processes wanted to explore AI technology while complying with strict data governance and audit controls.

Problem

Finance teams processed large volumes of incoming documentation (contracts, invoices, grant applications) with complex requirements and processes. A large turnover of staff made training difficult to keep up with. The organisation was reliant on several finance experts on the team, who instead of delivering outcomes, were spending their time responding to queries.

There was a need to be able to provide a service that could answer complex queries, with up to date policy and process documentation.

Action

- Assisted the customer in selecting and deploying a private LLM built on open-source models to ensure full control over data and meet governance regulations.
- Integrated the model with their existing finance management documentation.
- Developed a front-end interface for staff to use to submit their queries which utilises single sign on to control access to sensitive information.
- Provided prompt-engineering training via an eLearning platform to improve the efficiency of the system.

Outcome

- Reduced admin load from finance experts while maintaining compliance with all data governance requirements.
- Eliminated the need for sending sensitive data to external AI providers, ensuring compliance and audit readiness at every stage.
- Freed finance team capacity for higher-value analysis and decision-making, supported by secure, traceable query responses.
- Created a flexible and easily updatable repository of information with full audit trails and change management controls.

Public Sector Relevance

This model can be applied to other agencies and local authorities with GDPR-sensitive financial or case management workflows that could benefit from AI-driven automation without reliance on public AI models.

Rapid Enablement of Cloud Services Post-COVID-19 for a Large Government Department

Customer Context

A large central government department needed to urgently enable secure, remote access for several hundred staff members in the wake of the COVID-19 pandemic. Previously reliant on on-premises systems, it faced limited remote access capabilities and the risk of business disruption.

Problem

- Due to security requirements remote working and tools were not widely available.
- Multiple departmental teams had no secure method to share documents and coordinate projects from home.
- There were strict requirements for data security and compliance with the NCSC Cloud Security Principles.

Action

- Conducted a rapid discovery and readiness assessment to identify critical services and data for migration.
- Designed and deployed a secure Amazon Web Services subscription to provide a number of key business applications, including Oracle Apex/ORDS, LimeSurvey, Moodle as well as custom built software
- Delivered virtual training workshops and user guides to accelerate adoption of cloud technologies.

Outcome

- Full departmental remote working capability enabled within several months. Work had begun on this work prior to the pandemic and so the capability was deployed ahead of schedule.
- Improved cross-team collaboration by introducing secure cloud workspaces, role-based access controls, and encrypted communication channels, enabling teams to share information faster without compromising government security requirements.
- Enabled remote learning, providing cost savings by reducing the need for expensive training courses.
- The solution has since been adopted permanently, reducing dependency on on-premise infrastructure and improving disaster resilience.

Public Sector Relevance

This approach can be replicated across other government bodies or NHS trusts requiring rapid, secure environments that meet UK government security standards.

6. Clients

AtkinsRéalis



UK Government

T3 TwentyThreeHundred



7. Contact Details

Keith Wilkinson

sales@base3.co.uk