



G-Cloud 15

Service Definition

Database and Server Managed Services

Lot 3 Cloud Support Services (Additional Services)

1. Introduction	4
Company overview	4
Value proposition	5
What our service provides	6
Social Value	8
Overview of the G-Cloud Service	8
Associated services	10
2. Data Protection	11
Information assurance	11
Data Backup	12
Business continuity plan	13
Privacy by design	15
3. Using the service	17
Ordering Process	17
Invoicing	18
Trial Services	18
Onboarding process	19
Off-boarding process	20
Service migration	21
Training facilities	21
Implementation Plan	22
Cloud support service management	22
Certifications and Standards	23
Managing Constraints and Incidents	24
Managing continuous improvement	25
Service constraints	25
Service levels	26
Outage and maintenance management	27
Financial Recompense Model for not Meeting Service Levels	28
4. Provision of the service	28
Customer Responsibilities	28
Technical and client requirements	29
Outcomes and deliverables	30
After-sales	31
Termination Process	33
5. Our experience	34

Case Studies	34
Clients	38
Technologies	40
Contact Details	40

1. Introduction

Company overview

As an established UK service provider of database and cloud support, our organisational expertise and capability to successfully deliver works for each call-off contract for Public Sector Buyers, as evidenced by our 26 years' industry experience providing end-to-end cloud support services for private and public sector organisations such as:

- Gosport Borough Council
- Rushmoor Borough Council
- Home Plus Housing Association
- York and Scarborough NHS Trust
 - Devon and Somerset Fire and Rescue
 - The Brooke Animal Hospital
 - Historic England
 - St Austell Brewery

 150 contracts held nationally	 94% Customer satisfaction rating
 20 directly employed engineers	 12-minute average incident response time

As a trusted supplier on the G-Cloud framework since G-Cloud 10 we continue to support public sector organisations through G-Cloud 15. Additionally, our team has grown alongside the development of cloud technologies, building strong partnerships as a Microsoft Gold Partner and a long-standing Oracle Partner. This enables us to deliver expert support across leading platforms while continually adopting new technologies and innovations to meet evolving client needs.

We provide services that include migration to cloud platforms, ongoing managed support, and proactive system administration with our focus on helping organisations achieve stable, secure and efficient IT environments while adapting to the opportunities of cloud computing.



Value proposition

Based on our 26 years' experience providing database and cloud support services, we acknowledge that public sector organisations face increasing pressure to modernise digital services, manage data securely, and reduce costs while maintaining resilience. Additionally, many departments still operate legacy IT systems that are expensive to maintain, prone to downtime, and create challenges in migrating to modern cloud environments. These issues hinder service delivery, pose cybersecurity risks, and limit the agility needed to meet their customers' evolving needs.

Our Cloud Managed Service directly addresses these challenges by providing end-to-end support for cloud adoption and ongoing operations including migrating fully to the cloud or implementing a hybrid solution through ensuring a smooth transition, proactive management, and continuous optimisation.

Key problems our services solve include, but are not limited to:

 Complexity of migration	Many public sector organisations still rely on legacy, on-premise systems that are business-critical but difficult to migrate, such as large relational databases, bespoke applications, or estates spread across multiple platforms. Our in-house team of 20 directly employed engineers will provide structured migration, consolidation and transformation services, enabling public sector bodies to move critical workloads such as databases, applications and messaging systems to secure, scalable cloud platforms with minimal disruption.
 Operational risk and downtime	Acknowledging government services are increasingly expected to be available on a 24/7 basis, whether for citizen-facing applications or internal systems such as HR, finance, and communications, even short outages disrupting service delivery generate negative public perception and create compliance risks. Our team will reduce this risk by delivering 24/7/365 monitoring, proactive daily checks, automated alerting, and guaranteed incident response times under the SLA, such as an incident response (live/DR systems) time within one hour. This will provide assurance that services remain available whenever citizens and staff need them.
 Security	Public sector organisations handle sensitive and personal data that must be protected in line with GDPR and government security standards, with legacy systems and inconsistent patching regimes often creating vulnerabilities. Our service embeds strong security practices through certified processes

Cybersecurity concerns	(ISO 27001, Cyber Essentials Plus, vendor-certified engineers) and strict role-based access controls. Regular patching, upgrades and vulnerability management will reduce exposure to threats, while audit trails and documentation support compliance reporting and assurance.
 Client in-house skills shortages	Many public sector organisations lack specialist database and cloud expertise. Our service provides access to a pool of 20 vendor-certified engineers, with a lead database administrator (DBA) assigned to act as a single point of contact who will develop a thorough understanding of the client's systems and requirements. The lead DBA will be supported by a secondary DBA for continuity reasons (e.g. in the event of absence) and a service delivery manager assigned to every client. This will ensure continuity of expertise, remove single points of failure, and provide the ability to scale up the resource assigned through our wider team for more extensive projects.
 Transparency and value for money	Budget pressures mean public sector organisations must demonstrate efficiency and transparency in all IT spend. Complex pricing models and unexpected costs often undermine confidence in external support arrangements. To provide cost certainty and transparency, we provide fixed-price contracts that include unlimited incident support, and detailed monthly reporting. This will allow clients to forecast costs accurately, benchmark service performance, and demonstrate accountability to internal stakeholders and auditors.

What our service provides

Our Cloud Managed Service supports public sector organisations in adopting, operating and optimising cloud-based systems including, but not limited to:

- **Types of projects** supported:
 - ✓ **Minor upgrades** and security patching.
 - ✓ **Major version upgrades** for database and application platforms.
 - ✓ **Database and system migrations** (on-premise to cloud, between cloud platforms, or consolidation of estates).
 - ✓ **Transformation projects** (optimising, re-platforming, or restructuring databases and applications).
 - ✓ **Deep-dive health checks** and performance reviews.

- **Technologies supported:**
 - ✓ **Major cloud platforms** such as Oracle Cloud, Microsoft Azure, Amazon Web Services (AWS).
 - ✓ **Operating systems** including Linux, Windows Server, and associated environments.
 - ✓ **Database platforms such as** Oracle, Microsoft SQL Server, open-source databases, such as PostgreSQL, MySQL, MariaDB, MongoDB and other vendor-certified technologies.
 - ✓ **Monitoring and reporting tools** deployed via secure client-specific jump boxes.
- **Cloud migration and transformation:** Planning and delivery of full or partial migrations to Oracle Cloud, Microsoft Azure, AWS, or hybrid environments, including consolidation of existing estates.
- **Ongoing system management:** Proactive daily checks, patching, performance monitoring, and space/capacity management to keep systems stable and 'business ready' every day.
- **24/7/365 monitoring and support:** Continuous monitoring with defined SLA response and resolution times, supported by an on-call roster of engineers.
- **Database expertise:** Full life cycle management of databases including schema management, user/role control, backup and recovery, upgrades and troubleshooting.
- **Disaster recovery support:** Assistance in creating, testing and executing DR plans to ensure critical systems can be restored quickly in the event of an outage.
- **Security assurance:** Access management, patching and compliance with ISO 27001 and Cyber Essentials Plus to protect sensitive data and maintain integrity of services.
- **Client engagement and reporting:** Comprehensive documentation (login guides, operational guides, issues/observations logs) plus monthly availability, performance and capacity reports for full transparency.
- **Dedicated service team:** Each client will be allocated a lead database administrator (DBA) as their single point of contact who will develop a thorough understanding of the client's systems and requirements, a secondary DBA for continuity (e.g. to cover the primary DBA for any absences such as holidays), and a service delivery manager, ensuring continuity of knowledge and a single point of accountability.

The above services will ensure reliable and secure cloud-based systems, reduced downtime, tested and verified backup/recovery processes, and transparent service delivery that aligns with public sector compliance requirements.

Social Value

During the mobilisation phase of each call-off contract awarded under this framework, our Social Value Champion Head of HR, Marion Shanly will agree a social value delivery plan with the customer, tailoring our initiatives to their specific objectives, and the requirements of the local community. The specifics of the proposed offerings will be refined and agreed with the customer during mobilisation

Overview of the G-Cloud Service

As a supplier on the G-Cloud framework since G-Cloud 10, we have extensive experience providing support to public sector organisations in setting up, migrating to and maintaining cloud-based services to ensure that systems remain secure, resilient and aligned with operational requirements, as outlined below:



Key Service capabilities

- **Cloud migration and setup:** Planning and delivery of migrations to public, private or hybrid environments, including Oracle Cloud, Microsoft Azure, AWS and mixed estates. Activities will cover system audits, data consolidation and transformation projects.
- **Database and system management:** Life cycle support for databases and associated infrastructure, including the assigned DBA undertaking daily morning checks, patching, upgrades, schema management, capacity planning and performance monitoring.
- **24/7/365 monitoring and incident response:** Continuous monitoring of supported environments, with defined SLA targets for response and resolution times, such as an incident response (live/DR systems) time of one hour. Issues will be logged and managed through our dedicated service desk and escalated as required.
- **Security management:** Application of vendor security patches, user and role management, and compliance with recognised standards including ISO 27001, ISO 20000, ISO 9001, Cyber Essentials Plus.
- **Disaster recovery and continuity:** Development and support of client-specific disaster recovery plans, including backup and restoration, tested regularly through clone builds and recovery exercises to ensure feasible restoration.
- **Documentation and reporting:** Provision of operational and procedural guides, login details, and issues/observations reports. Clients will receive daily system readiness checks, monthly reporting (availability, capacity, performance and activity), and quarterly service delivery reviews.
- **Dedicated service team:** Each client will be allocated a lead DBA as their single point of contact who will develop a

	thorough understanding of the client's systems and requirements, a secondary DBA for continuity (e.g. to cover the primary DBA for any absences such as holidays), and a service delivery manager, ensuring continuity of knowledge and a single point of accountability.
 Typical activities	➤ Daily system checks confirming system availability and highlighting potential risks. ➤ Continuous monitoring of events such as outages, performance degradation or capacity thresholds. ➤ Routine patching and bug fixing to maintain supported versions. ➤ Regular database housekeeping, including updating statistics, rebuilding indexes and managing space. ➤ Backup scheduling and validation using test restores to confirm reliability. ➤ Migration and upgrade projects, carried out with test environments built from backups to minimise disruption to live systems. ➤ Quarterly service delivery meetings (or to a preferred client frequency) to review performance, risks and planned improvements.
 Cloud Characteristics	➤ On-demand support: Services are available as required by clients, with unlimited incident support included in the contract. ➤ Resource pooling: Clients benefit from access to a team of 20 certified engineers, with continuity maintained through assigned primary and secondary DBAs. ➤ Scalability: Support scales from single systems to large estates, with additional services such as operating system support, health checks, and consultancy available. ➤ Broad network access: Remote management will be provided via secure, client-specific connection machines, ensuring secure separation between clients. ➤ Measured service: Monitoring and reporting will provide transparency of usage, system performance and availability.
	➤ Cost control through proactive capacity management. For example, engineers will monitor storage usage and trends to prevent systems exceeding their allocated storage allowance, helping clients avoid unexpected charges from cloud providers. ➤ Reliable and resilient systems through proactive monitoring, cluster failover and DR planning.

Benefits delivered

- **Reduced downtime** via 24/7/365 incident management and SLA-backed response/resolution times.
- **Compliance with public sector data security and GDPR** requirements through certified processes and secure connectivity.
- **Transparent service performance** with daily readiness updates and structured reporting.
- **Continuity of expertise** and assurance of cover through dedicated engineers and defined escalation routes.

Associated services

The Cloud Managed Service includes a core set of managed support activities, with optional additional services that can be added depending on client requirements.

Included within the fixed-price contract to provide cost certainty and transparency to clients which also provides unlimited incident support:

- **Core database and system management:** Daily checks, monitoring, performance management, patching, bug fixing, schema management and capacity planning.
- **Incident management:** 24/7/365 monitoring and incident response with defined SLA targets for live, DR, test and development environments.
- **Backup and recovery:** Support for scheduling, testing and validating client-defined backup and recovery processes.
- **Disaster recovery support:** Assistance with creation and execution of DR plans, including clone testing from backups.
- **Client documentation:** Login guides, operational/procedural guides and issues/observations logs maintained and updated throughout the contract.
- **Reporting:** Daily status updates, monthly performance/capacity/availability reports and quarterly service delivery meetings.
- **Dedicated service team:** Allocation of a primary and secondary DBA plus a Service Delivery Manager for continuity and escalation.
- **Unlimited incident and service request support:** within the agreed scope of the contract.

Option / bolt on services

- **Enhanced detailed reporting analysis** of availability, performance, capacity and security to be made available to clients as a self-service option in 2026.
- **Database migrations, consolidation and transformation projects** including movement to cloud environments or re-platforming onto fewer servers.
- **Deep-dive health checks** with formal reviews of database or system instances, delivered with written reports.

- **Optional server / operating systems** under the supported database for patching, bug fixes and maintenance of operating systems in addition to database management.

Not included

- **APIs**, the service does not provide custom API development
- **Storage** is not provided for this service
- **Hardware provision** except where supporting the overall cloud solution, physical hardware supply is out of scope under G-Cloud.
- **Bespoke software development** beyond database-related scripting or development support.

2. Data Protection

Information assurance

Our ability to complete cloud management services and maintain a comprehensive approach to information assurance to ensure client data is managed safely, securely and in compliance with legislative and best practice requirements is evidenced by our accreditations, memberships, secure operational processes and facilities, summarised below:

Accreditations and Certifications

- **ISO 27001:2022 Information Security Management:** Providing a structured framework for protecting the confidentiality, integrity and availability of client data, reducing the risk of breaches.
- **ISO 20000-1:2018 Service Management:** Demonstrating our adherence to IT service management best practice, ensuring consistent, high-quality delivery of cloud support services.
- **ISO 9001:2015 Quality Management:** Guaranteeing continual improvement and a quality-focused approach across all processes, ensuring services evolve to meet client needs.
- **Cyber Essentials Plus** validating our protection against cyber threats and providing assurances that systems are resilient against external attack.
- **Oracle Partner / Microsoft Gold Partner**, providing assurances that our engineers are trained and certified to work to vendor best practices, maximising the security and stability of supported platforms.
- **Database Vendor Certified engineers to confirm** that technical staff have deep platform-specific knowledge to implement secure configurations and respond effectively to incidents.

Processes and facilities

- **Staff security clearance:** All staff undergo security clearance at induction and are rechecked every three years via Agenda screening to minimise the risk of insider threat and ensure staff remain compliant with evolving standards in compliance with BS: 7858:2019 standards.
- **Secure remote access:** Remote connectivity is established using VPNs or token-based methods, agreed with the client, ensuring only authorised access is permitted.
- **Access control and monitoring:** Database roles, users and permissions ensures users can only access data relevant to their responsibilities.
- **Patch and vulnerability management:** Regular updates, bug fixes, and security patches are applied in line with vendor guidelines to maintain secure environments.
- **Comprehensive documentation:** Operational and procedural guides, login details, and issues/observations reports are maintained and updated by the Lead DBA as changes are made to the systems., providing clients with full visibility and auditability.

Data Backup

As part of the onboarding process, the assigned lead database administrator (DBA) will outline our flexible and robust approach to data backup and restoration, tailoring our approach to meet the specific operational and compliance needs of the client. Our approach to ensure protection against client data loss is summarised below:

Backup plans and processes

- **The DBA will agree the backup frequency** with each client as part of service onboarding to meet their operational needs. For example, clients may require backups two to three times per day using online or hot backup methods, while other clients may set less frequent schedules depending on system criticality.
- **Clients will be able to define the type** (e.g. full, incremental and log backups), frequency and retention of backups. These requirements will be documented in the Order Form Operations Manual and reviewed during account reviews by the DBA with the client to guarantee they remain aligned with evolving business needs.
 - ✓ **The DBA will recommend backups are stored out of contact with the live system** (off-site or in segregated environments) to ensure that, in the event of a malware or ransomware attack on the live system, the backup data cannot be simultaneously compromised.
- **All clients will be required to maintain a disaster recovery plan**, with the DBA able to provide support in developing, testing and refining these plans to ensure resilience.

Testing and Validation

- **Backups will be taken and actively tested** by building clones and test systems from backup files to ensure that the backup data is complete, reliable, and can be used for recovery if needed.
- **Before migrations or upgrades, the DBA will create test environments** from backups rather than from live systems to reduce the load and risk on production environments to protect live operations while verifying that the backup process itself is functioning correctly.
- **For clients not undergoing migrations or upgrades**, backup testing will be scheduled every two months, with frequency increased when changes (e.g. minor upgrades) are planned.

Business continuity plan

In accordance with our formally documented business continuity plan (BCP) and disaster recovery processes (DRP), measures to ensure continuity of our services for our clients are outlined below:

Backup plans and processes

- **The BCP / DRP covers all managed database and cloud support services** delivered under contract, including:
 - ✓ **Connectivity between WellData and client** environments.
 - ✓ **Database and application monitoring**, management and recovery.
 - ✓ **Daily checks**, reporting and incident handling.
 - ✓ **Disaster recovery support** for client systems.
- **The scope extends across our infrastructure**, including connection machines (CMs), primary and secondary data centres, and all client-facing monitoring and support functions.

Key business areas

- **Database and system monitoring**, including real-time and daily checks via dedicated jump boxes and monitoring tools.
- **Incident response and escalation**, managed 24/7 by engineers with escalation as required to:
 - ✓ **The primary DBA** (with an assigned deputy DBA to cover in the event of absence to ensure working knowledge of the client's systems).
 - ✓ **Team leaders** with the ability to assign multiple engineers to expedite issue resolution.
 - ✓ **General managers** where further expertise is required.

- ✓ **Managing Director Phill Clayton** as the ultimate point of escalation, with the authority to expedite resolutions without the need to escalate further.
- **Backup and disaster recovery management** including regular backups (defined by client system usage requirements, to be agreed during onboarding), clone testing and DR support.
- **Connectivity and remote access** managed via isolated CMs hosted in clustered environments.
- **Continuous reporting** on system availability, performance and capacity to proactively prevent developing issues.

Critical functions

- **Each client has a dedicated jump box with real-time up/down monitoring** and daily system checks to facilitate central reporting and trend analysis to proactively identify and rectify any issues.
- **Regular backups are tailored per client**, with clone and test systems built from backup files to confirm data integrity to ensure backups are genuinely useable for recovery.
- **Failover capability** includes:
 - ✓ **Connection machines are virtualised and isolated per client**, running on clustered servers. Failure of one or more hosts does not impact overall service.
 - ✓ **Normal equipment failures** are handled by cluster-level failover.
 - ✓ **In the event of a site failure** at our primary data centre in Byfleet, services will failover to our secondary Gatwick data centre within two hours.
- **Clients will have the visibility of their systems in real time** and will be able to extract monitoring reports as part of our upcoming self-service function in Q1 2026.

Dependencies

- **Each client specifies their own broadband/connection method**, typically via VPN from our data centre.
- **Data centre infrastructure**, with our primary site in Byfleet and secondary site in Gatwick for disaster recovery purposes.
- **The triplicated underlying servers**, allowing for redundancy. The critical dependency is the data centre facility, not the individual servers which are replicated.

Acceptable downtime

- **The assigned lead DBA will agree the acceptable downtime and data loss with clients for each system** as part of onboarding process and documented in the Operations Manual. For example, types of cover include:
 - ✓ **Seconds or near-zero tolerance** for mission-critical systems.
 - ✓ **Business hours coverage** for less critical workloads.
 - ✓ **Business hours + out-of-hours cover** for intermediate systems.
 - ✓ **24/7 coverage** for clients operating around the clock.
- **Response times** include:
 - ✓ **Live/DR systems:** Target response time of 1 hour; resolution or resolution plan within 4 hours
 - ✓ **Test/dev/UAT systems:** Target response time of 2 working hours; resolution or resolution plan within 8 hours

Plan to maintain operations

- **ManageEngine software will automatically monitor ours and client systems**, issuing alerts to ensure early detection of issues before they impact service.
- **On-call 24/7 engineers** will provide immediate response to incidents.
- **Client backup and recovery processes** will be regularly tested (every two months as a minimum, or more frequently if required such as when upgrading the system) by building clones and validating recovery from stored backups.
- **Disaster recovery planning** is carried out with each client during the onboarding process to align with business requirements and ensure systems can be restored in line with defined RPOs (Recovery Point Objectives) and RTOs (Recovery Time Objectives).
- **Assigned lead DBS will host quarterly service delivery meetings** via Teams to review continuity arrangements and update recovery processes as necessary in line with the client's evolving business requirements.

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

Privacy by design

*Our systems are Cyber **Essentials Plus**, 27001:2022 Information Security Management and ISO 20000-1:2018 Service Management certified, guaranteeing the protection of data in compliance with GDPR.*



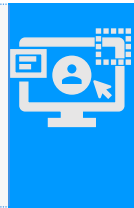
In accordance with our data protection policy, all data received, stored and processed to support delivery of our services will be managed in compliance with the UK-GDPR 2018 and the DPA 2018 with the following safeguards:

- **Data is only processed for the agreed purpose of providing cloud support** and management services.
- **Only the minimum data required** to deliver the service is collected and processed and access to client systems is configured to restrict visibility to operational data, avoiding unnecessary exposure of personal information.
- **All data is processed within our London-based data centres** and never transferred outside the UK.
- **Data is not collected or used for any purpose not related to the delivery of our service**, e.g. for third-party marketing activities.
- **Role-based access controls** ensure staff can only access data relevant to their work, with access removed when no longer needed.
 - ✓ **Role-based access control can also be configured at the client's request to their employees** and other external companies working on their systems, such as developers.
- **All data held is fully encrypted and secured behind firewalls**, with real-time threat detection and geofencing to monitor and control incoming and outgoing network traffic based on predetermined security walls, for example:
 - ✓ **Firewalls are configured to restrict inbound and outbound traffic** to only authorised services and protocols.
 - ✓ **Segmentation isolates internal systems** (e.g. operational, financial and client data) to reduce lateral movement in the event of a data breach.
- **Devices are password-protected**, with passwords meeting complexity requirements by including at least eight characters of different types and multi-factor authentication, ensuring sufficient mechanisms are in place to prevent access to data.
- **Emails received are subject to content filters and threat protection scans** to eliminate phishing.
- **All client environments are accessed via isolated connection machines and VPNs**, ensuring separation between clients and preventing unauthorised cross-access.
- **All staff undertake annual Data Protection and Cyber Security training** via the Information Security ISO 27001 Staff Aware e-learning course from IT Governance, covering:
 - ✓ Only viewing data related to their role
 - ✓ Ensuring data is not shared informally
 - ✓ Reporting any suspected data security breaches.
- **As a data processor, we maintain comprehensive records of personal data processing**, with records timestamped and capturing details of the user

who completed each processing task, ensuring our records are fully auditable to evidence compliance with GDPR obligations.

- **In line with our privacy policy notice, data subjects are provided with comprehensive notices** via email about the processing of their personal data, with clear instructions on how they can request access to rectification, deletion or portability of data.
- **Data is only stored for active contracts** and will be deleted following the culmination of services in accordance with the timescales required by the client for the purpose of aftercare services.

We have experienced no major cyber security breaches. 100% of low-level phishing and malware attempts have been contained and eradicated, with lessons learned including refining filters and issuing company-wide awareness sessions used to prevent recurrence.



3. Using the service

Ordering Process

Business as usual (BAU) operations will be conducted according to the following procedure:

- Prospective clients will be able to access our contact details via the Public Procurement Gateway as part of the G-Cloud 15 framework and will then submit an Order Form. **Requirements within CSS order forms** to provide a comprehensive quotation will include:
 - ✓ The scope of the estate to be maintained
 - ✓ Technologies to be serviced (SQL, Oracle) including any legacy versions
 - ✓ Extent of coverage required during managed service
- Once contact has been established between a client and our administrative team they will appoint a designated technical account manager within 2 hours to oversee the client-service relationship, and support, where necessary, the amending of the signed Order Form prior to finalisation of call-off contract terms. WellData can also support clients with completing/collaborating the call-off contract at no additional cost.
- **Support** for BAU works will be available to clients in the form of telephone and email, and technical guidance provided remotely through a team of support engineers scheduled on a rota basis. The support we provide will be continuous, and all responses will be immediate.

- ✓ Consultancy with a dedicated primary Database Administrator (DBA) will be provided to establish the scope and extent of support for larger-scale project works such as on-premises to cloud service migration.
- Once agreed, clients will receive an itemised bill of services according to our fixed priced methodology. We also possess the functionality to bill according to days and materials if required.

Invoicing

Invoices will be issued monthly in arrears and will outline agreed services to be provided including the above requirements and the following details:

- Our organisational details (address, legal name, VAT registration number)
- Unique invoice number and date
- Buyer details (billing address and finance contact), as well as Digital Marketplace ID.
- Sub-totals, VAT rate and amount
- Bank details and payment instructions.

Payment terms are 30 days net of receipt of invoice. We will provide monthly breakdowns of invoices processed as part of management information submitted to Crown Commercial Services via RMI system.

Trial Services

We will offer trials of our managed service whereby one or two client databases can be managed prior to formal agreement to terms of a G-Cloud call-off contract for up to three months. Historically this has included:

- **Provision of a designated Database Administrator** to provide a single point of contact representative of our customer service methodology
- **Assessment of existing infrastructure** to identify new patches or updates available
- **Health checks of existing systems**, to be provided with the guarantee that if clients confirm call-off contract terms a detailed report of these checks will be provided
- **Rectification works** if inefficiencies or faults are identified as business critical.

During trials, clients will be onboarded according to standard procedures whereby logins, applications and permissions are established, allowing for prompt and efficient transition to managed services if clients choose to accept terms.

100% of clients we have offered trials to in the past 6 years have confirmed they wish to transition to fully managed services.

Onboarding process

Kick-off meeting

Within 2 days of a signed Order Form being returned to a client with agreed terms, assigned staff to a client's managed service, including the primary database administrator (DBA) and accounts manager, will conduct a virtual (unless otherwise specified) kick-off meeting to establish and confirm:

- **The frequency of contact**, including service reviews and reporting submissions and the client's preferred communications channel.
- **The scope of managed services**, including technology types, estate size, and tasks to be conducted with responsibilities across both parties outlined.
- **Service level agreements** outlined in the Order Form, alongside clear and defined deliverables and timescales
- **Clear timescales and milestones** for full onboarding to be completed, including acquisition of permissions, authorisations and logins.

Dedicated point of contact

For the management of database and cloud services we will provide all clients as part of the G-Cloud 15 framework with a dedicated Primary DBA, supported by a dedicated Secondary DBA and up to 5 deputised DBAs, to ensure a continuity of service expertise and a dedicated expert familiar with client systems throughout the contract duration. The assigned DBA will manage agreed system maintenance and ensure timely and accurate reporting of health checks and work progress to clients through daily reviews of client systems. The limits of assistance our DBAs can provide will be agreed during kick-off; however, we possess the functionality to provide clients with 24/7/365 support immediately from commencement to ensure a smooth onboarding process.

Onboarding support

To ensure clients experience a seamless integration into our managed services we will conduct an assessment of existing systems and server architecture upon receipt of authorisation and permissions.

System specifications and compatibility will be reviewed against the outlined system estate detailed in the Order Form by the DBA, who will then highlight any discrepancies and escalate to the accounts manager to advise of any additional or amended scope required for successful onboarding.

Documentation provided

In addition to the signed order form detailing the terms and scope of the contract we will provide all clients (upon request) with evidence of the following certifications:

- **Cyber Essentials Plus**
- **ISO9001:2015**

➤ **ISO20001:2018**

➤ **ISO27001:2022**

A dedicated contact sheet will be provided detailing the availability and contact details for the primary DBA, accounts manager, and our 24/7 on-call helpdesk technicians should this be included in the terms of service. Further to this an agreed list of equipment and systems that are to be supported will be issued to clients for approval prior to service commencement, and from this document invoices will be based to maintain an up-to-date log of maintained systems.

Documentation provided as part of G-Cloud 15 contracts will be uploaded to our dedicated CRM system Zoho CRM by accounts managers and provided to clients upon request.

On-site training

Subject to agreement and requirement we will offer on-site assessment of existing systems; however, all details of maintained, patched and upgraded systems will be delivered to clients as part of a dedicated operations manual submitted upon completion of contract works.

Set-up help

DBAs will conduct daily checks of client systems from contract commencement to monitor existing managed systems and identify early warning signs that might further inform the scope of managed services if we are able to provide additional services to improve system efficiency and health. In doing this we will provide a proactive reporting methodology during client onboarding, relating the progress of system integration as often as dictated by client requirements.

Account management

Throughout and following integration of clients in the onboarding process we will provide regular service reviews at a frequency determined by client requirements, ranging from weekly to annually across our client base. The reports will include customised criteria for individual clients to be determined during kick-off but will as standard include a health check of systems as well as an integration progress against designated milestones such as the granting of system permissions.

Off-boarding process

Upon termination of contracted services, we will produce a notice of termination for our client at least 1 month in advance of managed services ceasing, and will meet with client representatives to outline timescales and milestones for removal of services. During this period, DBAs will continue to support clients in exporting of relevant data to their required destination.

Service migration

Where clients require system migration, for example transition from an on-premise deployment to a cloud-based system, we will undertake these works according to the same methodology as large-scale infrastructure projects including:

- **Production of a statement of work (SOW)**, outlining preparatory tasks to be completed to allow system migration to commence
- **Timescales and milestones** for completion
- **Technological and resource requirements** including Network Access and provision of a 'jumpbox' or 'jump server' allowing single point of entry for DBAs.

Continually referencing and working in accordance with our SOW we will operate either a 'Big Bang' approach, ceasing existing service to launch newly migrated cloud services, or a 'Parallel Running' methodology where existing systems are integrated over time, subject to client requirements.

Training facilities

Upon contract commencement we will provide a designated 'cross-training' process to all clients during phases of work, e.g. onboarding, managed service, successful delivery of project works such as patches and upgrades.

This process will involve regular and informal online meetings with the client and their primary database administrator (DBA) subject to the requirements of the works and the communication preferences of individual clients, outlining:

- **Completed and upcoming works** as well as the methodological approach to maintaining, patching and upgrading databases.
- **Early warning notices on managed systems** including proposals for rectification based on daily checks conducted by the DBA, with issues being classified according to a red-amber-green system based on severity.
- **Signposting clients to operational user information** for accessing and using managed systems.

Upon finalisation of contracted services, or upon go-live of newly patched and upgraded systems, the DBA will provide an operations manual outlining contact services during standard working hours (9–5) and out-of-hours points of contact, as well as 'observations' in which the specificity of a client's architecture, which may need to be preserved, is outlined as part of our methodological approach to ensure future maintenance does not affect this.

Online help and assistance

As part of our managed services we will provide clients with access to a 24/7/365 available service helpdesk provided by external partners JAM which will monitor incoming client queries. Once a client contacts JAM, the query will be entered into

our Fresh ticketing system where, on average, we maintain a response rate of approximately 12 minutes, demonstrating our prompt and attentive service levels.

Implementation Plan

A detailed implementation plan can be provided to the buyer on request but will include the following. The details of WellData Managed Service requirements for on-boarding are:

- Remote access
 - Creation of client connection VM in WellData's environment (WELLDATA)
 - Creation of management server in client's environment (CLIENT)
 - Identify remote connectivity method (e.g. site-to-site VPN, software VPN, Bastion, virtual desktop) (CLIENT)

N.B. There is no requirement for a permanent connection.

- Remote connection testing (WELLDATA / CLIENT)
- Accounts/permissions
 - Creation of accounts in the client's environment for WellData engineers (CLIENT)
 - Assignment of relevant permissions applied to the accounts (CLIENT)
 - Accounts and permissions testing (WELLDATA)
- Monitoring
 - Installation, configuration and testing of monitor tools (WELLDATA)
- System Review
 - Review of in-scope system to ensure acceptance into service (WELLDATA)

Cloud support service management

People

1. **Database administrators (DBAs)** will be directly assigned to call-off contracts to provide clients with a single point of contact that will monitor and provide support to their services for the full duration of the contract length, with deputised DBAs assigned to provide contingency support.
2. Our **three Technical Team Leaders** will review contract performance data and progress to ensure client KPIs are met or bettered on a weekly basis.
3. A **dedicated Account Manager** who will coordinate individual call-off contracts for the G-Cloud 15 Framework and provide commercial support to ensure clients are satisfied with services provided

4. **Managing Director Phil Clayton** will provide organisational oversight and client support for all cloud support and managed services, and serves as the final point of escalation for all clients using his 45 years' industry experience.

Processes

In addition to senior management supervision, DBAs will monitor their own work capacities through daily checks of client systems and delegate additional tasks and collaborate with deputised secondary DBAs to ensure capacity is available where needs change. This involves delegating tasks and work streams to DBAs who are less busy, ensuring nobody's workload exceeds their capacity. This collaborative approach builds trust and co-operation amongst employees, which is used for training, cross training and skills management appropriate to jobs at hand.

Technology

DBAs will use the ManageEngine monitoring tool to oversee client servers 24/7, using predetermined thresholds on key metrics to identify potential server security and performance issues. They will then feedback to technical team leaders weekly informally as to project progress to ensure timescales and KPIs are adhered to.

An added benefit of this tool is that it triggers an alarm within our system when agreed thresholds are broken, alerting the on-call member of staff, who can respond and carry out remedial actions in line with SLAs. This proactive, real-time monitoring identifies changes in behaviour that could lead to more severe issues.

Client documentation, preferences, and contract agreements will be logged in our Central Management System (CMS) system to provide an auditable record of contract agreements and ensure that services can be tailored to customisable requirements. Entries in our CMS system will be managed by our Accounts Manager.

Certifications and Standards

We have been selected as suppliers on G-Cloud frameworks providing cloud support and managed database services since the launch of G-Cloud 10. To demonstrate the efficacy of our approach our procedures and management systems are certified to the following standards:

- **ISO 9001:2015 (Quality)**
- **ISO 27001: 2022 (Information Security)**
- **ISO 20000-1:2018 (IT Service Management)**
- **Cyber Essentials Plus**

Maintaining the highest levels of IT Industry accreditations, we have held Oracle Partner Network status since 2006 and Microsoft Gold status in 'Data Platform', 'Application Integration' and 'Data Analytics' since 2014, reflecting our commitment to delivering high-level knowledge, support and added value solutions for clients.

Managing Constraints and Incidents

Incidents can be raised through the following methods:

- **Tickets sent to our FreshService support desk** via emailed or entered directly into our portal, where the notification and escalation procedure starts
- **Threshold breaches detected via our installed monitoring tools**, which will provide 24/7 alerts (with an on-duty DBA always available to respond)
- **Telephone call to our support desk**, forwarded to an assigned DBA
- **Our job request portal**, to which authorised users have direct access to track calls
- **Email directly to WellData support** (helpdesk@welldata.co.uk), resulting in a ticket raised in our job management system
- **Direct-dial access to a member of the assigned DBA team**, from which a primary and secondary DBA will always be allocated during contracted hours.

If the incident in question is sufficiently complex, e.g. resolution for live system is not possible within four hours due to underlying infrastructure faults, an incident resolution plan of action will be created with a stated resolution time which shall not exceed one business day unless otherwise agreed (and shall be addressed within four hours).

Service level response	Target response time
Response time to all incidents (and priorities) 24/7/365 raised by HE for 24/7 covered systems:	30 minutes, 24/7
Response time to incidents raised by HE for business hours covered systems:	One working hour
Incident resolution	Four hours (live/DR systems) Eight hours (test/DEV/UAT systems) but if the incident in question is sufficiently complex e.g. resolution for live system is not possible within four hours due to underlying infrastructure faults, an incident resolution plan of action will be created with a stated resolution time which shall not exceed one business day unless otherwise agreed (and shall be addressed within four/eight hours).

Managing continuous improvement

We will enact a Plan, Do, Check, Act methodology to outline opportunities to improve the efficiency, quality, and impact of our services through regular quarterly managerial meetings between Account Managers and Technical Managers whereby contract performance data will be reviewed to identify trends and patterns in performance.

Based on these reviews we will be able to proactively identify if performance is trending below Acceptable Performance in order to put in place SMART action plans for remediation of this, with a clearly structured programme of meetings to discuss the progress of these plans implemented within 10 days of identification.

Service constraints

Our Cloud Managed Service is designed to provide flexible, continuous support, with the following constraints noted below to ensure predictable delivery:

➤ Performance and availability:

- ✓ **Core support hours** are 09:00 – 17:30, Monday to Friday, excluding UK public holidays. For clients with non-business critical database usage requirements where incidents that occur outside working hours can wait until the next working day, this can provide a cost-effective service.
- ✓ **24/7/365 monitoring and incident response** is available via our extended cover option, supported by an on-call roster of engineers based at our UK service desk.
- ✓ **Daily checks are performed** by the clients' assigned lead DBA each morning to confirm systems are 'business ready.'

➤ Maintenance windows:

- ✓ **Routine maintenance and patching of live systems are normally undertaken outside business hours**, at times and dates that will be agreed by the lead DBA with the client during onboarding.
- ✓ **Maintenance on test or development systems** may take place during business hours by agreement with the client.
- ✓ **Major upgrades** are treated as planned change events and scheduled with the client in advance.

➤ Customisation and flexibility:

- ✓ **Our service operates on a roll-on/roll-off basis**, whereby clients can request new systems or services to be added during the contract term, or remove those no longer required to provide a cost-optimised and flexible service. For example, this model applies to consolidation projects (e.g. moving from multiple databases to a single instance), ensuring services remain aligned with current client needs.

➤ **Major upgrades:**

- ✓ **While minor upgrades, patching and bug fixes are included within the fixed-price contract**, major version upgrades (e.g. significant vendor version changes) are excluded.
- ✓ **Major upgrades** will be delivered as additional projects on a fixed-cost basis, defined with a Statement of Work.

➤ **Feature and functionality life cycle**

- ✓ **Service scope may be adjusted** in line with technology life cycle changes (e.g. vendor deprecation of software versions).
- ✓ **Our team will work with clients to plan upgrades or migrations** to supported versions, ensuring continued stability and security.

Service levels

Our clearly defined service levels (SLAs) covering performance, availability, support hours and incident response are designed to ensure continuity of client operations while offering flexibility to align with each organisation's requirements. The assigned lead DBA will agree SLAs with the client during onboarding which will be documented in the Order Form. Support hours and availability options will include:

- **Core hours:** 09:00 – 17:30, Monday to Friday (excluding UK public holidays) to provide a cost-effective service for organisations with non-business critical database usage requirements.
- **Extended cover:** 24/7/365 incident support and monitoring available, with an on-call directly employed UK-based engineer roster in place.

Our response times following receipt of an incident or service request are outlined below:

Incident Type	Response time
Incident response (live/DR systems)	1 hour
Incident resolution (live/DR systems)	4 hours, or a resolution plan with clear timescales within 4 hours
Incident response (test/dev/UAT)	2 working hours
Incident resolution (test/dev/UAT)	8 hours, or a resolution plan with clear timescales within 8 hours
Service request response	Within 1 working hour (live/DR) or 2 working hours (test/dev/UAT).

Once the engineer has diagnosed the issue with the client, the account manager will provide a resolution plan within four hours outlining the proposed action, indicative

timescales and any additional costs to be agreed prior to the order being placed. For clarity, our fixed priced contract covers unlimited service requests and incident support at no extra cost, with only extensive projects, such as major system upgrades, incurring additional costs.

*In 2025, we have **achieved an average incident response (live/DR systems) time of 12 minutes**, bettering our one-hour target response time and enabling us to expedite resolutions of client system issues.*



Outage and maintenance management

Our Cloud Managed Service is designed to proactively minimise the risk of service disruption while ensuring essential maintenance will be completed with minimal impact to client operations through:

- **Outage avoidance:** Client systems will be proactively monitored by Zabbix and ManageEngine software, providing real-time visibility and alerting using a RAG (red, amber and green) alerting system. Amber and red alerts, such as risks to disk space and capacity thresholds, system performance, memory usage and deadlocks will be investigated immediately to address issues before they escalate into outages.
 - ✓ **Connection machines** will be deployed on clustered infrastructure, allowing for failover in the event of hardware failure.
- **Service performance planning:** Trend analysis and performance reports will be generated monthly to identify risks such as capacity limits or unusual load patterns. Based on the results, the assigned lead DBA will provide recommendations to clients to adjust configuration or capacity before service degradation occurs.
 - ✓ **For planned upgrades or migrations**, performance testing will be carried out on cloned systems built from backups, eliminating risk to live environments to guarantee there is no system disruption.
- **Measuring downtime:** Our target downtime is 0 and monthly availability reports (or to a client's preferred timescale) will be issued to demonstrate system performance.
 - ✓ **When outages are unavoidable** (e.g. for major upgrades), these are scheduled with the client to minimise disruption, with the lead DBA coordinating timeframes with the client to ensure these are undertaken outside their business hours for live systems.

*Over the past 15 years, we have consistently **maintained unplanned downtime levels at less than 1%** across our 120 clients' databases.*



- **Preparing for ad hoc service need:** Our 20 directly employed UK based engineers enable us to dynamically assign additional technical resources to support unplanned projects, incidents, or peaks in demand.

Financial Recompense Model for not Meeting Service Levels

This is not something we offer.

4. Provision of the service

Customer Responsibilities

- The Client shall be responsible to WellData for ensuring the accuracy of all information provided to WellData (including but not limited to information about Client Systems and information supplied in the Order Form) and for giving WellData any necessary information, facilities, specifications, instructions and responses required by WellData to enable WellData to provide the Services in accordance with this Agreement (“Client Information”).
- The Client shall grant or procure the grant of access to such of the Client Systems, premises and resources as WellData may reasonably require performing the Services.
- If the Client requests Additional Services from WellData, WellData shall have sole discretion to determine whether to accept or decline such requests. WellData shall not provide any Additional Services without the Client’s express consent. Any Additional Services shall be charged for by WellData in accordance with the Charges Schedule applicable at the time.
- The Client is responsible for keeping safe and available back-up copies of Client Systems and all other data which it owns and/or controls.
- The Client shall indemnify and keep indemnified WellData from and against all direct losses, claims, demands, damages, compensation, liabilities, costs and expenses (including reasonable legal expenses on an indemnity basis) paid, suffered or incurred by WellData arising out of or in connection with any claim that access to the Client System or provision of the Services in respect of the Client System infringes any rights of any third parties, including in respect of any Intellectual Property Rights.
- The Client shall be responsible for:
 - ✓ obtaining all necessary consents, licences and permits relating to its receipt of the Services for the Client Systems and warrants that provision of the Services and access to Client Systems by WellData shall not breach any third-party rights, or contract terms;

- ✓ ensuring that there is a current and tested disaster recovery plan. As part of the Services, WellData shall assist in the preparation and testing of these plans, but it remains, at all times, the Client's responsibility;
 - ✓ executing the agreed backup regime;
 - ✓ day-to day administration of the Client's application software, including, but not limited to, the addition and removal of users, security, privileges, etc;
 - ✓ providing reasonable access to site to ensure that WellData's staff can achieve the contracted level of service. Subject to the Client's normal security and data protection procedures;
 - ✓ if required to come to site, providing a 'workstation / desk' for use by the WellData technical staff when working on-site;
 - ✓ if required to come to site, providing free access to Internet-Broadband when working on-site;
 - ✓ ensuring a safe working environment at all times in conformance with all relevant health and safety laws provided that WellData shall be responsible for ensuring its personnel comply with any instructions or health and safety policies for on-site visits;
 - ✓ maintaining a public liability insurance policy in accordance with the relevant laws;
 - ✓ ensuring that it and its staff shall cooperate with WellData in the performance of the Services.
- WellData, on request and by agreement, shall attend discussions with the Client's other suppliers, particularly software vendors, that have supplied, or will supply, Hardware, Software or Applications to run on the Client's supported systems.
- ✓ The purpose of this attendance shall be to facilitate that technical input is given to assure the smooth running and/or deployment of the Client's existing, or newly supplied, Hardware and/or Software.
 - ✓ Attendance at such discussions shall be restricted to the systems set out in the Supported Systems Schedule and is not available for general use.

Technical and client requirements

Our Cloud Managed Service is optimised to minimise the number of client-side technical and resource requirements which the account manager will agree with the client during onboarding to be documented in the Order Form, as outlined below:

System Requirements

- **Each client must provide a jump box** (physical or virtual machine) within their network which will be used for daily checks, monitoring and management.
 - ✓ **The jump box should be a medium-sized Windows or Linux server** that will enable all monitoring and access to remain securely inside the client's network.
- **Network access** between the client environment and ours is required, typically via VPN for streamlined secure access with minimal input required.

Client Resources

- **Minimal ongoing input resource** will be required from the client. The Lead DBA and account manager will arrange meetings with the client as frequently as the client requires, but these will not be essential for routine service delivery.
- **For projects** such as migrations, consolidations, or major upgrades, the client will be asked to define their objectives and requirements, with minimal input required thereafter, such as user acceptance training if required by the client.

Outcomes and deliverables

This service will deliver:

- **Initial assessment and setup**
 - ✓ **Audit of the client's existing database** and cloud environment.
 - ✓ **Migration or consolidation plan** where required (e.g. moving from multiple databases to a single instance).
 - ✓ **Deployment of a secure client-side jump box** for monitoring and management.
- **Ongoing service deliverables**
 - ✓ **Daily checks** will be reviewed by the assigned lead DBA and emailed to the client before 9am, providing a status snapshot of the system including to confirm they are operational ('business ready').
 - ✓ **Continuous monitoring** with alerts for space, performance, memory usage and deadlocks (via Zabbix and ManageEngine).
 - ✓ **Routine maintenance** including patching, bug fixing, index/statistics management and capacity planning.
 - ✓ **SLA-backed incident response and resolution times** (live, DR, test and development systems).
- **Resilience and recovery**
 - ✓ **Client-specific backup scheduling and restoration** testing through clone builds.

- ✓ **Disaster recovery planning and support** aligned with recovery time objectives (RTOs) and recovery point objectives (RPOs).
- ✓ **Failover capability** to secondary data centre in the event of site failure.
- **Documentation and transparency**
 - ✓ **Operational and procedural guides**, login documentation, and issues/observations logs.
 - ✓ **Daily status updates**, monthly availability/performance/capacity reports, and quarterly service delivery reviews.
 - ✓ **Clear record of all maintenance**, incidents and changes.
- **Dedicated service team**
 - ✓ **A named lead DBA**, secondary DBA and service delivery manager assigned to each client.
 - ✓ **Defined escalation routes** for service issues.
- **Client outcomes**
 - ✓ **Secure and resilient cloud-based systems** with minimal downtime.
 - ✓ **Avoidance of unexpected cloud costs** through proactive storage and capacity management.
 - ✓ **Assurance of compliance** with ISO 27001, ISO 20000, ISO 9001, Cyber Essentials Plus, and GDPR obligations.

Reduced reliance on scarce in-house skills, with continuity of expertise built into service delivery.

After-sales

*Our ability to build and maintain long-term client relationships through a structured account management model, proactive service reviews, and a focus on client satisfaction and continuous improvement is evidenced through **our long-standing relationships with clients such as Müller Dairy and Knight Frank, each retained for over 24 years.***



Our after-sales approach to building and maintaining client relationships includes:

Single Point of Contact and Escalation

- **Each client has a dedicated primary DBA** as their day-to-day point of contact, ensuring technical continuity and familiarity with their systems.
- **Issues can be escalated to the account manager**, who oversees service delivery, quality assurance, and contract management.

- **The account manager also provides quarterly recommendations** on new services, improvements, or additional products that may benefit the client, complete with a cost-benefit analysis to their business to inform decisions.
- **Where clients share upcoming departmental plans** (e.g. new data storage needs, data support requirements), the account manager advises on how existing services or new offerings can provide support.



Systems Administrator Sarah Giles for Rushmoor Borough Council, stated:

'WellData has made the day-to-day running of the system and major upgrades faster, and less disruptive to the service and provides the in-house team both IT and Revenue with expert advice and peace of mind.'

Communication and Reviews

- **Daily updates and monthly reports** (covering availability, capacity, performance and activity) ensure transparency and regular communication.
- **Quarterly service delivery meetings** provide a structured forum for reviewing SLA performance, addressing any issues in service, and identifying opportunities for improvement.
- **Issues and observations are logged and shared**, ensuring transparency and ongoing service refinement.

Customer Satisfaction and Retention

- **Our roll-on/roll-off service** allows clients to add or remove services as their needs change, ensuring flexibility and long-term value.
- **Account managers undertake client satisfaction reports** gathered during quarterly meetings with clients with all compliments and complaints recorded for trend analysis and shared with the wider team to demonstrate instances of exemplary customer care or lessons learned. Resolutions to any complaints are actioned within 24 hours of receipt.
- **Based on client feedback**, the top five reasons for our success in retaining clients and building strong relationships are:
 - ✓ **Cost certainty** through fixed-price contracts, with unlimited incident support
 - ✓ **Continuity of expertise** from assigned DBAs and engineers
 - ✓ **Flexibility** through the roll-on/roll-off service model
 - ✓ **Proactive issue resolution** and regular service reviews
 - ✓ **Quality assurance** embedded into daily operations and escalations

Our ability to maintain long-term relationships is evidenced through maintaining a **customer satisfaction rating of 9.5/10** measured using NLP client satisfaction scores from feedback gained during quarterly meetings.



Growing the Business Partnership

- **The lead DBA provides feedback to the account manager** on the state of client systems, proactively identifying areas for future implementation or optimisation. For example, opportunities for service improvements, consolidations, or migrations are proactively discussed during review meetings.
- **Account managers** use this feedback to plan ahead with clients, ensuring that improvements are aligned with both current and anticipated requirements.
- **This approach ensures services remain** relevant, cost-effective, and able to evolve alongside the client's digital transformation journey.

Head of IT Mike Calverley for Charlie Bigham's, stated:



'Following the recent completion of our ERP migration from on-premise to Microsoft Azure using SQL MI, WellData was integral to the success of this very strategic project. They provide my team with the technical leadership and resources for the SQL expertise we require. They are always there for us and attended all project meetings, workshops and catch-ups and would always jump on calls at a moment's notice – Welldata are like an extension to my team, and we get on so well with all of them – they can't do enough for us.'

Termination Process

Our termination process is designed to be transparent, fair and aligned with the principles of the G-Cloud 15 Framework, (i.e. *Call-Off Contract RM1557.15*). Both parties' rights and responsibilities will be clearly set out in the Order Summary and associated contractual documentation, summarised below:

Termination Clauses

- **Either party may terminate the agreement** in the event of:
 - ✓ **Non-payment** of fees by the other party.
 - ✓ **Breach of contractual obligations**, including failure to maintain a disaster recovery plan.
 - ✓ **Force majeure events** preventing either party from fulfilling its obligations.
 - ✓ **Insolvency or bankruptcy** of either party.

Rights and Responsibilities

- **Client responsibilities:**
 - ✓ **Provide notice of termination in writing**, as set out in clause 10 of the *Call-Off Contract RM1557.15*.
 - ✓ **Ensure any required access or information is made available** to facilitate orderly off-boarding.
- **Our responsibilities:**
 - ✓ **Support the client with a structured off-boarding process**, including handover of documentation and assistance with data migration.
 - ✓ **Ensure that termination does not disrupt the client's** ability to access or manage their data.
 - ✓ **Maintain confidentiality** and information security obligations after termination.

Early Termination and Costs

- **No lock-in:** We do not charge onboarding or termination fees, providing clients the ability to terminate services early as per clause 10 of the *Call-Off Contract RM1557.15* without incurring additional cost.

Off-Boarding Support

- **A tailored exit plan** will be agreed with the client if additional assistance (e.g. managed migration away from the service) is required.
- **All necessary documentation** (operational guides, access credentials, backup schedules, etc.) will be provided to ensure continuity.
- **Data export facilities** are available to allow clients to retain and manage their own information following termination.

5. Our experience

Case Studies

Rapid Recovery For An Intensive Care Unit

[Database Migration Services | Case Study | Intensive Care NHS](#)

Database Migration Services and Management Support for the NHS

The Issue

The Barnet ITU had switched from paper-based records to digital records in the early 2000s.

The switch allowed for more transparency and reduced risk of human error, as well as offering the ability to extrapolate data for analytical purposes.

It then fell to Dr Tony Wolff, Barnet Hospital Intensive Care Unit, who was also the doctor running the ITU and had designed the information system, to ensure that the system was up and running and the database secured.

In his own words, ***‘it was challenging and stressful looking after the databases with not being a DBA and being a one man band’***.

Without daily database management support, the situation was challenging to sustain: the old operating system and the lack of consistent maintenance meant that the system was difficult to **DBA** upkeep and at risk of failure.

With the clock ticking, and the first news of a deadly virus appearing, WellData was called in.

The Solution

WellData didn't waste any time: the first step was to secure the infrastructure, migrate the operating system to Windows and to upgrade the database from Oracle 11g to Oracle 19c.

Once the data was secured, and the immediate need resolved, the **WellData team proceeded to provide ongoing support**: these were the early days of the March 2020 lockdown, as admissions skyrocketed, WellData stepped in to take over housekeeping and capacity planning.

The Results

The migration took less than 8 weeks to be completed.

By the time the pandemic had reached its peak, the ITU team was able to rely on a modern Windows operating system and on on-going support of a team of experienced DBAs.

Before the migration and the outsourced database management, the ITU had so much unkept data that any new information could hardly be added without risk of destabilising the whole system.

Now, the Royal Free Hospital is able to confidently and efficiently record and track every new patient, taking the burden off the already stretched medical team.

Graduated Database Management for the University of Exeter

[Database Managed Services Case Study: Exeter University | WellData](#)

Background

The University of Exeter is a member of the prestigious Russell Group of research intensive universities. Offering a wide range of subject areas in a welcoming and an international environment.

The Issue

The University of Exeter were in need of a stable and reliable SQL Server and Oracle solution for the management of their databases.

The challenge was two-fold:

1. Exeter wanted to avoid cost increases over the term of the contract while guaranteeing a better service that could ensure 24/7/365 support.
2. The geographical position of the University made it extremely challenging to find teams with suitable skills.

That's when the University looked for an alternative solution: moving the day-to-day management of their databases to a fully managed service.

The Challenges

Cost of 24/7/365 database managed services

Exeter University relies on a database estate consisting of Oracle, SQL Server and MySQL for their daily operation.

Due to the complexity of this estate the University had to employ a minimum of three full-time Database Administrators (DBAs) to ensure that the databases were managed 24/7/365.

Ever-changing technology landscape

In an age when technology is in constant development, the University recognised the critical importance of entrusting their database estate to someone that could ensure the most up-to-date expertise for their database managed services.

Specific database issues

Exeter University needed a strategic partner to support and develop their database estate for large scale digital transformation.

One single point of failure

Due to budget pressures, that affect Universities across the country, combined with the Exeter location, finding the right database management services skills was challenging and the University couldn't secure a formal oncall-rota given the limited number of positions combined with the technical complexity in the estate.

Managed Database Service

In a search to control costs while ensuring the University could rely on the right level of support and expertise, the Solutions Delivery team started to look for an alternative solution.

A Managed Database Service was a first-time experience for the University in this area, but the team realised that managed services could be the only way to address the challenges they were facing and decided to embark on a thorough research process to understand the market.

A professional and rigorous approach was used to make sure any future solution would work for the University.

The tender exercise took many months and required a very detailed response from the multiple companies that applied.

At the end of the process, Exeter selected WellData as their partner of choice.

The systems are better maintained and have higher efficiency, resilience and performance. Exeter University is now able to focus on strategic projects, rather than having to invest time and resources on daily database management.



Assistant Director for the University of Exeter:

‘The biggest pleasant surprise has been the realisation that every request is addressed in the space of a few minutes and that there is an expert person at the other end of the phone ready to answer our team’s queries, any time. A fantastic result.’



Development Manager for the University of Exeter:

“You now cover out of hours fully for us, although with your proactivity we probably don’t need it now.”

The Solution

24/7/365 database managed services

Continuous monitoring, with no limit on the amount of advice, interventions or support offered.

- 24/7/365 monitoring, problem resolution, and root-cause analysis
- Proactive health checks
- Continuous operational improvements
- Change requests for design and implementations
- Configuration management
- Backup monitoring
- Capacity planning
- Upgrade and migration planning
- Backup/export on-demand service

Day-to-day database maintenance

- Performance tuning, high availability testing, and disaster recovery
- Service pack, patching and hot fixing
- Database refresh of development/test installations

Database implementation services

– project basis

- Database upgrades, installation, and configuration
- Schema/table verification

- Database migrations
- Pre-deployment testing
- Deployment to production services
- New database design service
- Log interrogations
- Database decommissioning
- Database licence optimisation
- Provide advice and guidance on migration to the cloud

Clients

Public Sector



University
of Exeter



University
of Exeter

RUSHMOOR
BOROUGH COUNCIL

Private Sector



Charlie Bigham's

prodrive

Technologies



Contact Details

- ✓ Steve Brown
- ✓ Business Development Manager
- ✓ Tel: 0800 389 4051
- ✓ Email: digitalmarketplace@welldata.co.uk