MANAGED UKCLOUD

Enterprise Compute Cloud

G Cloud 9 Service Definition
Lot 1: Cloud Hosting

Datapipe Europe Ltd

East One
20-22 Commercial Street
London, E1 6LP

For all enquiries, please contact

George Earp, Public Sector Specialist:

t: +44 (0)7788 721 069

e: gearp@datapipe.com

DATAPIPE.CO.UK
0800 634 3414

CONTENTS

OVERVIEW

Datapipe delivers managed access to UKCloud platforms and services, providing public sector organisations with on-demand, scalable compute, storage and network resources to deliver transformational projects.

This Service Definition covers **Datapipe's Managed UKCloud Enterprise Compute Cloud** offering.

AT A GLANCE

THE BEST OF G CLOUD	MEASURED USAGE
UKCloud accredited and approved infrastructure services delivered by Datapipe at zero margin, with enterprise-grade Datapipe service management wrap	True consumption-based pricing from just 1p per virtual machine per hour from the UK public sector's #1 accredited cloud platform
MIGRATION & IMPLEMENTATION SERVICES	**UK SOVEREIGN**
Experienced delivery of efficient transition and transformation projects in the public sector. Straightforward and pain free process, with a clear path to benefit	An assured cloud platform delivered from two secure UK data centres by a UK-based company with UK Government security-cleared staff
DISASTER TOLERANT	**OPTIMISED FOR OFFICIAL**
Two Tier 3 specification UK data centres separated by more than 100km and securely connected by high-bandwidth, low-latency dedicated connectivity enabling synchronous replication	Extensive independent validation (including CESG PGA). Fully aligned with the CESG 14 Cloud Security Principles, ideal for all data classified at OFFICIAL (including OFFICIAL SENSITIVE) and legacy IL0–IL3 solutions
FLEXIBLE CONNECTIVITY OPTIONS	**PROVEN & AUDITED**
Connect for free to the Internet (with DDoS protection provided as standard), PSN (Assured service) and JANET. Other aggregated (chargeable) services include PSN Protected service, N3 or legacy networks including PNN) or HybridConnect	Independently audited and verified by trusted public sector organisations, including HSCIC (NHS Digital), MoJ and the Police (Police Approved Secure Facility — PASF), for workloads requiring a higher assurance for sensitive data (for example, MoD Defence-as-a-Platform)

Typical Use Cases

- Organisations wanting to consolidate or grow their existing infrastructure by migrating to a secure cloud platform, significantly reducing the complexity and constraints of traditional hosting models
- Organisations looking to quickly prove concepts without the traditional constraints of complex CAPEX or procurement procedures
- Organisations who want to complement their existing on-premise or private cloud solutions by using ‘cloud bursting’ for limited periods when demand on their dedicated resources exceeds available capacity
- Channel/ intermediary organisations including Systems Integrators and ISVs who need specialist infrastructure skills to deliver Government contracts.

WHY UKCLOUD & DATAPIPE?

IT in the public sector is changing, disaggregating IT expenditure to create loosely coupled technology solutions that demonstrate best in class services and deliver tangible, swift return on investments.

UKCloud and Datapipe Europe (known previously as Adapt Services Ltd) have been part of the G Cloud Framework since it was created in 2012. Experienced in the successful delivery of framework services, we have supported many Government departments with digitalisation and disaggregation initiatives that enable cost-effective access to flexible and secure fully managed cloud services.

Datapipe & UKCloud together offer the optimal blend of enterprise-grade, commercially critical production delivery and deep public sector knowledge and experience. On UKCloud’s foundation of commodity infrastructure services, Datapipe layers premium, deep service management expertise to bring the best of both worlds to the public sector. Datapipe’s award-winning managed service wrap and secure, efficient, experienced planning, implementation and migration services are the ideal complement to UKCloud’s commoditised infrastructure proposition - this clear understanding of the demarcation of responsibility plays to each organisation’s core strengths and creates joint scale.

ABOUT DATAPIPE

Datapipe in the UK is a leading end-to-end managed cloud service specialist and integrator. We manage critical production infrastructure for some of the UK’s most high profile, tech-dependent, heavily regulated public and private organisations, so organisations can be confident we have the service experience and ability to keep their environments rock solid and running optimally. Strengthened by the acquisition of Adapt Services Ltd in 2016, Datapipe helps public sector customers work smarter with highly secure, compliant enterprise-grade IT that delivers real-world advantage, transforming price performance and enabling change.

Some of Datapipe’s public sector direct and end-user customers include (initially contracted as Adapt Services Ltd):

Ministry of Justice

Cabinet Office

Department for Environment Food & Rural Affairs

Department for Culture Media & Sport

Department for Transport

Datapipe is ISO27001, ISO9001 and PCI level 1 certified. Services are managed by a dedicated 24/7 team across Datapipe's 3 UK operations centres. Our teams of highly skilled engineers maintain a detailed understanding of customers' infrastructure environments and their relative priority and criticality at any given time. We also support a number of PSN Codes of Connection with our customers.

ABOUT UKCLOUD

UKCloud is a UK company founded in 2011 and is unique amongst cloud providers in maintaining an exclusive focus on the UK public sector. UKCloud was one of the first G Cloud providers to successfully achieve CESG Pan Government Accreditation and remain unique in delivering a pure cloud for UK Government. UKCloud's range of on-demand, pay for what you use, no minimum commitment cloud services are suitable for OFFICIAL and OFFICIAL SENSITIVE (formerly IL0 through IL4) data, delivered from two secure Tier 3 UK data centres separated by more than 100km and securely connected by dedicated high-bandwidth and low latency CESG assured circuits enabling synchronous replication.

UKCloud solutions also help public sector organisations lower CO2 emissions through reduced energy consumption, sustainable procurement and better hardware utilisation. UKCloud is a CarbonNeutral® Company whose data centres have a low carbon footprint and low PUE rating, and comply with the EU Data Centre Code of Conduct.

OUR PARTNERSHIP

Our partnership is designed to make Datapipe and UKCloud easy to work with:

- Standardised managed cloud services, clear service enhancement options. No hidden charges, transparent management, marginless UKCloud service pass through
- Perfectly aligned to Government's vision for service delivery: service agility and security at scale, delivered through multi-SME engagement
- Real, enduring partnership; both parties completely aligned to outcome delivery for your users

FLEXIBLE SERVICES

Datapipe layers our managed services on top of the UKCloud infrastructure platforms. Our managed service fee is directly aligned to cloud usage, offering public sector organisations an OPEX model for managed cloud which is optimised in line with how their business consumes infrastructure cloud services.

UKCloud offers simple products to deliver complex solutions, all designed to reduce security risks without decreasing the flexibility of a cloud platform. UKCloud's differentiated, commoditised products provide a choice of IaaS, PaaS and SaaS and a range of service levels, virtual machine sizes and security levels.

UKCloud provides innovative ancillary solutions to further increase cloud flexibility such as the Cross Domain Security Zone which facilitates Internet facing Assured OFFICIAL applications to connect to data stored within its Elevated OFFICIAL domain. These options allow customers to keep their data safe, whilst allowing citizens to interface with the information they need.

INFORMATION ASSURANCE

Datapipe and UKCloud understand the importance and value of your data. All data is exclusively located in highly secure UK data centres, managed in UK and subject to UK regulation – removing the risk of international surveillance or disclosure. Services are assessed and recognised against international standards ISO 9001, ISO20000 and ISO27001 and are subject to regular official audits and assessments.

Datapipe managed services and UKCloud cloud services are delivered and built with clear alignment to the 14 CESG Cloud Security Principles that all UK public sector organisations use when assessing managed cloud solutions. The UKCloud cloud benefits from extensive independent validation via certifications ranging from international standards (for example, ISO9001, ISO27001, ISO20000) to UK public sector specific standards (for example, PSN, N3/HSCIC). UKCloud's Cloud Platforms are subject to regular, extensive IT Security Health Check (ITSHC) CHECK Tests by independent, CESG-approved assessors to ensure that customers have confidence in the physical and technical security controls which have been implemented to protect their valuable data assets. An Evidence Pack is available which demonstrates the breadth and depth of UKCloud's security credentials.

Datapipe's managed services are delivered in line with these security standards. Our staff are SC cleared and vetted where necessary. Datapipe is also certified under the Cyber Essentials Plus Scheme and can deliver specialist security services as required to meet your security and compliance standards.

ON-BOARDING & OFF-BOARDING

The Digital Marketplace creates opportunities for performance-based, short-medium term engagements with public sector organisations so the ability to on and off-board effectively is critical to success in this arena. Datapipe has over a decade of experience on-boarding customers into our virtual infrastructure environments. Typical considerations include network connectivity and migration options - we will walk you through all considerations as your requirements develop, ensuring we balance risk, cost, timescale and priorities for your organisation.

If you decide to switch providers, we will work with you to expedite the off-boarding of your services to the new environment. Datapipe's solutions are all based on standardised infrastructure and software, designed with robust migration processes and portability in mind. Our consistent documentation makes knowledge transfer straightforward, accurate and complete.

CONNECTIVITY

UKCloud solutions offer resilient connections to secure UK Government networks such as PSN Assured, PSN Protected and N3, as well as large scale, DDoS protected internet connectivity. It is also possible for customers to present their own connections (such as direct connectivity into MPLS, or inexpensive point to point connections via leased lines) and the Secure Remote Access solution to allow security assured VPN access to the Elevated OFFICIAL domain.

UKCLOUD SOLUTIONS

UKCloud's platforms provide public sector customers with on-demand, scalable compute capacity. Datapipe harnesses these commodity resources to deliver transformational initiatives with a proven, deep and robust managed service wrap. Together, we offer public sector the best of both worlds – on-demand, consumption based cloud with the structure, support and governance of a leading UK sovereign service provider.

These service enables the Government's digital transformation initiatives and supports the Cloud First policy by delivering a PSN-accredited true cloud computing service that adheres to the NIST definition of cloud (includes resource pooling, on-demand, rapid scalability and transparent, utility-style billing).

Our services help public sector organisations:

- Reduce costs by increasing operational efficiency
- Add operational resilience to existing facilities or extend estates to cope with growing workloads via hybrid cloud solutions
- Prolong the life of existing applications by removing tight coupling with ageing hardware
- Deliver digital transformation projects that require high levels of security and assurance
- Enable transformation of legacy services by facilitating test and proof-of-concept exercises
- Transition to a platform that increases scalability and resilience.

SUMMARY FEATURES & BENEFITS

FEATURES	BENEFITS
Elasticity	Straightforward scale that directly aligns usage to expenditure. Complex workload delivery supported by dynamic auto-scaling
Enterprise-grade service as standard	Datapipe's deep expertise and secure, efficient managed options free your resources to focus on business-enhancing activities
Simple provisioning	Build and configure VMs within minutes via a secure self-service portal; add or reduce resources as needed
Simple configuration	Configure the solution that is right for you and your application with a range of service levels, VM sizes and licensing options billed on a utility basis per hour
Geographic diversity	Confidently architect solutions, knowing that applications and services will remain available whilst achieving your compliance requirements
Proven cloud security	Utilise cloud infrastructures which directly align to CESG's 14 Cloud Security Principles in turn minimising your audit and security overhead
Modular approach	Mix and match virtual machine sizes and service levels to suit the requirements of your enterprise workloads

ENTERPRISE COMPUTE CLOUD PLATFORM FEATURES

Unlike cloud-native applications, enterprise applications were designed in the age of virtualisation and traditional hosting. These workloads support a wide variety of business processes: from back-office systems (such as payroll) to line-of-business applications (such as case management). Some enterprise applications have particular requirements in relation to virtual machines (VMs), storage, resilience, assurance, and network connectivity to legacy systems and secure communities of users.

UKCloud Enterprise Compute Cloud provides you with the trusted, connected and flexible Assured OFFICIAL and non-internet connected Elevated OFFICIAL cloud platforms you need to deliver your critical enterprise applications in the cloud.

All enterprise workloads deployed using UKCloud's compute platform benefit from the following features as standard:

- **Proven compatibility.** Powered by leading enterprise technologies from VMware (including vSphere ESX), EMC and Cisco, Managed UKCloud Enterprise Compute Cloud provides a familiar and proven technology platform that de-risks running your applications in the cloud (compared to other non-enterprise cloud platforms which are often based on unproven open-source or proprietary technology).

- **Choice of location.** We provide a variety of options that enable you to build resilience into your applications.
    - Managed UKCloud Enterprise Compute Cloud is offered from two geographically distinct regions, both located in the UK and separated by over 100 km for excellent geo-diversity
    - In addition, each region offers multiple physically separated availability zones, providing you with multiple options to build the resilience you require into your solution

- **Protective monitoring.** Both our Assured and Elevated OFFICIAL security domains feature enhanced Protective Monitoring (SIEM) at the hypervisor layer and below to provide the highest levels of assurance aligned with NCSC good practice guidance.

KEY MANAGED SERVICE FEATURES

ALIGNMENT FOCUS

Our people focus on applying their diverse range of knowledge and skills to earn trust and confidence. Leveraging years of proven experience, we develop a deep understanding of our customers' business objectives and take personal interest in helping them achieve those goals. We call this Operational Empathy® and at Datapipe, it is how we do business.

Transparency and collaboration are critical attributes of the ongoing service relationships we build. Our teams have a shared understanding of our customers' drivers and their outcomes. We pride ourselves on implementing effective governance models; aligning the right members of the team with the right key customer stakeholders at all levels.

- Account Team (Lead): *Planners and Thinkers*
    - This team is responsible for understanding and communicating the required customer outcomes to the rest of the Datapipe business.

- Service Delivery Managers: *Completers and Analysts*
    - This team is responsible for managing the delivery of customer outcomes that have been set by the account team during the presales process and during live service.

- Operations: *Engineers and Problem Solvers*
    - This team is responsible for maintaining and continuously improving the day to day delivery of services with people that are directly accountable for the customer solution

This holistic approach to service drives the following customer experience outcomes:

- A high touch, business-aware, customisable service wrap around application environments
- A layer of additional security controls and governance measures that protect customer data and workloads in living environments
- Trusted faces and names that will become an extension of customers' own teams
- Integrated commercial and technical management to ensure that pragmatic, relevant approaches to innovation are brought to the customer's attention.

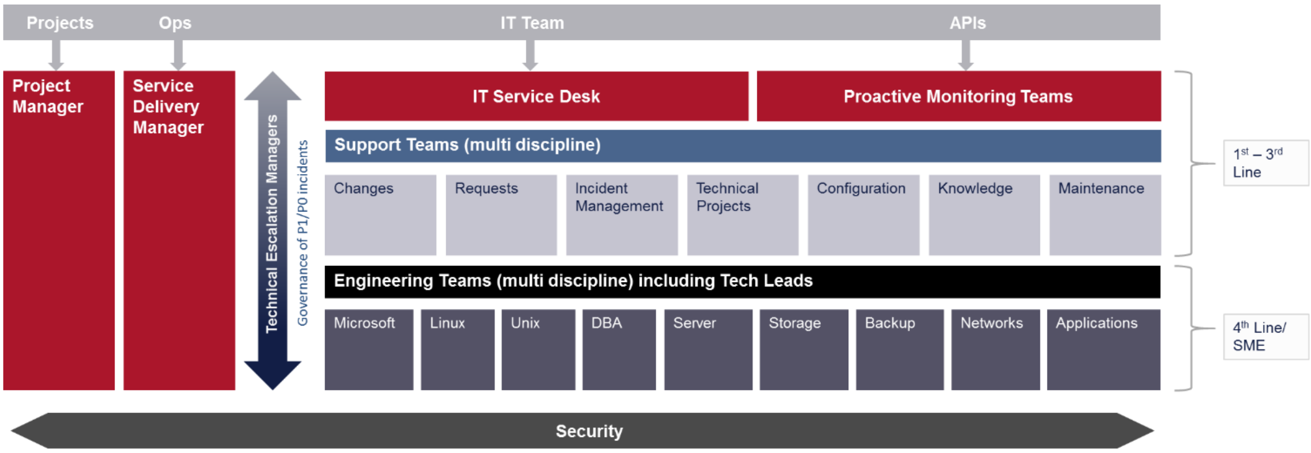
This structure is proven over time to deliver an outstanding customer experience and ultimately drive value based on our customer's technical and business requirements.

SERVICE DELIVERY MODEL

The Datapipe Managed Service Centre (MSC) is operational 24/7, including weekends and Bank Holidays and is contactable by telephone, email and via our customer portals. Specifically, this is our 1st, 2nd and 3rd line support as recognised by the traditional ITIL model.

Technical teams operate in accordance with ITIL best practice, following standard incident, change and problem management processes ensuring the highest quality levels of support are provided and maintaining service delivery against specified service levels. The diagram below shows our ITIL aligned support model integrated with tools, processes and people.

Datapipe Managed Service Centre



The 1st line comprises two distinct disciplines: Service Desk who are accountable for call handling and ticket management and Proactive Monitoring who are focused on event management and proactive system checks. All calls logged with Datapipe are managed via our principle customer portal, Datapipe One, which is built on ServiceNow, a cloud based solution developed around the ITIL framework. For public sector customers that also run ServiceNow, Datapipe is able to offer e-bonding capability to create seamless workflows and a single view of configuration items between customer and Datapipe systems.

2nd and 3rd line support is provided by our Support teams (Change, Request, Incident and Configuration Management). We typically close circa 90% of all incidents raised at 1st and 2nd line.

ENHANCED SUPPORT

Our Engineering teams (Server, Infrastructure, Network and Application) provide 4th line expertise and are subject matter experts within our business.

The efficiency of our model frees up time for proactive 4th line support, delivered via our team of 'Tech Leads'. Where appropriate Datapipe may assign a Tech Lead to customer accounts on either a shared or dedicated basis depending on requirements: an experienced engineer with a deep knowledge and understanding of the customer's technical solution and business. The Tech Lead is supported by a team of engineers comprising technical experts from multiple disciplines (e.g. Microsoft, Network, DBA and UNIX). We have created this resourcing model to provide a level of depth, ownership and accountability which is seldom seen in a shared services delivery model.

Our Tech Leads work with our solution architects and account and service delivery teams to provide a continuous feedback loop on customer environments, starting during the onboarding and build process then going on to run it with an emphasis on collaboration and strong communication.

Unlike the more traditional support model, which typically comprises assigned primary and secondary engineering resource with no understanding of individual customers or their businesses, the Datapipe support model removes any potential single point of failure and reduces operational handoffs.

The Tech Lead takes complete ownership of customers' technical solution; acting as technical ambassadors, proactively reviewing and assessing capacity, performance and risk. The Tech Lead also joins the Service Delivery Manager at Service Reviews, Quarterly Business Reviews and other meetings as required.

The additional accountabilities of the Tech Leads include:

- Taking the lead on issues, coordinating the wider team where required
- Ensuring colleagues have a deep understanding of the solutions they are supporting
- Technical design (maintaining the Low Level Design and creating and maintaining Technical Runbooks)
- Quality Assurance including sign off on builds and changes, effective monitoring being in place and regularly reviewed and ensuring the CMDB is completed and maintained.

PROACTIVE MONITORING

Datapipe deploys a number of industry leading monitoring tools. Monitoring views are constantly reviewed and managed by Proactive Monitoring Engineers working within the 24/7 Service Desk team in our Managed Service Centre. Should a threshold be breached, an Incident Ticket is automatically raised in ServiceNow and assigned by the Service Desk to the appropriate resolver group.

Tech Leads are accountable for conducting a Proactive Monitoring Review of customer services on a 6 monthly basis. In addition to implementing any recommendations resulting from these reviews, the Technical Lead will produce a report of their findings.

MANAGED SERVICES INCLUDED AS STANDARD

Server Management

This Datapipe managed service includes all aspects of the build, management, maintenance and monitoring of the server up to the operating system (OS) level, including:

- Server build and test, including installation and configuration of the chosen operating system (e.g. Windows Server 2012R2, RHEL 6.5)
- Monitoring, reporting and resolution of errors and events generated by the operating system
- Patching and fulfilment of customer-requested OS related change requests

- AV deployment and management
- Capacity management, CPU / RAM / Disk
- Performance analysis & management
- Incident management
- Problem management
- Configuration and change management
- Availability management
- ITIL-compliant service management
- 24/7 Operations Bridge
- Preventative maintenance

Database Management

The Datapipe service includes all aspects of the build, management, maintenance, backup and monitoring of databases including:

- Database build & test following our best practice procedure
- Operations management including event monitoring & resolution
- Backup management & restores
- Database patching
- Configuration & change management
- Capacity management & planning
- Incident management
- Problem management
- Availability monitoring & management
- Performance management

Datapipe supports MySQL, Microsoft SQL Server, DB2 and Oracle databases in a variety of configurations to meet the customer's requirements. Datapipe works with our customers and their application providers to ensure the highest levels of performance and availability of specific databases. Datapipe will not take responsibility for the content of these databases, but will assist in the ongoing integrity checking, tuning, availability, backups and maintenance as advised by the vendors.

Managed Firewall Services

Managed Firewall Services filter traffic based on specified requirements, detecting and deflecting unwanted attempts to penetrate the client network, creating a critical layer of security between the organization and the Internet. Firewalls are initially configured to block all incoming traffic, allowing for an immediately secure solution. Datapipe also provides a variety of standard security policies, and works with clients to develop custom policies that address the specific solution requirements. Only an authorised user can request firewall changes. An audit of all rules in place can be provided at client's request.

Datapipe's hardware firewalls are managed and supported by a full team of experts with in-depth knowledge of client solutions. Firewalls are available in single-node configuration or in high-redundancy setups, depending on firewall capability. In high redundancy configurations Datapipe deploys firewalls capable of stateful failover, maintaining session connectivity in the event of a firewall hardware failure. Datapipe firewalls are backed by a one-hour hardware replacement guarantee.

Managed Virtual Private Network Services

A Virtual Private Network (VPN) encrypts all traffic between two Internet points, providing a secure communication channel for individual users, user groups, contractors, vendors and remote offices. Managed VPN Services provide a high level of data integrity and protection of key corporate information assets.

VPN services may consist of site-to-site VPNs used by many users simultaneously, or client VPNs used by individual users on an ad-hoc basis. Two-factor VPN authentication utilizes certificates for authentication, and is available as an additional service.

Managed Exchange as a Service

Datapipe's Managed Exchange as a Service solution delivers a secure, consistent, and efficiently managed messaging infrastructure that is configured to meet client needs and enhance their communication capabilities. Built on Microsoft Exchange, the solution provides managed administration services, including 24x7x365 monitoring and support, diagnostics, problem resolution, migration, patching, and upgrades for critical messaging applications.

The solution also offers the benefits of flexible implementation, delivering services that enable clients to customize email size limits and retention periods. Enhanced security features prevent data leaks and help maintain compliance with government and/or regulatory requirements.

Datapipe architects an Exchange solution for each individual client's specific needs, including the option to integrate virtual machines, providing the economic and scalability benefits of a cloud-based service in a private environment. This approach also adds hardware resiliency and the supporting infrastructure that is required to meet each client's expanding business needs.

Active Directory Domain Services

Managed Active Directory Services (ADS) are available to clients, where Datapipe's team of Microsoft experts will design, implement, monitor and manage the ADS infrastructure. Clients may implement a separate instance of ADS hosted at Datapipe, or configure an extension of an existing remote ADS infrastructure, typically run over a VPN tunnel or dedicated link. The standard service does not include user management.

Managed Load Balancer Service

Datapipe's Load Balancing team can design, implement, and support customer's load balancing requirements with on best in class deployment models based on a client's unique needs. Load balancers are typically deployed in an active/passive failover cluster for resilience. Advanced load balancing and traffic management functionality is available, on request, at an additional charge.

Managed Backup

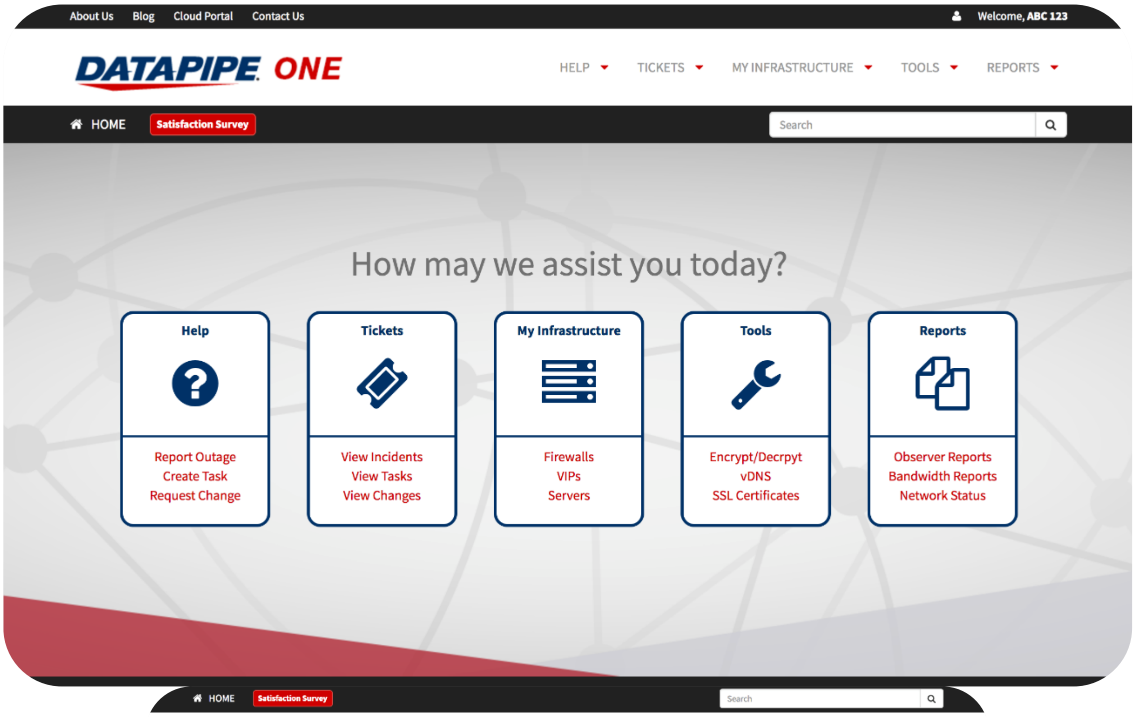
Datapipe will provide fully managed backup of all workloads hosted within the environment. The method of backup will vary across the environment and is workload dependent. For the most part, Agentless API based (snapshot) backups will be taken to provide a restore point for workloads.

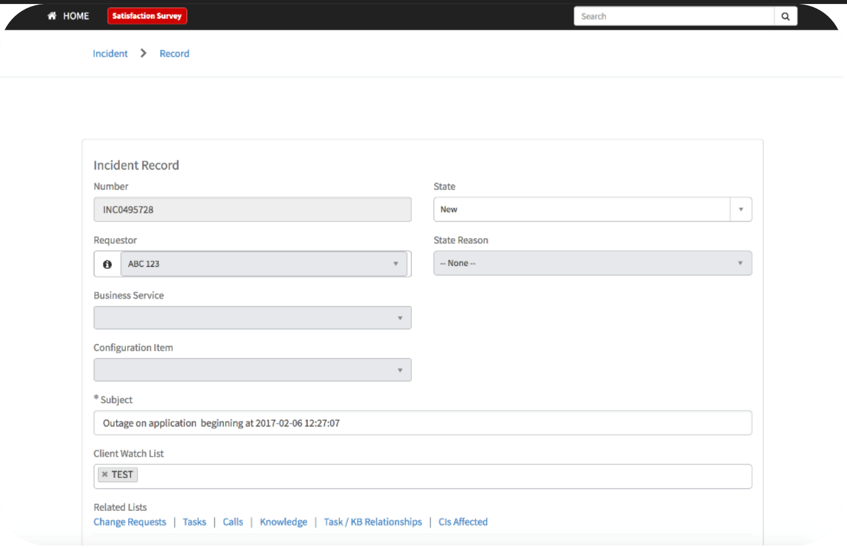
Backups will provide for a standard RPO of 24 hours (lower for transactional technologies where log backups are also taken). Longer retention periods are available if needed.

PORTAL

Public Sector customers will be able to harness the full value of on-demand, in-depth access to comprehensive reporting through customised solution dashboards. Our ticketing and event management portal Datapipe One, coupled with a custom dashboard view of monitoring, allows customers to manage their solution in real-time through a secure interface with the following capabilities:

- View current monitoring configuration per server
- Submit and/or view open/closed incidents, changes, and tickets
- View device information by individual server or by application group, including uptime, CPU, memory and virtual memory and storage
- Review the latest backup status
- Submit and/ or view escalation, alerts and notifications
- Update contact information
- Utilise as a repository of all assets
- Monitor, filter, and view events and event history for devices
- Historical record of events, incidents, tickets and inventory
- Run custom reporting on performance statistics and workflow management





Incident Record

Number: INC0495728

State: New

Requestor: ABC 123

State Reason: -- None --

Business Service:

Configuration Item:

* Subject: Outage on application beginning at 2017-02-06 12:27:07

Client Watch List: × TEST

Related Lists
Change Requests | Tasks | Calls | Knowledge | Task / KB Relationships | CIs Affected

This portal enhances our Operations teams’ ability to address any major or minor issues relating to customer solutions and provides visibility into issue resolution. The portal keeps customers informed using communication tools with each reported Incident’s status throughout the Incident Management process. The portal has the ability to link business services to assets and, with a fully integrated Monitoring Service, allows all assets to be properly tracked. A built-in knowledgebase allows Datapipe staff to access various customer-specific support information ensuring that the support team has access to the most current and accurate information at all times.

REPORTING

Cloud Service Review

Datapipe proactively evaluates Managed Cloud customer accounts for optimisation opportunities, security considerations, growth strategies and cost savings. Datapipe Service Delivery Managers

(SDMs) regularly collaborate with customers to review their entire cloud environment, using deep analytical tools to develop customised and comprehensive service reports.

These strategic account reviews provide a tangible demonstration of how Datapipe tends to each customer's managed environment, anticipating their needs before issues arise. A high level of visibility, detailed reporting capabilities and expert analysis facilitate customer awareness of potential issues for which Datapipe will provide guidance and remediation support. Additionally, Cloud Service Review capabilities and outputs are customised to unique needs and feedback.

Reporting & Frequencies

- Monthly Service Review Report
- Incident Activity Monthly Report
- Incident Activity for Network Report
- Service Improvement Initiatives - Monthly
- Ticket Activity Report – Monthly
- Change Request Activity Report - Monthly
- Incident Activity and Average Response Time
- Bandwidth Utilisation Report
- Major Incidents Report
- Service Uptime Report

IMPLEMENTATION & MIGRATION

Datapipe excels at cloud migration and implementation. Our experience in delivering transition and transformation in the public sector makes the process straightforward and pain free for customers, with a clear path to benefit delivered by an efficient and highly secure migration and implementation strategy. We work with customer IT teams to deliver the most effective migration strategy that makes optimal use of existing skilled resources. Please see Lot 3 for Datapipe's Cloud Support Services (Planning, Setup & Migration and Ongoing Support) for more detail of our capability.

SECURITY & GOVERNANCE

INFORMATION SECURITY POLICIES & PROCESSES

In order to protect both ourselves and our customers, we have invested in maintaining core security certifications for ISO 9001:2008, ISO/IEC 27001:2013, Cyber Essentials Plus and PCI DSS 3.2. The Datapipe Executive Team are committed to providing a robust framework that prioritises security across our business. The board have recognised Information Security and Cyber Security are vital to the protection of any organisation's key assets and supporting the global digital economy. Security risks, requirements and controls are primarily designed around the CIA Triad, which relates to Confidentiality, Integrity and Availability.

Managing security in this manner allows for a practical, applicable and cost effective design that meets our business, regulatory and compliance requirements. As we are fully certified in both ISO27001 and PCI we have robust compliant policies that are regularly audited by ourselves and externally validated through our external certification auditors. Policy implementation is measured though metrics which are reported quarterly to the board, direction is then communicated to heads of department for rectification.

Information Assurance

We are committed to meeting the requirements of information security good practice and proactive identification of new and emerging vulnerabilities. To this end, we maintain an Information Security Management System (ISMS) which is certified against the requirements of ISO 27001.

Datapipe's managed services are delivered in line with these security standards. Our staff are SC cleared and vetted where necessary if sponsored by the customer. Datapipe is also certified under the Cyber Essentials Plus Scheme and can deliver specialist security services as required to meet customer security and compliance standards.

Datapipe understands the importance and value of public sector customer data. All data is exclusively located in highly secure Tier 3 specification UK data centres, managed in the UK and subject to UK regulation – removing the risk of international surveillance or disclosure. Services are assessed and recognised against international standards ISO9001 and ISO27001 and are subject to regular official audits and assessments.

Services can be designed and built with clear alignment to the 14 CESG Cloud Security Principles that all UK public sector organisations use when assessing cloud hosted solutions.

PRINCIPLE		IMPLEMENTATION
1	**Protecting data in transit and at rest**	This is usually through specific encryption requirements agreed with the customer. This includes the transfer of bulk data into or out of the service. Datapipe's Secure Management Environment (SME) operates using only secure or authorised and reviewed protocols to ensure that management of the SME and associated data between machines is protected.
2	**Protecting assets**	Datapipe fully supports the requirement for customers to know the locations at which data is stored, processed and managed (including service management data). The Datapipe SME has a resilient, virtual architecture and benefits from all the characteristics of a virtualised environment. The Datapipe SME data centre (Global Switch, London East) is a Tier III specification data centre providing physical protection in the UK. All customer data can be stored, accessed and managed from the UK by UK Staff. The UK Datapipe ticketing system has DR capability in Europe.
3	**Separation between different consumers**	Separation between different consumers at all levels of the service is required to prevent malicious or compromised customers from affecting the service or data of another. Datapipe services have been designed and implemented in accordance with industry good practice, where applicable, which includes a high level of internal network segregation and strength in depth controls. There is also a Walled Garden Architecture between the SME and customer environments.
4	**Governance**	Datapipe reports against and comply with legal and regulatory reporting requirements. This requirement can usually be evidenced through our ISO27001 and PCI DSS certifications. Datapipe has a long history of compliance with industry leading security certifications and as such have developed a certified governance framework, which ensures security is at the heart of the organisation.
5	**Operational security**	Datapipe uses the shared security model concept of agreeing security responsibility boundaries. We agree early in the engagement process who is responsible for the operational security of the services above the hypervisor layer. Operational security for the SME is dealt with under our certified Information Security Management System (ISMS) and ISO27001:2013 certification. *Configuration Management* Datapipe has implemented an enterprise-level Configuration Management Database (CMDB) that is used to capture the components that form the SME. Under the shared security model Datapipe does offer these services below the hypervisor on the community platforms. If using new dedicated hosting then these also need factoring in at the design stage. *Vulnerability Management* Datapipe has in place a series of vulnerability management activities that together provide a powerful solution for early identification and remediation of vulnerabilities within its platforms. *Protective Monitoring & Security Incident Management* The Datapipe SME delivers full Security Information and Event Management (SIEM) capabilities for its platforms. Datapipe's incident management processes are

		aligned with ITIL v3. Datapipe only monitors the platform (hypervisor and below). Direct security SME console monitoring and proactive defence is carried out during core business hours. Alarms of a critical nature are immediately raised to our 24/7/365 service desk for triage & security Incident response.
6	**Personnel security**	Every Datapipe employee is subject to security clearance prior to employment which consists of checks that are Baseline Personnel Security Standard (BPSS) or equivalent. Datapipe also has a number of employees who possess SC Clearance and are willing to support further clearances if sponsored by the customer.
7	**Secure development**	Datapipe services are designed and developed to identify and mitigate threats to customer security. Our service design and any development activity is carried out in line with industry good practice regarding security. This includes coding, testing and deployment. Datapipe has in place a security systems engineering principles policy, which is aligned to the National Institute of Standards and Technology (NIST).
8	**Supply Chain Security**	Datapipe ensures that our supply chain satisfactorily supports all of the security principles that the service claims to implement. Datapipe has in place an Interested Parties and Supplier process, which is managed within the ISO27001:2013 certified ISMS.
9	**Secure consumer management**	Our service ensures consumers are securely authenticated & authorised before being allowed to view or perform management activities, report faults or request changes to the service. We also make sure that we provide sufficient confidence that other consumers cannot access, modify or otherwise affect the service management portal. This includes maintaining the need to know and least privilege principles. Consumers are not provided access to any of the management interfaces within the Datapipe SME. Consumer access is restricted to the portal, which makes use of basic authentication.
10	**Identity and authentication**	All service interfaces are constrained to authenticated and authorised individuals only over secure channels. In order to authenticate into the SME, each user must use Two-Factor Authentication, which uses a Radius Server that offloads to the Two-Factor Authentication server. From within the Datapipe SME there is a high level of network segregation, authentication of users is performed via Active Directory.
11	**External interface protection**	Within the Datapipe SME there are very few external interfaces, which are regularly scanned for vulnerabilities (interfaces exposed directly to the Internet). This has been specifically designed to provide a reduced attack plane and risk profile. This is accompanied with strict Access Control Lists (ACLs), Intrusion Prevention System (IPS) technology and provides enterprise-class stateful firewall inspection
12	**Secure service administration**	The Datapipe SME is accessed from issued desktops and/or laptops onto the virtual separated management environment. These associated authorised endpoints (laptops, desktops etc) have been subject to external testing under the Cyber Essentials Plus Scheme (CES Plus).
13	**Audit information provision to consumers**	Platform data is primarily managed by Datapipe's protective monitoring solution and retention guidelines and are aligned with PCI DSS. Service audit data can be provided as part of the service if requested.

14	**Secure use of the service by the consumer**	Datapipe provides a customer handbook that details SLAs, escalation, and acceptable use of service. Customers are also subject to full on-boarding processes, which includes project meetings, technical workshops and hands-on delivery work in collaboration with customers to ensure secure use of the service by the consumer.

PROTECTIVE MONITORING

Datapipe utilises a leading technology for our protective monitoring solution on our management system and supporting platforms. The Datapipe SIEM combines five essential security capabilities, Asset Discovery, Behavioural Monitoring, Vulnerability Assessment, SIEM and Intrusion Detection into a single management plane. Datapipe has a complete view of our platform and management estate ensuring the complete integrity of our systems by identifying potentially compromised systems and suspicious behaviour, assess vulnerabilities, correlate and analyse security event data.

Protective monitoring solutions for customer workloads vary and are dependent on the security, compliance and governance practices and processes of the particular organisation. Whilst Datapipe provides Protective Monitoring to manage risk for all our customers on our platforms and management systems; where protective monitoring is required for customer workloads, Datapipe works with an appropriate partner to meet the customer's security, compliance and risk mitigation requirements.

CERTIFICATIONS & STANDARDS

Datapipe’s platform and management system is certified or accredited to the following standards:

- **ISO/IEC27001:2013**

  The ISO 27001 standard for information security specifies the requirements necessary to establish, implement, maintain, and improve an Information Security Management System (ISMS). The certification ensures Datapipe provide a reliable platform, properly protect information, manage associated risks and demonstrates our reliability, thereby ensuring that confidentiality, integrity, and availability of information that is owned by our customers are preserved, in compliance with applicable legal and customer requirements.

- **Cyber Essentials Plus Certification**

  This certification is based on an assessment of the Cyber Essentials test cases applied to Datapipe’s external infrastructure and workstation assessment

- **PCI DSS v3.2 Certification**

  PCI DSS is the worldwide security standard set up to help businesses process card payments securely and reduce card fraud. With customers across all sectors including retail and finance.

- **ISO/IEC9001:2008 Quality Management Systems (QMS)**

Datapipe has deployed a Quality Management System (QMS) based on the ISO standards covering the design, development, implementation and ongoing support of secure, scalable enterprise grade hosted infrastructure services. The Business Management System, based on the application of the ongoing improvement lifecycle and process management, is designed to ensure the quality of Datapipe services and the efficient operation of the organisation, thereby meeting customer demands and increasing customer satisfaction

IDENTITY & AUTHENTICATION

Secure Identity and Access Management (IAM) is architected as a core principle of the Datapipe Secure Management Environment. This solution has been based on a defined Role Based Access Control (RBAC) deployment, which consists of defined roles and the minimum required privileges to perform each role. Datapipe operational staff require two-factor authentication to access the SME, with single sign on capabilities once authenticated into the SME.

Once access is gained into the SME, an additional level of authentication will be required into each customer environment. A self-signed Certificate Authority (CA) is used to authenticate the machines within the SME domain. Monitoring of IAM activity and privilege users will be conducted using Datapipe’s protective monitoring solution.

CHANGE, INCIDENT, PROBLEM & KNOWLEDGE MANAGEMENT

Change Management

The Change Management process provides a mechanism to control and manage the initiation, implementation, and review of all proposed changes to the operational IT infrastructure. This minimises the impact of change-related incidents upon service delivery. Integrated change request/release management is configured to customer requirements.

- **Logging (Capturing):** This feature ensures that all changes are tracked in a centralized repository, allowing the information to be applied to other Operations Process services.
- **Assessment:** All changes are assessed based on their impact, cost, benefit, and risk to the customer
- **Scheduling:** Changes are scheduled based on their business impact and the availability of appropriate resources needed to deploy the needed change.
- **Testing & Plans:** This ensures that all changes are appropriately tested and certified and that the appropriate implementation and remediation (fallback/ back out) plans are developed/available.
- **Communications:** Change plans, change schedules, and change status are communicated to appropriate stakeholders and affected users.
- **Reporting:** General reporting capabilities check against the repository of changes and provide trending information and specific metrics relevant to the process.
- **Governance:** Change Process Owners and a Change Advisory Board (CAB) verify and validate all changes, as well as the continual effectiveness of the Change Management Process

Incident Management

The primary objective of Incident Management is to return service to users as quickly as possible. The Incident Management process provides the tools and mechanisms for a quick recovery of service issues to the agreed service level (response and fix times). The service levels are defined within a Service Level Agreement (SLA) and assigned to calls when first logged. Incident recording, resolution, and tracking of SLAs through email notifications and escalations are central to all systems.

- **Record & Classify:** Response teams quickly record, classify, diagnose, and resolve Incidents.
- **Workarounds:** Prompt workarounds allow customers to continue with work while formal corrective and preventative actions are pursued and deployed.
- **Escalation:** Incidents are escalated to applicable support teams, system owners, and applicable management personnel. Datapipe teams can collaborate with customer teams if they require custom escalation strategies.
- **Identifying Root Cause & Problems:** If an Incident is due to an unknown cause, a Problem task is created to initiate the Root Cause Analysis and Problem Management process, which investigates and eliminates the root cause.
- **Keeping Customers Informed:** Communication tools within the portal keep customer teams informed on each Incident's status throughout Incident Management process.
- **Confirm Closure:** Confirm the closure of Incidents upon receipt of a resolution or a workaround.

Problem Management & Root Cause Analysis

The primary objectives of Problem Management and Root Cause Analysis (RCA) are to prevent future Incidents and minimise the impact of Incidents that might occur. This process analyses Incident records, uses collected process data to identify trends or significant problems, and eliminates the cause(s) permanently.

- **Identification of Needed Changes:** Problem Task resolution and elimination of Root Cause often call for a Change to a configuration item in the customer's environment, allowing Datapipe to proactively identify needed Changes.
- **Continual Service Improvement:** An RCA Committee will review all pertinent information and stakeholders involved, and ensure timelines of the response are appropriate.
- **Mitigation:** Resolving Problem Tasks prevents related Incidents from occurring in the future.

Knowledge Management

Our portal features a built-in knowledge base that allows Datapipe staff to access various customer-specific support information, including customized Solution Escalation Action Plans (SEAPs), customer device group information, and customer device information.

- **Communication & Awareness:** Support information from various sources is continually synchronized and imported into the portal. This helps ensure that Datapipe's support teams have access to the most current and accurate information at all times.
- **Customised Support Materials:** Specific knowledgebase articles can be accessed directly from a ticket request via the portal's web interface.
- **Controlled Information:** Knowledgebase articles can only be edited by the service delivery team, and edited articles must be reviewed and approved before being published.

By providing an integrated view into a customer's entire infrastructure, our portal allows Datapipe to continue meeting the highest service level expectations.

DATA PROTECTION

Protecting our customer's data is fundamental to Datapipe's business and we therefore use a multi-layered approach to ensuring that data is protected in transit, at rest and when decommissioned.

In transit

Datapipe operates using only secure or protected protocols, which ensures that management of the SME and associated data between machines is protected. Authentication data that is used across the SME is performed using an initial two-factor authentication solution, using encryption ciphers that meet requirements of the Payment Card Industry Data Security Standard (PCI DSS). Any traffic traversing non-owned circuits is encrypted and there are a series of IPSec tunnels, which are configured in accordance with CESG PRIME guidance where appropriate.

Datapipe works with customers to ensure that data in transit protection is sufficient for the type of data being transmitted. Secure protocols (such as TLS or IPSec) are always recommended as a base level of protection as it removes the doubt of meeting compliance requirements.

At rest

Management Data at rest is protected via physical security mechanisms, as the storage arrays are located within our highly secure data centre. We employ layers of controls such as a request and approval from Datapipe Service Desk, physical security controls of the building, proximity readers for data halls, locked cage and additional locked racks. Any movement of equipment must follow Datapipe's ISO27001 requirement, which involves specific approval from Datapipe management.

Data at rest protection within customer virtual machines and applications would be architected to meet the specific requirements of the customer working with UKCloud.

Disposal

When equipment is disposed of, Datapipe uses multiple partners to perform secure physical destruction services. Dependent on business requirements, this equipment is disposed of either on-site or sent to a secure site. Each physical asset is tagged and after destruction is performed, Datapipe obtains certificates of physical destruction.

Equipment disposal must achieve and meet the Destruction outcomes that are highlighted within the CPNI Secure Destruction of Sensitive Items Standard, Annex A.

CLOUD SERVICE BUILDER

We understand that each enterprise application has its own set of technical and service requirements that must be addressed on an individual basis. Many cloud platforms force you to compromise, but Enterprise Compute Cloud is highly configurable, and gives you the flexibility to use different service levels, VM sizes, security domains, connectivity and data protection options.

To help you choose the right combination of options for your solution, consider the following:

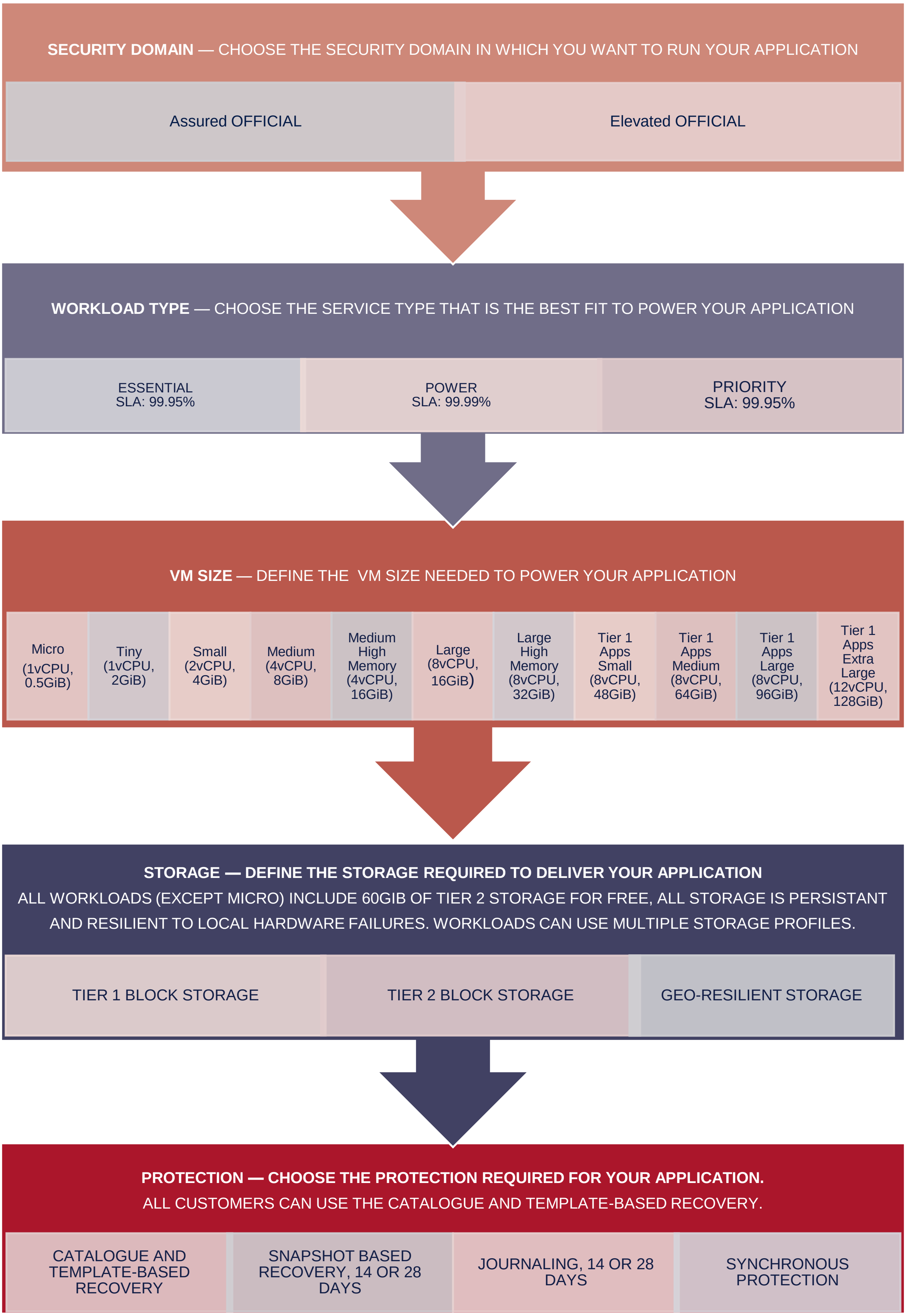
- **What are you your workload characteristics?** Tailor the compute characteristics of the VM to support the requirements of your workload. Some workloads require the highest levels of resilience and performance, some are sensitive to changing conditions, whereas others merely require access to on-demand infrastructure resources.
- **What type of storage do you need?** Does your workload require high-performance or longer-term retention storage? Choose from a variety of options and even deploy mixed environments to deliver exactly what you need.
- **What type of data protection does your application require?** Whether you're driven by recovery point or recovery time, you can choose the right level of automated, on-platform protection for your environments.

As a guide to what's achievable, the table below provides a high-level overview of some of the more common deployment combinations on the UKCloud platform.

COMMON DEPLOYMENT COMBINATIONS

YOUR WORKLOAD CHARACTERISTICS	UKCLOUD RECOMMENDS		
	WORKLOAD TYPE	STORAGE OPTION	PROTECTION OPTION
LOWER-PRIORITY WORKLOADS, SUCH AS TEMPORARY APPLICATIONS, DATA PROCESSING OR SYSTEM MODELLING TASKS	**ESSENTIAL**	**TIER 2 BLOCK STORAGE**	**CATALOGUE AND TEMPLATE-BASED RECOVERY**
	VMs can have contended resource allocation. Automated rebalancing is enabled to ensure the workload receives the requested performance.	General all-purpose storage providing a balance between performance and cost.	Configuration management solution can re-provision stateless servers to a new VM when required, using standard, and catalogue-based VM templates.
KEY WORKLOADS THAT ARE RESOURCE INTENSIVE SUCH AS WEB AND APPLICATION WORKLOADS MID-SIZED DATABASES, AND CACHING SERVICES	POWER	TIER 2 BLOCK STORAGE	SNAPSHOT PROTECTION
	VMs have an uncontended compute (CPU/GiB) resource allocation. Automated rebalancing is enabled to pre-emptively optimise performance and availability.	General all-purpose storage providing a balance of performance and cost.	Automated daily backup solution of the entire VM. Simple backup protection for data that has an RPO of 24 hours.
CRITICAL WORKLOADS HANDLING IMPORTANT BUSINESS PROCESSES THAT BENEFIT FROM A STEADY STATE OF OPERATION WITH REDUCED WORKLOAD REBALANCING, VM MOBILITY AND CONTENDED RESOURCES	PRIORITY	TIER 1 BLOCK STORAGE	JOURNALING-BASED PROTECTION
	VMs have an uncontended compute (CPU/GiB) resource allocation. Automated rebalancing is configured to reduce workload movement around the platform, reducing workload disruption.	Fast storage optimised for data warehouses, busy transactional databases and other high IO workloads.	A non-invasive disaster recovery solution with configurable recovery points, providing near real-time data protection. Ideal for protecting important data with a high rate of change.

You can build completely tailored solutions by mixing and matching service options as outlined in the following diagram. The choice doesn't lock you to one service or size and you can always change it later.



SECURITY DOMAIN — CHOOSE THE SECURITY DOMAIN IN WHICH YOU WANT TO RUN YOUR APPLICATION

Assured OFFICIAL	Elevated OFFICIAL

WORKLOAD TYPE — CHOOSE THE SERVICE TYPE THAT IS THE BEST FIT TO POWER YOUR APPLICATION

ESSENTIAL SLA: 99.95%	POWER SLA: 99.99%	PRIORITY SLA: 99.95%

VM SIZE — DEFINE THE VM SIZE NEEDED TO POWER YOUR APPLICATION

Micro (1vCPU, 0.5GiB)	Tiny (1vCPU, 2GiB)	Small (2vCPU, 4GiB)	Medium (4vCPU, 8GiB)	Medium High Memory (4vCPU, 16GiB)	Large (8vCPU, 16GiB)	Large High Memory (8vCPU, 32GiB)	Tier 1 Apps Small (8vCPU, 48GiB)	Tier 1 Apps Medium (8vCPU, 64GiB)	Tier 1 Apps Large (8vCPU, 96GiB)	Tier 1 Apps Extra Large (12vCPU, 128GiB)

STORAGE — DEFINE THE STORAGE REQUIRED TO DELIVER YOUR APPLICATION

ALL WORKLOADS (EXCEPT MICRO) INCLUDE 60GIB OF TIER 2 STORAGE FOR FREE, ALL STORAGE IS PERSISTANT AND RESILIENT TO LOCAL HARDWARE FAILURES. WORKLOADS CAN USE MULTIPLE STORAGE PROFILES.

TIER 1 BLOCK STORAGE	TIER 2 BLOCK STORAGE	GEO-RESILIENT STORAGE

PROTECTION — CHOOSE THE PROTECTION REQUIRED FOR YOUR APPLICATION.

ALL CUSTOMERS CAN USE THE CATALOGUE AND TEMPLATE-BASED RECOVERY.

CATALOGUE AND TEMPLATE-BASED RECOVERY	SNAPSHOT BASED RECOVERY, 14 OR 28 DAYS	JOURNALING, 14 OR 28 DAYS	SYNCHRONOUS PROTECTION

COMMERCIALS

Our standard commercial model describes a contractual relationship with Datapipe, with UKCloud as sub-contractor. This is the natural model for a commercial relationship to take as Datapipe maintains overall responsibility for service availability, of which UKCloud infrastructure is part. It also allows Datapipe to on-board services in an effective and efficient manner, ensuring services are fit for purpose and achieve objectives set during procurement.

Unit-based pricing for the compute is outlined below, broken down into UKCloud and Datapipe services. For the avoidance of doubt, Datapipe will not make any margin on UKCloud services - instead these flow through at cost alongside Datapipe's infrastructure management and service charges.

HOW MUCH DOES IT COST?

Building your application environment with UKCloud and Datapipe is easy, and our transparent pricing lets you understand all the components of your solution and assess the value it offers. The process mirrors the steps defined in the Cloud Service Builder in the service description documents to help you specify your solution and calculate the costs.

Enterprise Compute Cloud Assured OFFICIAL Domain

	VM (per hour)						VM Protection (per hour)[2]				
	2GHz vCPU	RAM (GiB)	ESSENTIAL	POWER	PRIORITY		14-day Snapshot	28-day Snapshot	14-day Journaling	28-day Journaling	Synchronous [5]
Micro[1]	1[1]	0.5	£0.01	£0.02	£0.030		£0.02	£0.02	£0.10	£0.10	£0.22
Tiny	1	2	£0.03	£0.09	£0.135		£0.04	£0.04			£0.18
Small	2	4	£0.04	£0.12	£0.180		£0.06	£0.06			£0.20
Medium	4	8	£0.06	£0.22	£0.330	+	£0.08	£0.08			£0.19
Medium High Memory	4	16	£0.14	£0.35	£0.520		£0.08	£0.08			£0.30
Large	8	16	£0.18	£0.45	£0.675		£0.18	£0.18	£0.20	£0.20	£0.40
Large High Memory	8	32	£0.35	£0.55	£1.125		£0.25	£0.25			£0.80
Tier 1 Apps Small	8	48	£0.50	£0.60	£1.575		£0.35	£0.35			£1.05
Tier 1 Apps Medium	8	64	£0.70	£0.99	£2.085		£0.41	£0.41			£1.26
Tier 1 Apps Large	8	96	£0.95	£1.45	£2.675		£0.70	£0.70			£1.90
Tier 1 Apps Extra Large	12	128	£1.30	£2.30	N/A		£0.75	£0.75			N/A

Block Storage (per GiB/per month)[6] [7]	
Tier 1	£0.25
Tier 2 [4]	£0.10
Geo-resilient [5]	£1.10

+

Block Storage Protection (per GiB/per month)				
£0.20	£0.30	£0.60	£0.90	N/A
£0.10	£0.20	£0.30	£0.45	N/A
Inc.	£0.15	N/A	N/A	Inc.

+

Licensing										
VM Size	**Microsoft Windows Server OS**		**Microsoft SQL Standard** [3]		**Microsoft SQL Enterprise** [3]		**Microsoft RDS**		**Red Hat Enterprise Linux**	**Bring Your Own Subscriptions**
	£ / hour / VM	**Academic £ / hour / VM**	**£ / hour / VM**	**Academic £ / hour / VM**	**£ / month / VM**	**Academic £ / month / VM**	**SAL Licence per month**	**Academic SAL Licence per month**	**Subscribe through UKCloud £ / hour / VM**	
Micro, Tiny VM	£0.012	£0.002	£0.266	£0.054	£725.70	£195	£4.19	£0.44	£0.04	No charge
Small VM	£0.023	£0.003								
Medium VM	£0.046	£0.007								
Medium High Memory	£0.046	£0.007								
Large VM, Large High Memory, Tier 1 Apps	£0.135	£0.020	£0.513	£0.15	£1460.25	£390			£0.09	

[1] Micro VM pricing has 500MHz, 10GiB of Tier 2 storage; all other VMs include 60GiB of Tier 2 storage.
[2] You must choose the same protection option for both VMs and storage.
[3] SQL Enterprise is bought on a monthly basis. You must report the quantity of SQL Standard and Enterprise licences you need each month to UKCloud.
[4] 60GiB of Tier 2 storage is included in the pricing for all VMs whilst they are powered on, except for Micro. For VMs in powered-off state, consumed storage will be charged at the prevailing rate.
[5] Geo-resilient storage and synchronous protection must be purchased together.
[6] Consumed storage includes VM catalogue images and snapshots.
[7] VMs with additional allocated storage will be charged at the prevailing storage rate regardless of their powered-on/off state.
[8] If you wish to host Oracle solutions on our platform, please consult our Cloud Architects, or consider our Dedicated Compute or Enterprise Compute Cloud – Oracle services to avoid licensing issues.

Enterprise Compute Cloud Elevated OFFICIAL Domain

VM (per hour)					
	2GHz vCPU	RAM (GiB)	ESSENTIAL	POWER	PRIORITY
Micro[1]	1[1]	0.5	£0.02	£0.04	£0.060
Tiny	1	2	£0.05	£0.12	£0.180
Small	2	4	£0.06	£0.15	£0.225
Medium	4	8	£0.10	£0.26	£0.390
Medium High Memory	4	16	£0.18	£0.40	£0.600
Large	8	16	£0.22	£0.50	£0.825
Large High Memory	8	32	£0.35	£0.75	£1.350
Tier 1 Apps Small	8	48	£0.60	£1.05	£1.800
Tier 1 Apps Medium	8	64	£0.80	£1.39	£2.375
Tier 1 Apps Large	8	96	£1.10	£1.85	£3.300
Tier 1 Apps Extra Large	12	128	£1.45	£2.65	N/A

+

VM Protection (per hour)[2]				
14-day snapshot	28-day snapshot	14-day Journaling	28-day Journaling	Synchronous [5]
£0.02	£0.02	£0.10	£0.10	£0.28
£0.07	£0.07			£0.31
£0.12	£0.12			£0.36
£0.19	£0.19			£0.41
£0.25	£0.25			£0.65
£0.35	£0.35	£0.20	£0.20	£0.85
£0.60	£0.60			£1.40
£0.85	£0.85			£1.90
£1.05	£1.05			£2.40
£1.55	£1.55			£3.50
£1.60	£1.60			N/A

+

Block Storage (per GiB/per month)[6] [7]	
Tier 1	£0.25
Tier 2 [4]	£0.10
Geo-resilient [5]	£1.10

+

Block Storage Protection (per GiB/per month)				
£0.20	£0.30	£0.60	£0.90	N/A
£0.10	£0.20	£0.30	£0.45	N/A
Inc.	£0.15	N/A	N/A	Inc.

+

Licensing										
VM Size	Microsoft Windows Server OS		Microsoft SQL Standard [3]		Microsoft SQL Enterprise [3]		Microsoft RDS		Red Hat Enterprise Linux	Bring Your Own Subscriptions
	£ / hour / VM	Academic £ / hour / VM	£ / hour / VM	Academic £ / hour / VM	£ / month / VM	Academic £ / month / VM	SAL Licence per month	Academic SAL Licence per month	Subscribe through UKCloud £ / hour / VM	
Micro, Tiny VM	£0.012	£0.002	£0.266	£0.054	£725.70	£195	£4.19	£0.44	£0.04	No charge
Small VM	£0.023	£0.003								
Medium VM	£0.046	£0.007								
Medium High Memory	£0.046	£0.007								
Large VM, Large High Memory, Tier 1 Apps	£0.135	£0.020	£0.513	£0.15	£1460.25	£390			£0.09	

[1] Micro VM pricing has 500MHz, 10GiB of Tier 2 storage; all other VMs include 60GiB of Tier 2 storage.
[2] You must choose the same protection option for both VMs and storage.
[3] SQL Enterprise is bought on a monthly basis. You must report the quantity of SQL Standard and Enterprise licences you need each month to UKCloud
[4] 60GiB of Tier 2 storage is included in the pricing for all VMs whilst they are powered on, except for Micro. For VMs in powered off state, consumed storage will be charged at the prevailing rate.
[5] Geo-resilient storage and synchronous protection must be purchased together.
[6] Consumed storage includes VM catalogue images and snapshots.
[7] VMs with additional allocated storage will be charged at the prevailing storage rate regardless of their powered-on/off state.
[8] If you wish to host Oracle solutions on our platform, please consult our Cloud Architects, or consider our Dedicated Compute or Enterprise Compute Cloud – Oracle services to avoid licensing issues.

Managed Service Uplift

The Datapipe Managed Service for UKCloud is calculated as a percentage uplift of the total UKCloud spend under management, with a minimum service fee of £1,000.

Tiers	% Fee	From	To
Tier 1	30%	£0	£20,000
Tier 2	27%	£20,000	£40,000
Tier 3	24%	£40,000	£80,000
Tier 4	21%	£80,000+	

The managed service fee is tiered, so the fee for the first £20,000 of spend in a given billing month is calculated at the tier one percentage, the next £20,000 of UKCloud spend in the same month is calculated at the tier two percentage, etc.

WHAT'S INCLUDED

Managed UKCloud Enterprise Compute Cloud includes as standard:

- Virtual firewalls
- IPsec and SSL VPN/SDN. Create secure connections between users and other environments using a variety of included tunnelling technologies.
- VMware HA (High Availability) protection
- Basic load balancing
- Persistent storage
- Free DDoS-protected internet access

OPTIONAL EXTRAS

Service*	Unit	Monthly Service Charge (£)
Protective Monitoring	Solution	On request
Identity & Authentication	Solution	On request
Compliance & Audit Support	Solution	On request
Customer Application Management	Solution	On request
Implementation & Migration**	Service	On request

**Please see Lot 3 for Datapipe's Cloud Support: Planning and Setup & Migration Services for more detail of our capability.

LICENSING

The standard terms and conditions from Microsoft state that if you want to run a Windows Server operating system in the cloud, you must license it via the Government Service Provider Licence Agreement (G-SPLA), which must be provided by UKCloud. Microsoft Developer Network (MSDN) and Windows desktop operating system licences are generally not permitted by Microsoft's terms and conditions.

UKCloud offers the option for you to bring your own Red Hat licensing, or certain Microsoft application licensing under Microsoft Mobility using software assurance.

If you're licensing Microsoft Windows Server OS, Microsoft SQL Server, Microsoft RDS or Red Hat Enterprise Linux, licensing charges apply. See the pricing guide for details.

CONNECTIVITY OPTIONS

UKCloud provides one of the best connected cloud platforms for the UK public sector. We offer a range of flexible connectivity options that enables access to our secure platform by virtually any government user community or system. The variety of government, public and private networks is shown in the following diagram:

Connection type	DDoS-protected internet	PSN Assured	PSN Protected	N3/HSCN	Janet	Hybrid Connect	RLI
Starter pack price (per month)	FREE	FREE	£250	£250	FREE	N/A	N/A
Subsequent price (per GB outbound)	FREE	£0.25	£1.00	£1.00	FREE	N/A	N/A
Set-up fee	N/A	N/A	N/A	N/A	N/A	£2,000	£2,000

PSN Assured: The general-purpose unencrypted Public Services Network. Connected to most central, local and devolved government organisations.

N3/HSCN: The NHS National Network. Connected to all health and social care organisations nationwide.

Janet: The UK's research and education network. Connected to all education organisations and research councils.

PSN Protected: Encrypted higher-security Public Services Network. Connected to legacy IL3 networks including GSI, PNN, CJX, GSE, GSX and others.

HybridConnect: Supports a variety of flexible private connectivity options. Enables connection to Crown Hosting (CHDC) and other third-party facilities.

RLI: A high-security network for defence and industry partners. Connection to RLI is subject to extensive vetting and approval from the MoD.