MANAGED SECURE PRIVATE CLOUD

(Multi Tenant)

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's managed multi-tenant private cloud gives public sector organisations access to highly efficient, secure infrastructure at an affordable price point. Datapipe's private cloud services are straightforward and extremely flexible, building on a range of standardised solutions with smart customisation options that deliver customer requirements as cost effectively as possible.

AT A GLANCE

UK SOVEREIGN	STRAIGHTFORWARD MIGRATION & IMPLEMENTATION
An assured, secure cloud platform delivered from two secure UK data centres by a UK-headquartered company with BPSS and UK Government security-cleared staff	Experienced delivery of efficient transition and transformation projects in the public sector. Straightforward and pain free process, with a clear path to benefit
DISASTER TOLERANT	**OPTIMISED FOR OFFICIAL**
Two Tier 3+ specification UK data centres separated by more than 70km and securely connected by high-bandwidth, low-latency dedicated connectivity enabling synchronous replication	Fully aligned with the CESG 14 Cloud Security Principles, ideal for all data classified at OFFICIAL and legacy IL0–IL3 solutions
FLEXIBLE CONNECTIVITY	**BROAD RANGE OF OPTIONS**
Connect to the Internet and PSN (Assured service) as an option. Other aggregated chargeable services include DDoS, PSN Protected service, Janet, N3 or legacy networks (including PNN)	A range of virtual machine configuration options including dual site virtual machines (RPO 0) or single site. Multi cloud or hybrid

Typical Use Cases

- High performance, secure compute infrastructure for line-of-business applications on a cost-efficient consumption model
- Alternative to more costly dedicated private cloud solutions whose only advantage would be contention guarantees at large scale, not additional security or compliance
- Migrate away from inflexible IT environments for specific applications/ workloads
- Enables rapid infrastructure deployment for new projects and ventures
- Secure Disaster Recovery environments to replicate primary workloads

WHY 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.

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's secure, multi tenant private cloud can be integrated with other technology solutions and environments from different providers and is fully portable when/ as requirements change over time. Datapipe's multi tenant private cloud is based on reference architectures from our technology partners EMC, VMware and Dell. These pre-approved designs are built with security in mind to ensure customer data is never shared and always logically separated from other Datapipe customers. 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.

PCI DSS COMPLIANT | CERTIFIED ISO 9001:2008 COMPANY | Information Security Management System ISO 27001 Certified | CYBER ESSENTIALS PLUS | PSN Public Services Network

KEY PLATFORM FEATURES

Datapipe's on-demand infrastructure ensures that users and customers get the best possible experience from systems and services. We give public sector organisations access to a highly flexible 'pay as you grow' model that precisely aligns spend with evolving needs, with zero upfront capital investment.

The solution allows network, compute and storage to be dynamically adjusted to cope with fluctuations in demand by software and services, delivering powerful management and monitoring up to the operating system (OS) layer.

Datapipe has a significant presence in multiple Tier 3+ specification data centres in the UK and offers single or dual site configurations. Datapipe's highly resilient infrastructure ensures that services continue to operate optimally, even in the event of the total loss of a data centre (in the case of dual site configuration). High performance virtual servers come with a variety of management options and can be integrated with colo and other cloud services managed cloud services.

Datapipe's Multi Tenant Private Cloud is an enterprise-grade virtual server and storage platform, spanning two physical data centres and capable of operating as a single infrastructure. The flexibility of this system enables us to offer a blend of services and service levels that cater for diverse requirements, from core critical production systems that demand high levels of resilience through to temporary test and development systems. For critical production systems, our innovative platform design enables Datapipe to migrate operational virtual servers seamlessly between physical data centre facilities with zero loss of service.

This design also enables failover and backup between data centres, providing HA and disaster avoidance (DA). The data centres are connected via Datapipe's own low latency dark fibre metro network: a complete round trip between data centres takes sub-2mS, enabling either synchronous or asynchronous data replication.

BACKUP, RESTORE & DR FACILITY

We offer a range of data protection offerings from disk based backup through to crash-consistent replication enabling restoration to any point in time (effectively a rewind service for the most critical data). We will work with public sector organisations to ensure the protection is appropriate to the requirements of workload and business. Included as standard is backup of the operating system element of the VM to enable SLAs to be met. Further backups are on a simple £/ GB/ Month basis. Longer retention (including out to tape) is also available.

Spread across two data centres, the combination of data protection technologies and infrastructure replication means we can offer the most stringent levels of service for Backup and Disaster Recovery.

SLAS & KPIS

Our availability SLA for a single site VM is 99.9%. For dual site, it is 99.99%. These SLAs are underpinned by a straightforward service credit model in line with G Cloud guidelines.

EVENT TYPE	DESCRIPTION	DATAPIPE PERFORMANCE STANDARD	KPI
Severity Level 1 Event	Initial response to event reported by Datapipe's monitoring system or Client	10 mins	Less than 3 cumulative Incident Management Failures within a month
	Datapipe will start to work on the resolution	10 mins	
	Status update	Every 60 mins	
Severity Level 2 Event	Initial response to event reported by the monitoring system or Client	10 mins	
	Datapipe will start to work on the resolution	30 mins	
	Status update	Every 2 hrs	
Immediate Support Request	Initial response	5 mins	
	Datapipe will start to work on the resolution	5 mins	
	Status update	Every 60 mins	

SUMMARY FEATURES & BENEFITS

FEATURES	BENEFITS
FLEXIBLE MANAGED DEPLOYMENT	Migrate away from inflexible IT environments for specific applications/ workloads. Quickly on-board and off-board instances as requirements change, with new projects and ventures. Integrate with other cloud & physical environments rapidly & securely
SMART-ALIGNED TO APPLICATION & WORKLOAD PROFILES	Align organisational requirements with IT spend for the optimal blend of price/performance
EASY SCALE	Scale private cloud services up and down as requirements change in a controlled way
MODULAR APPROACH	Can be integrated with other technology solutions from different providers

SECURITY	Deliver appropriate security levels on a per application/ workload basis. This can include Secure Disaster Recovery environments to replicate primary workloads
STRONG SUPPORT FOR DATABASE ENVIRONMENTS	Performant, secure and workload-optimised databases underpinning application delivery to provide users with the optimum experience

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.

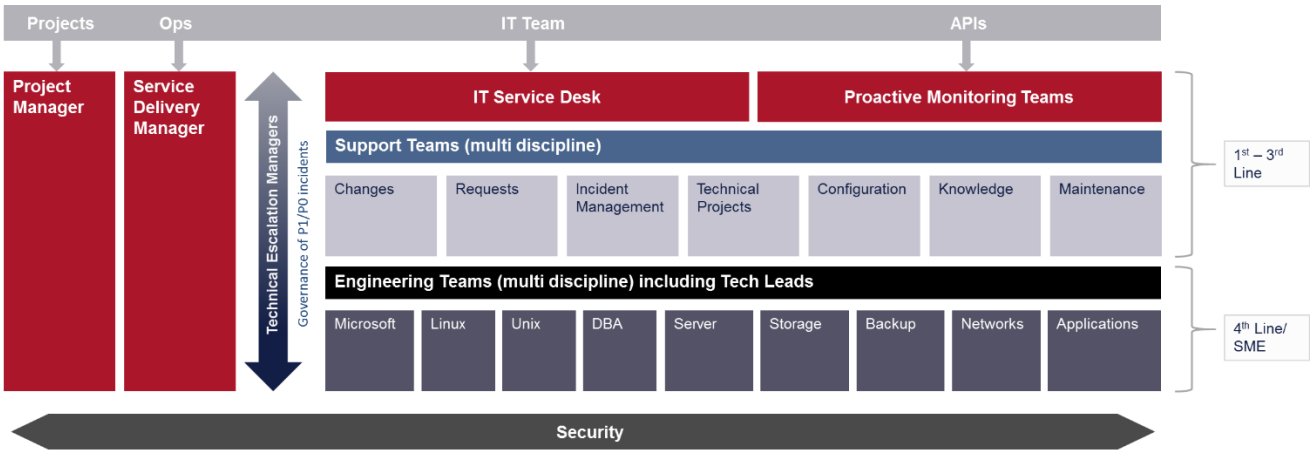
This structure is proven over time to deliver an outstanding customer experience and ultimately drive value based on our customer's technical and business requirements.

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.

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

Datapipe can manage 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, MongoDB 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 those 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.

Database management is optional and incurs an additional charge. Please refer to the commercial section for details.

BACKUP

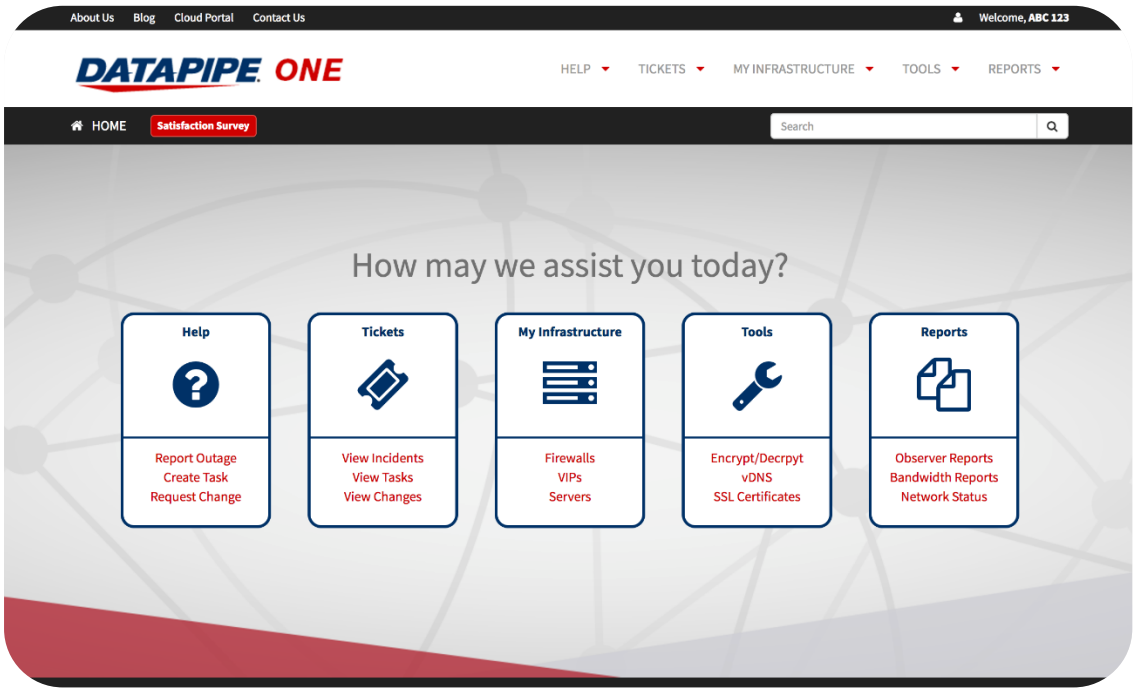
Datapipe will provide fully managed backup of all workloads hosted within the environment. The method of backup will vary across the environment and is workload dependent. For the most part, Agentless API based (snapshot) backups will be taken to provide a restore point for workloads.

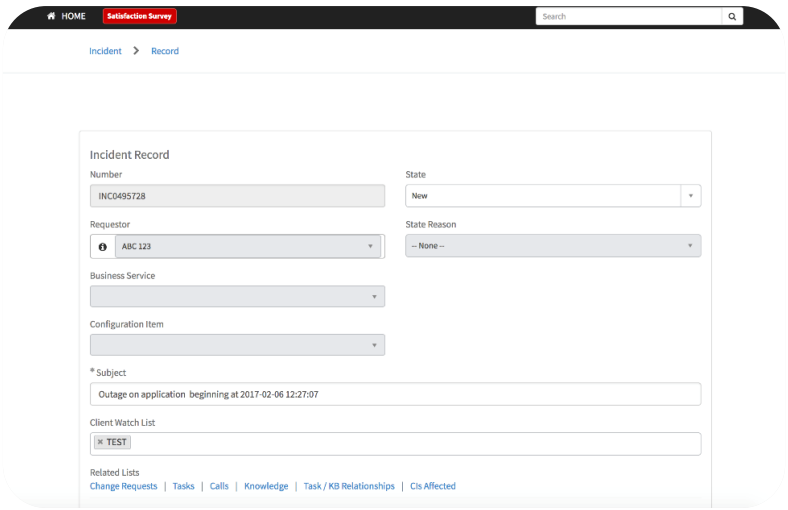
Backups will provide for a standard RPO of 24 hours (lower for transactional technologies where log backups are also taken). Longer retention periods are available if needed.

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





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.

ONBOARDING & OFFBOARDING

Onboarding

Datapipe has years of experience on-boarding customers into our virtual and cloud infrastructure environments. We walk customers through all considerations (typically including network connectivity and migration options) as requirements develop, ensuring we balance risk vs cost vs timescales in the right way for the customer's organisation.

Datapipe's proven, expert service management delivers a single point of contact for customer teams. Our Service Delivery Managers are responsible for the running of services and create custom engagement schedules for review and discussion. The Service Delivery Manager also collaborates with customers to create a custom handbook, which clearly lays out all information, contacts and processes relating to the daily management of environments. Your SDM will also provide one-on-one training to ensure a high level of comfort and familiarity with our interfaces and portals. This can be achieved over a WebEx for large distributed groups of end users or at your premises, depending on your preference.

Offboarding

Where a customer feels the need to switch providers, we will work with them to expedite the off-boarding of services to another environment. Datapipe's solutions are all based on standardised infrastructure and software, with robust migration processes and consistent documentation that make knowledge transfer straightforward and complete.

As standard, Datapipe will provide secure access to third parties to extract customer data and application configurations. Users can extract their data across the network via VPN or other secure network protocol. Snapshots of virtual machine images can be provided if required which can then be

transferred across a secure link. In the event a live migration of virtual machines or database data is required, replication services may be configured, subject to analysis by Datapipe, which may incur additional costs.

Design and service documentation is located on the Datapipe portal and can be downloaded to provide a permanent record. Other documentation, where available or feasible to produce, can be provided on request. Depending on the customer's target end state and specific schedule, there may be additional professional services charges applicable to help ensure that the migration and cutover of services to the new provider are aligned precisely with requirements.

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.

COMMERCIALS

The table below shows the standard components required to deliver virtual machines on Datapipe's multi-tenant private cloud platform or the dedicated compute platform.

Customers are able to configure the virtual machine in line with the requirements of their applications and workloads, ensuring they drive the best value from their cloud based service. In the configurator below, we provide the 'per unit' pricing to allow public sector organisations to specify the number of units required to meet a given configuration.

The unit rate below can be used to calculate the solution cost based on the infrastructure components required, licensing and any further service components.

Should you require further help on building the right solution for you and your teams, please contact a Datapipe representative.

Service Line	Resource Unit	Single Site Monthly Charge	Dual Site Monthly Charge
Infrastructure Components: Monthly Charges			
VM (managed to Operating System)	Server	£80.00	£105.00
vCPU (single site)	vCPU	£3.00	£5.00
Memory (single site) including VMware licensing	GB RAM	£6.00	£8.20
Platinum Storage	GB	£0.60	£1.20
Gold Storage	GB	£0.35	£0.70
Silver Storage	GB	£0.17	£0.34
Bronze Storage	GB	£0.08	£0.16
Managed Backup	GB	£0.14	£0.28
Managed Dedicated Compute Server (substitutes vCPU & Memory)	Server	£665.00	
VMWare Licensing for Dedicated Compute Server	GB RAM	£3.68	
Software Components: Monthly Charges			
SQL Standard 2012 (GSPLA)	Licence 2-pack	£96.00	
SQL Enterprise 2012 (GSPLA)	Licence 2-pack	£369.00	

Service Line	Resource Unit	Single Site Monthly Charge	Dual Site Monthly Charge
Other Services & Components: Monthly Charges			
Internet Provision	Mbit/s	£3.00	
Data Centre Hosting – Rack with 3kW power	Position	£690.00	
Data Centre Hosting - Additional Power	kW	£230.00	
Additional VLAN Allocation	VLAN	£10.00	
Resilient Connectivity over Dark Fibre	DWDM	£300.00	

WHAT'S INCLUDED

The following is included in the managed service:

- Operating System Server management including
  - Server build and test
  - Security patching
  - Fulfilment of customer-requested OS related change requests
  - Anti-malware deployment and management
  - Monitoring, reporting and resolution of errors and events generated by the operating system
  - Capacity management, CPU / RAM / Disk
  - Performance analysis & management
- 24*7 Service Desk (Incident, problem and change)
- ITIL service management and service reporting
- Preventative maintenance

OPTIONAL EXTRAS

Service*	Unit	Monthly Service Charge (£)
Standard Database Monitoring & Management	Per Instance	£400
Standard Active Directory Infrastructure Monitoring & Management	Per Domain	£300
Standard Exchange Management	Solution	£400
Standard VPN Management	VPN	£150
Standard Site to Site VPN Management	VPN	£150
Standard Cisco Firewall Management	Firewall	£180
Standard Switch Management	Switch	£125
Standard Load Balancer Management	Load Balancer	£180
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

*Where managed services are considered 'non-standard', referenced as 'on request' above or not covered in this table, Datapipe will charge the services through our SFIA rate card on a one-time charge basis or through monthly service bundles.
**Please see Lot 3 for Datapipe's Cloud Support: Planning and Setup & Migration Services for more detail of our capability