SECURE MANAGED CLOUD: AMAZON WEB SERVICES (AWS)

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 secure, managed access to Amazon Web Services (AWS) platforms and services, providing you with on-demand, scalable compute, storage and network resources to deliver transformational projects and digital solutions.

This Service Definition covers **Datapipe's Secure Managed AWS Cloud** offering.

AT A GLANCE

THE BEST OF G CLOUD	MEASURED USAGE
AWS services delivered by Datapipe, with enterprise-grade Datapipe service management wrap	True consumption-based pricing from just 1p per virtual machine per hour from the world's largest public cloud ecosystem
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 availability zones with a service management wrap by a UK-based company with UK Government security-cleared staff
DISASTER TOLERANT	**OPTIMISED FOR OFFICIAL**
Multiple UK availability zones securely connected by high-bandwidth, low-latency dedicated connectivity enabling near synchronous replication	Fully aligned with the CESG 14 Cloud Security Principles, ideal for all data classified at OFFICIAL (including OFFICIAL SENSITIVE) and legacy IL0–IL3 solutions
EXTENSIVE ECOSYSTEM	**CONTINUOUS INNOVATION**
Large number of AWS services to provide customers with a flexible, extensible ecosystem for building digital solutions	Rapidly evolving service features rolled out regularly, providing customers with new choices and options

Typical Use Cases

- Organisations looking to deploy digital solutions that harness a flexible and extensive ecosystem of services with true elasticity
- 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
- Organisations looking for a cost effective disaster recovery option
- Channel/ intermediary organisations including Systems Integrators and ISVs who need specialist infrastructure skills to deliver Government contracts.

WHY AWS & 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 Europe (known previously as Adapt Services Ltd) has 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 & AWS together offer the optimal blend of enterprise-grade, commercially critical production delivery and deep public sector knowledge and experience. On AWS’s foundation of commodity infrastructure services and an extensive ecosystem of supportive 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 AWS’s class-leading public cloud ecosystem.

Why Datapipe is your perfect managed cloud for AWS partner:

- **Talent & experience:** Access highly skilled engineers experienced in delivering Amazon services to enterprises across a number of sectors since 2010.
- **Security specialism:** Our deep expertise delivers advanced protection and threat defence in the public cloud with award-winning access and audit controls.
- **People that understand your business:** Named commercial and technical account management from a proactive expert service team that understands your estate inside out.
- **Powerful hybrid solutions:** Integrate your AWS estate with your private cloud and legacy environments for the optimal managed hybrid solution via Direct Connect.
- **DevOps enablement:** Prioritising your application roadmap and product strategy by supporting a dynamic, fluid, rapid rate of change for continuous integration & deployment.

Customer value	**AWS - managed on your terms, integrated into your business**	**Design, migration & hybrid integration support**	**Scalable security options that work hard for your business**	**Strategy & insight services to power the next step**
	A custom blend of people and automation that supports the way your business works Proactive, cloud-native managed service for AWS with enhancement options Rock solid commercial and technical governance with custom SLAs that reflect the business criticality of your workloads	Immediate access to AWS Certified and Accredited professionals to architect and execute your move to the cloud Expert workload migration services including engineering, provisioning & configuration management Hybrid capabilities for customised environments including AWS, private cloud or traditional IT	Take your infrastructure security policies and profiles into the public cloud safely and confidently Strengthen your defences with toughened, award-winning audit and access controls Maintain controlled compliance	AWS Professional Services proven to accelerate cloud adoption & implementations Plan your journey, optimise your existing estate or drive more business value from your investment Assess your business readiness and maturity for AWS: build roadmaps, test concepts, get expert opinion
Our role	**Creating custom journeys that offer public sector organisations more business value**	**Putting the right workloads on the right platforms in the right way**	**Consultative approach + advanced security skills**	**Expertise & experience wherever you are on the journey to the cloud**

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):

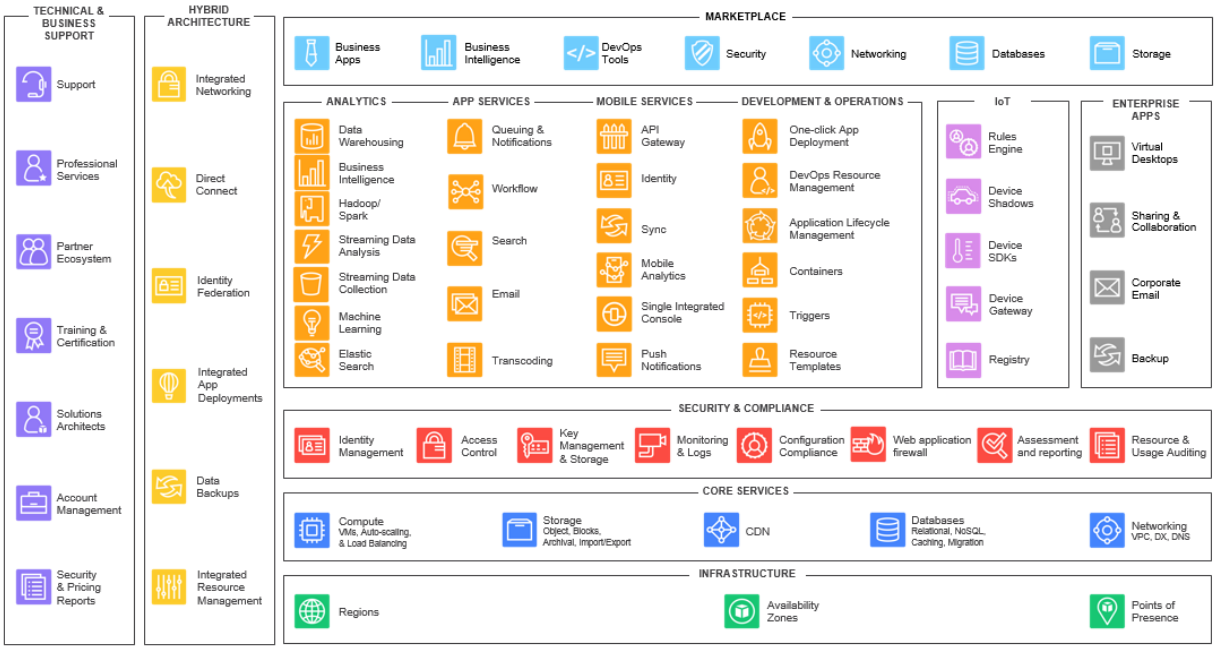
Ministry of Justice | Cabinet Office | Department for Environment Food & Rural Affairs | Department for Culture Media & Sport | Department for Transport

Datapipe is ISO27001:2013, ISO9001:2008 and PCI DSS 3.2 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 AWS

Amazon launched Amazon Web Services, Inc. (AWS) so that other organisations could benefit from Amazon's experience and investment in running a large-scale, distributed, transactional IT infrastructure. AWS has been operating since 2006 and currently supports an almost limitless variety of workloads for millions of active customers around the world.

The AWS Cloud is uniquely positioned to provide scalable, cost-efficient solutions to the UK public sector, helping find ways cloud services can be employed to meet mandates, reduce costs, drive efficiencies, and increase innovation. Over 2,300 government agencies are already using AWS to address a diverse set of use cases, from complex government systems to mission-critical intelligence projects dealing with large volumes of sensitive data. The AWS Cloud is also used by 7,000 educational institutions and 22,000 non-profit organisations. The following diagram is a simple view of the AWS services available globally.



OUR PARTNERSHIP

Datapipe is an AWS Premier Consulting partner. The depth of our partnership is designed to make Datapipe and AWS easy to work with:

- Standardised managed cloud services, clear service options. No hidden charges, transparent management, list price AWS services
- Perfectly aligned to Government's vision for service delivery: service agility and security at scale, delivered through SME engagement
- Real, enduring partnership; both parties completely aligned to outcome delivery for your users
- AWS Enterprise Support included in the managed service fee

FLEXIBLE SERVICES

Datapipe layers our managed services on top of the AWS 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.

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

INFORMATION ASSURANCE

Datapipe and AWS understand the importance and value of your data. All data can be 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 AWS cloud services are can be 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 AWS cloud benefits from extensive independent validation via certifications ranging from international standards (for example, ISO9001, ISO27001, ISO20000). AWS's Cloud Platforms are subject to regular, extensive security governance validations.

Datapipe's managed services are delivered in line with these security standards. Our staff are SC cleared and vetted where necessary and we support various departmental vetting requirements on a per customer need. 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 best practice architectures and software, designed with robust migration processes and portability in mind, which, complemented with AWS's suite of data migration services ensures there are many options available for workload portability. Our consistent documentation makes knowledge transfer straightforward, accurate and complete.

CONNECTIVITY

AWS solutions can offer resilient connections to secure UK Government networks such as PSN and N3, as well as large scale, DDoS protected, internet connectivity. It is also possible for customers to present their own connections (using DirectConnect) for guaranteed performance and security requirements.

AWS SOLUTIONS

AWS's platforms provide public sector customers with on-demand, scalable compute capacity and a large ecosystem of supportive services. 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 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 instances 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, instance 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, operating systems, storage options and database technologies

AMAZON WEB SERVICES PLATFORM FEATURES

The following lists the primary baseline services provided by Amazon Web Services which are then managed by Datapipe. For a complete list of services and the features and functionality available, please refer to the AWS documentation located at https://aws.amazon.com/.

- **Amazon EC2** is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.
- **Amazon EBS** provides persistent, available, and durable block-level storage volumes for use with Amazon EC2 instances in the AWS cloud. Amazon EBS volumes offer the consistent and low-latency performance needed to run your workloads. With Amazon EBS, you can scale your usage up or down within minutes, all while paying a low price for only what you provision.
- **Amazon VPC** lets you provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways
- **AWS Direct Connect** makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your data centre, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
- **Amazon S3** provides developers and IT teams with secure, durable, and highly scalable object storage. Amazon S3 is easy to use, with a simple interface to store and retrieve any amount of data from anywhere on the web. With Amazon S3, you pay only for the storage you actually use. There is no minimum fee and no setup cost.
- **Amazon RDS** is a web service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while managing time-consuming database management tasks, freeing you up to focus on your applications and business.
- **AWS IAM** enables you to securely control access to AWS cloud services and resources for your users. Using AWS IAM, you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.
- **AWS CloudTrail** is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.
- **AWS Config** is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. With AWS Config you can discover existing AWS resources, export a complete inventory of your AWS resources with all configuration details, and determine how a resource was configured at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.
- **Amazon EC2 Container Service** (Amazon ECS) is a highly scalable, high-performance container management service that supports Docker containers and allows you to easily run

applications on a managed cluster of Amazon Elastic Compute Cloud (Amazon EC2) instances. Amazon ECS eliminates the need for you to install, operate, and scale your own cluster management infrastructure.

- **Amazon CloudFront** is a global Content Delivery Network (CDN) service that accelerates delivery of your websites, APIs, video content, or other web assets. It integrates with other AWS products to give developers and businesses an easy way to accelerate content to end users with no minimum usage commitments.
- **AWS Web Application Firewall** (AWS WAF) is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

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.

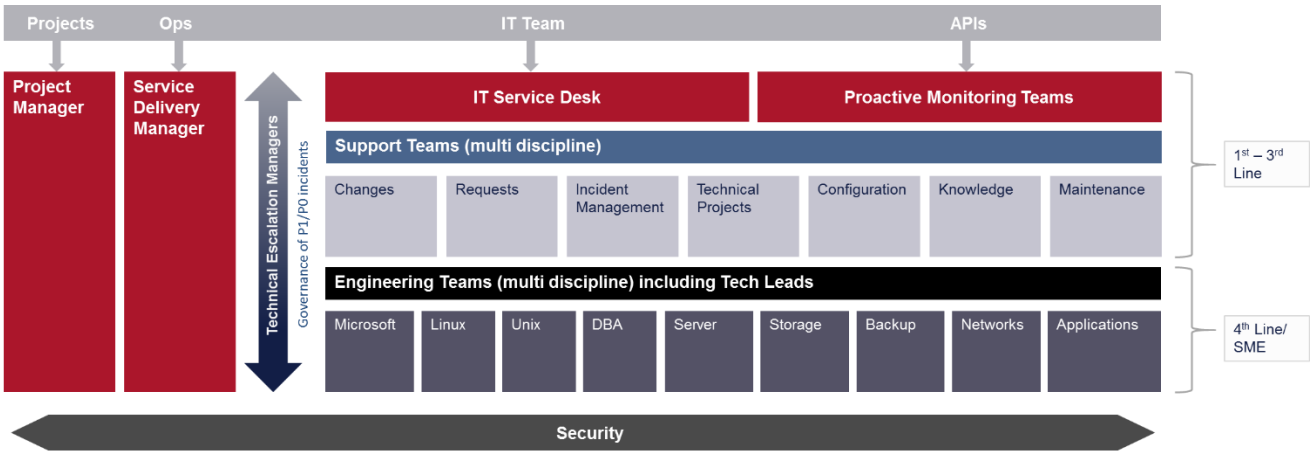
This structure is proven over time to deliver an outstanding customer experience and ultimately drive value based on our customer's technical and business requirements.

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:

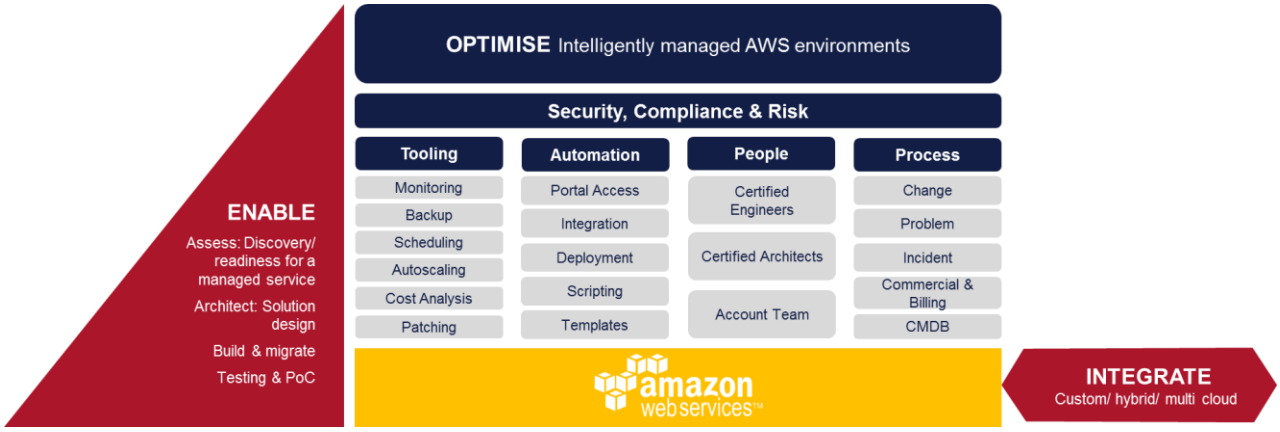
- Taking the lead on issues, coordinating the wider team where required
- Ensuring colleagues have a deep understanding of the solutions they are supporting
- Technical design (maintaining the Low Level Design and creating and maintaining Technical Runbooks)
- Quality Assurance including sign off on 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



Service Overview

- Custom onboarding services to take you from current state to 'run ready' included as standard
- Application-aware infrastructure deployments with 24x7x365 access to Datapipe's DevOps and SysOps engineers, DBAs, integration, automation and security specialists
- Cost management and optimisation to ensure you meet your ROI targets and maintain commercial control
- Insights into AWS spend, single vendor billing and governance over all accounts

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, Linux)
- 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, Postgres, MongoDB and Oracle databases in a variety of configurations to meet customer 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 Security and Network Services

The Datapipe service includes configuration, management and periodic review of security and network configuration within the solution. Virtual Private Clouds (VPCs) are created to logically isolate workloads with multiple subnets and security groups to provide layered security. Datapipe will run periodic reviews to ensure the security policy is being adhered to and that communication is limited to the minimum viable ports and protocols. VPN connectivity between corporate data centres and the VPC can be configured to provide a secure private communication link.

Managed Backup

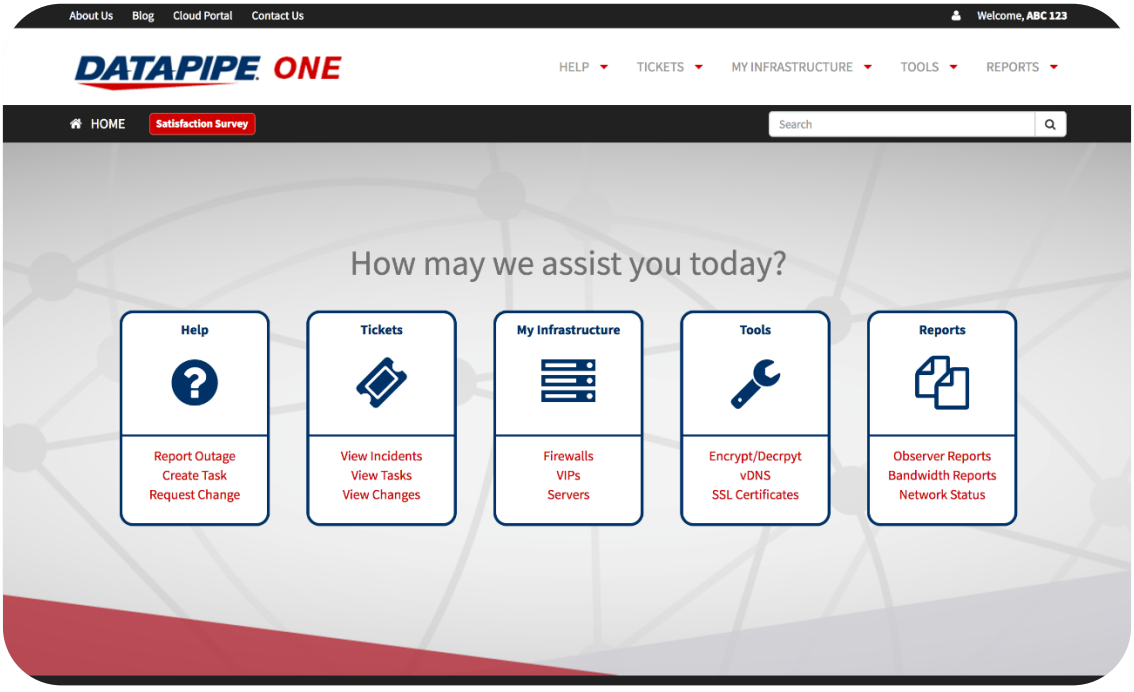
Datapipe will provide fully managed backup of all workloads hosted within the environment. The method of backup will vary across the environment and is workload dependent. For the most part, Agentless API based (snapshot) backups will be taken to provide a restore point for workloads.

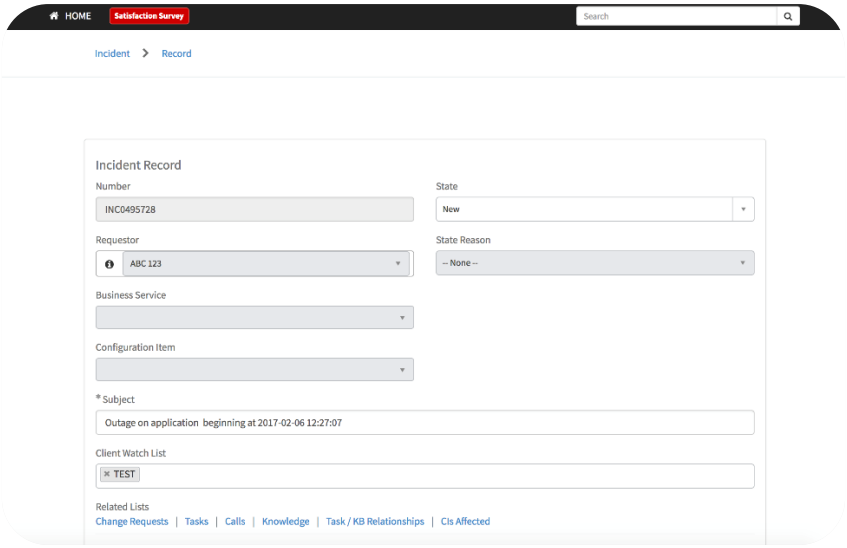
Backups will provide for a standard RPO of 24 hours (lower for transactional technologies where log backups are also taken). Longer retention periods are available if needed.

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
- Basic self-service and resource utilisation analytics





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.

Cloud Service Reviews also include cost analysis of the infrastructure deployed to ensure that the customer is balancing price and performance to ensure workloads are performing as required. Output from the cost analysis may include recommendations such as right sizing instances, adjusting the storage performance or purchasing reserved instances.

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.

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. 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 and AWS Identity and Access Management.
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) or the use of AWS Direct Connect are always recommended as a base level of protection as it removes the doubt of meeting compliance requirements.

At rest

Datapipe 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 AWS. The use of AWS services and features such as EBS encryption, the AWS Key Management Service or AWS CloudHSM are recommended to meet specific compliance requirements.

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

Our standard commercial model describes a contractual relationship with Datapipe, with AWS as sub-contractor. This is the natural model for a commercial relationship to take as Datapipe maintains overall responsibility for service availability, of which AWS 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 AWS and Datapipe services.

HOW MUCH DOES IT COST?

Building your application environment with AWS and Datapipe is easy, and our transparent pricing lets you understand all the components of your solution and assess the value it offers. For full details of Amazon pricing, please refer to https://aws.amazon.com/pricing/ . All pricing is exclusive of VAT and the currency is converted to sterling at the prevailing exchange rate on the date of invoice. For all services, billing is per unit or part thereof where applicable.

AWS Pricing (All London Region)

The table below is a snapshot example of the AWS pricing at the time of the G Cloud 9 submission.

AWS Service	Cost From	Cost To
Amazon EC2	$0.006 Per hour	$6.17 Per hour
Amazon EBS	$0.11 per GB per month	N/A
Amazon S3	$0.02 per GB per month	N/A
Amazon RDS	$0.04 per hour	$5.44 per hour
Amazon CloudFront	$0.085 per GB Transfer out	N/A

Managed Service Uplift

The Datapipe Managed Service for AWS is calculated as a percentage uplift of the total AWS spend for all AWS accounts under management, with a minimum service fee of $1,500.

Tiers	% Fee	From	To
Tier 1	40%	$0	$25,000
Tier 2	30%	$25,000	$50,000
Tier 3	20%	$50,000	$100,000
Tier 4	15%	$100,000+	

The managed service fee is tiered, so the fee for the first $25,000 of spend in a given billing month is calculated at the tier one percentage, the next $25,000 of AWS spend in the same month is calculated at the tier two percentage, etc. For example, a customer with $65,000 of AWS spend in a given month would be charged a managed service fee across tiers one to three, giving a bill of:

40% of $25,000 = $10,000 +
30% of $25,000 = $7,500 +
20% of $15,000 = $3,000 =
$20,500 TOTAL Managed Service Fee

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)
- Managed Infrastructure as Code, scripting and templates
- Database management
- Active Directory management
- Security best practices applied to reference architectures
- VPN management
- Basic scheduling for snapshot and AMI backup and powering instances on/off

- Basic auto scaling
- ITIL service management and service reporting
- Preventative maintenance
- Configuration management and CMDB
- Cost analysis
- Service reporting
- Account Team (account manager, service manager)

OPTIONAL EXTRAS

Service*	Unit	Monthly Service Charge (£)
Amazon DirectConnect Connectivity	Mbps	£10
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