



G Cloud 15

BT Service Definition for BT UK Secure Cloud Max

Contents

Page

1	Service Overview	3
2	Service Features and Benefits	5
3	UK Secure Cloud Max Architecture	7
4	Service, SLAs & Compliance	17
5	Pricing & Billing	23
6	Security Requirements	25
7	Personal Data	27
8	Other Service Considerations	28

1 Service Overview

1.1 BT Services

The Supplier offers UK Secure Cloud Max services to support Buyers looking to process and store data, workloads and applications in UK secure data centres. The services are designed to support demands for secure computing infrastructure that meets high standards of data residency, security, and compliance within the UK that are protected from the impact of non-UK legislation and oversight sometimes associated with general public cloud services.

BT is a suite of cloud solutions including managed services, developed in partnership with our IT strategic partners, and is an ideal solution for UK public and private sector organisations requiring secure cloud services with a flexible consumption model, all within UK sovereign boundaries.

1.2 BT UK Secure Cloud Max Framework

We achieve UK Secure Cloud Max requirements through our Secure Operations teams, our primary UK cloud partner Rackspace, and BT's critical national infrastructure in the UK.

BT is designed to be compliant with security controls and data handling requirements for sensitive information assets that achieve a 'Sovereign' level of compliance defined whereby:

- The information assets (data) will always reside within the UK and when decrypted will only ever be viewed within the UK.
- Information assets are capable of transit being isolated in the UK, but when acceptable to a customer project may be encrypted and transit the internet.
- The technical platforms that service the contextualised information assets are built and hosted in the UK.
- Support systems that handle and process contextualised information assets are in the UK.
- The operational people that support the contextualised information assets are in the UK, and depending on the data requirements, will be security vetted to appropriate levels.

Contextualised information means information that is sensitive when it is aggregated with other information or not encrypted or obfuscated. For example, a site address of a police station is public knowledge, but when aggregated with the service supplied to the location, the nature of applications used in the location and the timing of data or asset transfers, then the aggregated information must reside only in the UK.

BT provides additional sovereign resiliency through the use of its scaled out Critical National Infrastructure which achieves the highest certified levels of environmental engineering.

2 Service Features and Benefits

BT provides secure & industry compliant cloud compute platforms under dedicated and/or multi-tenant environments integrated with compute, storage, networking and cloud management platforms within UK. It's a fully managed service provided by BT in collaboration with our partner Rackspace following the ITIL framework and using a secure tool-set and personnel with required clearances and accreditations located in the UK.

The BT solution is offered in a dual DC architecture and supports 99.99% availability on an annualised basis.

The services are available in the UK for Public Sector Major and Local Government departments, Healthcare, Police & Emergency services & Commercial applications.

BT's UK Secure Cloud Max has 4 standard variants:

- **BT UK Government Cloud**
 - Central Government, Defence, Local Government
- **BT UK Healthcare Cloud**
 - NHS or any other who provide healthcare services
- **BT UK Police Cloud**
 - Policing and Blue Light Services
- **BT UK Commercial Cloud**
 - Commercial services that do not align into other 3 verticals including buyers who might interact with Public Sector but not from Public Sector.

BT provides managed cloud solutions. The addition of BT networking and security solutions can extend a managed service (with additional CCS registered framework products) across a customer's hybrid cloud environment.

Features include:

- Geographically diverse highly secure UK data centre locations
- Dedicated & multi-Tenant environments for Compute & Storage
- Supported by BT networking and security
- BT certifies to:
 - ISO/IEC 27001:2013
 - ISO 27017:2015
 - ISO/IEC 9001:2015
 - Cyber Essentials+ and
 - PSN certifications.

Managed from BT's Secure UK Operations teams residing in the UK and supported through UK-based, security cleared staff, the fully managed service includes:

- Guest OS support
- Backup & recovery and disaster recovery
- Firewall management and security incident logging
- Vulnerability scanning & remediation, anti-virus & malware endpoint protection
- Workload performance and capacity monitoring
- System patching
- SOC and SIEM services.

3 UK Secure Cloud Max Architecture

BT's UK Secure Cloud Max services are offered from two secure datacentres hosted in UK

- ARK1: Spring Park Campus, Corsham, Wiltshire, SN13 9GB
- ARK2: Cody Park, Farnborough, Hampshire, GU14 0LH

3.1 Services Components

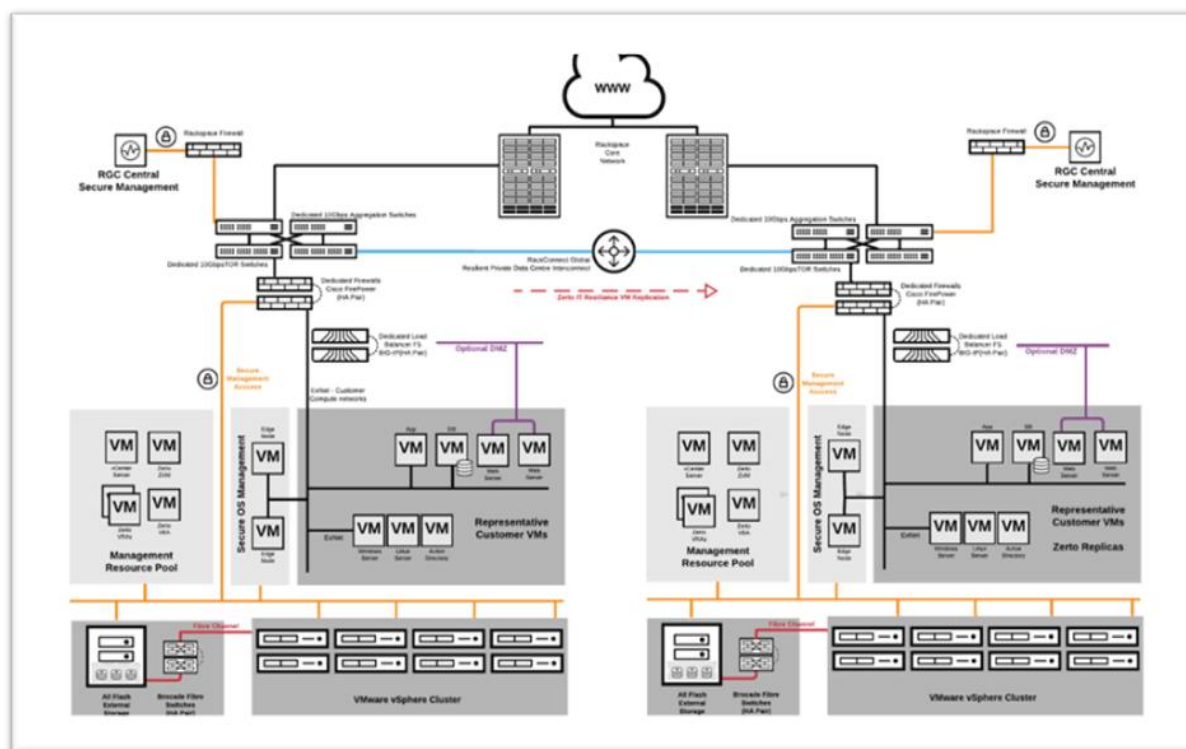
The service is provided as standard components and additional services which may include co-location, additional wide area networking and security.

3.2 Standard Services

BT offers Compute, Storage, Licenses, Disaster recovery, Backup, Lead Engineer Support (shared or dedicated) and Connectivity.

The diagrams below provide an example of the standard design of the solutions with the various standard configurations available; Standard Services are categorised as:

- Single Tenant
 - Full dedicated stack, including storage, compute and networking
 - Dedicated Compute with Dedicated Storage

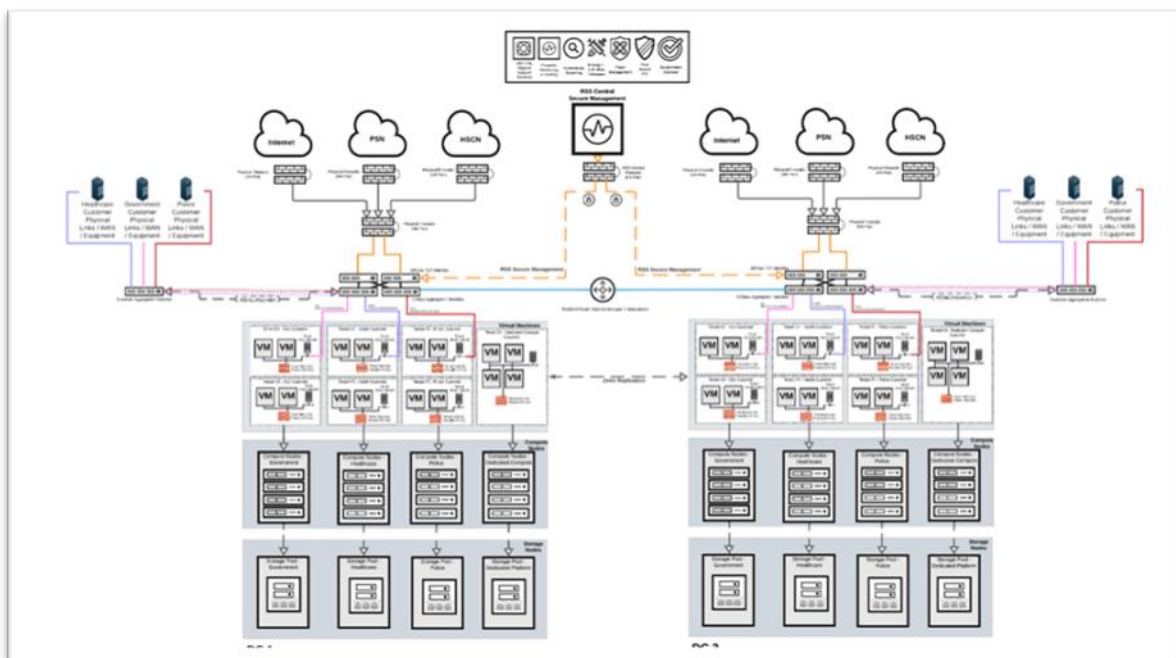


- Multi-Tenant
 - Dedicated and/or Shared compute and storage but on a shared platform, with shared network infrastructure, and dedicated firewalls on a shared firewall platform
 - Dedicated Compute with Multi-Tenant Storage
 - Multi-Tenant Compute with Multi-Tenant Storage (within that PoD)

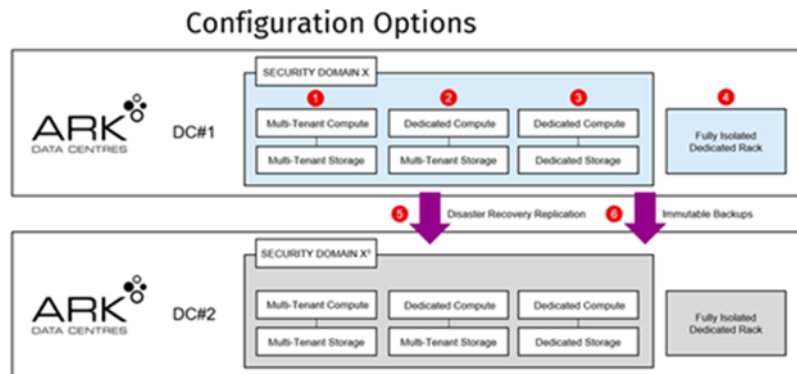
The data centre cloud fabric is split into multiple “Pods” of compute and storage which are dedicated/ shared to the vertical environments defined in BT’s standard product.

- BT UK Government Cloud
- BT UK Healthcare Cloud
- BT UK Police Cloud
- BT UK Commercial Cloud

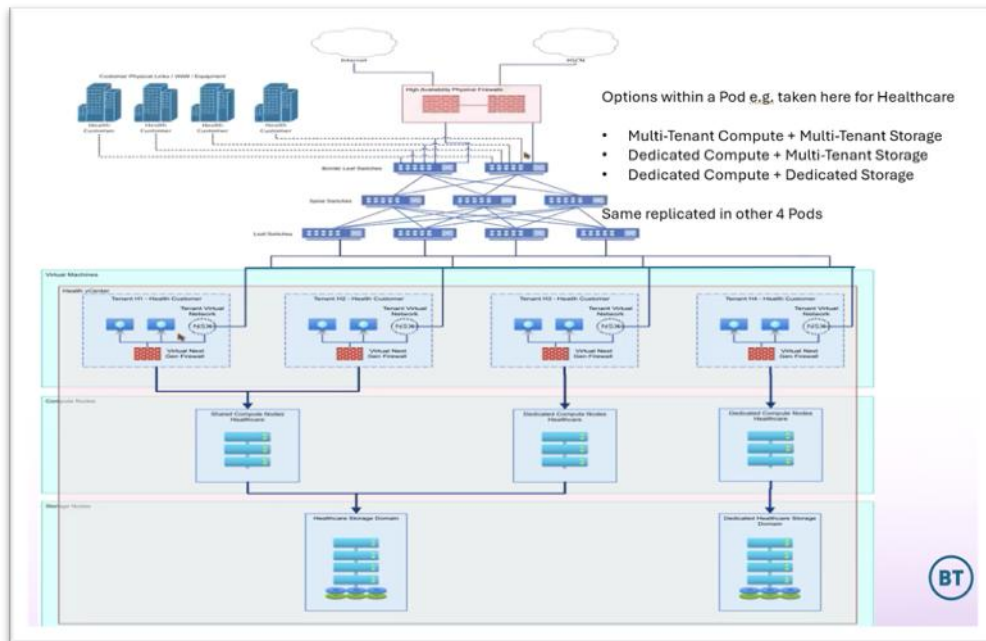
‘Pods’ refers to a platform that has dedicated/ shared compute and storage component for each customer vertical, ensuring full segregation of compute and storage services between customers. This approach ensures a cost-effective hosting solution for customers while providing the high levels of data security they require. Basis on the nature of the business, customer are provisioned as per their verticals Pods.



The diagram below depicts the overall BT's UK Secure Cloud Max configuration options for VM Management.



3.3 Architecture Features



3.3.1 Options Under Single/Multi-Tenant

- Dedicated Compute with Dedicated Storage
 - Customers will have their own isolated Hypervisors, with a dedicated VMware compute cluster, which will only contain that customers Virtual Machines. Storage is also dedicated to that customer with no other workloads / files being stored on there. All storage is encrypted.
- Dedicated Compute with Multi-Tenant Storage

- Customers will have their own isolated Hypervisors, with a dedicated VMware compute cluster, which will only contain that customers Virtual machines. The Storage will be on a shared vertical dedicated storage. For example, Healthcare Storage POD. This means that the shared storage tier would only be utilised by other Healthcare customers, although different Healthcare Customers would still be unable to see one another's data. This same model applies to each of the vertical solutions, Government, Healthcare, Police, etc. are all segregated from each other.
- Multi-Tenant Compute with Multi-Tenant Storage (within that POD)
 - The same storage solutions as above, but in this case the compute cluster is also shared with additional customers in the same vertical. For example, a Healthcare customer would share compute resource with other healthcare customers, but not with Government or police.
- Fully Isolated Dedicated Rack
 - The service supports multiple pre-defined options for virtual machines that utilise the platform.

3.3.2 Compute

The service is a Dell & VMware based platform for compute and storage and has options:

- General Compute/ Purpose
- High Performance Compute/ Purpose

Contention Ratios:

- For VMs, this is the ratio of virtual CPU (the number of CPUs in the Virtual machine) to physical CPU. The number of CPUs in the physical hypervisor being used to host the virtual machines. Normal contention is 4:1, so 4 Virtual Machine CPUs to every single physical CPU. There is also the option at a higher cost to have CPU dedicated to virtual machines, so 1 physical CPU per virtual machine CPU. This 1:1 would typically be used in high performance requirements such as database servers.

Naming Convention of Compute:

- For convention, gp.s.c4.1.2 means General Purpose, Shared, Contention Ratio 4:1, 1 vCPU & 2 Gig RAM

3.3.3 Storage

Storage is either shared or dedicated with performance layers. All flash storage tiered as Archive/ Bronze / Silver / Gold is assigned based on performance tiers, based on IOPS/GB per disk. The IOPS metric shows how many read and/or write operations a storage device can perform per second:

- Archive: 0 IOPS/ GB
- Bronze: 3 IOPS/GB
- Silver: 5 IOPS/GB
- Gold: 10 IOPS/GB

The relevant disk type would be matched to workload, disk intensive workloads such as SQL server would require Gold, other workloads would be more appropriate on silver or bronze or archive.

3.3.4 Network

Networking services support the following features:

- VMware NSX for East-West traffic
- Firewalls for North-South traffic
- To keep the traffic separate we have created VRFs for each customer and in NSX there is a dedicated router and using Palo-Alto we have dedicated VCIS so end to end for a specific customer, so they have a dedicated routing/ switching domain to move the traffic end to end and use NAT to translate to traffic to go to outer world
- WAN connection is provided by BT into the platform
- Management and monitoring network which is deployed on dedicated equipment
- North-South bound traffic is moving through the firewalls and which is connected to external cloud, is configured under VCIS (virtual instances) and will be required for each customer. These firewalls are configured under HA pair
- Both the Data Centres have resilient cross connectivity
- ARK1 (Corsham) & ARK2 (Farnborough) have identical size and capacity. DR on a virtual machine will be replicated to the secondary site
- Physical Port:
 - Physical ports required to plug in dedicated Customer Connectivity (MPLS etc.). So, if a customer requires MPLS connectivity they will also require physical ports to terminate this connectivity in the environment.
- Internet & Public Ips:
 - Internet is provided as a bandwidth on a shared internet provision for the platform. Public IPs pool of /29 & /28 is available as requested.
- Inter-site connections:
 - Inter-site connectivity is provided by the platform and provided as bandwidth on a shared connection.

3.3.5 Operating System Licenses / Additional Licenses

The operating systems used in the environment are Windows & Red Hat.

Additional licenses used are SQL Standard & SQL Enterprise

These licenses are provided using 2 options i.e. Supplier provided & Customer provided (BYoL)

The list of operating systems which are supported are mentioned below:

Guest OS Management	Standard Support	Cost Option
Hardened VM Images All supported OSs hardened to NCSC-compliant levels and maintained to ensure continued compliance. (for 'greenfield' VMs only)	✓	
Automatic VM tooling enrolment VM creation and ensuring all new servers are deployed with all tooling before release for use.	✓	
Red Hat Enterprise Linux 7 Support Instance creation, deletion, and management of Red Hat Enterprise Linux 7 OS	✓	
Red Hat Enterprise Linux 8 Support Instance creation, deletion, and management of Red Hat Enterprise Linux 8 OS	✓	
CentOS 7 Support Instance creation, deletion, and management of CentOS 7 OS	✓	
CentOS 8 Support Instance creation, deletion, and management of CentOS 8 OS	✓	
Debian 10 Support Instance creation, deletion, and management of Debian 10 OS	✓	
Ubuntu 18 Support Instance creation, deletion, and management of Ubuntu 18 OS		✓
Ubuntu 20 Support Instance creation, deletion, and management of Ubuntu 20 OS	✓	
Ubuntu 21 Support Instance creation, deletion, and management of Ubuntu 20 OS	✓	
Ubuntu 22 Support Instance creation, deletion, and management of Ubuntu 20 OS	✓	
Windows Server 2012 R2 Support Instance creation, deletion, and management of Windows Server 2012 OS	✓	
Windows Server 2016 Support Instance creation, deletion, and management of Windows Server 2016 OS	✓	
Windows Server 2019 Support Instance creation, deletion, and management of Windows Server 2019 OS	✓	
Windows Server 2022 Support Instance creation, deletion, and management of Windows Server 2022 OS	✓	

3.3.6 Disaster Recovery

Disaster recovery is between the two data centres and can be set up as requested in line with the Recovery Time Objective (RTO), and Recovery Point Objective (RPO).

- Recovery Point Objective is the maximum amount of data that would be lost.
- Recovery Time Objective is the time taken to restore the environment in the DR site (as long as DR has been selected).
- Solely where Customer purchases a DR service, then RPOs and RTOs shall not be set commensurate with the Compliance Baseline, but instead, the RPOs and RTOs shall be aligned with the Disaster Recovery Tier identified in the Service Order(s). Disaster Recovery Tiers RPO & RTO:
 - Bronze 24 Hours
 - Silver 12 Hours

- Gold 4 Hours
- Platinum 1 Hour
- For platinum as an example the recovery site would be active within 1 hour of DR being called (RTO), and no more than 1 hours of data would be lost (RPO). For bronze, these RTO's and RPO's would both be 24 hours.

Alternatively, customers can opt to deploy their production environments in an active-active configuration, in which the Production Environment can always be running in the Disaster Recovery Site concurrently. Notwithstanding, Active-active configuration is a customer's responsibility, outside of the scope of the base Services configuration, and would typically require application-level support.

3.3.7 Backup

VMware image backups of servers are taken daily and then retained as per the retention policy selected (see below). If required, agent backups can be used as an option. These would typically be used for SQL server workloads or large file servers, where application backups are required.

Backup is taken to a separate system, and if selected via backup policy replicated offsite to another data centre. Backups are immutable and additional security can be applied to further protect backups, if necessary, though at additional cost with an additional feature of Data Lock.

Backup Options:

- Basic – Single site backups only
- Standard – Backup Replication to a second data centre
- Enhanced – Backup replication of all backups to a second data centre.

Policies e.g.

- Basic 1- SHARED-B-7D-0W-0M-0Y
- STANDARD 1 - SHARED-S-14D-4W-0M-0Y
- ENHANCED 5 - SHARED-E-14D-12W-12M-5Y
- For above policies, D – Days, W – Weeks, M – Months, Y - Years

3.3.8 Support

- Fully Managed VM Support
 - Up to OS level, including patch management, vulnerability management, anti-malware protection, monitoring, backed by full ITIL service. Support of the environment to ensure that the environment is highly available (N+1) and no single physical device failure would impact the customer.
- Lead Engineer Support

- Resource that understands all the technical aspects of the deployment and liaises across customer and internal technical teams to provide an enhanced service.
- The customer account team includes a named lead cloud engineer (LE), a technical expert who will be responsible for managing the Supplier technical solution and ensuring customer systems are maintained to the required levels. The LE will be familiar with the customer's technical solution and requirements, allowing them to advise on service improvements and to co-ordinate support responses to customer queries of system issues.
- The LE is responsible for oversight and reporting on all aspects of the Suppliers technical solution, including:
 - Capacity management: advising the customer on potential capacity issues and providing effective solutions.
 - Performance management: monitoring the performance of the customer's environment, ensuring resources are applied effectively and advising the customer on resolving potential resource issues.
 - Patch compliance: co-ordinating patch deployment with the relevant support teams, liaising with the customer on patch deployment plans and reporting on patch compliance for the supported environment.
 - Vulnerability management: managing the monthly scans of the supported environment, advising on suitable mitigation or updates to address identified vulnerabilities, and providing monthly reports on vulnerability risk across the supported environment.
 - Change management: oversight and review of all Supplier driven changes and for customer changes where they impact Rackspace supported services.
- The Lead Engineer (LE) is a tiered service (Bronze, Silver, Gold & Platinum). The tiers reflect the time that the LE is assigned to the end customer.
 - Bronze (shared) - (2 Business Days / Per Month)
 - Silver - (8 Business Days / Per Month)
 - Gold - (18 Business Days / Per Month)
 - Platinum - (Dedicated to the Customer/ Per Month)

3.3.9 Add-On Device Hosting

The service offers shared (between multiple customers in the same security domain, healthcare) co-location space that a customer can use to host customer owned equipment.

We provide tap-off, power, cooling and smart hands plus the ports needed to connect these devices to UK Secure Cloud Max. BT would normally be responsible and accountable for any customer equipment hosted in the colocation racks plus any cables connecting this equipment to the power and/or data within the colocation racks.

3.4 Sustainable Data Centres

- Ark Data Centre's, working with manufacturer BladeRoom, have developed innovative direct air-cooling technology that dramatically lowers energy consumption and cost. So far, ARK has delivered over 40MW of usable IT power, operating free cooling for 99% of every year. The use of sophisticated technology ensures that the data centre cooling adapts to IT load in real time to reduce wasted energy and to deliver cooling of up to 50kW per rack.
- Maintaining industry leading PUE figures, Indirect Air-Cooled facilities use High-tech adiabatic coolers and specifically designed heat exchangers.
- ARK's indirect air-cooled facilities are designed to Uptime Institute Tier III standards as an alternative to Direct Air. Adiabatic Cooling and inert Heat Pipe technology still deliver the best available PUE figures using sophisticated technology to ensure that data centre cooling adapts to IT load in real time to reduce wasted energy.
- At Cody and Spring Park, Ark builds secure data centre to the highest level of HMG security markings. Our private 200kW data rooms are designed to deliver the most robust physical security required by Government or industry regulations while maintaining our commitment to operational excellence and service.
- Chilled water-cooling solutions are effective where a closed loop system is required. ARK have applied innovations to enhance traditional chilled water designs to improve efficiency and to ensure they can deliver a product that lives up to ARK's ambitious standards for efficiency and precision cooling.
- ARK's system is designed to run on ambient air where conditions permit, reducing the burden of electricity consumed in the cooling process, and the subsequent carbon emissions.
- By employing innovative thinking the team at Ark has developed a 'Water Buffering and Saving Mode' for our cooling equipment which reduces our original peak water usage by a staggering 85%.
- By capturing water from the roof and from the 'run-off' of the car parks it is possible for the data centre evaporative cooling systems to operate solely on

harvested rainwater (apart from the first year where there was an initial fill of the storage tanks).

- Ark has developed innovative direct air evaporative cooling capability that dramatically lowers energy consumption and cost, capable of providing compressor free cooling for 100% of every year.
- ARK have removed all diesel from our standby generator fuel tanks and replaced it with Hydrotreated Vegetable Oil (HVO). This will reduce our existing limited Scope 1 fossil emissions by 90%, NOx emissions by >15% and particulate emissions by >25%.
- ARK's factory focused modular building process not only reduces the construction time on site (along with the health & safety risks of a construction site) but it also favours steel over concrete and allows it to be recycled up to 90% of the building fabric in the future; thereby lessening the overall environmental impact of buildings, when compared to a traditionally constructed building.
- Each Ark facility has significant provisions to accommodate and encourage the use of electric vehicles including dedicated sections of the car parks equipped with Multiple EV Chargers with provision for up to 20% of car parking spaces in the future.
- ARK's Living Walls on urban data centre contain 'planters' at each floor level which act as significant flower beds with ample soil and water retention that can be easily maintained, producing a real living garden.
- In addition to encouraging biodiversity, the vegetation produces its own 'microclimate' absorbing heat when the weather is hot preventing it from getting into the building and acting as an insulator when it is cold.
- For the last 6 years, all Ark facilities have been powered by 100% renewable energy.

4 Service, SLAs & Compliance

BTs UK Secure Cloud Max provides a comprehensive Service Level Agreement (SLA) based upon service availability. The Service has 99.99% availability on annual basis. Any outage incident must be reported by the Customer to the BT Secure Service Desk who will acknowledge the incident and instigate the necessary actions.

Should BT fail to meet its obligations laid out in a supplier agreement, BT will provide service credits.

4.1 Service Desk Locations

- BT Secure desks are hosted in our Belfast & Sheffield secure site facilities.
- Staff are security cleared and accredited to UK Government vetting up to DV.

All secure contracts are managed on BTs SSP platform using a secure ServiceNow instance and dedicated instances of our monitoring tools.

4.2 Service Desk Performance: Measurement

- The SLA will be measured for each Priority Level (as defined in the Priority Level Table below), the SLA clock will run during Business Hours from the time an Incident is received into the Supplier ITSM tool or created in the Supplier ITSM tool, until the time it is set to be resolved in the Supplier ITSM tool, excluding any time the Incident is placed on hold.
- In the case of any Incident, change, request or any other ITIL based ticket the SLA timer will be placed on hold when awaiting any response from the Customer.
- The target means times described are in Business Hours, not elapsed time for priority 3 and 4. For clarity, in any change freeze periods notified in advance and / or agreed with the Customer, the SLA for priority 4 tickets will still be valid but placed on a hold status during these times.
- Priority levels will be dynamic depending on the severity and impact of the Incident, for example, where an incident starts its lifecycle as a Priority 1 and the initial impact has been resolved via a temporary fix, the ticket will be closed, and a problem ticket opened to progress the permanent fix. Likewise, tickets can be escalated in levels with the agreement of the Supplier service desk in line with the impact to the Customer.

Priority Level Table across all Services:

Priority Level	SLA Clearance Time across all services	Target Mean Time to Resolve across all Services or Schedule (a KPI not a Service Level)	Typical Description (These may vary according to the Service requirements)
1	90% <4 hours	2 hours	The highest priority level. This classification indicates a major incident, loss of service or serious impairment of service, which cannot be immediately circumvented.
2	90% < 8 hours	4 hours	This classification indicates an issue that it is not major service affecting fault, and generally constitutes a failure of a service component of the Service, which does not have a significant impact on the service as a whole.
3	90% <24 hours	12 hours	This classification indicates an issue that is not service affecting. There is no service impairment to the service for any customer.
4	90% <120 hours	60 hours	Only used for service requests, measures time to schedule.

Examples of Priority Incidents:

Priority Level	Typical Description (These may vary according to the Service requirements)	Examples
1	The highest priority level. This classification indicates a major incident, loss of service or serious impairment of service, which cannot be immediately circumvented.	Major failure in infrastructure (Hypervisors) that would cause a production environment to be unavailable.
2	This classification indicates an issue that it is not major service affecting fault, and generally constitutes a failure of a service component of the Service, which does not have a significant impact on the service as a whole.	Loss of platform management plane, unable to access environment but workload is still running / executing.
3	This classification indicates an issue that is not service affecting. There is no service impairment to the service for any customer.	A loss of a drive in a vSAN cluster, no service impact however disk needs to be replaced.
4	Only used for service requests, measures time to schedule.	Including but not limited to requests for information, documentation and Smart Hands requests.

The Service Desk performance criteria are as follows:

Net Percent Calls Answered	Monthly average: 98.5% of calls to be answered before call drop off. Measurement: Based on all BT customers receiving Services Exclusion: calls that drop within the first 30 seconds
Percent Calls Answered	Monthly average: 94.5% of calls to be answered within 30 seconds. Measurement: Based on all BT customers receiving Services Exclusion: calls that are wrong number or mis-dialled.
Ticket assignment	Monthly average: 95% of tickets should be assigned to a resolver within 15 minutes and 100% within 30 minutes. Measurement: Based on all BT customers receiving Services Exclusion: This may not always be the final resolver group, as diagnosis of the incident progresses other resolver groups may be assigned to work on the incident and there is no penalisation as part of this measure for moving the incident between resolver groups to support resolution within the Priority SLA, Note: Automate assignment to a resolver group is acceptable.

4.3 Problem Management

The key objectives of Problem Management are to prevent problems and resulting incidents from happening, to eliminate recurring incidents and to minimize the impact of incidents that cannot be prevented. Problem Management includes diagnosing causes of incidents, determining the resolution, and ensuring that the resolution is implemented.

Problems are categorised in a similar way to incidents, but the goal is to understand causes, automate and document workarounds, and request changes to permanently resolve the problems.

4.4 Change Management

Change management is the process for controlling the Lifecycle of all Changes to the underlying architecture and system implemented in the delivery of the BT's UK Secure Cloud Max. The purpose of the Change Management process is to ensure that standardised methods and procedures are used for efficient and prompt handling of all changes such that overall business risk is optimised.

4.5 Complaints

A Customer complaint may be made via the BT Service Desk, via an Account or Service Manager, via a Sales Channel, or via any other BT person. A complaint is regarded as any Customer's clear expression of dissatisfaction with the service being provided by BT.

All complaints will be logged onto the BT Complaint Handling System and managed to resolution by the receiving person or unit. The process will be overseen by the Complaint Handling Team to ensure consistency of approach, speedy response, and resolution, and to facilitate root cause analysis and corrective actions if appropriate.

In the case of a complaint being made directly or indirectly to the Service Desk, they will:

- Provide a consistent Customer experience through utilisation of the BT Customer Experience and Quality Call guidelines.
- Register any Customer's clear expression of dissatisfaction with the service as a complaint.
- Provide a receipt and ownership point for Customer complaints with formal acknowledgement to the Customer within 24 hours.
- Provide further updates to the Customer within 5 days of complaint being received.
- Ensure that a final response is provided to the Customer within 10 days.
- Manage all Customer complaints according to best practices defined in British Standard BS8600 and as defined within standard BT internal procedures.

- Record all complaint information in the Complaint Handling System, and ensure regular updates are maintained to the progress log.
- Identify owners best able to resolve the complaint and track it through to resolution.
- Wherever possible ensure that Customers are completely satisfied with the outcome of the complaint process.
- Prepare and issue Customer reports on service/provision failures to support complaint management where necessary.
- Manage corrective actions resulting from a complaint investigation through to completion.
- Manage Customer claims for Service Level Availability (SLA) compensation payments in line with published SLA service descriptions for associated services.

4.6 In-Life Management

The resources consumed in BT's environment such as VMs, storage, network etc. will be available with Secure Team only. Also, additional resources/services can be purchased through the standard ordering process at any time and are subject to any initial terms of elements previously purchased and operational.

4.7 Virtual Machine Access

There are three methods of access: console using a browser; Virtual Private Network; or alternatively public access using common clients such as Remote Desktop Protocol or Secure Shell etc. As no physical access to the BT data centre will be granted it is necessary for the Customer to create a remote connection using tools such as Remote Desktop Protocol or Secure Shell.

4.8 Console Access

Console access is available through the Portal to each of the individual VM thereby allowing the Customer quick and direct access.

4.9 Public Access/Client Access

The Customer can choose to create firewall rules through Secure Team to allow access to their VMs directly, via remote desktop protocol or secure shell.

4.10 Modifying/Ceasing the Service

Any Modify request will be through the BT Account Team that will subsequently follow a standard ordering process.

To completely cease the service i.e., have the account deleted the Customer can contact their Service Desk or Account Manager who will provide them with a short form to be completed. Following acceptance of the form the Account will be terminated and all associated VMs, storage volumes etc. deleted. Once an Account has been terminated it cannot be brought back.

Accounts can also be suspended. This state is used by BT to control the Account following contractual disputes for non-payment. They differ from a termination as the Account is still live, but the use of the service is restricted or removed entirely. Accounts in a suspended state can be reinstated.

4.11 Compliance

- Service Compliance
 - Fully aligned to the highest level of NCSC guidance.
 - Fully managed services offered in UK region using the secure tools set and staff with all the necessary clearances and accreditations.
 - Fully compliant with NCSC, DSP toolkit & PCI standards
 - ISO 27001, ISO 9001, Cyber Essentials+ and PSN Service Provider certified
- Managed Guardrails
 - Strict role-based access control
 - Dedicated SIEM solution
 - ITIL framework
- NCSC Compliant VMWare Environment
 - Single Tenant
 - Dedicated VMware infrastructure and storage.
 - Dedicated cabinets with full access management and auditing.
 - Fully resilient dual-DC design with fully managed Disaster Recovery.
 - Fully configured and hardened PP Compliant (EAL4+) firewalls.
 - NCSC-compliant AD policy with OS hardening as standard.
 - Automatic enrolment of all VMs in management tooling.
 - Multi-Tenant
 - Choice of dedicated or shared hypervisors (Within the same security domain)
 - Shared storage with the same security domain

- Dedicated cabinets to Sovereign Services with full access management and auditing.
- Fully resilient dual-DC design with fully managed Disaster Recovery.
- Fully configured and hardened PP Compliant (EAL4+) firewalls.
- NCSC-compliant AD policy with OS hardening as standard.
- Automatic enrolment of all VMs in management tooling.

4.12 Information Assurance

BT and Cloud partners hold ISO27001 certification for the UK Secure Cloud Max Service .

- Quality assurance, performance and testing:
- Government security clearance up to Developed Vetting (depending on project requirements)
- Cyber Essentials certification.
- SOC 2.
- The Supplier's partners can work in conjunction with the Buyer's testing and quality assurance team, to assess the cloud infrastructure in order to compare or improve performance.
- Customer support is available 24/7.

5 Pricing & Billing

5.1 Pricing

Charging within BT's UK Secure Cloud Max will be charged on a monthly subscription. Any single tenant/ multi-tenant requires fully managed VM support. Any other add-ons require mutual agreement with signed supplier agreements.

The VMware Cloud service components are provided in a consumption-based model.

Please note that Pricing is accurate at the time at publication. The Supplier reserves right to change for any rolling contracts we would give 120 days' notice.

We will not change the price during a committed term for Customer contracts while indexation for resources for managed services may apply.

5.2 Billing

One Month subscription charges of the Service will be billed as One-Time Charge as an advance that will be adjusted towards the end of the contract.

A master Order Form and supplemental Order Form(s) shall include multiple Services which may be invoiced together or separately.

Selected Service components shall be billed based on usage. Such service components will be shared compute, storage and network.

Monthly recurring charges will include additional charges based on usage (as applicable).

Any Discounted Charges agreed shall be based on minimum volume and/ or Term commitment. Such minimum committed charges will be charged during the subscription term of the contract irrespective of usage from the start date as per BT's discretion. Any additional services or usage charges over and above the minimum commitment listed in the service order form of BT's UK Secure Cloud Max, will be charged as per the mutually agreed pricing that vary from time to time.

Additional nodes and/ or VMs and/ or Storage and/ or Licenses and/ or Backup and/ or Disaster Recovery and/ or Network and/ or Service(s) of BT's UK Secure Cloud Max, shall be purchased and billed additionally with or without the minimum order quantity.

Service charges mentioned in the quote are an estimate and will be billed based on the consumption that needs to be equal or greater than the committed minimum spend (if applicable). Otherwise, the minimum committed spend will be billed.

The Customer may not downgrade the minimum commitment during the Subscription Term. The only change to the minimum monthly spends during the Subscription Term will be an increase if requested by the Customer.

Billing should be customised based on the solution and the expected changes during in-life.

5.3 Contracting

Each Customer need to sign a contract to use the service. The fixed term has a minimum commitment term of 12 months to a maximum committed term of 60 Months subject to review year on year. Customers are billed monthly in advance.

Should Customers want the service for more than the committed term, they will have to sign a new contract upon the expiry of their existing agreement.

In addition to the provisions of the Governing Agreement, if any Service is terminated by the Customer for convenience (or terminated by BT due to material breach by the Customer) prior to the end of the Subscription Term, next to any de-installation Charges the Customer will pay any outstanding Charges until the date of termination and will compensate BT. Early Termination Charges (ETC) are invoiced in full and apply if any On-Demand Service with an associated Minimum Monthly Charge is terminated prior to the expiry date of the Subscription Term.

Early Termination Charges are equal to 100% of the MRC for each month until the end of the Subscription Term.

6 Security Requirements

Due to the nature of the service within scope of this service offer, optional Call-Off Schedules 9A (Security: Short Form), 9B (Security: Consultancy), 9C (Security: Development), 9D (Security: Supplier-led Assurance) and 9E (Security: Buyer-led Assurance) are excluded and the **Suppliers standard Security Management Plan applies only**.

Additionally, BUYER'S SECURITY REQUIREMENTS AND ICT POLICY SECURITY REQUIREMENTS within the Call-Off Order Form will be marked with the option **There are no Security Requirements for the purposes of this Call-Off Contract** and SECURITY ASPECTS LETTER will be marked as **not applicable**.

6.1 The Security Management Plan

The Security Management Plan (SMP) defines the security measures that are implemented, and maintained, by BT. BT will maintain the adherence to the contracted security measures.

The plan supports the provision of the services in scope of this service offer and covers the following:

- Our approach to security
- Our information security policy
- External parties
- Human resource security
- Physical and environment security
- Asset management
- Operation of the plan
- The security lifecycle

6.2 Security Accreditation and Governance Standards

Security accreditation and governance standards will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

6.3 Operational Security

Operational security will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

6.4 Asset Protection

Operational security will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

6.5 Cyber Essentials Certification

Cyber essentials certification was a mandatory requirement to secure a place on the framework as a Supplier and to maintain our place on the agreement, all Suppliers must present evidence to Crown Commercial Service (CCS) of their continued certification.

Therefor the option under CYBER ESSENTIALS CERTIFICATION within the Call-Off Order Form under is marked as not applicable and for the purposes of Call-Off Schedule 27 (Cyber Essentials Scheme), clauses 2.1 to 2.4 are not used.

6.6 Staff Vetting Requirements and Background Checks

Staff vetting requirements will be in line with the details defined within the Suppliers Digital Marketplace submission and this Service Definition document and STAFF VETTING REQUIREMENTS within the Call-Off Order Form will be marked accordingly.

Our recruitment process includes pre-employment screening and vetting prior to placement to ensure adequate levels of confidentiality are maintained, screening includes:

- Application for a criminal record check
- Giving us contact details for reference checks
- Health declaration
- CIFAS- Staff Fraud Database check.

Additional checks are made when dealing with particularly sensitive positions (such those involved with sensitive contracts). The normal undertakings signed by individuals at recruitment include non-disclosure provisions and it is a disciplinary offence to misuse any information obtained from Supplier systems. Offenders are subject to disciplinary action up to and including dismissal and may be subject to prosecution, while ensuring compliance with local legislation.

Due to the nature of the service within scope of this service offer, optional Call-Off Schedule 18 (Background Checks) is excluded and in the event that Supplier Staff do not have the necessary clearance required, the Parties will agree an acceptable alternative such as escorted access.

7 Personal Data

Personal data in relation to services in scope of this service offer is divided into 2 areas:

- Managing the contract
- Managing the services

Personal data, where required to be managed, complies with the requirements of clause 17 Data protection and security, within the Framework Core Terms including new Clause 17.7 included via Framework Special Term 13

7.1 Managing the Contract

Joint Schedule 10 (Processing Data) will be completed to define what types of personal data in relation to managing the contract may be held, the nature and purposes of the processing and will confirm The Parties are Independent Controllers of Personal Data.

7.2 Managing the Service

Where personal data is held as part of delivering the service, how this will be managed will be defined, where applicable, within the Suppliers product specific Terms and Conditions that are attached to the Suppliers Digital Marketplace entry for this service offer. The Suppliers Digital Marketplace entry also confirms details of data storage and processing locations specific to this service.

The Supplier, including any Sub-processors of the Supplier, may from time to time use back-office support and system functions which are located or can be accessed by Users from outside of the UK and/or the European Economic Area. Any such processing will be in accordance with Joint Schedule 10 Paragraph 5.5.2, and for the purpose of clause 5.5.2 (a), the Buyer consents to the disclosure and transfer of Data, including Personal Data, as required in order to provide the Service.

7.3 Sub-processing

The Buyer consents to the Supplier's use of Sub-processors in accordance with the Framework Agreement. The Supplier will ensure that data protection obligations in respect of Processing Buyer Personal Data that are broadly comparable to those set out in the Framework Agreement and will be agreed with any Sub-processors.

The Supplier will inform the Buyer of intended changes to its Sub-processors from time to time, either by providing the Buyer with online access to intended changes or by such other means as the Supplier may determine. If the Buyer does not object to the proposed change within 30 days of this notice, the Buyer will be deemed to have authorised the use of the new Sub-processors.

8 Other Service Considerations

The service described in this Service Definition is based on the Supplier's standard offering for this cloud service and the contract is not defined as a Critical Service Contract. It should be noted that the G Cloud 15 Call-Off Order Form has a number of mandatory schedules, optional schedules and Call-Off Order Form options, and this section clarifies the position of these options for this service as provided by the Supplier. The service will additionally be delivered in line with the Supplier Terms and Conditions included within the Suppliers Digital Marketplace submission.

8.1 Modern Slavery, Environmental Requirements and Sustainability

To comply with the reporting requirements to the Buyer as defined within Joint Schedule 5 (Sustainability) the Buyers can access the Suppliers annual Modern Slavery Report, and where required (for lots 1a and 1b only) its Carbon Reduction Plan here [Our reports & policies - Responsible business | BT Plc](#)

Optional Call-Off Schedule 25 (Additional Sustainability Requirements) is excluded. The Suppliers approach to sustainability, managing our environment, and our modern slavery policies can be found here [Our reports & policies - Responsible business | BT Plc](#)

For the purpose of Call-Off Schedule 26 (Carbon Reduction), the following optional clauses are not used: 3.1.1, 4.2 to 4.5, 8, 10 and optional paragraphs under Annex A. For the purpose of reporting on our Carbon Reduction Plan (clause 11), Buyers can access the plan direct at [Our reports & policies - Responsible business | BT Plc](#)

8.2 Financial Difficulties

For the purpose of Joint Schedule 7 (Financial Difficulties), the Ratings Agencies listed within Annex 1 (Rating Agencies and their standard Rating System) will be Standard & Poor and Moody's and for Annex 2 (Credit Rating Thresholds) these will be BB+ for Standard and Poor and Ba1 for Moody's.

BT's published ratings are available [here](#)

8.3 Guarantee

For the purpose of Joint Schedule 8 (Guarantee), the Buyer does not require a Guarantee from the Supplier to award the contract.

8.4 IPR

For the purpose of Call-Off Schedule 1 (Intellectual Property Rights) **Part A Option A3: Supplier ownership of all New IPR with Buyer rights for the current contract only;** applies and is not further amended on the Call-Off Order Form under INTELLECTUAL PROPERTY RIGHTS.

8.5 Staff Transfer

No staff transfer is required and for the purposes of Call-Off Schedule 2 (Staff Transfer) **Part C: No Staff Transfer on the Start Date** only applies.

8.6 ICT Services

The Supplier will not be required to comply with the Buyers ICT Policies and the Call-Off Order Form option under ICT POLICY will confirm **For the purpose of Call-Off Schedule 6 (ICT Services) Supplier is not required to comply with the ICT Policy.** Any maintenance of the ICT environment, where applicable, will be defined within this Service Definition document and the option under MAINTENANCE OF THE ICT ENVIRONMENT within the Call-Off Order Form will be marked as **Maintenance Schedule to be provided by the Supplier NO**

8.7 Business Continuity and Disaster Recovery

Call-Off Schedule 8 (Business Continuity and Disaster Recovery) will be based on the details within this Service Definition document and the Suppliers standard BCDR plan and **optional clause 2.3.4 and optional supporting clause 10 (Insolvency Continuity Plan (Section 4)) is marked as not used.** For the purpose of clause 6 (Review and changing the BCDR Plan) and clause 7 (Testing the BCDR Plan), this will be carried out by the Supplier **in line with the details defined within the Suppliers standard BCDR plan.**

8.8 Corporate Resolution Planning

Due to the nature of the services within scope of this service offer, which is available only when the Call-Off Contract is not a Critical Service Contract, clauses 3 to 5 shall apply to Call-Off Schedule 24 (Corporate Resolution Planning).

8.9 Exit Management

Optional Call-Off Schedule 10 (Exit Management) is excluded and at the end of the Call Off Contract Period, the offboarding process will be managed in line with the details defined within the Suppliers Digital Marketplace submission and where applicable within this Service Definition document. The Call-Off Order Form SPECIFIC EXIT MANAGEMENT ASSISTANCE (LOT 1A AND LOT 1B ONLY) and VIRTUAL LIBRARY will both also marked as not applicable.

8.10 Installation Works

Due to the nature of service within scope of this service offer, optional Call-Off Schedule 11A (Installation Works – Crown Hosting) is excluded . If required, optional Call-Off Schedule 11 (Installation Works) will apply only.

8.11 Clustering and Leasing

Services will be contracted and invoiced to the Buyers detailed within Framework Schedule 6 (Order Form Template) and as such optional Call-Off Schedule 12 (Clustering) is excluded.

Due to the nature of the services within scope of this service offer, leasing of services is not applicable and as such, optional Call-Off Schedule 22 (Lease Terms) is also excluded.

8.12 Implementation Plan and Testing

Due to the nature of the services within scope of this service offer, optional Call-Off Schedule 13 (Implementation Plan and Testing) is excluded and the services in scope will be implemented and tested in line with the details defined within the Suppliers Digital Marketplace submission and this Service Definition document.

8.13 Performance Levels

Due to the nature of the service within scope of this service offer, optional Call-Off Schedule 14 (Performance Levels) is excluded and the service levels provided are as defined within the Suppliers Digital Marketplace submission and this Service Definition document.

8.14 Service Credits

Any service credits for the services within scope of this service offer will be as detailed, where applicable, within this Service Definition document and SERVICE CREDITS within the Call-Off Order Form will be marked accordingly.

8.15 Call-Off Schedule 17 (MOD Terms)

Where optional Call-Off Schedule 17 (MOD Terms) is required, this will be based on no additional DEFCONS or DEFFORMS being added within Annex 1 which incurs additional costs to the Supplier.

8.16 Call-Off Specification and Deliverables

The services will be delivered in line with the Suppliers Digital Marketplace submission and this Service Definition document and as such, optional Call-Off Schedule 20 (Call-Off Specification) is excluded.

8.17 Call-Off Special Terms

Due to the nature of the services within scope of this service offer based on the Supplier's standard offering for this cloud service, no additional call off special terms are introduced into the Call-Off Order Form under CALL OFF SPECIAL TERMS

8.18 Service Request Process

The service request process will be as defined within the Suppliers Digital Marketplace submission and this Service Definition document and SERVICE REQUEST PROCESS within the Call-Off Order Form will be marked accordingly.

8.19 Minimum Commitments

Any MINIMUM COMMITMENT(S) where applicable noted within Call-Off Order Form will be aligned to those as defined within the Suppliers Digital Marketplace submission and Suppliers Price Card where applicable and MINIMUM COMMITMENT(S) within the Call-Off Order Form will be marked accordingly.

8.20 Maximum Liability

The limitation of liability for this Call-Off Contract remains as stated in Clause 14.2 of the General Terms (as that Clause 14.2 has been amended pursuant to Framework Special Term 12 as set out in the Framework Award Form) and is not further amended on the Call-Off Order Form under MAXIMUM LIABILITY.

8.21 Additional Insurances

There is no requirement for additional insurances which will remain as defined within Joint Schedule 3 (Insurance Requirements) and ADDITIONAL INSURANCES on the Call-Off Order Form will be marked as not applicable.

8.22 Product Roadmaps

Any defined product roadmaps, where applicable, will be defined within this Service Definition document and PRODUCT ROADMAP (IF APPLICABLE) within the Call-Off Order Form will be marked as not used.

8.23 Quality Plans

Any defined quality maps, where applicable, will be defined within this Service Definition document and the option under QUALITY PLANS within the Call-Off Order Form will be marked as not applicable.

8.24 Social Value Commitment

Social value is at the heart of our purpose, driving impactful initiatives that address the needs of diverse communities across the UK. Our dedicated Social Value team have a focus on sustainability, community, sponsorship, charity, and the environment.

We're increasing digital inclusion and giving back to local communities through on-the-ground initiatives that make real-world positive changes.

The five pillars of social value at BT are:

- Outreach: no one is forgotten in our social value delivery.
- Improvement: continuous improvement in our delivery.
- Sustainability: our incentives are built to last.
- Engagement: user voice at the forefront and not an afterthought.
- Equity: leveraging our power to mobilise individuals, institutions, and communities

Details and reporting on what we are doing around social value can be found here [Social Value At BT | About Us](#) and SOCIAL VALUE COMMITMENT within the Call-Off Order Form will be marked accordingly and no additional bespoke commitments or reporting will be included.



Copyright

© British Telecommunications plc 2026

Registered office: One Braham, Braham Street, London, E1 8EE

Registered in England no. 1800000

BT is an ISO 9001 Registered Company

Company information

Parent Company: BT Group plc

Company Legal Entity Name: British Telecommunications plc

Company Trading Name: BT

Address: One Braham, Braham Street, London, E1 8EE

Web Address: <https://business.bt.com/>