Sovereign Cloud
Schedule to the General Terms

Part A – The Sovereign Cloud Service

1 Service Summary

BT's Sovereign Cloud Service is a fully managed service whereby BT will provide, manage and monitor your single and/or multi-tenanted virtual infrastructure, comprising:

1.1 the Standard Service Components; and

1.2 any of the Service Options as set out in any applicable Order,

up to the point of the Service Management Boundary as set out in Paragraph 4 ("**Sovereign Cloud Service**").

2 Standard Service Components

BT will provide you with the following standard service components ("**Standard Service Components**") in accordance with the details as set out in any applicable Order:

2.1 **An ITIL aligned secure Cloud Infrastructure platform** that will allow BT to build Virtual Machines as well as amend, add or remove various computing elements and associated services on your behalf (the "**Sovereign Cloud Platform**");

2.2 **A minimum set of computing elements to create a Virtual Machine**:

2.2.1 **An Operating System:** for the Virtual Machine being created to build the Sovereign Cloud Service;

2.2.2 **A Hypervisor**: being a hardware virtualisation technique that allows multiple guest Operating Systems to run on a single host system at the same time. The guest Operating System shares the hardware of the host computer such that each Operating System appears to have its own processor, memory and other hardware resource;

2.2.3 **Other compute components**: vCPUs, vRAM and C drive / root storage;

2.2.4 **Dedicated or shared storage**: the Virtual Machine will include storage allocation and a C drive / root storage where the Operating System will reside. A build consists of processors, RAM and C drive / root storage;

2.2.5 **Affinity rules**: between the Virtual Machine and the host; and

2.2.6 **Licences**: for using the Virtual Machine.

2.3 **An NCSC-compliant VMware environment** based on one of two options:

2.3.1 **Single tenant:**

(a) Dedicated VMware infrastructure and storage;

(b) Dedicated cabinets with full access management and auditing;

(c) Fully resilient dual-data centre design with fully managed Disaster Recovery;

(d) Fully configured and hardened protection profile compliant EAL4+ (Evaluation Assurance Level) firewalls;

(e) NCSC-compliant active directory policy with OS hardening as standard; and

(f) Automatic enrolment of all VMs in management tooling.

2.3.2 **Multi-tenant:**

(a) Choice of dedicated or shared Hypervisors (within the same security domain);

(b) Shared storage with the same security domain;

(c) Dedicated cabinets to the Sovereign Cloud Service with full access management and auditing;

(d) Fully resilient dual-data centre design with fully managed Disaster Recovery;

(e) Fully configured and hardened protection profile compliant EAL4+ firewalls;

(f) NCSC-compliant active directory policy with OS hardening as standard; and

(g) Automatic enrolment of all VMs in management tooling.

2.4 **Lead Engineer**

2.4.1 BT will provide access to a lead engineer during Business Hours to remotely conduct ongoing operational review, assessment, and reporting to support operational management, strategic planning and cost

optimisation for supported Production Environment(s), per the service tier and cadence set out in the Order ("**Lead Engineer**").

2.4.2 Lead Engineers assigned as part of the Sovereign Cloud Service are not dedicated or integrated into your business and may be reallocated to other projects and replaced with substitute Lead Engineers.

2.5 **Managed Virtual Machine**

2.5.1 BT will monitor the performance, availability and network connectivity of your Production Environment(s). For these purposes, a Virtual Machine will be deployed to provide centrally managed security and monitoring capabilities for the applicable elements within your Production Environment(s), consisting of:

(a) end-point security management;

(b) File Integrity Monitoring ("**FIM**"); and

(c) monthly vulnerability scanning.

2.6 **Proactive Operational Management:**

2.6.1 **Firewall management**: firewalls are fully managed by BT to ensure network traffic follows the pre-defined routing within the Production Environment, and that the firewall configuration is maintained to comply with NCSC guidance.

2.6.2 **Security incident logging**: Security incident and event monitoring ("**SIEM**") solution to support security incident investigation and remediation activities. SIEM logs are retained for a minimum of 12 months.

2.6.3 **Guest OS support**: Linux and Windows Operating System versions for your workload.

2.6.4 **Backup and recovery**: All requested Virtual Machines are enrolled for image-level backups of the Operating System and associated local storage as standard backup for your workload.

2.6.5 **Disaster Recovery**: Virtual Machines nominated for Disaster Recovery are replicated to the second site. A tiered service is offered based on mutually agreed RTO and RPO.

2.6.6 **Vulnerability scanning and remediation**: BT will configure monthly scans which includes a vulnerability management solution as standard.

2.6.7 **Anti-virus and malware endpoint protection**: An anti-malware protection tool is deployed to all supported Virtual Machines. The tool will deploy an agent to each Virtual Machine that checks for updates and can work in isolation should circumstances require. Alerts generated by the service are monitored 24/7, with alerting configured to meet NCSC security monitoring standards.

2.6.8 **Workload monitoring**: BT will deploy a standard monitoring configuration but can support customer-specific configurations if needed. Any change to standard monitoring may incur additional setup costs and ongoing management Charges.

2.6.9 **System patching**: BT is responsible for maintaining patch levels on all supported elements within your workload. The Sovereign Cloud Service includes a patching solution that can be configured to meet your individual operational restrictions. BT will work with you to design a suitable maintenance schedule, ensuring that patching does not interfere with critical business operations. Any critical 'out-of-band' patch requests may require the waiver of relevant Service Levels.

3 Service Options

BT will provide you with any of the following options ("**Service Options**") as set out in any applicable Order and in accordance with the details as set out in that Order:

3.1 **Virtual Machine Configuration (Type and Size):**

3.1.1 You will select the type of Virtual Machine you require from the Virtual Machine attributes made available to you by BT.

3.1.2 You may, in order to increase the size of the Virtual Machine (in terms of CPU and RAM), request that BT either builds a new Virtual Machine or modifies your then-current Virtual Machine.

3.2 **Templates**

3.2.1 You will select the Operating System for the Virtual Machine from the Templates made available to you by BT.

3.3 **Storage**

3.3.1 You may order additional drives in order to increase the storage for the Virtual Machine. BT will make a number of different size drives available to you or provide the option to purchase a customer-defined

capacity. Any additional storage beyond the standard storage capability set out in Paragraph 2.2.4 will be subject to additional Charges, as specified in the applicable Order.

3.4 **Network connectivity**

3.4.1 You may order different network offerings to provide connectivity between Virtual Machines and to and from the Internet and/or private network (MPLS VPN) and/or inter-Site connectivity between the data centres.

3.4.2 Additional BT (or other licenced operators) network services are not part of the Sovereign Cloud Service. You may order them separately and separate terms and conditions and Charges will apply.

3.5 **Backup**

3.5.1 You may order VM Snapshots to provide back up for the Sovereign Cloud Service. VM Snapshots are defined per Virtual Machine disk volume, and you may specify the frequency and timing of VM Snapshots from the available options, as agreed with BT.

3.6 **Managed Services**

3.6.1 Managed OS

(a) Where a Virtual Machine is enrolled in OS administration, BT will create a configuration management database record of the Virtual Machine and securely store OS login credentials provided by you.

(b) BT will, on your request, access the guest OS of a Virtual Machine using secure, time-limited and audited access in order to provide troubleshooting services for supported systems.

3.6.2 Managed OS Patching

(a) BT will provide a managed OS patching service for supported operating systems. The patching schedule will be set by you and BT will configure the guest OS to use Supplier-provided patching sources so that only approved patches are delivered and installed on your machines.

3.6.3 Managed OS Monitoring

(a) BT will install, configure, and respond to monitoring alerts from an installed OS agent for OS and application alerts and conditions on Virtual Machines. The installed OS agent will be used to provide monitoring of guest OS service availability on a network, internal OS system resources, OS services operational status, and error conditions , using default thresholds.

3.6.4 Managed OS Antivirus

(a) BT will take all reasonable steps (including testing) to ensure that any Software used in the Virtual Machine will provide protection against viruses.

(b) You are responsible for ensuring that necessary resources are available within the Virtual Machines to support the performance of the anti-virus Software, and that application-level or customer-specific network policies or equivalents do not impair its effective operation.

3.7 **Additional Licences**

3.7.1 You may order additional licences to use the Sovereign Cloud Service from BT as set out in the applicable Order.

3.8 **ISO Images**

3.8.1 Where you require a particular Operating System that is not available as a Template, BT may build the Virtual Machine using an ISO Image as agreed with BT.

3.9 **Disaster Recovery**

3.9.1 BT will provide you with the ability to build a Virtual Machine with or without Software, network and licences, for use in the event of a disaster affecting the Virtual Machine at the primary Site ("**Disaster Recovery**").

3.9.2 You are responsible for ensuring that you have processes and procedures in place to invoke Disaster Recovery.

4 Service Management Boundary

4.1 BT will provide and manage the Sovereign Cloud Service in accordance with Parts B and C of this Schedule and as set out in any applicable Order up to the Hypervisor layer including the management stack ("**Service Management Boundary**").

4.2 You will be responsible for managing your Operating System and application environments.

4.3 Except for items described above in Paragraphs 2 and 3 and as set out in any applicable Order, BT accepts no responsibility for any virtual or physical infrastructure or Enabling Services. If BT provides you with any Enabling Services, these are provided in accordance with their separate terms.

4.4 BT will have no responsibility for the Sovereign Cloud Service outside the Service Management Boundary.

4.5 BT does not make any representations, whether express or implied, about whether the Sovereign Cloud Service will operate in combination with any Customer Equipment or other equipment and software.

5 Associated Services

5.1 You will have the following services in place that will connect to the Sovereign Cloud Service and are necessary for the Sovereign Cloud Service to function and will ensure that these services meet the minimum technical requirements that BT specifies:

5.1.1 remote access capability;

5.1.2 network connectivity; and

5.1.3 secure tunnelling capability (each an "**Enabling Service**").

5.2 If BT provides you with any services other than the Sovereign Cloud Service (including but not limited to any Enabling Service) this Schedule will not apply to those services, and those services will be governed by their separate terms.

6 Specific Terms

6.1 **Minimum Period of Service**

6.1.1 BT will provide you with the Sovereign Cloud Service for the Minimum Period of Service.

6.1.2 You may request an extension to the Sovereign Cloud Service for a Renewal Period by Notice in writing to BT at least 120 days before the end of the Minimum Period of Service or Renewal Period ("**Notice of Renewal**").

6.1.3 If you issue a Notice of Renewal in accordance with Paragraph 6.1.2, BT will extend the Sovereign Cloud Service for the Renewal Period and:

(a) BT will continue to provide the Sovereign Cloud Service;

(b) the Charges applicable during the Minimum Period of Service may cease to apply and BT will inform you of any new Charges and invoice you the new Charges as set out in your new Order from expiry of the Minimum Period of Service; and

(c) both of us will continue to perform each of our obligations in accordance with the Contract.

6.1.4 If you do not issue a Notice of Renewal in accordance with Paragraph 6.1.2, BT will cease delivering the Sovereign Cloud Service at the time of 23:59 on the last day of the Minimum Period of Service or subsequent Renewal Period.

6.1.5 BT may propose changes to this Schedule or the Charges (or both) by giving you Notice at least 90 days prior to the end of the Minimum Period of Service and each Renewal Period ("**Notice to Amend**").

6.1.6 Within 21 days of any Notice to Amend, you will provide BT Notice:

(a) agreeing to the changes BT proposed, in which case those changes will apply from the beginning of the following Renewal Period;

(b) requesting revisions to the changes BT proposed, in which case both of us will enter into good faith negotiations for the remainder of that Minimum Period of Service or Renewal Period, as applicable, and, if agreement is reached, the agreed changes will apply from the beginning of the following Renewal Period; or

(c) terminating the Contract at the end of the Minimum Period of Service or Renewal Period, as applicable.

6.1.7 If we have not reached agreement in accordance with Paragraph 6.1.6(b) by the end of the Minimum Period of Service or the Renewal Period, the terms of this Schedule will continue to apply from the beginning of the following Renewal Period unless you give Notice in accordance with Paragraph 6.1.6(c) or BT may give

Notice of termination, in which case BT will cease delivering the Sovereign Cloud Service at the time of 23:59 on the last day of the Minimum Period of Service or subsequent Renewal Period as applicable.

6.2 **Termination for Convenience**

For the purposes of Clause 17 of the General Terms, either of us may, at any time after the Service Start Date and without cause, terminate the Sovereign Cloud Service by giving 120 days' Notice to the other (the "**Notice Period**").

6.3 **Customer Committed Date**

6.3.1 If you request a change to the Sovereign Cloud Service or any part of the Sovereign Cloud Service, then BT may revise the Customer Committed Date to accommodate that change.

6.3.2 BT may expedite delivery of the Sovereign Cloud Service for operational reasons or in response to a request from you, but this will not revise the Customer Committed Date.

6.4 **IP Addresses**

6.4.1 Except for IP Addresses expressly registered in your name, all IP Addresses made available with the Sovereign Cloud Service will at all times remain BT's property or the property of BT's suppliers and are non-transferable.

6.4.2 All of your rights to use IP Addresses will cease on termination or expiration of the Sovereign Cloud Service.

6.5 **EULA**

6.5.1 You will comply with any registration or authorisation process that BT or the Supplier presents to you in order to use any Software provided as part of the Sovereign Cloud Service.

6.5.2 If applicable, you will accept and enter into any end user licence agreement that BT or the Supplier provides to you and as may be amended or supplemented from time to time by BT or the Supplier ("**EULA**"). The details of such EULA will be set out on the Order.

6.5.3 Unless otherwise permitted by the terms of the applicable EULA, you may not:

(a) assign, grant, or transfer any interest in third party services or third party software to another individual or entity;

(b) reverse engineer, decompile, copy, or modify the third party software;

(c) modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the third party software; or

(d) exercise any of the reserved Intellectual Property Rights provided under the laws of England and Wales.

6.5.4 You will observe and comply with the EULA for any use of the applicable Software. In addition to any rights BT may have under Clause 15 of the General Terms, if you do not comply with the EULA, BT may restrict or suspend the Sovereign Cloud Service upon reasonable notice, and:

(a) you will continue to pay the Charges for the Sovereign Cloud Service until the end of the Minimum Period of Service; and

(b) BT may charge a re-installation fee to re-start the Sovereign Cloud Service.

6.5.5 You will enter into the EULA for your own benefit and the rights, obligations, acknowledgements, undertakings, warranties, and indemnities granted in accordance with the EULA are between you and the Supplier and you will deal with the Supplier with respect to any loss or damage suffered by either you or the Supplier as such loss or damage will not be enforceable against BT.

6.5.6 Where the EULA is presented in a 'click to accept' function and you require BT to configure or install software on your behalf, BT will do so as your agent and bind you to the EULA. For this purpose, you hereby grant to BT a mandate to enter into the EULA in your name and on your behalf. BT and you may for this also execute a power of attorney as part of the Order.

6.5.7 If you use any non-BT or non-Supplier provided software on the Customer Configuration, then you represent and warrant that you shall maintain:

(a) the legal right to use the software; and

(b) as applicable to the Sovereign Cloud Service, adequate original software vendor support (or similar authorized support) permitting BT to perform any installation, patching, upgrades, or management which BT has agreed to provide under the Contract.

6.5.8 On BT's request, you shall sufficiently certify in writing (or, as reasonably requested, evidence) that you are compliant with this section and any other licence or support obligations under the Contract. If you fail to certify licensing or support as requested, BT may charge you its standard fee for licenced use of the software, until the required certification is provided.

6.5.9 You may only use third party services and third party software provided for use as part of the Sovereign Cloud Service (as identified on the Order) on that portion of the Customer Configuration for which it was originally

provided, subject to any additional restrictions identified in the Order. You shall not be permitted to access any third party software which BT installs solely to assist the delivery of the Sovereign Cloud Service.

6.5.10 Upon termination of the Sovereign Cloud Service, you shall permit removal of any third party software installed by BT or its representatives on the Customer Configuration.

6.6 **Invoicing**

6.6.1 BT will invoice you for the following Charges in the amounts set out in any applicable Order:

(a) Installation Charges, on the Service Start Date;

(b) On the Customer Committed Date, you will be invoiced for the first and second month's Recurring Charges, except Usage Charges, in advance. Thereafter Recurring Charges, except Usage Charges, will be invoiced in advance on the first day of the relevant month and for any period where the Sovereign Cloud Service is provided for less than one month, the Recurring Charges will be calculated on a pro rata basis;

(c) Usage Charges, monthly in arrears on the first day of the relevant month, calculated at the then current rates;

(d) Professional Services Charges;

(e) De-installation Charges within 60 days of de-installation of the Sovereign Cloud Service; and

(f) any Termination Charges incurred in accordance with Paragraph 6.8 upon termination of the relevant Service.

6.6.2 BT may invoice you for any of the following Charges in addition to those set out in any applicable Order:

(a) Charges for investigating Incidents that you report to BT where BT finds no Incident or that the Incident is caused by something for which BT is not responsible under the Contract;

(b) Charges for commissioning the Sovereign Cloud Service in accordance with Paragraph 7.2 outside of Business Hours;

(c) Charges for expediting provision of the Sovereign Cloud Service at your request after BT has informed you of the Customer Committed Date; and

(d) any other Charges as set out in any applicable Order or as otherwise agreed between both of us.

6.7 **Cancellation and Charges at the end of the Contract**

6.7.1 Cancellation Charges

For the purposes of Clause 16 of the General Terms, if you cancel an Order, or part of it, any time before the Service Start Date you will pay BT the Cancellation Charges as set out below:

(a) the Termination Charges detailed in your Order; or

(b) If the Order does not include Termination Charges, you will pay the Supplier Termination Charges.

6.8 **Charges at the end of the Contract**

6.8.1 If you terminate the Contract or the Sovereign Cloud Service for convenience in accordance with Clause 17 of the General Terms you will pay BT:

(a) all outstanding Charges or payments due and payable under the Contract (including for any services that are or would have been performed during any Notice Period whether or not the Notice Period is adhered to);

(b) De-installation Charges;

(c) any other Charges as set out in any applicable Order; and

(d) any charges reasonably incurred by BT from a supplier as a result of the early termination.

6.8.2 In addition to the Charges set out at Paragraph 6.8.1 above, if you terminate during the Minimum Period of Service, you will pay BT:

(a) the Minimum Period Termination Charges; and

(b) BT will refund to you any money you have paid in advance after deducting any Charges or other payments due to BT under the Contract.

6.8.3 In addition to BT's other rights and remedies, the Charges set out at Paragraphs 6.8.1 and 6.8.2 will also apply where BT terminates the Contract or the Sovereign Cloud Service under Clauses 18.1.1 or 18.1.2 of the General Terms.

6.9 **PCI DSS Compliance Obligations**

6.9.1 The Sovereign Cloud Service is not compliant with PCI DSS, and you will not use the Sovereign Cloud Service for the processing, storage or transmission of any Cardholder Data or any data that is subject to PCI DSS.

6.9.2 You will indemnify BT for any Claims, losses, costs or liabilities that it incurs as a result of you storing, processing or transmitting data that is subject to PCI DSS.

6.10 **Export of Content using Cloud Services**

6.10.1 The Service comprises a cloud service that utilises Software and technology that may be subject to export control laws of various countries. You are solely responsible for any compliance related to the way you use the Service and the location the Service is used including access by Users to the Service and for your Content transferred or processed using the Service, including any publication of such Content.

6.10.2 You will indemnify BT against all Claims, losses, costs or liabilities brought against BT as a result of, or arising out of or in connection with, your non-compliance with any laws (including sanctions and export control laws) of any country you use, access or transfer Content to.

6.11 **Supplier Product Terms and Indemnity**

6.11.1 You acknowledge that you have read and agree to be bound by and to ensure that any of your Users will comply with:

(a) generally accepted Internet standards; and

(b) the Supplier Product Terms and the Supplier Acceptable Use Policy as set out in Part D.

6.11.2 In the event of a third-party claim against BT and/or BT's Supplier arising out of your breach of Paragraph 6.11.1, you shall hold BT and its Supplier harmless and pay the cost of defending the claim (including reasonable legal and professional charges and expenses) and any damages, losses, fines, or other penalties resulting from the claim. The indemnification obligations set out in this Paragraph 6.11.2 are applicable only to the extent that such claims are arising out of your acts or omissions (inclusive of claims resulting from any portion of the Customer Configuration being accessed due to failure to use reasonable security precautions, even when access or the acts or omissions of such persons were not authorised by BT).

6.12 **End of Life**

6.12.1 Where the Sovereign Cloud Service is designated as a Deprecated Service by BT's Supplier, BT has no obligation to continue providing the Sovereign Cloud Service and/or any manner of support for the Sovereign Cloud Service.

6.12.2 If the Sovereign Cloud Service is designated as a Deprecated Service by BT's Supplier, BT may at any time in its sole discretion on at least 60 days' Notice terminate that portion of the Sovereign Cloud Service pursuant to which the Deprecated Service was purchased, and BT will remove all associated service elements from the Customer Configuration, except where such Deprecated Service is determined by BT to pose an un-remediable security risk to BT, the Supplier or BT's customers, in which case BT will immediately terminate such Deprecated Service.

6.13 **Customer Hosted Data**

6.13.1 All Customer Hosted Data shall be stored and processed in the UK. Some business support data which may include data required to configure the Sovereign Cloud Service or for order and Incident management and billing may be processed outside of the UK.

6.13.2 In the event that BT or the Supplier cannot resolve an Incident, BT or the Supplier may engage support services located outside of the UK and provide access to your Sovereign Cloud Platform. Prior to providing this access BT will:

(a) Provide you with notice of the reasons for the access; and

(b) Obfuscate as far as practicable any Customer Hosted Data.

6.13.3 BT's commitment to storing and processing Customer Hosted Data in accordance with this Paragraph 6.13 shall not apply to any third-party services, software, technology or licences used in connection with the Sovereign Cloud Service which are not provided by BT.

Part B – Service Delivery and Management

7 BT's Obligations

7.1 **Service Delivery**

7.1.1 Before the Service Start Date, BT will provide you with contact details for the Service Desk.

7.2 **Commissioning of the Service**

Before the Service Start Date, BT will:

7.2.1 configure the Sovereign Cloud Service;

7.2.2 conduct a series of standard tests on the Sovereign Cloud Service to ensure that it is configured correctly;

7.2.3 connect the Sovereign Cloud Service to each Enabling Service; and

7.2.4 on the date that BT has completed the activities in this Paragraph 7.2, confirm to you the Service Start Date.

7.3 **During Operation**

On and from the Service Start Date, BT:

7.3.1 will respond and use reasonable endeavours to remedy an Incident without undue delay if BT detects or if you report an Incident;

7.3.2 will work with the Supplier to restore service as soon as practicable during Local Contracted Business Hours if BT detects, or if you report an Incident;

7.3.3 may carry out maintenance from time to time and will use reasonable endeavours to inform you at least three Business Days before any Planned Maintenance on the Sovereign Cloud Service, however, BT may inform you with less notice than normal where Maintenance is required in an emergency;

7.3.4 may, in the event of a security breach affecting the Sovereign Cloud Service, require you to change any or all of your passwords.

7.4 **The End of the Service**

On termination of the Sovereign Cloud Service by either of us, BT:

7.4.1 will provide configuration information relating to the Sovereign Cloud Service provided in a format that BT reasonably specifies;

7.4.2 will decommission all network and applications supporting the Sovereign Cloud Service; and

7.4.3 may delete any Content, including stored logs or any configuration data relating to BT's management of the Service.

8 Your Obligations

8.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the Sovereign Cloud Service, you will:

8.1.1 provide BT with access to any Site(s) during Business Hours, or as otherwise agreed, to enable BT to set up, deliver and manage the Sovereign Cloud Service. In particular, for the Lead Engineer services, you will:

(a) provide access credentials to systems and accounts, technical assistance, documentation, and configuration data;

(b) coordinate maintenance windows and liaise with BT stakeholders; and

(c) not unreasonably withhold, delay or condition any approval, consent or authorisation required for provision of the Service;

8.1.2 without undue delay provide BT with any information or assistance reasonably required by BT to enable it to comply with Applicable Law and perform its obligations hereunder with respect to the Sovereign Cloud Service;

8.1.3 in jurisdictions where an employer is legally required to make a disclosure to its Users and other employees:

(d) inform your Users that as part of the Sovereign Cloud Service being delivered by BT, BT may monitor and report to you the use of any targeted applications by them;

(e) ensure that your Users have consented or are deemed to have consented to such monitoring and reporting (if such consent is legally required);

(f) be responsible for your Content and your Users' Content (including any Content hosted by you or any User on behalf of third parties); and

(g) agree that BT will not be liable for any failure by you to comply with this Paragraph 8.1.3, you will be liable to BT for any Claims, losses, costs or liabilities incurred or suffered by BT due to your failure to comply with this Paragraph 8.1.3.

8.2 **During Operation**

On and from the Service Start Date, you will:

8.2.1 ensure that Users report Incidents to the Customer Contact and not to the Service Desk;

8.2.2 ensure that the Customer Contact will take Incident reports from Users and pass these to the Service Desk using the reporting procedures agreed between both of us, and is available for all subsequent Incident management communications;

8.2.3 where you have provided your own or a third party Enabling Service, ensure and confirm to BT that the Enabling Service is working correctly before reporting Incidents to BT;

8.2.4 inform BT of any planned maintenance on any third party provided Enabling Service;

8.2.5 provide service assurance support to BT, where reasonably requested, to progress the resolution of Incidents for any BT equipment installed on an Enabling Service that is not being provided by BT;

8.2.6 monitor and maintain any Customer Equipment connected to the Sovereign Cloud Service or used in connection with a Sovereign Cloud Service;

8.2.7 ensure that Customer Equipment that is connected to the Sovereign Cloud Service or that you use, directly or indirectly, in relation to the Sovereign Cloud Service is:

(a) connected using the applicable connections, unless you have BT's permission to connect by another means;

(b) adequately protected against viruses and other breaches of security;

(c) technically compatible with the Sovereign Cloud Service and will not harm or damage BT Equipment, or any of BT's suppliers' or subcontractors' infrastructure or equipment; and

(d) approved and used in accordance with relevant instructions, standards and Applicable Law and any safety and security procedures applicable to the use of that Customer Equipment;

8.2.8 immediately disconnect any Customer Equipment, or advise BT to do so at your expense, where Customer Equipment:

(a) does not meet any relevant instructions, standards or Applicable Law; or

(b) contains or creates material that is in breach of the Acceptable Use Policy and you are contacted by BT about such material,

and redress the issues with the Customer Equipment prior to reconnection to the Sovereign Cloud Service;

8.2.9 be responsible for the management of your account (including creation, change management and termination), and enforcement of related remote working and password controls;

8.2.10 distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the Sovereign Cloud Service;

8.2.11 maintain a written list of current Users and provide a copy of such list to BT within five Business Days following BT's written request at any time;

8.2.12 ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with the Sovereign Cloud Service and:

(a) immediately terminate access for any person who is no longer a User;

(b) inform BT immediately if a User's ID or password has, or is likely to, become known to an unauthorised person, or is being or may be used in an unauthorised way;

(c) take all reasonable steps to prevent unauthorised access to the Sovereign Cloud Service;

(d) satisfy BT's security checks if a password is lost or forgotten; and

(e) change any or all passwords or other systems administration information used in connection with the Sovereign Cloud Service if BT requests you to do so in order to ensure the security or integrity of the Sovereign Cloud Service;

8.2.13 Where you require physical access to a Site, the Customer Contact shall submit a Site visit request to BT in writing at least forty-eight (48) hours prior to the proposed visit with the following details:

(a) Customer name;

(b) Visiting engineer name (who must present government issued photo ID when visiting);

(c) Date and time of the Site visit;

(d) The relevant cabinet or rack to be accessed; and

(e) Purpose of the Site visit

Shorter notice may be accepted on case-by-case basis, in the event of an emergency or where it is required to comply with Applicable Law;

8.2.14 ensure that the maximum number of Users will not exceed the permitted number of User identities as set out in any applicable Order; and

8.2.15 not allow any User specific subscription to be used by more than one individual User unless it has been reassigned in its entirety to another individual User, in which case you will ensure the prior User will no longer have any right to access or use the Sovereign Cloud Service.

9 Notification of Incidents

Where you become aware of an Incident:

9.1 the Customer Contact will report it to the Service Desk;

9.2 BT will give you a Ticket;

9.3 BT will inform you when it believes the Incident is cleared and will close the Ticket when:

9.3.1 you confirm that the Incident is cleared within 24 hours after having been informed; or

9.3.2 BT has attempted unsuccessfully to contact you, in the way agreed between both of us in relation to the Incident, and you have not responded within 24 hours following BT's attempt to contact you.

9.4 If you confirm that the Incident is not cleared within 24 hours after having been informed, the Ticket will remain open, and BT will continue to work to resolve the Incident.

9.5 Where BT becomes aware of an Incident, Paragraphs 9.2, 9.3 and 9.4 will apply.

Part C – Service Levels

10 Service Availability

10.1 **Availability Service Level**

10.1.1 From the Service Start Date, BT will provide the Sovereign Cloud Service with a monthly service availability target across the Sovereign Cloud Service of 99.999% ("Availability Service Level"). The measurement of service unavailability starts when BT acknowledges your Incident report with a Ticket. The period of unavailability will end when BT informs you that the Sovereign Cloud Service is available, unless you advise BT that the Sovereign Cloud Service remains unavailable.

10.1.2 The Availability Service Level is calculated as the Health Check availability measurements over the entire month (excluding any scheduled downtime).

10.1.3 BT will provide you with monthly Health Check reports via the Sovereign Cloud Service.

10.2 **Availability Service Credits**

10.2.1 The Availability Service Credit applicable for failure to meet the monthly Availability Service Level will be an amount equivalent to the average daily Charge for the Sovereign Cloud Service based on the total monthly Charges from the previous calendar month in which the Incident occurred divided by the number of days in that month.

10.2.2 Where the Availability Service Level is maintained via high availability, Disaster Recovery or other methods (e.g. your application based high availability, caching services), Availability Service Credits will only apply if the Sovereign Cloud Service is unavailable below the Availability Service Level and is evidenced and agreed to have been down in this period by both the Supplier and BT.

10.2.3 For each day during a calendar month where the Availability Service Level has not been met, you may submit a claim to BT for review. If upheld, the Availability Service Credit will be added to your account, subject to the following conditions:

(a) You may only make one Availability Service Level failure claim per month (for the avoidance of doubt, such single claim may cover multiple Availability Service Level failures within that month); and

(b) The aggregate Availability Service Credit amount shall never exceed the monthly Charges for the Sovereign Cloud Service.

10.3 **Disaster Recovery Service Levels**

10.3.1 Where you purchase the optional Disaster Recovery service set out in Paragraph 3.9, RPOs and RTOs shall not be set commensurate with the Compliance Baseline, but instead, the RPOs and RTOs shall be aligned with one of the following Disaster Recovery tiers set out in the applicable Order ("**Disaster Recovery Service Levels**"):

(a) Bronze - 24 hours

(b) Silver - 12 hours;

(c) Gold - 4 hours; or

(d) Platinum - 1 hour.

10.4 **Disaster Recovery Service Credit**

10.4.1 You shall be entitled to a Service Credit of £250 for each failure by BT in meeting the Disaster Recovery Service Levels.

11 Requests for Service Credits

11.1 You must make any request for applicable Service Credits in any one calendar month within 10 days of the end of the calendar month in which a Severity Level 1 Incident occurred by providing details of the reason for the claim. Any failure by you to submit a request in accordance with this Paragraph 11.1 will constitute a waiver of any claim for Service Credits for that calendar month.

11.2 If a single Severity Level 1 Incident or connected series of Incidents results in more than one Service Level failure, you shall have the right to select any one of such Service Level failures for which you shall be entitled to receive a Service Credit. You shall not be entitled to a Service Credit for the other Service Level failures related to the same Severity Level 1 Incident.

11.3 Upon receipt of a valid request for Service Credits in accordance with Paragraph 11.1:

11.3.1 BT will issue you with the applicable Service Credits by deducting those Service Credits from your invoice within three billing cycles of the request being received;

11.3.2 following expiry or termination of the Contract where no further invoices are due to be issued by BT, BT will pay you the Service Credits in a reasonable period of time; and

11.3.3 All Service Levels and Service Credits will be calculated in accordance with information recorded by, or on behalf of, BT.

11.4 The Service Levels under this Schedule will not apply:

11.4.1 in the event that Clause 8 or Clause 23 of the General Terms applies;

11.4.2 as a result of failures during any period when you elect not to release the Sovereign Cloud Service for testing and/or repair and you continue to use the Sovereign Cloud Service; or

11.4.3 during any trial period of the Sovereign Cloud Service.

Part D – Supplier Product Terms and Supplier Acceptable Use Policy

12 Supplier Product Terms

The following terms apply to your use of the Sovereign Cloud Service:

12.1 **Service Restrictions**

12.1.1 As part of the multi-tenant version(s) of the Sovereign Cloud Service, the Sovereign Cloud Platform will not grant you direct access to the following, without limitation:

(a) vCentre;

(b) multi-tenant firewall;

(c) host console; or

(d) switch configuration.

12.1.2 Eligibility to request access to the above features/components will be limited to the dedicated Sovereign Cloud Platform and access may be granted by exception only.

12.2 **Hardening**

12.2.1 BT hardens OSIs (Red Hat Enterprise Linux and Microsoft Windows Server only) and network devices to its configuration baseline based on the centre for internet security ("CIS") benchmarks. Any hardening requirements defined by you in addition to, or in lieu of, the CIS benchmarks configuration baseline shall be identified and set forth in the applicable Order(s), inclusive of any additional implementation and management Charges, prior to being implemented and provided as part of the Sovereign Cloud Service.

12.3 **Encryption**

12.3.1 Compliance Baseline encryption requirements for any software or program installed on top of the Supplier provided and managed OSIs are your sole responsibility.

12.4 **Backups**

12.4.1 BT performs image-based changed block tracking backups of Production Environment OSIs and Customer Appliances once per day. If file-level, database-level, or otherwise application-aware backups are required, you are responsible for providing a compatible backup solution – e.g., database-native backup to a local disk included in the daily image backup. Unless otherwise specified in the Order, the backups for Production Environment OSIs and Customer Appliances shall be available onsite for 14 calendar days, and the Production Environment backups shall be replicated from the primary backup location to the archival backup location available in the Disaster Recovery Site for the same 14-day period. You may request additional services for longer retention periods, as defined in the Order. Any required restores shall only be created from BT-provided disk images and presented to the OSI as a full disk. You may choose to replace the existing disk or mount as an additional disk; but all file-level, application or database recovery efforts are your responsibility.

12.5 **Customer defined controls**

12.5.1 Other controls, as additions to, or in lieu, of the provisionally authorized controls may be mutually agreed upon and included, provided there is no conflict with Applicable Law. All such controls shall be identified in the Order as a one-off set up Charge for the primary and secondary data centres inclusive of any additional implementation and management Charges, prior to being implemented and provided as part of the Sovereign Cloud Service.

12.6 **Quarterly Configuration Compliance Scanning and Reporting**

12.6.1 BT scans the managed OSIs for compliance with the BT-defined hardening configuration standard. The raw, unmodified compliance scan results shall be provided quarterly to you for each Production Environment. Any hardening configurations defined by you, other than the BT-defined configuration baseline, shall be stated in the applicable Order, which shall include additional implementation and management Charges. Any custom-configuration compliance scanning and associated reporting shall be stated in any applicable Order(s), which shall include additional implementation and management Charges.

12.7 **File Integrity Monitoring**

12.7.1 Monitoring the integrity of your data and/or application files installed by you on OSIs is excluded from the FIM solution monitoring scope of services. BT provides ongoing management of the FIM management servers; agents installed on OSIs; and associated configurations, updates, and policy management. In the event a FIM event is detected, BT shall notify and collaborate with you to determine the appropriate actions.

12.8 **Monthly Vulnerability Scanning**

12.8.1 BT performs monthly vulnerability scanning for each of your BT managed OSIs within your Production Environment(s). The scans are performed by BT, and the raw, unmodified vulnerability scan results shall be provided to you. We shall mutually agree on a monthly scanning schedule for the duration of the Sovereign Cloud Service. Any custom vulnerability scanning activities and associated reporting requested by you shall be stated in any applicable Order(s), which shall include additional implementation and management Charges. Your security obligations include immediately remediating any known security vulnerability of any Customer Appliance, or any software or program installed on top of the BT provided and managed hardware and software services.

12.9 **Customer-requested screening**

12.9.1 If you require personnel security approvals or clearances outside of BT's standard background investigation, then BT reserves the right to submit for approval and/or clearance its entire operations and security teams associated with the Sovereign Cloud Service to enable adequate support. You shall bear the costs and expenses incurred by BT in connection with obtaining approvals or clearances required to allow BT to perform its obligations hereunder.

12.10 **Contingency Planning**

12.10.1 BT maintains a Contingency Plan for the Cloud Infrastructure as required by Compliance Baseline requirements. BT shall support your Contingency Plan efforts by meeting the Recovery Point Objective and Recovery Time Objective in the event of a major disruption to the Production Environment. The SEAP shall be used to define the tools, processes, and procedures within BT's and your areas of responsibility. BT shall provide one Disaster Recovery Test per year, upon your request with written notice 30 days prior. This can include turning on Virtual Machines at a secondary facility; running specific workloads at a secondary facility in a temporary, non-impactful way; verifying data backup integrity; or testing for hardware outages.

12.11 **Disaster Recovery**

12.11.1 BT provides replication of your Production Environment OSIs and Customer Appliances to a Disaster Recovery Site. BT manages the Disaster Recovery Site and provides disaster recovery support services in accordance with the SEAP. Upon a Disaster Declaration, replicated VMs are activated by BT in the Disaster Recovery Site to seek to restore the Sovereign Cloud Service to support Restoration Success within the RPO and RTO. RTO does not include any third-party dependencies outside of BT's control, including Content from the Cloud Infrastructure coming back online and time required for external third-party components and network protocols to be migrated by third-party providers. Any other application-level activities to recover and reconstitute the Production Environment are your responsibility.

12.12 **Relocation**

12.12.1 BT may on reasonable notice move or relocate your Production Environment and disaster recovery services within or between data centre locations (located in the same country as the origin data centre and at the same security level). Additionally, BT may make changes to the provision of the Sovereign Cloud Service (including, but not limited to, changing the assigned IP addresses and DNS records and zones on BT or Supplier operated or managed DNS servers as BT deems necessary for the operation of the shared network infrastructure). BT will work with you to migrate to any other location.

12.13 **Customer Hosted Data**

12.13.1 BT makes no warranty as to the quality, contents, or formatting of Customer Hosted Data. You accept and acknowledge the limitations of data replication, specifically that data corruption and deletion within the Production Environment, both intentional and unintentional, will be replicated to the Disaster Recovery Site. As such, Disaster Recovery shall not be used as a replacement for application state and database backups, which remain your sole responsibility. Additionally, the rate at which the data in the Production Environment can be transferred to the Disaster Recovery Site shall vary depending on the rate of change, amount and type of data, constraints inherent in the Sovereign Cloud Service, and fluctuations in bandwidth availability. Therefore, at any given time, the Disaster Recovery Site may not be completely up to date. In the event of a failover to the Disaster Recovery Site, data that has not yet completed transfer from the Production Environment shall be lost commensurate with the Recovery Point Objective. You also accept and acknowledge that this same risk of data loss exists during execution of Disaster Recovery Testing. BT is not liable for any data loss as a result of performing Disaster Recovery Testing initiated by you, nor by executing your instructions in the event of a legitimate Disaster Declaration.

12.13.2 Customer Hosted Data is, and at all times shall remain, your exclusive property. You remain the primary system and account administrator and are responsible for the integrity, security, maintenance and appropriate protection of Customer Hosted Data including by:

(a) selecting, purchasing, and properly configuring appropriate services;

(b) implementing adequate controls to maintain appropriate security, protection, and deletion of Customer Hosted Data (which shall include end-to-end encryption of sensitive data in transit and at rest, and logical access measures);

(c) ensuring that BT is not provided with any access to Customer Hosted Data (including protected health information), except as required to deliver the Sovereign Cloud Service; and

(d) using the data integrity controls to allow you to restore the availability of Customer Hosted Data in a timely manner (which shall include routine backups and archiving of Customer Hosted Data in an environment separate from the Customer Configuration). BT makes available a number of security controls that you may elect to purchase as part of the Services. BT will only back up data to the extent purchased by you as part of the Sovereign Cloud Service and stated in the applicable Order.

12.13.3 The Sovereign Cloud Service provides you with controls that you may use to retrieve, correct, or delete Customer Hosted Data prior to expiry or termination of the Contract. Your access to the Customer Configuration or Customer Hosted Data may be restricted during a suspension or following termination of the Sovereign Cloud Service or the Contract. You are responsible for retrieving a copy of Customer Hosted Data prior to the termination of the Contract. BT may delete Customer Hosted Data at any time following termination of the Contract.

12.13.4 You will cooperate with investigation and resolution of outages and security incidents. BT is not responsible to you or any third party for unauthorized access to Customer Hosted Data or for unauthorized use of the Sovereign Cloud Service, including any losses or damages resulting from such unauthorized access or use, that is not solely caused by BT's failure to meet its security obligations under the Contract.

12.14 **Disaster Recovery and Business Continuity**

12.14.1 The Disaster Recovery services provided are not a full business continuity solution. They are intended to be a component in your managed and executed business continuity plan. As such, BT takes no responsibility for, and does not guarantee, any business continuity capabilities as a result of your use of the Disaster Recovery services.

12.15 **Baseline RPO and RTO**

12.15.1 Where you have not purchased Disaster Recovery services, the Sovereign Cloud Service shall be capable of meeting the RPOs and RTOs aligned with the Compliance Baseline. Unless otherwise specified in the Order the default RPOs and RTOs are both 24 hours.

12.16 **VM Replication Enhanced Edition.**

12.16.1 Solely where you purchase a Disaster Recovery service, 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 Order.

12.17 **Active-Active**

12.17.1 Alternatively, you can opt to deploy your Production Environments in an active-active manner, in which the Production Environment can also always be running in the Disaster Recovery Site. Notwithstanding, active-active configuration is your responsibility, outside of the scope of the base Sovereign Cloud Service configuration and would typically require application-level support.

12.18 **Security Incident Response**

12.18.1 In the event of a security incident in your Infrastructure, such as a denial-of-service attack, BT reserves the right to suspend the Sovereign Cloud Service without notice as necessary (e.g., powering off or network-isolating Customer Appliances and OSIs), until completion of remediation.

13 Supplier Acceptable Use Policy

13.1 You shall not use the Sovereign Cloud Service or any related software, system, or network to engage in, foster, solicit, or promote illegal, or irresponsible behaviour including:

13.1.1 intentionally, knowingly, or recklessly introducing any malicious code into the Sovereign Cloud Service;

13.1.2 conduct violating rules and conventions of any domain registrar, email service, bulletin board, chat group, or forum used in conjunction with the Sovereign Cloud Service or network (including using false, misleading, or deceptive TCP-IP packet header information in an email or newsgroup posting);

13.1.3 deceitfully collecting, transmitting, or using information, or distributing software which covertly gathers or transmits information about a User;

13.1.4 distributing advertisement delivery software unless the user affirmatively consents to download and installation based on clear and conspicuous notice of the nature of the software, and can easily remove software using standard tools included on major operating systems;

13.1.5 conduct likely to result in retaliation or adverse action against the Sovereign Cloud Service, BT, its Supplier, or BT or its Supplier's network, website, or representatives (including resulting in listing of BT or Supplier's IP space on an abuse database);

13.1.6 use of any BT or Supplier-provided shared system in a way that unnecessarily interferes with the normal operation of the shared system, or consumes a disproportionate share of system resources;

13.1.7 gambling activity violating any applicable codes of practice, required licences, or technical standards; and

13.1.8 in any situation where failure or fault of the Sovereign Cloud Service could lead to death or serious bodily injury of any person, or to physical or environmental damage (including in connection with aircraft or other modes of human mass transportation, or nuclear or chemical facilities).

13.2 **Mail Requirements**

13.2.1 For bulk or commercial email sent by or on behalf of you using the Sovereign Cloud Service or from any network that directly or indirectly refers recipients to a site hosted using the Sovereign Cloud Service (including using third party distribution lists), you shall:

(a) post a privacy policy for each associated domain;

(b) post an email address for complaints in a conspicuous place on any associated website, promptly respond to messages sent to that address, and have means to track anonymous complaints;

(c) obtain affirmative consent to receive e-mail from intended recipients using reasonable means to verify ownership of the e-mail address, honour and notify recipients of consent revocation, and evidence consent within 72 hours of the recipient's or BT's request; and

(d) include the recipient's e-mail address in the e-mail body or "TO" line.

13.3 **Domain Names, IP Addresses and DNS Records**

13.3.1 You must maintain valid information with your Domain Name registrar for any domain hosted on the Sovereign Cloud Service and only use IP Addresses assigned to you by BT in connection with the Sovereign Cloud Service. You agree that BT or its Supplier may modify, transfer, or delete any DNS record or zone on the Supplier managed or operated DNS servers or services upon request from the registrant or administrative contact according to the registrar's WHOIS system.

Part E – Minimum Period Termination Charges

		Minimum Period of Service		
Month of Minimum Period of Service when termination is effective ("**Termination Date**")		12 months	36 months	60 months
	Month 0-3	64%	49%	42%
	Month 4-6	68%	50%	43%
	Month 7-9	80%	52%	43%
	Month 10-12	100%	53%	44%
	Month 13-15	N/A	54%	45%
	Month 16-18		56%	46%
	Month 19-21		58%	47%
	Month 21-24		60%	48%
	Month 25-27		63%	49%
	Month 28-30		68%	50%
	Month 31-33		79%	51%
	Month 34-36		100%	52%
	Month 37-39		N/A	53%
	Month 40-42			54%
	Month 43-45			55%
	Month 46-48			56%
	Month 49-51			67%
	Month 52-54			78%
	Month 55-57			89%
	Month 58-60			100%

Example: a Termination Date within Month 0-3 of a 12-month Minimum Period of Service would result in Termination Charges equal to 64% of your remaining Recurring Charges for the Sovereign Cloud Service.

Part F – Defined Terms

14 Defined Terms

In addition to the defined terms in the General Terms, capitalised terms in this Schedule will have the below meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms, these defined terms will take precedence for the purposes of this Schedule). BT has repeated some definitions in this Schedule that are already defined in the General Terms. This is to make it easier for you to find the definitions when reading this Schedule.

"**A&A Package**" means the assessment and authorization set of documents, consisting of the System Security Plan, supporting security plans, test results, plan of action, and milestones.

"**Affinity**" means an affinity rule which ensures that a Virtual Machine remains attached to or runs on a specific host even after events like a stop/start, maintaining placement consistency.

"**Availability Service Credit**" means the Service Credit available for a failure to meet the Availability Service Level, as set out in Paragraph 10.2.1.

"**Availability Service Level**" has the meaning given in in Paragraph 10.1.

"**Business Hours**" means between the hours of 0900 and 1700 in a Business Day.

"**Cardholder Data**" means the unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

"**C drive / root storage**" means the storage location for the Operating System.

"**Cloud Infrastructure**" means the hardware and Software resources, which are located in enterprise-grade data centres, used to deploy the Sovereign Cloud Service, including the host servers, switches, firewalls, Hypervisor, and Operating System Instances provided by BT, as set forth in the Order(s). This excludes Customer Appliances.

"**Compliance Baseline**" means the defined set of security controls to which the Sovereign Cloud Service is managed.

"**Content**" means applications, data, information (including emails), video, graphics, sound, music, photographs, software or any other material.

"**Contingency Plan**" means the artifact of the Compliance Baseline A&A Package required by all cloud service providers. It denotes interim measures to recover information system services following an unprecedented emergency or system disruption.

"**CPU**" means central processing units.

"**Customer Appliance**" means any Virtual Machine owned and managed by you.

"Customer Configuration" means your information technology system (hardware, software, and/or other information technology components) which is the subject of the Sovereign Cloud Service or to which the Sovereign Cloud Service relates.

"**Customer Equipment**" means any equipment including any Purchased Equipment and any Software, other than BT Equipment, used by you in connection with a Sovereign Cloud Service.

"**Customer Hosted Data**" means all data which you receive, store, or transmit on or using the Customer Configuration.

"**De-installation Charges**" means any de-installation charges payable by BT to the Supplier.

"Deprecated Service" means a Supplier-provided element of the Sovereign Cloud Service, which may include Software, hardware, networking, storage, support, or any component thereof, that is designated "End of Sale", "End of Support" or "End of Life" by the Supplier.

"**Disaster Declaration**" means the submission by the authorised Customer Contact of a Ticket, via the process set out at Paragraph 9, declaring a disaster event and requesting that BT initiate a restoration of the Production Environment at its Disaster Recovery Site.

"**Disaster Recovery Site**" means the secondary site where your production data will be replicated.

"**Disaster Recovery Test**" or "**Disaster Recovery Testing**" means verifying the processes and services in place through simulated recovery of a mutually agreed-upon portion of the Production Environment in the Disaster Recovery Site.

"**Domain Name**" means a readable name on an Internet page that is linked to a numeric IP Address.

"**Enabling Service**" has the meaning given in Paragraph 5.1.

"**File Integrity Monitoring**" or "**FIM**" has the meaning set out at Paragraph 2.5.1.

"**General Terms**" means the general terms to which this Schedule is attached or can be found at www.bt.com/terms, and that form part of the Contract.

"**Health Check**" means the monthly reports for overall availability of each of the occupied PODs.

"Hypervisor" means the Software that provides the capability to deliver Virtual Machines.

"**Incident**" means an unplanned interruption to, or a reduction in the quality of, the Sovereign Cloud Service.

"**Installation Charges**" means those Charges set out in any applicable Order in relation to installation of the Sovereign Cloud Service.

"**Internet**" means a global system of interconnected networks that use a standard Internet Protocol to link devices worldwide.

"**Internet Protocol**" or "**IP**" means a communications protocol for devices connected to the Internet that specifies the format for addresses and units of transmitted data.
"**IP Address**" means a unique number on the Internet of a network card or controller that identifies a device and is visible by all other devices on the Internet.
"**ISO Image**" means a computer file that is an exact copy of an existing file system.
"**ITIL**" means Information Technology Infrastructure Library.
"**Local Contracted Business Hours**" means the times during which maintenance is provided, which are Business Hours unless set out otherwise in any applicable Order.
"**Minimum Period Termination Charges**" shall mean the Charges set out in Part E.
"**Minimum Period of Service**" means a period of 12, 36 or 60 consecutive months as specified in the Order beginning on the Service Start Date, unless set out otherwise in any applicable Order.
"**NCSC**" means National Cyber Security Centre.
"**Notice of Renewal**" has the meaning given in Paragraph 6.1.2.
"**Notice to Amend**" has the meaning given in Paragraph 6.1.5.
"**Operating System(s)**" or "**OS**" means a set of Software that manages computer hardware resources and provides common services for computer programs.
"**Operating System Instance**" or "**OSI**" means an independent, functional virtual or bare metal server running an operating system that is both supported by the operating system manufacturer and offered by BT. This excludes Customer Appliances.
"**PCI DSS**" means the Payment Card Industry Data Security Standards, a set of policies and procedures, issued by the PCI Security Standards Council LLC (as may be adopted by local regulators) and intended to optimise the security of credit and debit card transactions and protect cardholders against misuse of their personal information.
"**Planned Maintenance**" means any Maintenance BT has planned to do in advance.
"**POD**" means a cloud infrastructure grouped by industry (e.g. police, healthcare, commercial). PODs refer to a platform that has dedicated/shared compute and storage component for each end customer sector i.e., ensuring full segregation of compute and storage services between end customers. End customers are provisioned as per their PODs, depending on the nature of their business or their activities.
"**Production Environment**" means your total environment, encompassing the entirety of the Sovereign Cloud Service being delivered to you, but explicitly excludes any resources designated "non-production" and/or "dev/test". This is inclusive of Cloud Infrastructure, Customer Appliances, OSIs, Compliance Baseline, and any optional services as provided by BT and set forth in the Order(s).
"**Professional Services**" means those services provided by BT which are labour related services.
"**Qualifying Incident**" means an Incident, except where any of the following events have occurred:

(a) the Sovereign Cloud Service has been modified or altered in any way by you, or by BT in accordance with your instructions;
(b) Planned Maintenance;
(c) you have performed any network configurations that BT did not approve;
(d) an Incident has been reported, and BT cannot confirm that an Incident exists after performing tests; or
(e) you requested BT to test the Sovereign Cloud Service at a time when no Incident has been detected or reported.

"**RAM**" means random access memory.
"**Recovery Point Objective**" or "**RPO**" means the maximum period of permitted data loss upon Restoration Success, measured in hours preceding the time of failure.
"**Recovery Time Objective**" or "**RTO**" means the duration of time, measured in hours, between BT confirmation of a Disaster Declaration and Restoration Success.
"**Recurring Charges**" means the Charges for the Sovereign Cloud Service or applicable part of the Sovereign Cloud Service that are invoiced repeatedly in every payment period (e.g. every month), as set out in any applicable Order.
"**Renewal Period**" means for each Sovereign Cloud Service, the initial 12-month period following the Minimum Period of Service, and each subsequent 12-month period or such renewal period as otherwise mutually agreed in the Order.
"**Restoration Success**" means that the Operating System Instances at the Disaster Recovery Site are online and available for you to use.
"**Service Desk**" means the helpdesk that you are able to contact to submit service requests, report Incidents and ask questions about the Sovereign Cloud Service.
"**Service Management Boundary**" has the meaning given in Paragraph 4.1.
"**Service Options**" has the meaning given in Paragraph 3.
"**Severity Level 1 Incident**" means a Qualifying Incident that cannot be circumvented and that constitutes a complete loss of service.
"**Site**" means a location at which the Sovereign Cloud Service is provided.
"**Solution Escalation Action Plan" or "SEAP**" means the jointly prepared customer management plan that shall define the steps to be taken by BT when responding to incidents, tickets, and alerts. Specific monitoring thresholds are also documented in the SEAP.

"**Sovereign Cloud Service**" has the meaning given in Paragraph 1.
"**Standard Service Components**" has the meaning given in Paragraph 2.
"**Supplier**" means Rackspace International GmbH or any other supplier BT may use to deliver the Sovereign Cloud Service.
"**Supplier Termination Charges**" means any charges, costs, fees or expenses payable by BT to the Supplier upon cancellation prior to the Service Start Date by the Customer.
"**System Security Plan**" means the main document of the A&A Package detailing how a cloud service provider manages the security controls throughout the lifecycle of the Sovereign Cloud Service, in accordance with the Compliance Baseline. In addition to the narrative of the security control implementation, it also includes a system description of the components and services inventory, and depictions of the system's data flows and authorization boundary.
"**Template**" means a configuration used to create a Virtual Machine with a specific Operating System build.
"**Ticket**" means the unique reference number provided by BT for an Incident and that may also be known as a "**fault reference number**".
"**Usage Charges**" means the Charges for the Sovereign Cloud Service or applicable part of the Sovereign Cloud Service that are calculated by multiplying the volume of units that you used or incurred in a period with the relevant fee as set out in any applicable Order.
"**vCPU**" means virtual central processing units.
"**Virtual Machine**" or "**VM**" means a self-contained operating system that functions as a separate server.
"**VM Snapshot**" means the file-based snapshot of the state, disk data, and configuration of a Virtual Machine at a specific moment in time.
"**vRAM**" means virtual random-access memory or virtualised memory available to a Virtual Machine.