Service Description

Cloud Hosting

UK Commercial Backup (unclassified data)

G-Cloud 10

Contents

1 CARRENZA OFFICIAL INFRASTRUCTURE AS A SERVICE (IAAS) OVERVIEW

1.1 General

Under G-Cloud 10 we are bidding for Cloud Hosting. Any Features not included in Cloud Hosting are not covered in this Service Definition.

1.1.1 Green IT

Carrenza' IaaS services support the governments Greening ICT Strategies. Carrenza recognises that its operations can impact both directly and indirectly on the environment. Our goal is to protect the environment through good management and by adopting best practice throughout our organisation. We work to integrate environmental considerations into our business decisions, consultancy and client solutions. Indeed one of the Equinix data centres that we utilise won the Green Data Centre award from DataCenter Dynamics. This innovative use of sustainable and renewable energy technology was a key factor for us to select that facility as a part of our operations. We also have the EU Code of Conduct Energy Efficiency Award certifying that our data centre has adopted energy efficiency best practices: our Birmingham Central site has a PUE of less than 1.3 indicating our commitment to green initiatives.

1.2 IaaS Services

The Carrenza Remote Cloud Backup Service is delivered using the Carrenza Commercial IaaS with options to utilise the Carrenza OFFICIAL IaaS and the major public cloud providers based on data classification levels.

The Service enables you to build and scale your Remote Backup and Restore solution based on requirements and data criticality, as opposed to forcing you into a one-size-fits-all solution. Services can be mirrored across multiple infrastructure nodes in the UK and Europe with instant recovery and full server restores.

The service is available with PSN Assured and PSN Protect connectivity via our OFFICIAL IaaS if required.

The table on the next page gives a high-level overview of our Cloud portfolio.

	ENTERPRISE CLOUD	PUBLIC SECTOR CLOUD	PUBLIC CLOUD
Cloud Infrastructure	Designed for commercial mid-market and Enterprise organisations requiring geo-diversity and private connectivity. Delivers highly available application uptime for critical business applications.	Designed for the Public Sector, including local authorities. Capable of delivering services to organisations connected via the Public Services Network (PSN) Up to OFFICIAL classification, including OFFICIAL SENSITIVE handling.	Designed to support organisations with highly fluctuating requirements and global installation requirements across availability zones. Certified Azure and AWS partner.
	BACKUP	DISASTER RECOVERY (DR)	PUBLIC CLOUD DR
Business Continuity	Designed to protect Servers and Desktops, full machines and at file level. Gives peace of mind for data integrity with a customisable range of options for replication frequency and length of retention.	Designed to replicate servers from on-premises/colocation or Enterprise/Public Sector Cloud. Allows continuous replication and failover to restore service in a severe failure scenario.	Replicates services from Private Cloud to Public Cloud, delivering cloud-neutral protection for critical workloads.
	MODERN WORKPLACE	DATA AND BI	UNIFIED COMMS
Cloud Applications	Office 365 – provides the market-leading services for business productivity tools, including Exchange, SfB, SharePoint and OneDrive. Email security, continuity, archiving and backup. Anti-virus and anti-malware protects your server and desktop estate.	Business Data intelligence and analytics. Utilising the market-leading CXAir product suite to create business insights and rich presentation from structured and unstructured data.	Skype for Business and Avaya services enrich worker collaboration and communication. Empowers employees from all locations to be productive.
	MANAGED SERVICES		
Cloud Managed Services	WeManage – Network / Firewall & Load Balancing WeManage – Server / Active Directory / SQL / Application Uptime WeManage – Office 365 / VDI / RDS		
	SUPPORT SERVICES		
Cloud Support Services	WeSupport – Cloud Premium / Platinum WeSupport – Service Management WeSupport - End User Service Desk (1st line)		
	CONSULTANCY AND PROFESSIONAL SERVICES		
Cloud Professional Services	WeConsult– Cloud Readiness Assessments WeConsult – Data Centre Optimisation Assessments WeTransform – Server Migration WeTransform – O365 Migration		

1.2.1 Compliance

Where Carrenza is providing Services that are Compliant with a Specified Standard, you should be aware that only the Services we are providing carry an accreditation. Anything you use those services for does not inherit the accreditation from the Services on which it sits.

1.2.1.1 PCI DSS

Carrenza ensure all of its accredited PCI DSS Services are maintained according to the relevant PCI DSS requirements to ensure the security of cardholder data on behalf of the Customer. This statement ONLY applies to Services that Carrenza provides. The Customer must ensure that all of its own functions relating to cardholder data, application or otherwise, are both PCI DSS accredited and maintained, and that all relevant steps are taken to protect cardholder data.

1.3 Definitions

- "vCPU" (or in the plural "vCPUs"): is defined as one or more virtual central processing unit(s) (CPUs) compatible with Intel x86 instruction sets
- "vRAM": is defined as virtual random access memory used for real-time processing
- "Storage": is defined as non-volatile media for storing files, databases, applications or virtual servers
- "VMDK": is defined as Virtual Machine Disk, the file stored on a data store representing each individual disk configured within a virtual machine
- "IOPS": is defined as the number of input/output operations per second on a disk
- "GiB": is defined as 1,024MiB
- "TiB": is defined as 1,024GiB
- "RTO": Recovery Time Objective
- "RPO": Recovery Point Objective
- "ATOT": At Time Of Test
- "ATOD": At Time Of Disaster
- "Compute": A combination of vCPU and vRAM resources
- "SMC" – Service Management Centre
- "CMDB" – Configuration Management Database

In addition to the definitions above, in this document we use the "RACI" Responsibility Matrix. It is used to denote our role and your role in various Sections in this document. Each role has one or more of the following letters:

- "R" shall denote "responsible" indicating the party who does the work to achieve the task;
- "A" shall denote "accountable" indicating the party who:
  - i) is ultimately answerable for the correct and thorough completion of the task,
  - ii) delegates the work to the responsible party; and
  - iii) approves the work that the responsible party provides.
- "C" shall denote "consulted" indicating the party whose opinions are sought and with whom there is two-way communication; and
- "I" shall denote "informed" indicating the party who shall be are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

2 PUBLIC SECTOR CLOUD

2.1 Public Sector Cloud Architecture

Carrenza Public Sector Cloud has been designed to provide exceptional levels of resiliency, incorporating a minimum of N+1 resiliency across all components. The platform is designed to provide a highly available, highly scalable Infrastructure as a Service (IaaS) platform for customer solutions.

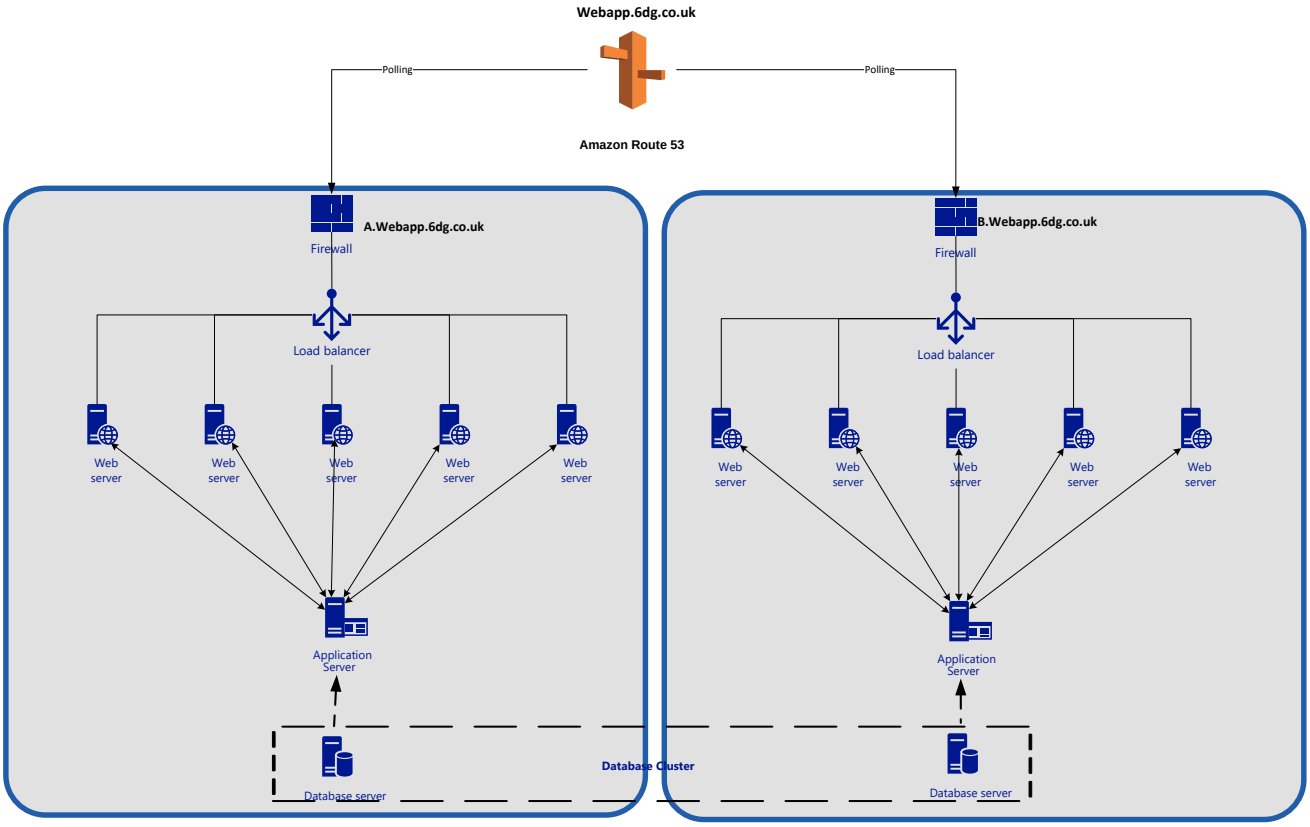
Based on Tier 1 Enterprise-grade hardware, the platform includes the following:

- Resilient connectivity to the Carrenza core Next Generation Network, each network stack is connected to two independent Carrenza Core nodes
- N+N network fabric resiliency with two physically separate fault domains for the network fabric
- N+1 storage fabric resiliency with two physically separate fault domains for storage
- Resilient storage and network connectivity to all compute hardware split across both fault domains
- N+1 compute nodes in each chassis providing high availability
- Delivered from UK-based ARK data centres in Corsham and Farnborough, as well our London and Slough based data centres

At a functional level the Public Sector Cloud platform delivers the following:

- Options for virtual or physical servers
- Options for resource pools or named servers
- Options for management including OVM, RDP, vCloud Director and API
- Geo diverse data centres
- Options for Managed or Unmanaged Virtual Firewalls
- Options for Managed or Unmanaged Virtual Load Balancers
- Internet and L3VPN (MPLS) connectivity

Below is an example of a Dual Site (GEO HA) replicated solution. Public Sector Cloud is deployed in 2 availability zones (DCs), including multiple application tiers, managed virtual load balancer, managed virtual firewalls and a 3rd party Global Load Balancing solution.



2.1.1 OFFICIAL Vulnerability Management & Protective Monitoring

Regular IT Health Checks will be conducted to ensure Carrenza Technology Group Ltd systems remain patched. To provide interim views of vulnerabilities, Carrenza Technology Group Ltd operate a proactive Nessus scanning service, which alerts on any unpatched or at risk services.

Carrenza Technology Group Ltd ensure all 5 key aspects of protective monitoring are conducted on our secure Public Sector Cloud as part of our protective monitoring strategy:

- Business traffic crossing a boundary
- Activity at a boundary
- Alerting on events
- Accurate time in logs
- Data backup status

Originally aligned to GPG 13 (Protective Monitoring for HMG ICT Systems), Carrenza Technology Group Ltd visualised monitoring and auditing platform ensures the right measures are being interrogated to avoid complexity and maintain the secure operation and continuation of our IaaS platform.

The configuration and associated processes of Carrenza Technology Group Ltd OFFICIAL management platform relate to the highest levels of implementation guidance for NCSC's 14 Cloud Security Principles:

1. Data in transit protection
2. Asset protection and resilience
3. Separation between consumers
4. Governance framework
5. Operational security
6. Personnel security
7. Secure development
8. Supply chain security
9. Secure consumer management
10. Identity and authentication
11. External interface protection
12. Secure service administration
13. Audit information provision to consumers
14. Secure use of the service by the consumer

2.2 Platform Options

Within the Public Sector Cloud Platform, customers can choose between a Community Cloud Service or a Dedicated Private Cloud Service:

	Public Sector Cloud	
	Community Cloud	Dedicated Cloud
What you get	• Shared hardware with options for physical servers – proven best practice architecture, built and managed by Carrenza	• Hardware dedicated to the customer – designed to a Carrenza proven architecture, built and managed by Carrenza
How you manage it	• Direct RDP to servers, through VCloud Director, OVM or API	• Through vCloud Director, vCenter, OVM or API
Why you would choose this	• Platform built and managed natively by Carrenza, locally in the UK from ARK Data Centres providing local accountability and control • Flexibility of design and capability beyond public cloud • Predictable costs	• Security or performance conscious. • Not wishing to share resources with other customers. • Specific compliance requirements
What you need to consider	• Cannot use existing Windows Server licences • Need Software Assurance on existing licences for mobility • Ceiling limits on some resources	• The platform has to be specified to cater for all fluctuations of use; does not benefit from consume on demand capability • OPEX and no hardware EoL. • The customer can utilise their existing licensing without requiring Software Assurance • Leverages a proven design and expert resource to build and manage
Availability/Pricing	• Standard product and pricing including PAYG model, available immediately	• Built on demand to the customer requirement

2.3 Community Cloud

2.3.1 Network

Within the customers' Public Sector Cloud solution, Carrenza will provide a number of core network components that will include the following:

- Virtual Server Network Card – Up to four network cards per virtual server which can be connected to any VLAN's within the customer's environment
- VLAN – Dedicated VLAN's per customer solution for use as LAN or DMZ networks
- Internal IP Addressing – A /24 private IP address range will be assigned to each VLAN be default, optionally this can be extended up to a /21 private IP range upon request
- Public IP Addresses – /29 (3 useable), /28 (11 useable) or /27 (27 useable) blocks of useable public IP addresses
- Public DNS Services – Carrenza will provide access to our public facing DNS service for Internet name resolution
- Managed Virtual Firewall – A range of Managed Virtual Firewalls are available including a selection of bandwidth, add-on services and high availability
- NSX Virtual Firewall –NSX Edge firewall appliance provided on a per customer basis configurable through the vCloud Director web or API interfaces
- Managed Virtual Load Balancer – An optional element is a range of virtual load balancers
- NSX Virtual Load Balancer – Load balancing provided by the NSX Edge appliance provided on a per customer basis configurable through the vCloud Director web or API interfaces
- Internet Breakout – 100MiBps of resilient Internet breakout is provided as standard, additional bandwidth can be purchased on request
- L3VPN Connectivity – Resilient or non-resilient connectivity to a Carrenza L3VPN service
- DDoS mitigation service protecting against flood type attacks (e.g. DNS amplification & SMURF attacks) for all external IP addresses
- PSN Connectivity

2.3.1.1 Virtual Server Network Card

Within each virtual server, Carrenza supports up to four virtual network cards. Each virtual server can be connected to any VLAN available within the customer solution. The virtual network cards can be configured as E1000 (1GiBps) or VMXNET 3 (10GiBps) adapters. Within a virtual resource pool, all network cards are connected to customer specific VLAN's on a shared distributed virtual switch.

2.3.1.2 VLAN

VLAN's are configured within a customer VRF providing logical per customer isolation. VLAN's are per cloud platform. During the initial deployment Carrenza will deploy VLAN's in line with the agreed solution design, customers can configure additional VLAN's as required through the vCloud Director Web interface or API.

Within the Public Sector Cloud platform site, any VLANs created will be available to the virtual platform as well as any dedicated physical or other platform services, such as OVM, that Carrenza might provide. Carrenza does not support stretched VLAN's between data centres.

2.3.1.3 Internal Private IP Addressing

For each VLAN provisioned, Carrenza will allocate a /24 private IP address range, if this range conflicts with an existing IP address range within the customer's network, the customer can request that is it changed prior to the configuration of any virtual machines for no additional cost.

Once virtual machine and firewall configuration has been completed, changing the private IP address range will be charged at standard professional services rates.

2.3.1.4 Public IP Addresses

Non-transferable Public IP addresses blocks are provided by Carrenza. Within a public IP address block, three addresses are used to support the highly available network infrastructure leading to the following IP address availability:

- /29 – 3 useable public IP addresses
- /28 – 11 useable public IP addresses
- /27 – 27 useable public IP addresses

Larger Public IP Address blocks can be provided on request.

2.3.1.5 Public DNS Service – Internet Name Resolution

Carrenza will provide two public facing DNS service IP addresses. The service is built on a resilient multi-site infrastructure ensuring continuous availability.

2.3.1.6 Virtual Firewall

As part of the Public Sector Cloud solution, Carrenza will provision a virtual firewall solution. A range of options are available for the virtual firewall solution including both unmanaged and managed solutions.

Full details of the Cloud Firewall specification, functionality and operations are located in the Carrenza Cloud Firewall Service Description, available within the customer's portal at https://servicedesk.carrenza.com portal.

2.3.1.7 Perimeter Firewall

As part of the Public Sector Cloud infrastructure Carrenza deploy and manage a perimeter firewall for all customers, this appliance provides a second layer of stateful firewall protection in addition to any firewall solution the customer deploys.

2.3.1.8 Virtual Load Balancer

Within the Public Sector Cloud Platform, Carrenza provides the option of a dedicated virtual load balancer. A range of options are available for the virtual load balancer including both unmanaged and managed solutions.

Full details of the Cloud Load Balancer specification, functionality and operations are located in the Carrenza Cloud Load Balancer Service Description, available within the customer's portal at https://servicedesk.carrenza.com portal.

2.3.2 Internet Breakout

As standard, if the customer has purchased Internet breakout, Carrenza will provide a resilient 100MiBps Internet service. This service is an unfiltered Internet service delivered through the Public Sector Cloud resilient network fabric.

If additional bandwidth, Internet Protection (such as DDOS) or security services are provided, these are available as optional add-on products.

2.3.2.1 L3VPN

The Public Sector Cloud platform fully supports the delivery of Carrenza L3VPN connectivity directly into the platform providing connectivity to existing customer sites.

L3VPN connectivity will be terminated on the 10GiBps Public Sector Cloud network fabric and delivered over the resilient network connectivity to the customer cloud network.

If the customer has an existing 3rd party MPLS, Carrenza can integrate with it by utilising a cross connect at any one of our nationwide POP's. From there, Carrenza will use our Next Generation Network to deliver the customer's services as a L3VPN to the Public Sector Cloud platform.

Please note there may be additional charges from the customer's MPLS provider to cross connect with Carrenza.

2.3.3 DDoS Mitigation

All ingress internet traffic to the public-sector cloud is subjected to volumetric (L3/L4) DDOS mitigation protection. This is achieved by passing all traffic via a UK primary scrubbing centre, with 4 Tbps of attack ingestion capacity, before delivering clean traffic, using BGP routing, to the Carrenza public sector cloud. DDOS protection is always on capturing attacks at the moment they occur, using advanced behaviour analytic technology and reactive IP filtering through null routes and limited ACL filtering.

2.3.4 PSN Connectivity

Our services can utilise an assured data transport mechanism. Carrenza Technology Group Ltd can provide PSN Protect network connectivity.

2.3.5 Purchasing Model

The Customer may purchase Public Sector Cloud resource in two models. Each platform solution is restricted to a consistent model.

- PAYG – Under this model Carrenza provides access to our Public Sector Cloud platform, resources can then be consumed on a PAYG basis
- Resource Pools – A resource pool provides the customer with a pool of vCPU, RAM and storage with the capability to create, remove or resize virtual servers as required
- Named Servers – Named Servers are pre-defined virtual or physical servers with a defined resource configuration for the term of the contract, if the customer wishes to modify the resource specification of the server this would be treated as a change order

The customer can choose to purchase a resource pool with shared resource or the customer can choose to have dedicated resource, meaning that vCPU and RAM will be provided from dedicated hardware.

The customer specifies the amount of resource they require in terms of vCPU, vRAM and Storage. Then, through VMware vCloud Director or the OVM Portal, the customer controls what servers they deploy. The customer can change resource specifications and servers as often as they like within the confines of the resource pool they have purchased.

2.3.5.1 PAYG

The options available under the PAYG model are as follows:

- vCPU– 1 TO 1500
- vRAM 1 TO 3500TiB
- SAN Storage – 100GiB to 100TiB

The compute resource is provided from a pool of multi-tenant compute nodes. These nodes are configured as a single, shared compute cluster with N+1 high availability at a platform level.

If there is a requirement for node affinity or resources split across multiple compute clusters, these features are available within the dedicated resource pool.

Within the platform, there are a predefined maximum per virtual server configuration rules in place. These include:

- vCPU –Maximum of 16 vCPU per virtual server
- vRAM – Maximum of 128GiB RAM per virtual server
- Storage – Maximum volume size of 2TiB with no more than 10TiB per Virtual Server

Under the consumption-based model, Carrenza commits to ensuring capacity is available to support incremental growth of 20% of capacity with a minimum of 224 vCPU, 465GB RAM and 4TB of storage available. If additional capacity is required beyond this amount, the customer must notify Carrenza and a lead time of six weeks will apply to the capacity increase.

2.3.5.2 Resource Pool – Virtual

The options available for a virtual resource pool are as follows:

- vCPU– 1 TO 1500
- vRAM 1 TO 3500TiB
- SAN Storage – 100GiB to 100TiB

Within a virtual resource pool, the compute resource is provided from a pool of multi-tenant compute nodes. These nodes are configured as a single shared compute cluster with N+1 high availability at a platform level.

If there is a requirement for node affinity or resources split across multiple compute clusters, these features are available within the dedicated resource pool.

Within a virtual resource pool, there are a predefined maximum per virtual server configuration rules in place. These include:

- vCPU –Maximum of 16 vCPU per virtual server
- vRAM – Maximum of 128GiB RAM per virtual server
- Storage – Maximum volume size of 2TiB with no more than 10TiB per Virtual Server

Resource Pools are available as a static pool limited to the committed resource level, or on a consumption-based model. When a consumption-based model is chosen, the resource pool will be configured with no resource limits thus allowing the customer to scale resources as required.

Within the consumption-based model, Carrenza commits to ensuring capacity is available to support incremental growth of 20% of capacity with a minimum of 224 vCPU, 465GB RAM and 4TB of storage available. If additional capacity is required beyond this amount, the customer must notify Carrenza and a lead time of six weeks will apply to the capacity increase.

Within a virtual resource pool it is also possible to purchase “reserved resources”. These “reserved resources” provide guaranteed access to additional vCPU, VRAM and SAN Storage for burst purposes. In addition, these “reserved resources” can be used to ensure the appropriate resource is available if the customer has a predictable burst event.

2.3.5.3 Resource Pool – Dedicated

The options available for a dedicated resource pool are as follows:

VCPU	VRAM	STORAGE	PHYSICAL COMPUTE NODE	EXPANSION INCREMENT
224	115	100GiB to 100TiB	Dual 2.6Ghz 14 Core CPU, 128GiB RAM	Per 224 vCPU and 115GB RAM
224	230	100GiB to 100TiB	Dual 2.6Ghz 14 Core CPU, 256GiB RAM	Per 224 vCPU and 230GB RAM
224	465	100GiB to 100TiB	Dual 2.6Ghz 14 Core CPU, 512GiB RAM	Per 224 vCPU and 465GB RAM
448	930	100GiB to 100TiB	Dual 2.6Ghz 14 Core CPU, 512GiB RAM	Per 224 vCPU and 465GB RAM
672	1,395	100GiB to 100TiB	Dual 2.6Ghz 14 Core CPU, 512GiB RAM	Per 224 vCPU and 465GB RAM
896	1,860	100GiB to 100TiB	Dual 2.6Ghz 14 Core CPU, 512GiB RAM	Per 224 vCPU and 465GB RAM
1,120	2,325	100GiB to 100TiB	Dual 2.6Ghz 14 Core CPU, 512GiB RAM	Per 224 vCPU and 465GB RAM
1,344	2,790	100GiB to 100TiB	Dual 2.6Ghz 14 Core CPU, 512GiB RAM	Per 224 vCPU and 465GB RAM
1,568	3,255	100GiB to 100TiB	Dual 2.6Ghz 14 Core CPU, 512GiB RAM	Per 224 vCPU and 465GB RAM

Within a dedicated resource pool, the underlying compute hardware is dedicated to the customer. Carrenza recommend a maximum over subscription ratio of 4:1 which equates to 224 vCPU per physical compute node. However, the customer may choose to exceed this amount if their workload is appropriate.

The underlying compute hardware will be configured in an N+1 configuration providing high availability in the event of a compute node failure; the useable vRAM purchased takes into account the N+1 configuration.

Carrenza recommends a minimum of 75GiB of storage is allocated for system drives on all virtual servers.

For customers with a dedicated resource pool, there must be 10% space free on all data stores to enable the platform-level snapshots to complete successfully. If the free space falls below this amount, the daily platform level snapshots will not be available.

Within a dedicated resource pool there are a predefined maximum per virtual server configuration rules in place, these include:

- vCPU –No limit
- vRAM – Limited by the per compute node physical RAM, recommendation that no virtual machine exceeds 25% of the underlying per compute node RAM as listed in the specification table above
- Storage – Maximum volume size of 2TiB with no more than 10TiB per Virtual Server.

2.3.6 Management of Resource Pools

Virtual and Dedicated resource pools can be managed using vCloud Director or OVM, this facility provides a web-based interface for resource management allowing the customer to allocate resources, control and access virtual servers. In addition, customers can use the vCloud or OVM API to provision and manage virtual servers.

2.3.7 Named Servers

By purchasing named servers, the customer does not have to purchase a pool of resource that may not be fully utilised. The customer gets to choose between virtual servers and physical servers.

The following specifications are available:

VIRTUAL SERVERS	PHYSICAL SERVERS
vCPU – 1 to 16	CPU – Choice of: • 2*4 Core 2.6GHz • 2*10 Core 2.4GHz • 2*14 Core 2.6GHz • 2*18 Core 2.7GHz
vRAM – 1 to 128GiB **RAM deployed as fixed – not contended*	RAM – 64, 128, 256, 384, 512, 768GiB
System Drive – 50GiB to 500GiB Available in 50GB increments	Local Drive - Choice of: • 2x600GiB 15K SAS RAID 1 • 2x480GiB SSD RAID 1 • 6x600GiB 15K SAS RAID 6 • 6x480GiB SSD RAID 6
Storage Drive – 100GiB to 2TiB Up to five storage drives per Virtual Server Available in 100GB increments	Shared SAN storage may also be provided for physical servers

All virtual servers are fully licensed for any current edition of Microsoft Windows Server; for Physical Servers the appropriate licensing must be specified and purchased.

2.3.8 Oracle SPARC

Oracle SPARC is only available per physical server based on a minimum 12 month commitment. As standard each physical server is an Oracle T7 server with 32 cores (224 vCPU) and 488GB RAM. Other configurations are available on request.

2.3.9 Storage and Storage Presentation

The Public Sector Cloud Platform utilises Solid State Drives (SSD) to deliver a high performance, highly resilient storage architecture. All storage is provided from Enterprise-grade SAN's with integrated resiliency, RAID and hot spare drives.

Additional storage types including guaranteed IOPS storage are available on request.

Storage is presented to virtual machines as a VMDK within the Virtual Cloud Platform. If support for RDM's (Raw Device Mapping) is required Carrenza can provide this functionality on request.

For customers with a dedicated resource pool, storage is presented as data stores available within vCloud Director and OVM, Carrenza recommends thin provisioning for virtual servers.

2.3.9.1 Bandwidth and Throughput

Server performance is highly affected by storage throughput Read/Write speeds. These can vary during the day and throughout each month on the platform due to usage patterns. Please note that different applications can utilise storage in different ways: the default file sizes that they read and write, and how reading/writing is processed with single or multiple threads. Both can affect the performance the customer may see for typical transfer speeds.

The storage platform is designed to provide 2 IOPs per GiB storage per logical disk, higher performance tiers of storage including guaranteed IOPS are available on request.

2.4 Service Options and Service Implementation OFFICIAL Data Management & Handling

2.4.1.1 OFFICIAL Data security policy

Carrenza Technology Group Ltd is an accredited company under ISO/IEC 27001:2013 and OFFICIAL / OFFICIAL SENSITIVE and, as such, adheres to the approved security policy noted below.

It is the policy of the organisation to ensure that at Carrenza Technology Group Ltd:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained and tested
- Information security training will be available to all staff
- All breaches of Information Security, actual or suspected, will be reported to and investigated by the Information Security Manager.

2.4.1.2 OFFICIAL Information Assurance

It is the policy of the company to protect all information against unauthorised access while maintaining the confidentiality and integrity of that information. We comply with all regulatory and legislative requirements and maintain and test a comprehensive business continuity plan.

2.4.1.3 Data Processing

Carrenza Technology Group Ltd is registered as a data controller under the Data Protection Act 1998 and has a Data Protection Officer to oversee the specific administrative implications of this particular Act who can be contacted regarding any Data Protection issues.

2.4.1.4 Data Migration

Carrenza Technology Group Ltd can and will return all customer generated data as agreed in a relevant call-off agreement. Once data has been returned and confirmed by the customer and, if asked to do so, Carrenza Technology Group Ltd will purge and destroy all data belonging to the customer or consumer from any computers, storage devices and storage media that are to be retained after the end of the subscription period and the subsequent extraction of consumer data.

2.4.1.5 Data Storage and Processing locations

Our IaaS services are delivered for the Public Sector Cloud platform from four locales; these sites are physically and geographically separate, with no interdependencies. Data is unable to pass from one locale to another without being deliberately migrated as a result of a customer decision to do so.

2.4.1.6 OFFICIAL Data Handling

Carrenza Technology Group Ltd and their suppliers adhere to SPF information handling requirements that have been agreed with HMG and ICO.

Carrenza Technology Group Public Sector Cloud documentation will be marked in accordance with their internal data classification policy (and under the new GSC is likely to be considered OFFICIAL Sensitive at most) with stringent need to know controls applied.

Documents relating to the IaaS environment, its design and operation are kept under lock and key in a secure office when not in use.

Controls employed for secure erasure of media will be detailed in Carrenza Technology Group Ltd Public Sector Cloud SysOPS documentation developed by the appropriate service provider. These must conform to Carrenza Technology Group Ltd standing documentation, HMG policy and IAS5 as agreed with the service Accreditor.

2.4.2 Management of Virtual and Dedicated Resource Pools

2.4.2.1 vCloud Director and OVM

For services purchased as virtual or dedicated resource pools, Carrenza will provision the resource pool, network components and virtual firewall in accordance with our default configuration (available in the Carrenza Managed Virtual Firewall Service Description).

Optionally, Carrenza can provision individual Virtual Servers to a defined base template. The customer must specify the quantity of virtual servers required along with CPU, RAM, storage partitioning, network information and the operating system selection. Carrenza will deploy a template virtual server to the defined specification and update the server with the latest available security and critical updates.

2.4.3 Management of Named Virtual Servers and Physical Servers

For solutions with named virtual servers or physical servers, by default all network components and virtual servers are provisioned up to the operating system install. Root admin username and passwords are provided to the customer; it is strongly recommended that these are changed straight away.

Servers will be deployed within a workgroup unless additional professional services have been purchased for migration or further implementation work. In the event that these services have been purchased, such work will be captured in a Statement of Work separately and delivered by the Carrenza professional services team.

2.4.4 Carrenza WeManage – Server Management Services

If a customer has purchased Carrenza WeManage – Server management services, these must be allocated to named services. For services where a resource pool has been purchased, the customer must supply the named instances that they wish to allocate the server management services to in order to activate the service.

Once allocated, a WeManage service can be reallocated to a new virtual or physical server once a quarter or when the currently allocated server is decommissioned.

For full details of the services and functionality available, please see the Carrenza WeManage - Server Service Description available within the customer https://servicedesk.carrenza.com self-service portal.

2.4.5 Managed AntiVirus

Carrenza optional Managed AntiVirus can be purchased with any virtual server, resource pool or physical server. A prerequisite for taking the Managed AntiVirus service is that the virtual or physical server must already be covered by the Carrenza WeManage service.

If purchased, Carrenza will provision a dedicated web portal for the customer to access and manage the deployment of the AntiVirus software.

It is the customer's responsibility to ensure the software has been deployed to all virtual or physical servers, Carrenza monitors any active servers within the Managed Antivirus platform. In the event an infection is identified, a P2 incident will be raised within ServiceNow and the issue will be investigated.

For full details of the services and functionality available, please see the Carrenza Managed AntiVirus Service Description available within the customer https://servicedesk.carrenza.com self-service portal.

2.4.6 Licensing

As part of the Carrenza Public Sector Cloud platform, there are multiple licensing options available. These include:

- **Microsoft SPLA** – Carrenza can provide Microsoft licences for SQL and Applications on a monthly basis, these licences are rented and can be used within the Carrenza Public Sector Cloud platform or on-premises where the servers are under Carrenza administrative control. Customers utilising this licensing model have included software assurance to always be able to use the latest version of the software, it also includes downgrade rights enabling the use of previous versions of Microsoft products.

- **Microsoft CSP** – Carrenza is a Microsoft Cloud Solution Provider (CSP), this status enables us to provide Office 365 based licensing for use within our Public Sector Cloud platform, as well as Public Cloud services on Azure and Office 365.
- **Open/Select/EA** – If a customer has an existing volume licence agreement, certain licences can be used within the Carrenza Public Sector Cloud as long as they have active Software Assurance, exceptions include Windows Server and Microsoft Office licences. In the event that a customer wishes to utilise their existing licensing, they must complete a Licence Verification Mobility form and submit this to their Microsoft representative or reseller.

NOTE: It is the customer's responsibility to ensure they are appropriately licensed for all software used within the Carrenza Public Sector Cloud platform above the Operating System.

2.4.6.1 Supported Operating Systems

All solutions are fully licensed for any currently supported release of Microsoft Windows Server; however, other operating systems are available, including Red Hat Enterprise Linux.

It is the customer's responsibility to ensure that the appropriate licensing has been purchased for any virtual servers running on the Carrenza Enterprise Cloud platform.

Supported Operating Systems include the following:

MICROSOFT WINDOWS	LINUX
Microsoft Windows Server 2008	CentOS 6
Microsoft Windows Server 2008R2	CentOS 7
Microsoft Windows Server 2012	Suse Linux Enterprise 11
Microsoft Windows Server 2012R2	Suse Linux Enterprise 12
Microsoft Windows Server 2016	Red Hat Enterprise Linux 6
	Red Hat Enterprise Linux 7
	Ubuntu 14 Server
	Ubuntu 16 Server
	Ubuntu 17 Server

2.4.6.2 Consumption-based Licensing

Where the customer is using a consumption-based billing model for the Public Sector Cloud platform, it is important to note that, although the platform is fully licensed for Windows Server, any other chargeable licences have a minimum term of one (1) month. In the event that a virtual server is started using a chargeable licence, the customer will be charged for a minimum of one (1) months' worth of licence usage.

2.4.7 Capacity Management, Expansion and Reporting

2.4.7.1 Resource Pool – Virtual

It is the customer's responsibility to manage resource consumed within the resource pool; the customer must order additional resource in advance of being required.

Total resource available will be as invoiced and resource consumed will be the sum of the provisioned machines – which can be found through OVM or vCloud Director in the vOrg resource allocation properties.

Carrenza operates an industry standard ratio of 4:1 for virtual to physical core allocation.

Resource pools can be specified with burst capability. In which case there would be no vCPU, vRAM or storage restrictions, thus it would allow the customer to burst beyond the contracted resource level. Burst usage will be billed as detailed in the Carrenza payment and billing policy.

2.4.7.2 Resource Pool – Dedicated

It is the customer's responsibility to manage resource consumed within the resource pool; the customer must order additional resource in advance of being required.

Additional resource can be added in fixed quantities as per the table in Section 2.3.5.3.

Total resource available will be as invoiced and useable resource can be found through the vOrg resource allocation properties in vCloud Director. Please note that the resource information displayed will include the HA blade which must be subtracted from the resulting total.

Resource consumed will be the sum of the provisioned machines, which can be found through OVM or VCloud Director vOrg resource allocation properties.

2.4.7.3 Named Virtual Servers

It is the customer's responsibility to manage resource consumed within a named virtual server.*

Virtual Servers can be expanded via a sales order. Physical server RAM and storage can be upgraded in line with the defined physical server models available. Physical server CPU's are fixed after the initial purchase.

*WeManage - Server management services can be purchased to cover individual server capacity management reporting – please see the WeManage – Server Product Overview and Service Description for more information.

2.4.8 Logging

Carrenza will maintain the following logs for our Public Sector Cloud platform:

ITEM	TYPE	LIVE	ARCHIVE
Network Fabric	Critical and Warning	1 Year	2 Years
Storage Fabric	Critical and Warning	1 Year	2 Years
Storage Array	Critical and Warning	1 Year	2 Years
Compute Hardware	Critical and Warning	1 Year	2 Years
VMWare ESXi Host	Critical and Warning	1 Year	2 Years
OVM for X86	Critical and Warning	1 Year	2 Years
Oracle SPARC	Critical and Warning	1 Year	2 Years

Current logs are immediately available, archive logs are available on request and will be provided within 48 hours.

2.4.9 Platform Patching

As part of providing the Public Sector Cloud platform, Carrenza provide ongoing maintenance and management of the underlying hardware supporting that platform. Patching of the platform will be carried out in line with our platform patching policy that is available in your https://servicedesk.carrenza.com portal.

All patching is carried out using the following process:

- Scan of the device to identify missing Critical and Security patches
- All patches are identified patches are tested within our lab environment prior to production deployment
- Request for Change (RFC) raised internally to approve patch installation during a pre-agreed maintenance window
- Patches installed during the maintenance window

The only exception to the above will be in the event of a known critical exploit. In the event of a critical exploit being identified, Carrenza reserves the right to carry out emergency maintenance on the platform to address the exploit.

2.5 Data Migration and Implementation

Carrenza has a wide range of migration, implementation and other professional services available beyond the standard Public Sector Cloud build. These services integrate closely with our Public Sector Cloud platform to provide a seamless customer experience from the provision of virtual machines to the migration of data or services into the Public Sector Cloud Platform. If you're interested in these services, please contact your Account Manager.

2.6 Bespoke Solutions

If the solution the customer requires is not covered by the specifications provided within this document, Carrenza can provide a wide range of bespoke solutions utilising our knowledge of industry best practice design to deliver a custom Public Sector Cloud platform that meets the customer's specific requirements.

For any custom solution, Carrenza will work closely with the customer to build a clear detailed specification and to agree the statement of work and deliverables ensuring that the solution delivered meets the customer expectations.

2.7 Offboarding

Carrenza provides offboarding capabilities following the end of the customer's initial contract term; virtual machines can be exported and made available for download over SSL.

Please note that customers will not be granted hypervisor level access to Carrenza Public Sector Cloud platform for data migration purposes.

2.8 Decommissioning Process

For services provided on the Carrenza Public Sector Cloud platform, Carrenza cannot provide any form of certified destruction due to the shared nature of the underlying hardware infrastructure. However, the customer is free to move their data away from our service at any time and, once notified, Carrenza will remove all customer data from the platform using the standard platform tools.

3 BUSINESS CONTINUITY SERVICE PORTFOLIO

Carrenza Business Continuity portfolio provides a breadth of recovery services suited for customer needs. Our portfolio ranges from data protection as part of the Backup offering, to system replication and failover as part of the DR offering. Both the Backup and DR offering are available at Carrenza data centres.

There are many variations of Tiers. However, the concept is pretty straightforward whereby the top Tier workloads are usually mission-critical, require extremely fast recovery e.g. active-active scenario, and the cost is significantly higher. As one goes down the stack, the RTO (Recovery Time Objective) and RPO (Recovery Point Objective) requirement is slower and, likewise, the cost is lower.

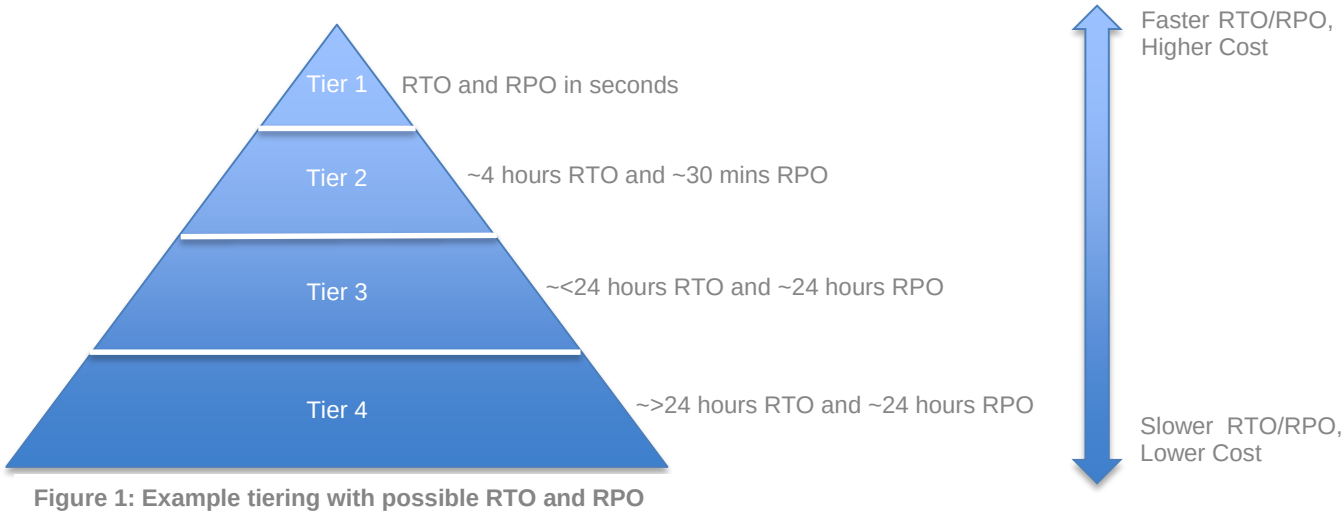


Figure 1: Example tiering with possible RTO and RPO

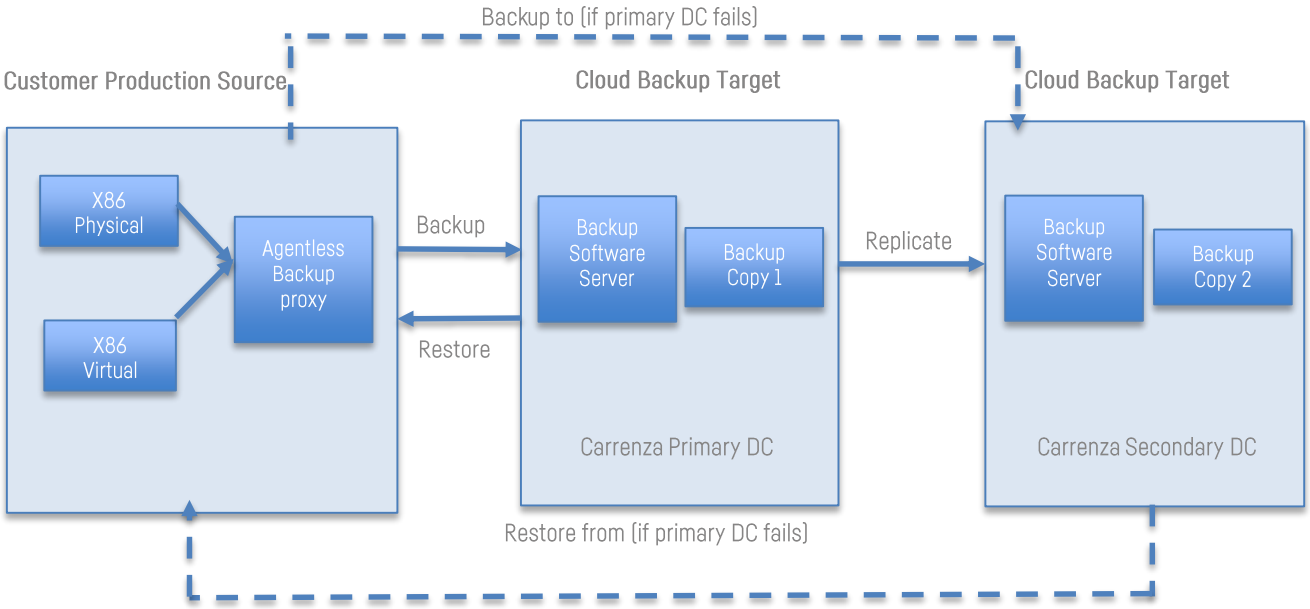
Typically, Carrenza' business continuity offering falls under Tier 2 (Disaster Recovery as a Service) and Tier 3 (Backup as a Service) category. Sections 3.1 through Section 3.1.14.2 focuses on the Carrenza Backup as a Service offering.

Nevertheless, Carrenza is able to offer Tier 1 (active-active) architecture using our Enterprise Cloud supporting High Availability and GEO-High Availability deployments for applications that require this configuration.

3.1 Backup as a Service Overview

Carrenza Backup as a Service (also known as BaaS) is for customers who need to protect their physical or virtual x86 workloads to an offsite cloud backup target location (i.e. Carrenza), and, at the same time, have full control of their backup process. This process could also complement their existing local backup in a situation where their local backup is not accessible. Carrenza provides a truly Enterprise- grade backup infrastructure with granular level restores e.g. file, folder, database and full system. It also comes with the common backup properties such as deduplication, compression and encryption that you would expect from an Enterprise offering.

By default, the Carrenza BaaS offering comes with built-in resiliency by having two identical copies of the data across two different Carrenza data centres. BaaS is a self-service offering: the customer is in control to configure and manage their backup scheduling, retention, monitoring and encryption process to meet their business policies and demands.



PRIMARY ITEM	DESCRIPTION
Primary Management Support	Self-service (after initial onboarding)
Primary Workload Support	Physical and Virtual x86
Primary Recovery Targets	Carrenza Data Centres in the United Kingdom
Primary Support Staff	24x7 onshore, UK-based team

At a high-level, Carrenza Backup as a Service is designed for customers who need a cloud-based backup platform to manage and retain full control of their backup process.

	Carrenza will...	Customer will...
BaaS (Self-Service)	Set-up the backup platform for customer and maintain the overall backup infrastructure, storage, licence and software at the target site, including capacity management of the multi-tenant platform. Deploy agentless software to demo successful live link to protect one (1) server to target platform.	Deploy remaining servers to be protected, configure, schedule, deploy, monitor, report and manage their backup/restore activities and processes, including their capacity requirement, throughout the lifecycle of the contract.

3.1.1 Backup as a Service Features

This section describes the features of Backup as a Service.

FEATURES	DESCRIPTION
Ease of Deployment	Agentless proxy software for backing up required workloads
Built-in Resiliency	Two identical copies of data across two different data centres
Cost Efficiency	De-duplication and compression to optimise on data storage at target. Carrenza charges for stored data at target
Secure Data	Encryption for data in transit and rest controlled by customer
Granular Backup and Restore	Backup and restore capability at file, folder, database and full server level
Support Model	24x7 local, UK-based support team
Pricing Model	Based on data storage at target site (after de-duplication and compression)
Flexible Configuration	Customer controlled backup scheduling and retention to meet business needs
System Protection	Physical or Virtual x86
Workload Protection	Windows or Linux
OPEX Model	No capex, licence nor management outlay to build, maintain and improve backup infrastructure
On Demand Reporting	Build, produce and analyse on demand reports to understand the backup performance
Long Term Retention	Retain data up to the number of years required for auditing and regulatory reasons
Backup Technology	Asigra
Monthly Storage Usage	There are 2 models from which a customer can choose: • Commit + Burst Model: Customers are allowed to burst 100% above their committed storage • Full Usage Model: Customers are allowed to use as much or little as required, based on available overall capacity *NOTE: Neither model implements a hard cap on usage; however, Carrenza may delay providing the capacity until additional storage is provisioned and enabled.*
BaaS Escrow (*optional*)	Secure encryption key storage and retrieval service

3.1.2 Backup as a Service Options

This section describes the Backup as a Service Options.

BACKUP AS A SERVICE OPTIONS	MODEL	SET-UP FEE	MONTHLY COMMIT	MONTHLY USAGE
Self-Service	Commit + Burst Model	Yes – basic onboarding *Optional* – full onboarding	Yes – minimum storage commit	Yes – additional storage above and beyond committed storage
	Full Usage Model	Yes – basic onboarding *Optional* – full onboarding	No – zero storage commit	Yes – high watermark storage used

3.1.3 Purchase Model

Customers can purchase BaaS in two different ways, which are outlined below:

3.1.3.1 Option 1 – Minimum commit on storage with a burstable usage model.

Customer simply commits to a minimum storage amount every month, at a rate per/GB, defined per the contract. Additional storage used above and beyond the committed storage in a given month will be charged at 1.5x the rate per/GB defined in the contract. If more than one contract exists with varying rates, then the most recent contract will be used to work out the additional usage rate. The charges for the additional storage used in a given month will be calculated based on the high watermark storage.

3.1.3.2 Option 2 – Full Usage model with zero commit.

Customer does not commit to a minimum storage amount every month. Instead the customer will be charged on a monthly basis, and it will be based on their high watermark storage used in a given month. The rate per/GB on the contract will be used to calculate the total monthly usage.

NOTE: this rate per/GB is higher than the commit rate per/GB in Option 1.

3.1.4 Set-up Fee

By default, both options listed above in Section 0 come with the basic onboarding effort, which is a fixed fee irrespective of the BaaS scope. Unless stated otherwise, these tasks will be delivered remotely.

3.1.4.1 Default – Basic Onboarding Effort

Carrenza will ensure the BaaS platform is ready for the customer to start performing their backup activities. However, in addition to that, the basic onboarding effort will consist of the following tasks:

SERVICE ONBOARDING	CARRENZA	CUSTOMER
BASIC ONBOARDING		
Facilitate a remote training call using the backup software and admin portal	RA	C
Configure and schedule a backup process for 1 instance	RA	C
Demo restore function (this function can only be used after the initial seeding process)	RA	C
Demo BaaS escrow process	RA	C

3.1.4.3 Optional – Full Onboarding Effort

The Full Onboarding Effort is an optional service and can be provided upon customer request. This setup fee is highly dependent on the scope of the contract and will be based on a daily rate card.

SERVICE ONBOARDING	CARRENZA	CUSTOMER
FULL ONBOARDING		
Facilitate a remote training call using the backup software and admin portal	RA	CI
Configure and schedule backup process for 1 instance	RA	CI
Demo restore function (this function can only be used after the initial seeding process)	RA	CI
Demo BaaS escrow process	RA	CI
Configure and schedule backup process for all instances in-contract	RA	CI
Ensure all instances in-contract complete initial seeding and synchronisation process	RA	CI
Help configure BaaS escrow process	RA	CI
Perform acceptance test, including restore test(s)	RA	CI
Sign-off and handover completed; environment given to customer to continue performing lifecycle management.	RA	CI

3.1.5 BaaS Escrow Service

Currently, BaaS Escrow option is not a chargeable service.

3.1.6 Product Items

3.1.6.1 Storage

Customers are charged on the “stored storage”, measured in GB, on the target site. The stored storage on the target site will typically be smaller in size than the protected storage on the source site. This size difference is simply due to the de-duplication and compression mechanism in place; hence, ultimately passing the cost savings on to customers. However, because different file types have different compression ratios, the customer needs to be aware that Carrenza is unable to provide the exact storage that the customer will use during pre-sales. Instead, customers will be provided an estimate and any additional storage deltas will be charged accordingly.

3.1.6.2 Backup Target Locations

Customer data is backed up to the following primary Carrenza data centre location(s). By default, the data is then replicated into the secondary Carrenza location to provide built-in resiliency. These are multi-tenant environments.

- Primary Birmingham
- Secondary London

3.1.7 Backup as a Service Implementation

After Order Acceptance, we will implement the Service as outlined in the table below:

BAAS SERVICE IMPLEMENTATION	CARRENZA	CUSTOMER
Phase 1: BaaS Infrastructure and Platform Set-Up		
Send Welcome Pack and Technical Data Capture form to Customer	RA	I
Complete and return Technical Data Capture form to Carrenza	I	RA
Place orders for network connectivity (if Customer procured connectivity from Carrenza)	RA	CI
Confirm projected Ready for Service Date with Customer (this date is usually the same as the contract commencement date)	RA	CI
Provide virtual or physical server resources and SQL server resources for Client Host(s)	CI	RA
Prepare backup storage and platform (both Primary and Secondary sites)	RA	I
Implement/Configure Backup network connectivity	RA	CI
Run internal acceptance tests to confirm environment is ready for customer	RA	I
Facilitate a training call on using the BaaS software and admin portal	RA	C
Deliver Backup licences and provide technical support	RA	I
Demo and test connectivity between BaaS Client Hosts and Backup Storage for one protected server	RA	CI
Initiate 'Ready for Service' and BaaS Handover Pack environment to customer	RA	I
Exit Phase 1: Start billing customer after 48 business hours (unless issues are encountered on the platform)	RA	I
Phase 2: Backup Configuration and Initial Seeding		
Install and undertake initial backup seeding and testing for the remainder of the servers to be protected	CI	RA
Configure backup schedule and retention for all protected servers	-	RA
Provide remote technical support during installation e.g. using desktop sharing	RA	CI
Implement and safely store BaaS encryption keys	-	RA
Implement and safely store encryption keys via Carrenza BaaS Escrow process (optional)	CI	RA
Ensure data seeding between source and target are synchronised	I	RA
Perform acceptance test (including restore activity) and highlight any issues found *NOTE: Issues on backup software may involve working with 3rd party vendor*	I	RA
Work to resolve highlighted issues (may involve working with 3rd party vendor)	RA	CI
Exit Phase 2: Successful backup seeding and moves to steady state	I	RA

3.1.8 Ready for Service

The 'Ready for Service' Date will be the date when Carrenza have the Backup as a Service platform ready for Customer to configure their environment to perform Backup operations.

3.1.9 BaaS Service Operations

3.1.9.1 BaaS Platform Administration

Carrenza Service Operations will be initiated once BaaS moves into Ready for Service. Listed below are the key activities that the customer should expect from the Carrenza' BaaS platform administration perspective with a RACI matrix.

BAAS PLATFORM ADMINISTRATION	CARRENZA	CUSTOMER
Carrenza Backup infrastructure (primary and secondary) maintenance and monitoring, including storage	RA	I
Carrenza Backup Software maintenance, monitoring and upgrade	RA	CI
Troubleshooting and resolving infrastructure issues	RA	CI
Work with 3rd party vendor and supplier for hardware, software and license issues and upgrades	RA	CI
Backup escrow service for secure storage (optional)	-	RA
Backup escrow service for secure retrieval (optional)	RC	AI

3.1.10 BaaS Monitoring

We continually monitor the BaaS infrastructure elements of the Primary Backup Storage and the Secondary Backup Storage. Where a fault is identified, we will create an Incident in our Service Request System and work to resolve it immediately.

3.1.11 BaaS Self-Service

BAAS SELF-SERVICE	CARRENZA	CUSTOMER
Configuring retention policy, backup schedules, process restores	I	RA
Management of initial backup and ongoing backup management	I	RA
Monitoring of Backup Storage utilisation	I	RA
Set alerts specific to customer's backup process	I	RA
Respond/Resolve to alerts specific to customer's backup process	CI	RA
Generating on-demand backup reports via portal	-	RA
Restore from backup as required	-	RA
Backup escrow service for secure storage	-	RA
Backup escrow service for secure retrieval	RC	AI

3.1.12 Encryption Key Retrieval from BaaS Escrow

In the event that your private encryption key is lost, you can raise a Service Request with us to request the reconnection of a new Client Host installation to the BaaS platform. We will authorise the recovery of the key from within the BaaS platform and you will be able to reconnect to the BaaS Storage provided you do so from the new Client Host within twelve (12) hours.

3.1.13 Decommissioning Process

The backup data on the target environment can be decommissioned for various reasons, which are outlined below in a RACI matrix.

BAAS DECOMMISSIONING PROCESS	CARRENZA	CUSTOMER
Inform Carrenza of the decommissioning of the servers/data. *NOTE: Customers may still be charged if they are in-contract.*	CI	RA
All backup agentless software/proxy and related components on the source side are deleted.	CI	RA
Delete relevant data on target site (Carrenza) via the portal. *NOTE: This process is irreversible once initiated.*	CI	RA
All customer backup data, related components and environment are completely deleted from the target site both, primary and secondary Carrenza data centres.	RA	CI

BAAS DECOMMISSIONING PROCESS	CARRENZA	CUSTOMER
NOTE: This process is irreversible once initiated.		

3.1.14 Backup as a Service Requirements and Dependencies

3.1.14.1 Customer Dependencies

We provide Backup as a Service subject to the following dependencies:

DEPENDENCIES	DESCRIPTION
Virtual or Physical server client host	This host needs to be provided to deploy the agentless software. It needs to be per Site and by workload types i.e. Windows vs. Linux. e.g. If customer has Windows and Linux workloads to backup and restore, then, at a minimum, two (2) client hosts would be required, one for each type of workload.
Microsoft SQL database for client host	This database is required to run the backup processing software. NOTE: SQL Express can be used for a smaller environment.
Restore capability	This capability will only be available after the initial seeding of the backup data is completed.
Network connectivity from source to target	This connectivity either needs to be procured from Carrenza or provided by Customer in the form of standard internet or dedicated connection. *NOTE: Network connectivity is only required from customer Source to Carrenza Target (primary data centre). The replication copy from Carrenza primary to secondary data centre will be taken care of by Carrenza as it forms the standard offering.*
Project Lead and Technical contacts	Customer will designate these focal points with the appropriate level of expertise to support the successful implementation and operation of the service.
Full Scope Details	Customer will provide all information and configuration details to onboard the service. *NOTE: Carrenza reserves the right to amend the fees and/or contract should there be any changes to customer requirement(s) from the initially agreed contract.*
Additional charges for out of hours work	All implementation work will be carried out during business hours. Carrenza will invoice additional charges for work carried Out of Hours.
Customer's 3rd party management	Customer will manage any 3rd party activities during Service Implementation and Operations.
BaaS bandwidth capacity	Customer will ensure there is sufficient bandwidth capacity for the data to be backed up.
Backup and restore via portal	This self-service offering requires that customer's staff have relevant technical skills to manage their backup process via this BaaS offering. Carrenza will provide initial training courses as part of the onboarding of the service. Any additional training required will incur charges.
BaaS Escrow (*optional*)	This service is an optional one to store and retrieve the encryption keys in the event the customer loses the encryption keys. *NOTE: Only the customer knows the unique encryption keys. If the encryption keys are lost they will be unable (and neither will Carrenza) to decrypt the stored data. Customer must make their own arrangements to retain a copy of the encryption keys unless this BaaS Escrow option is taken.*

3.1.14.2 Supported Data Sources and Resource Requirements

By means of Data Sources, the customer will configure the BaaS Client Host to backup different operating systems, databases, applications and data types. The list of compatible capabilities for Windows and Linux workloads are found in the customer https://servicedesk.carrenza.com self-service portal.

By means of Resource Requirements, customer will configure the agentless software/proxy on the client host at the source site. The resource requirements for the client host are found in the customer https://servicedesk.carrenza.com self-service portal. Please contact your account manager to retrieve a copy of these requirements if you are unable to access the links above. These additional documents should be reviewed in conjunction with the BaaS Service Description.

3.2 Disaster Recovery as a Service (DRaaS) Overview

Typically, Carrenza' business continuity offering falls under Tier 2 (Disaster Recovery as a Service) and Tier 3 (Backup as a Service) category. Sections 3.2.1 thru 3.2.10 focuses on the Carrenza Disaster Recovery as a Service offering.

Nevertheless, Carrenza is able to offer Tier 1 (active-active) architecture using our Enterprise Cloud supporting High Availability and GEO-High Availability deployments for applications that require this configuration.

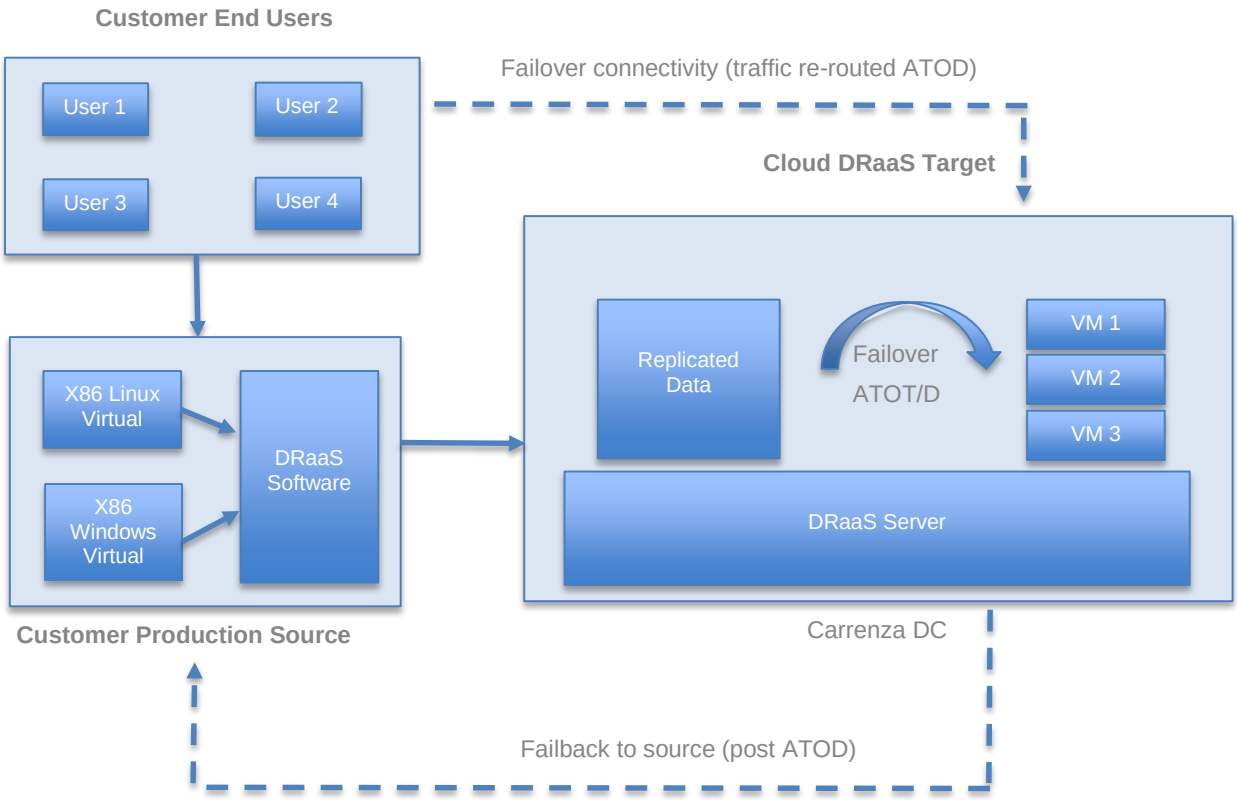
3.2.1 DRaaS Service Overview

Carrenza Disaster Recovery as a Service (also known as DRaaS) is for customers who need offsite protection for their virtual x86 workloads to the Carrenza Cloud target and, at the same time, want to have full control of their DR process. This service is a hypervisor-based, storage agnostic replication that has RPO with a sliding point in time (down to increments in seconds) with no impact to RTO.

This service could complement a customer's existing local backup in a situation where their local systems or entire production systems are not accessible. Carrenza provides a truly Enterprise-grade DRaaS platform with typical RTO and RPO capability between minutes and hours. It also comes with replication properties such as compression (in order to optimise data transfers between source and target), and orchestrated failover of a subset (or the entire) protected systems with boot order recovery priorities that you would expect from an Enterprise offering.

By default, the Carrenza DRaaS offering comes with built-in storage and compute resources to replicate the data and failover ATOT or ATOD as and when you need it. DRaaS is a self-service offering: the customer is in control to configure and manage their replication, failover, monitoring and reporting process to meet their business policies and demands. Customer can also use the failback feature to re-replicate the data from the Carrenza Target back to their Source post-ATOD seamlessly. The service can be summarised in a logical diagram as shown below.

Diagram 1: DRaaS Summary



PRIMARY ITEM	DESCRIPTION
Primary Management Support	Self-service (after initial on boarding)
Primary Workload Support	Virtual x86 (Windows or Linux)
Primary Recovery Targets	Carrenza Data Centre in the United Kingdom
Primary Support Staff	24x7 onshore, UK-based team

At a high-level, Carrenza Disaster Recovery as a Service is designed for customers who need a cloud-based DR platform with replication and compute orchestration built in, providing under 4 hours RTO and RPO in minutes, and also want to manage and retain full control of their DR process.

	Carrenza will…	Customer will…
DRaaS (Self-Service)	Provide the DR platform and software with necessary storage and compute for replication. Maintain the target site including overall capacity management of the DR platform. Deploy agentless software to demo successful replication to protect one server to target platform.	Deploy remaining servers to be protected, configure and replicate source workloads to target site. Monitor, report and manage DR activities, tests and processes, including their capacity requirements, throughout the lifecycle of the contract.

3.2.2 DRaaS Service Features

This section describes the features of Disaster Recovery as a Service.

FEATURES	DESCRIPTION
Ease of Deployment	DR software is deployed on each Virtualisation Host. No agent is required on each Virtual Machine.
Orchestrated Failover	Built-in storage and compute resource for fast failover ATOT or ATOD
Transfer Efficiency	Data compression to optimise on bandwidth utilisation during replication
Service Options	Resource Pool - Virtual or Resource Pool – Dedicated
Service Type	Self-Service, putting customer in control of their DR process
Resiliency	Compute and Storage built on High Availability architecture
Support Model	24x7 local, UK-based support team
Pricing Model	Based on protected Storage and VM requirement
System Protection	Virtual x86
Virtualisation Support	VMware, OVM or HyperV
Workload Protection	Windows or Linux based workloads
Storage Support	Storage agnostic service
OPEX Model	No capex, licence or management outlay to build, maintain and improve DRaaS platform
On Demand Reporting	Build, produce and analyse on demand reports to understand the replication/failover performance
Retention	Default: 4 hours *Optional* : 48 hours *NOTE: The longer the retention, the bigger the storage requirement - which will have an impact on the price.*
Replication Technology	Zerto
Boot Order Recovery	Supports boot order sequence to ensure applications recover in a working state
RTO Capability	From 15 minutes* *NOTE: This time indication is not a SLA commitment.*
RPO Capability	From seconds* *NOTE: This time indication depends on bandwidth network and change rate. It is not a SLA commitment.*
Uninterrupted Replication ATOT	Perform ATOT process without interrupting live replication for the protected environment

3.2.3 DRaaS Service Options

This section describes the Disaster Recovery as a Service Options.

DR AS A SERVICE OPTIONS	MODEL	SET-UP FEE	MONTHLY COMMIT	MONTHLY USAGE
Self-Service	Resource Pool – Virtual	Yes – basic on boarding *Optional* – full onboarding	Yes – based on storage and compute commit	N/A
	Resource Pool - Dedicated	Yes – basic on boarding *Optional* – full on boarding	Yes – based on storage and compute commit	N/A

3.2.3.1 Purchase Model

Customers can purchase DRaaS in two different ways:

3.2.3.2 Option 1: Resource Pool – Virtual infrastructure with committed Storage and Compute resources

Customer commits to storage and compute resources that will be allocated from the Carrenza shared DR platform. Though shared, they are logically segregated by means of virtualisation software and logically separated volumes.

3.2.3.3 Option 2: Resource Pool - Dedicated infrastructure with committed Storage and Compute resources

Customer commits to storage and compute resources that will be dedicated to them from the Carrenza DR platform. Compute resources are delivered using one or more blade servers that are dedicated to the customer. Storage resources are delivered to the customer from our shared storage array.

3.2.4 Additional Information

Customer can mix and match between Virtual and dedicated components to meet their workload performance needs:

- Resource Pool – Virtual for shared Compute and Storage
- Resource Pool – Dedicated for dedicated Compute and shared Storage

Carrenza will reserve the contracted Resources (vCPU, vRAM and Storage) on the DR Target Environment. By using our Resource Admin Portal, the customer can assign and modify these Resources to VMs as required.

The vCPU Resource is allocated to VMs in units of vCPUs. The vRAM and Storage Resources are allocated to Virtual Machines in units of Gigabytes (“GiB”).

3.2.5 Set-up Fee

By default, both options listed above in Section 3.2.3 come with the basic onboarding effort, which is a fixed fee irrespective of the DRaaS scope. Unless stated otherwise, these tasks will be delivered remotely.

3.2.5.1 Default – Basic Onboarding Effort

Carrenza will ensure the DRaaS platform is ready for the customer to start performing their replication activities. However, in addition to that, the basic onboarding effort will consist of the following tasks:

DRAAS SERVICE ONBOARDING	CARRENZA	CUSTOMER
BASIC DRAAS ONBOARDING		
Facilitate a remote training call using the DR software and admin portal	RA	C
Configure and replicate data for one instance	RA	C
Configure VM sizing related to one replicated instance	RA	C
Demo failover function (this function can only be used after the initial seeding process)	RA	C

3.2.5.2 Optional – Full Onboarding Effort

The Full Onboarding Effort is an optional service and can be provided upon customer request. This setup fee is highly dependent on the scope of the contract and will be based on a daily rate card.

DRAAS SERVICE ONBOARDING	CARRENZA	CUSTOMER
FULL DRAAS ONBOARDING		
Facilitate a remote training call using the DR software and admin portal	RA	CI
Configure and replicate data for one instance	RA	CI
Demo failover function (this function can only be used after the initial seeding process)	RA	CI
Configure and replicate data for all instances in contract	RA	CI
Configure VM sizing related to all instances in contract	RA	CI
Ensure all instances in contract complete initial seeding and synchronisation process	RA	CI
Perform acceptance test, including failover test(s)	RA	CI
Sign-off and handover completed environment given to customer to continue performing lifecycle management.	RA	CI

3.2.6 Product Items

3.2.6.1 Storage and Compute

Customers are charged on the data protected (measured in GiB), and the compute contracted on the target site. Any additional VMs, outside of the contractual agreement, will not be protected unless specifically requested and agreed by Carrenza.

3.2.6.2 High Availability

Resource Pool - Virtual: All vCPU and vRAM resources are delivered on multiple blade server platforms that are able to take the loss of an entire blade, whilst maintaining our provisioning metrics.

Resource Pool - Dedicated: As standard, a resource pool – dedicated is provided without N+1 resiliency.

Storage: Delivered from an Enterprise-grade SAN with built-in high availability connected to an N+N storage fabric.

3.2.6.3 DRaaS Target Locations

Customer data can be replicated and failed over ATOT/D to the following Carrenza data centre location(s):

- Birmingham (Resource Pool - Virtual or Dedicated)
- London (Resource Pool - Virtual or Dedicated)

3.2.6.4 Connectivity Options

Replication Connectivity: used to replicate data from source to target (DRaaS platform) for customer's protected systems.

ATOT/D Failover Connectivity: used for users to connect to the target environment upon failover of the protected systems.

Carrenza connectivity options to the target DRaaS platform are as follows:

I) L3VPN
II) Point-to-Point Layer 2
III) Virtual Firewall Service

3.2.6.5 Backup Options

DRaaS is not a backup service hence it will not have any granular level restore, *e.g.* File or Folder, which customers would expect from a true backup service. Therefore, by default, replication retention is up to the previous 4 hours and can be extended to the previous 48 hours. But this DRaaS service is not designed to provide medium or long term retention. If you desire that retention, please consider our BaaS offering.

3.2.6.6 Resource Admin Portal

Customer will administer their target DRaaS resources using the vCloud Director or VMware vCenter GUI hosted at Carrenza. The customer will be provided the total contracted Compute resources which they will be able to set up and allocate accordingly using a catalogue of templates.

3.2.6.7 DRaaS Software

The DR Software is integrated into your VM production environment and includes a replication feature set to manage the applications and VMs. The replication software provides:

- Support for Windows and Linux applications,
- Management tools to test and automate failover,
- Management tools to provide grouping, templating and cloning,

- Data compression,
- Automated assignation of IP addressing to Virtual Machines and RPO characteristics on a per-VM basis.

When dimensioning the capacity of your VM platform, the Virtual Machines needed for DR Software need to be included.

When you create any new VMs on your production environment and then configure them on the DR Software, the changes are updated on the Target Environment in the VMware environment and, where configured to do so, the DR Software commences replication of the new VM(s).

The DR Software has a journal log which creates a set of recovery points over the previous 4 hours (by default). Any of those recovery points may be used to bring VMs back into service once the DR has been invoked. You must dimension the Replication Connectivity adequately to ensure that journal logs can be transferred to the Target Environment Resources to meet your RPO and retention objectives.

The DR Software allows for DR to be invoked either from your Site or from our Target Environment.

3.2.6.8 DR Software Administration

The DR Software is administered through the “DR Admin Portal” GUI. The key features of the DR Admin Portal are as follows:

- Overall Status – General information about the site, including the status of the Virtual Protection Groups being protected or recovered to the site.
- Virtual Protection Groups (VPGs) – All the VPGs from both the source and target sites are listed alongside summary details of each VPG.
- Virtual Machines – A list of all protected Virtual Machines, on both source and target sites, with summary information of each Virtual Machine.
- Sites – Details of the paired sites. This tab lists all the paired sites to the source site and provides summary details of each paired site.
- Setup – Details about Virtual Replication Appliances (VRAs), storage and repositories.
- Monitoring – Details about the alerts, events and tasks for the site.
- Reports – Replication and failover recovery reports to allow for DR process analysis.

3.2.6.9 ATOD DRaaS Platform Daily Usage Fee

In ATOD mode, customer can failover and use the DRaaS platform for up to 14 days without any charges. The DRaaS platform may be used for extended time as agreed with Carrenza and will incur daily usage fee beyond the initial free period.

3.2.7 DRaaS Service Implementation

After Order Acceptance, we will implement the Service as follows:

DRAAS SERVICE IMPLEMENTATION	CARRENZA	CUSTOMER
Phase 1: DRaaS Infrastructure and Platform Set-Up		
Send Welcome Pack and Technical Data Capture form to Customer	RA	I
Complete and return Technical Data Capture form to Carrenza	I	RA
Place orders for network connectivity (if Customer procured connectivity from Carrenza)	RA	CI
Confirm projected Ready for Service Date with Customer (this date is usually the same as the contract commencement date)	RA	CI
Provide virtual server resources at source to deploy DR software for Client Host(s)	CI	RA
Prepare replication storage and compute platform at target site	RA	I
Implement/Configure replication and failover network connectivity	RA	CI
Run internal acceptance tests to confirm environment is ready for customer	RA	I
Facilitate a training call on using the DRaaS software and admin portal including defining initial protection groups, RPOs and IP addressing schema	RA	C
Deliver DRaaS licences and provide technical support	RA	I
Demo and test connectivity between DRaaS Client Hosts and DRaaS target platform for one protected server	RA	CI
Complete high-level handover report specific to signed contract and agreed items during implementation	RA	I
Initiate 'Ready for Service' and DRaaS Handover Pack environment to customer	RA	I
Exit Phase 1: Start billing customer after 48 business hours (unless issues are encountered on the platform)	RA	I
Phase 2: DRaaS Configuration and Initial Seeding		
Install and undertake initial replication, seeding and testing for the remainder of the servers to be protected	CI	RA
Configure replication and failover properties for all protected servers	-	RA
Provide remote technical support during installation e.g. using desktop sharing	RA	CI
Ensure data seeding between source and target are synchronised	I	RA
Perform acceptance test (including failover activity) and highlight any issues found *NOTE: Issues on DRaaS software may involve working with 3rd party vendor*	I	RA
Work to resolve highlighted issues (may involve working with 3rd party vendor)	RA	CI
Exit Phase 2: Move to steady-state upon successful replication seeding and failover process	I	RA

3.2.8 Ready for Service

The 'Ready for Service' Date will be the date when Carrenza have the Disaster Recovery as a Service platform ready for Customer to configure their environment to perform DR process and operations.

3.2.9 DRaaS Service Operations

3.2.9.1 DRaaS Platform Administration

Carrenza Service Operations will be initiated once DRaaS moves into Ready for Service. Listed below are the key activities that the customer should expect from the Carrenza' DRaaS platform administration perspective.

DRAAS PLATFORM ADMINISTRATION	CARRENZA	CUSTOMER
Carrenza DRaaS platform maintenance and monitoring, including storage	RA	I
Carrenza DRaaS Software maintenance, monitoring and upgrade	RA	CI
Troubleshooting and resolving DRaaS platform issues	RA	CI
Working with 3rd party vendor and supplier for hardware, software and license issues and upgrades	RA	CI

3.2.9.2 DRaaS Monitoring

We continually monitor the DRaaS infrastructure elements and where a fault is identified, we will create an Incident in our Service Request System and work to resolve it immediately.

3.2.9.3 DRaaS Self-Service

DRAAS SELF-SERVICE	CARRENZA	CUSTOMER
Configuring replication and failover policy	I	RA
Management of initial seeding and ongoing replication	I	RA
Monitoring of RPO, RTO and replication Storage utilisation	I	RA
Set alerts specific to customer's DR process	I	RA
Respond/Resolve to alerts specific to customer's DR process	CI	RA
Generating on-demand DR reports via portal	-	RA
Failover from available RPOs ATOT and ATOD	CI	RA
Support ATOD and failback (back to source post DR)	RA	RA
Create Requests for change for modifications/additions of VMware Virtual Machines and DR Software using Change Control	C	RA

3.2.9.4 Decommissioning Process

The DR data on the target environment can be decommissioned for various reasons, as requested by the customer. Typically, this process is done at the end of a contract termination.

DRAAS DECOMMISSIONING PROCESS	CARRENZA	CUSTOMER
Inform Carrenza of the decommissioning of the servers/data. *NOTE: Customers may still be charged if they are in-contract.*	CI	RA
All DR agentless software/proxy and related components on the source side are deleted.	CI	RA
Delete relevant data on target site (Carrenza) via the portal. *NOTE: This process is irreversible once initiated.*	CI	RA
All customer DR data, related components and environment are completely deleted from the target site and both compute and storage resources are returned to the pool. *NOTE: This process is irreversible once initiated.*	RA	CI

3.2.10 DRaaS Service Requirements and Dependencies

3.2.10.1 Customer Dependencies

We provide Disaster Recovery as a Service subject to the following dependencies:

DEPENDENCIES	DESCRIPTION
Virtual Machine client host	This compute host needs to be provided in order to deploy the agentless DR software at the source site.
VMware	A VMware vCenter Server must be deployed within the source environment.
Hyper-V	System Center Virtual Machine Manager must be deployed within the source environment.
RPO capability	This capability will only be available after the initial seeding of the replication data is completed. It is also dependent on the network bandwidth in place.
RTO failover	The RTO is dependent on the recovery plan boot order priorities. Boot order priorities are in sequential order. Example: Customer has 5 systems in Priority 1 and 3 systems in Priority 2. Priority 2 systems will not start the booting process until Priority 1 is complete. Therefore, the total RTO will increase in this case.
Network connectivity from source to target	This connectivity either needs to be procured from Carrenza or provided by the Customer in the form of standard internet or dedicated connection. *NOTE: Customer should consider both replication connectivity and failover connectivity (for ATOT and ATOD).*
Initial Replication (seeding)	This initial seeding must be completed for the protected systems before an ATOT or ATOD failover can be initiated.
Project Lead and Technical contacts	Customer will designate these focal points with the appropriate level of expertise to support the successful implementation and operation of the service.
Full Scope Details	Customer will provide all information and configuration details to onboard the service. *NOTE: Carrenza reserves the right to amend the fees and/or contract should there be any changes to customer requirement(s) from the initially agreed contract.*
Additional charges for out of hours work	All implementation work will be carried out during business hours. Carrenza will invoice additional charges for work performed Out of Hours.
Customer's 3rd party management	Customer will manage any 3rd party activities during Service Implementation and Operations.
DRaaS bandwidth capacity	Customer will ensure there is sufficient bandwidth capacity for the data to be replicated and end user connectivity to failover target ATOT and ATOD.
DRaaS process via portal	This self-service offering requires the customer's staff to have relevant technical skills to manage their DRaaS process via this DRaaS offering. Carrenza will provide initial training courses as part of the onboarding of the service. Any additional training required will incur charges.

3.2.10.2 Supported Data Sources and Resource Requirements

The list of compatible capabilities for Windows and Linux workloads are found in the customer https://servicedesk.carrenza.com self-service portal.

The resource requirement for the agentless software/proxy on the client host at the source site are found in the customer https://servicedesk.carrenza.com self-service portal. Please contact your account manager to retrieve a copy of these requirements if you are unable to access the links above. These additional documents should be reviewed in conjunction with the DRaaS Service Description.

4 WEMANAGE SERVER SERVICE OVERVIEW

"WeManage - Server" provides you with add-on managed services for virtual servers hosted within Carrenza Public Sector Cloud platforms and also available for Tier 1 public clouds.

WeManage – Server is available in three variants:

- Monitoring – Provides predefined monitoring with alerts sent to the customer.
- Reactive – Providing predefined monitoring with alerts sent directly to the customer, access to the Carrenza SMC for platform support.
- Proactive – Providing custom monitoring and alerting with Carrenza SMC proactively troubleshooting incidents and contacting the customer. Support is included for issues up to the operating system.

WeManage – Server services can be purchased at any time as an add-on to the following Cloud Infrastructure products:

- Virtual Server – The service will be assigned to a specific Virtual Server.
- Resource Pool (Multi-tenant) – You purchase a quantity of the service. These Resource Pools will be assigned to nominated Virtual Servers and recorded within the Carrenza CMDB. The assignment can be updated once per quarter or upon the decommissioning of a Virtual Server.
- Resource Pool (Dedicated) - You purchase a quantity of the service. These Resource Pools will be assigned to nominated Virtual Servers and recorded within the Carrenza CMDB. The assignment can be updated once per quarter or upon the decommissioning of a Virtual Server.
- Physical Server (Dedicated) – The service will be assigned to a specific Physical Server (Dedicated).
- Microsoft Azure Virtual Machine – The service will be assigned to a specific name server.

All services include customer notification; notifications will be sent to a nominated customer email address or distribution list that must be supplied as part of service implementation.

4.1 WeManage Server Service Prerequisites

The following prerequisites are required to deploy WeManage – Server Services:

- A Carrenza monitoring probe software must be installed within the customer virtual infrastructure;
- The monitoring probe software must have network access to all virtual servers that are being monitored;
- A domain account is required to run the monitoring service, the account must have permission to access any virtual servers that are monitored;
- The monitoring service is supported on servers running a version of Microsoft Windows Server that is supported by Microsoft, for Linux only Red Hat Enterprise Linux is supported;
- The patching service only supports servers running a version of Microsoft Windows Server that is supported by Microsoft (Either in mainstream or extended support).

4.2 WeManage Server Service Features

The following is a high level overview of the functionality available within each respective variant of WeManage Server:

	Unmanaged	Monitoring	Reactive	Proactive
Host Level Monitoring	□	□	□	□
Platform Infrastructure Monitoring and Replacement	□	□	□	□
Infrastructure Incident Management	□	□	□	□
24x7 Monitoring & Alerting			□	□
Reactive Support			□	
Standard Performance Monitoring & Alerting		□	□	
Proactive Support				□
Patch Management (OS level) Critical and Security Patches				□
Custom Performance Monitoring and Alerting				□
Predefined run book capability				□

4.2.1 WeManage – Server Monitoring

WeManage – Server Monitoring provides customers with the following functionality:

4.2.1.1 Standard Performance Monitoring & Alerting

WeManage –Server Monitoring includes pre-defined monitoring and alerting capability. The monitoring set includes the following:

- Virtual Machine Status – Based on a ping response
- vCPU – Above 95% usage for 4 hours
- vRAM – Above 95% usage for 4 hours
- Network Interface Card – Above 95% usage for 4 hours
- Disk – Above 95% usage for 4 hours

All alerts generated by the monitoring system will emailed directly to an email address defined by the customer.

Customisable alerting is available with WeManage – Server Proactive.

4.2.2 WeManage – Server Reactive

WeManage – Server Reactive provides customers with the following functionality:

4.2.2.1 Standard Performance Monitoring & Alerting

WeManage –Server Reactive includes pre-defined monitoring and alerting capability. The monitoring set includes the following:

- vCPU – Above 95% usage for 4 hours
- vRAM – Above 95% usage for 4 hours
- Network Interface Card – Above 95% usage for 4 hours
- Disk – Above 95% usage for 4 hours

All alerts generated by the monitoring system will be raised as P2 level incidents.

Customisable alerting is available with WeManage – Server Proactive.

4.2.2.2 Reactive Support

In the event of an alert being received, you can contact the Service Management Centre for assistance with troubleshooting the issue if you believe the issue is at the operating system level or with the Cloud Platform.

4.2.3 WeManage – Server Proactive

WeManage – Server Proactive provides customers with the following functionality:

4.2.3.1 Custom Performance Monitoring & Alerting

The WeManage – Server Proactive provides customers with customisable monitoring and alerting capability with alerts sent to the Carrenza Service Management centre and proactively investigated by technical specialists.

The monitoring set includes the following:

- vCPU – Customisable above 80% for a minimum of 30 minutes
- vRAM – Customisable above 80% for a minimum of 30 minutes
- Network Interface Card– Customisable above 80% for a minimum of 30 minutes
- Disk – Customisable above 80% for a minimum of 30 minutes

Thresholds below this level can be configured in conjunction with a Statement of Works.

All alerts generated by the monitoring system will be raised as P2 level incidents.

4.2.3.2 Proactive Support

In the event of an alert being triggered, the Service Management Centre will triage the alerts and engage a technical specialist to investigate: the technical specialist will contact you in line with our support procedures documented in the operations manual, providing ongoing updates and agreeing remedial action as required.

4.2.3.3 Patch Management (Operating System level) Critical and Security Patches

WeManage – Server Proactive includes patching for Windows Operating System (OS) Critical and Security patches. The server patching will take place as follows:

- Monthly scan of the server to identify missing Windows Operating System Critical and Security patches on an pre-agreed date;
- Request for Change (RFC) raised with the customer to approve patch installation during a pre-agreed maintenance window;
- Patches installed during the maintenance window and customer notified upon completion.

4.2.3.4 Predefined Run Book Capability

WeManage – Server Proactive also includes run book capability enabling the Service Management Centre to execute pre-agreed run books in response to pre-defined alerts.

Run books must be supplied in the Carrenza run book template (available on request from the Service Management Centre), once submitted the run book must be approved by the Carrenza Management Centre before it becomes live.

Run books can be updated a maximum of once a quarter per run book, any changes to a run book must be approved by the Carrenza Management Centre before they go live.

This service is limited to five pre-agreed run books, for additional run books please contact your account manager.

4.3 WeManage Server Service Implementation

After Order Acceptance, we will implement the Service as follows:

SERVICE IMPLEMENTATION	CARRENZA	CUSTOMER
Customer to provide target email address for alerts	I	RA
Carrenza to deploy monitoring probe within the customers infrastructure	RA	I
Carrenza to configure standard monitoring and alerting for the specified virtual machine	RA	I
Carrenza to send test alert to the customer and confirm receipt	RA	CI
Carrenza to hand update the CMDB and hand the service over to BAU	RA	I

4.4 Ready for Service

The ‘Ready for Service’ Date will be the date when we mutually agree to start WeManage – Server Services.

5 MICROSOFT AZURE SERVICES

Carrenza Microsoft Azure service supports a subset of the Microsoft Azure portfolio, for full details of the products please see the information available at this web page: https://azure.microsoft.com/en-gb/services/

The following sections detail the individual portfolio components currently supported by Carrenza.

5.1 Compute

Within the Compute portfolio, Carrenza provides services based around the following components:

- Virtual Machines
- Virtual Machine Scale Sets
- Azure Container Service (AKS)
- Container Instances

5.2 Network

Within the Network portfolio Carrenza provides services based around the following components:

- Virtual Network
- Load Balancer
- Application Gateway
- VPN Gateway
- Azure DNS
- Traffic Manager
- ExpressRoute
- Azure DDoS Protection

5.3 Storage

Within the Storage portfolio Carrenza provides services based around the following components:

- Blob Storage
- Archive Storage
- Queue Storage
- File Storage
- Disk Storage
- Backup
- Site Recovery

5.4 Microsoft Azure Operations

5.4.1 Azure Portal Access

Carrenza will provision subscriptions for Microsoft Azure customers as new tenants within our Cloud Solution Provider portal. Customers will be provided with full access to their individual tenant portal enabling a customer to view all deployed resources and modify or updated as required.

For resources that Carrenza manages the customer must follow the agreed Request For Change process if any changes are required. Changes made outside of this process may disrupt the managed service that Carrenza is providing.

Any resources a customer deploys within their tenant portal will be billed as usage in arrears.

5.4.2 Azure Service Implementation

The Carrenza Service Implementation Team will handle the delivery of Microsoft Azure Services.

If you have selected the deployment of standard network, compute and storage services, we will provision a tenant portal and deploy the requested services in line with the agreed specification. Once complete, Carrenza will provide the customer with Microsoft Azure portal login details to access the deployed services.

If our professional services team has been engaged, and, once the standard products have been deployed, the professional services team will engage with the customer to complete the remaining consultancy in line with the Statement of Work approved during the sales process. Once complete, the customer will be provided with Microsoft Azure portal login details.

5.4.3 Carrenza WeTransform – Migration and Professional Services

The Carrenza Professional Services team provides a range of services to assists business with their migration to public cloud services. These include cloud readiness assessments, Microsoft Azure architecture and design guidance as well as complete end-to-end migration services.

As well as a number of packaged solutions, Carrenza can build custom solutions for customers to match your business requirements.

For full details of the services and functionality available, please see the Carrenza WeTransform - Server Service Description available within the customer https://servicedesk.carrenza.com self-service portal.

5.4.4 Carrenza WeManage – Server Management Services

If a customer has purchased Carrenza WeManage – Server management services, these must be allocated to named services. For services where a resource pool has been purchased, the customer must supply the named instances that they wish to allocate the server management services to in order to activate the service.

Once allocated, a WeManage service can be reallocated to a new virtual server once a quarter or when the currently allocated server is decommissioned.

For full details of the services and functionality available, please see the Carrenza WeManage - Server service description available within the customer https://servicedesk.carrenza.com self-service portal.

5.4.5 Managed AntiVirus

Carrenza optional Managed AntiVirus can be purchased with any virtual server. A prerequisite for taking the Managed AntiVirus service is that the virtual server must already be covered by Carrenza WeManage service.

If purchased, Carrenza will provision a dedicated web portal for the customer to access and manage the deployment of the AntiVirus software.

It is the customer's responsibility to ensure the software has been deployed to all virtual servers, Carrenza monitors any active servers within the Managed Antivirus platform. In the event an infection is identified, a P2 incident will be raised within ServiceNow and the issue will be investigated.

For full details of the services and functionality available please see the Carrenza Managed AntiVirus service description available within the customer https://servicedesk.carrenza.com self-service portal.

5.4.6 Data Migration and Implementation

Carrenza has a wide range of migration, implementation and other professional services available beyond a standard Public Sector Cloud build. These services integrate closely with our Public Cloud platform to provide a seamless customer experience from the provision of virtual machines to the migration of data or services into the Public Cloud.

6 AMAZON WEB SERVICES

6.1 Overview

Amazon Web Services (AWS) provide a range of compute, storage and related services that allow you to dynamically provision infrastructure in the cloud. The services are designed to make access to scalable services easy to consume for development and production services.

Carrenza Public Sector Cloud provides a mechanism for customers to procure Amazon Web Services. Procuring AWS services through Carrenza, in combination with other services, allows customers to create a managed and workable solution with the flexibility to mix security levels and information assurance requirements.

The Service provides the following functions:

- A mechanism for procuring any of the Amazon Web Services (AWS) services listed on the AWS website at: https://aws.amazon.com/products/
- If Carrenza' server support or server management services are purchased, access to a Service Desk for reporting incidents and Service Requests.

6.2 Support

If supported or managed by Carrenza, cloud services are underpinned by our ITIL aligned, 24x7 service desk and support services.

6.3 Data Centre Locations

Amazon Web Services is located in data centres worldwide and the customer can select where their data is held, although we recommend only using AWS' EU based data centres in Frankfurt and Dublin.

6.4 Severity Definitions

Amazon provides support based on the definitions and the support plan purchased by the customer at the following location: https://aws.amazon.com/premiumsupport/features/.

6.5 Service Constraints

6.5.1 Minimum Infrastructure Requirement

There is no minimum infrastructure requirement when using AWS. It is recommended for each customer that Carrenza procure Business Level Support as part of the AWS Cloud Compute service. This is currently priced at £100 or 10% of the customers' AWS spend per month.

6.5.2 Maintenance and Planned Outage

All AWS maintenance and planned outages are published online at: https://aws.amazon.com/maintenance-help/ . It is the responsibility of the customer to review this information and check when planned outages are scheduled. Carrenza are not liable should the customer fail to check and lose data as a result.

6.5.3 Customer Responsibilities

Customers must conform to the Carrenza acceptable use policy and the AWS Customer Agreement at: http://aws.amazon.com/agreement/

6.6 Onboarding and Offboarding Processes

6.6.1 Onboarding

For customers using AWS they must comply with AWS Customer Agreement at http://aws.amazon.com/agreement/.

6.6.2 Offboarding

Using AWS, the Customer has the ability to upload and download all data and delete the data from their AWS instance. Alternatively Carrenza can do this for the customer, if requested.

6.7 Commercial Relationship

6.7.1 Ordering

Services can be ordered by contacting Carrenza with your requirements. A call-off contract will need to be executed under the G-Cloud 10 Framework with a corresponding PO. Following the initial order, additional services can be ordered in a number of ways by authorised representatives of the Customer:

- By submitting an order form,
- By completing a ticket,
- By provisioning a service through the AWS portal.

6.7.2 Use by Other Suppliers

Our services are available for purchase by third parties who intend to supply services to government.

6.7.3 Invoicing

We invoice monthly in arrears on a 30 day credit invoice. Invoices are based on output from our capacity management system and bill on an hourly basis for the services used in a calendar month.

6.7.4 Termination by Customers

Termination by Customers is conducted in-line with the G-Cloud Framework Agreement.

6.7.5 Service Credits

For AWS, Service Credits are based on standard AWS terms and conditions: https://aws.amazon.com/agreement/.

6.7.6 Termination by Carrenza

Termination by Carrenza is on the same basis as termination by Customers unless specifically agreed in a call-off agreement.

6.7.7 Minimum Contract Period

The minimum contract period of the service is one hour.

6.8 Pricing

AWS Cloud Compute pricing is based on AWS list prices. Any AWS price changes during the lifetime of the applicable G-Cloud framework will be passed on to the Customer. Customers should always check the AWS website for up to date pricing.

Current AWS pricing is available at: http://aws.amazon.com/products/

The AWS Simple Monthly Calculator is available at: http://calculator.s3.amazonaws.com/index.html

It is recommended for each customer that Carrenza procure Business Level Support as part of the AWS Cloud Compute service. This service will be priced at £100 or 10% of the customers' AWS spend per month.

6.8.1 Monthly Managed Service

Carrenza also provide an AWS Cloud Compute Managed Service, starting at £500 per month. This bespoke service is designed with the specific needs of each customer in mind. Options range from basic support and help using AWS to delivering a full hybrid service to support workloads across multiple IaaS environments; e.g. using AWS for test and dev and Carrenza for PSN OFFICIAL workloads. Full pricing for this service is available on request.

7 CARRENZA SLA - INTRODUCTION

Carrenza offers a broad portfolio of Cloud Services to its clients. The following Sections: 7.1 thru 7.8 outline the Service Level Agreement, Service Credits and KPI's associated with these services.

7.1 Service Levels – Cloud Infrastructure

7.1.1 Compute & Storage Platform

SLA	SERVICE	PERIOD	AVAILABILITY TARGET	AVAILABILITY	SERVICE CREDIT
SLA – 1A	Enterprise Cloud – Virtual Private Cloud	Calendar Month	99.99%	99.98% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% 10% 15% 20% 25%
SLA - 1B	Enterprise Cloud – Dedicated Private Cloud	Calendar Month	99.99%	99.98% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% 10% 15% 20% 25%
SLA – 1C	Enterprise Cloud – Dedicated Physical Server	Calendar Month	99.9%	99.89% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% 10% 15% 20% 25%
SLA – 1D	Public Sector Cloud – Virtual Private Cloud	Calendar Month	99.99%	99.89% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% 10% 15% 20% 25%

7.1.2 Silver & Gold Virtual Firewall

SLA	SERVICE	PERIOD	AVAILABILITY TARGET	AVAILABILITY	SERVICE CREDIT
SLA – 2A	Virtual Firewall (Single)	Calendar Month	99.9%	99.89% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% 10% 15% 20% 25%
SLA – 2B	Virtual Firewall (HA)	Calendar Month	99.99%	99.98% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% 10% 15% 20% 25%

7.1.3 Silver & Gold Virtual Load Balancer

SLA	SERVICE	PERIOD	AVAILABILITY TARGET	AVAILABILITY	SERVICE CREDIT
SLA – 3A	Virtual Load Balancer (Single)	Calendar Month	99.9%	99.89% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% 10% 15% 20% 25%
SLA – 3B	Virtual Load Balancer (HA)	Calendar Month	99.99%	99.98% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% 10% 15% 20% 25%

7.1.4 Service Level Definitions: Cloud Infrastructure

SERVICE	AVAILABILITY DEFINITION
Compute Platform Availability	Positive TCP port open response on port 902
Storage Platform Availability	Storage connected and available from the server and operating within acceptable performance parameters as defined in both the Enterprise and Public Sector Cloud Service Descriptions
Virtual Firewall Availability	Positive TCP port response on the management interface port 443
Virtual Load Balancer Availability	Positive TCP port response on the management interface port 443

7.2 Service Levels – Business Continuity

7.2.1 Backup as a Service (BaaS)

The following Service Level KPI's are in place for the Carrenza BaaS Platform.

SLA	SERVICE	PERIOD	AVAILABILITY TARGET	AVAILABILITY	SERVICE CREDIT
SLA – 4A	BaaS	Calendar Month	99.99%	99.98% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% 10% 15% 20% 25%

7.2.2 Disaster Recovery as a Service (DRaaS)

The following Service Level KPI's are in place for the Carrenza DRaaS Platform.

SLA	SERVICE	PERIOD	AVAILABILITY TARGET	AVAILABILITY	SERVICE CREDIT
SLA – 5A	DRaaS Availability	Calendar Month	99.99%	99.98% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% 10% 15% 20% 25%

7.2.3 Veeam Cloud Connect Backup

The following Service Level KPI's are in place for the Carrenza Veeam Cloud Connect Backup Platform.

SLA	SERVICE	PERIOD	AVAILABILITY TARGET	AVAILABILITY	SERVICE CREDIT
SLA – 6A	Veeam Cloud Connect Backup	Calendar Month	99.99%	99.98% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% 10% 15% 20% 25%

7.2.4 Service Level Definitions - Business Continuity

SERVICE	AVAILABILITY DEFINITION
BaaS Platform Availability	Positive TCP port open response on port 4401
DRaaS Platform Availability	Positive TCP port open response on port 902
Veeam Cloud Connect Availability	Positive TCP port response on the management interface port 443

7.3 Service Levels – Cloud Applications

7.3.1 Mimecast

The following Service Level KPI's are in place for Mimecast services.

7.3.1.1 Email Delivery

This Service Level measures the ability to deliver email messages to or from Mimecast's servers.

SLA	SERVICE	PERIOD	SLA TARGET	EMAIL DELIVERY	SERVICE CREDIT
SLA – 7A	Email Delivery	Calendar Month	100%	99.99% - 99% 98.99% - 98% 97.99% - 97% 96.99 – 96% Less than 96%	10% 20% 30% 40% 50%

7.3.1.2 Spam Protection

This Service Level measures the effectiveness of the protection against receipt of spam for those Services that include such functionality. This Service Level is measured in terms of "False Positives" and "False Negatives" (defined below). This Service Level applies across all of a Customer's email traffic and SMTP connection attempts (any attempt to connect to a Mimecast SMTP mail gateway to send email).

Definitions:

"False Positive"

"False Positive" is an e-mail incorrectly classified as spam by the Service. False Positives do not include emails which:

- do not constitute legitimate business email;
- are sent from a compromised machine;
- are sent from a machine which is on a third party block list; or
- are sent from a mail server that does not fully comply with the SMTP delivery standards as defined in RFC 2821 & 2822.

SLA	SERVICE	PERIOD	SLA TARGET	FALSE POSITIVE CAPTURE RATE PER CALENDAR MONTH	SERVICE CREDIT
SLA – 7B	False Positive	Calendar Month	0.0001%	>0.0001% - <=0.001% >0.001% - <=0.01% >0.01% - <=0.1% >0.1%	10% 20% 30% 40%

"False Negative"

"False Negative" is a spam email that the Service does not identify as spam.

SLA	SERVICE	PERIOD	SLA TARGET	CONSECUTIVE DAYS WITH FALSE NEGATIVE RATE EXCEEDING 2%	SERVICE CREDIT
SLA – 7C	False Negative	Calendar Month	2%	2 – 3 4 - 5 6 - 9 10+	10% 20% 30% 40%

7.3.1.3 Anti-Virus Service

SLA	SERVICE	PERIOD	SLA TARGET	SERVICE CREDIT
SLA - 7D	Antivirus Infection	Calendar Month	>=1	Upon confirmation by Mimecast that the customer's system has been infected by one or more harmful viruses, the customer will be entitled to a 50% service credit for the affected calendar month.

This Service Level measures protection against infection of Customer's servers by a virus through the Services, for those Services that include anti-virus functionality.

7.3.1.4 Search Performance

This Service Level relates to the search time where Permitted Users access Mimecast's email archiving service. This Service Level measures the time elapsed between the receipt of the Permitted User's search request by Mimecast's systems and when the return of the search results is initiated by Mimecast (the "Query Time").

SLA	SERVICE	PERIOD	SLA TARGET	QUERY TIME*	SERVICE CREDIT
SLA – 7E	Search Performance	Calendar Month	<=6s	>7s - <=20s** >20s - <=25s** >25s - <=30s**	10% 15% 25%

** Service Level applies only where Customer has performed at least 250 searches in the given month.*

*** Query Time calculated via the median search times for Permitted Users searches in the given month.*

7.3.2 Office 365

Please refer to Microsoft Online Services Service Level Agreement document available here.

http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37

7.4 Service Level Agreement Uptime Values

The following table defines the downtime associated with the service levels listed in this document.

SLA	MAX DOWNTIME PER MONTH
99.99%	4min 23sec
99.9%	43min 49.7sec
99.5%	3hr 39min 8.7sec
99%	7hr 18min 17.5sec
98%	14hr 36min 34.9sec

7.5 Key Performance Indicators (KPIs)

KPI	SERVICE MANAGEMENT PROCESS	METRIC	MEASURE & METHOD	TARGET(S)
1	Service Desk	Call Answering Performance	Total of inbound calls answered	>90% within 20seconds
2	Incident Management	Service Desk Response Times	Time to respond to Incident case – from when first logged.	>90% within 30mins for P1 (24x7) >90% within 30mins for P2 (24x7) >90% within 1 hour for P3 (Business Hours) *Business Hours = 09:00 – 18:00, Monday - Friday
3	Incident Management	Service Desk Resolution Times	Time to resolve service measured from the time it was first raised – may involve a workaround before a permanent fix is implemented.	>90% within 4 hours for P1 (24x7) >90% within 6 hours for P2 (24x7) >90% within 8 hours for P3 (Business hours)
4	Major Incident Management	Major Incident Status updates	Updates to status page or similar	Hourly updates to customers
5	Incident Management	Major Incident Review Performance	Report delivery with root case	Reason For Outage document provided within 5 working days
6	Change Management	Maintenance Notifications	Maintenance notified 5 days in advance	>95% achieve this
7	Change Management	Change Success	% of changes completed successfully	>95% achieve this
8	Service Request Management	Service Request Performance	Service Request Response	>90% response within 4 hours and
9	Complaints	Customer Complaint Response	All complaints will be investigated will receive a formal response within 10 working days	100%

7.6 Service Continuity Management

In the event of a failure, Carrenza provides the following targets to ensure service continuity.

SLA	SERVICE	METRIC	TARGET
1	Enterprise & Public Sector Cloud – Virtual Private Cloud	Host failure	All virtual machines online with 15 minutes
2	Enterprise Cloud – Dedicated Physical Server	Standalone host failure	Service restored within 8 hours
3	Enterprise Cloud – Dedicated Physical Server	Host failure as part of an active-active configuration	Service restored within 1 hour
4	DRaaS	RPO (Recovery Point Objective) average per calendar month	<= 5 Minutes
5	DRaaS	RTO (Recovery Time Objective) from point of invocation	<= 4 Hours1

[1] – Subject to a successful DR test completing within 4 hours.

7.7 Service Level Agreement Exclusions

The following circumstances for the period, and to the extent that they apply, shall not count towards any service level as a failure to perform the services:

a) A force majeure event as defined in the contracted Services Agreement (MSA/MRA).
b) A suspension of the service in accordance with the Services Agreement (MSA/MRA)
c) Scheduled or Emergency maintenance as required.
d) Faults that are a result of the Customer or End User not complying with Carrenza' Security Policy.
e) Faults proven to be caused by a virus introduced negligently or otherwise by the Customer or End User onto its service.
f) Faults or omissions of the Internet or private connectivity. If connectivity is provided by Carrenza, such a remedy is covered in the Data Service Level Agreement.
g) Faults or omissions in equipment, wiring, cabling software or other services including faults on the customer network or customer's own equipment which are not maintained by Carrenza.
h) Failure to comply with capacity management recommendations issued by Carrenza.
i) During any trial or proof of concept period.
j) Customer is not using the Services in accordance with the Documentation (including the best practice implementation policies therein) as well as reasonable usage allowances.
k) Unreasonable delay by the Partner of Customer during an incident where their assistance is required as part of the resolution in accordance with the service levels.
l) If the service can be connected to via any applicable means, then the service is not deemed unavailable.
m) Loss of resilience is not considered loss of service.
n) Loss of access to control panels or support portals are not deemed as service unavailability.
o) Services procured from 3rd parties and not procured through Carrenza.
p) Services that are not "Ready for Service" due to customer delay during implementation

7.8 Service Credits

Service Credits will be issued in line with the Carrenza Master Service Agreement, as such the following terms apply:

- Service credits are calculated based on a percentage of the Recurring Fees payable for the service as indicated in the per product Service Level Agreement.
- The maximum Service Credit allowable in any given calendar month is limited to the amount of Recurring Fees payable in that calendar month directly associated with the service.
- A Service Credit shall not be credited to the Customer's account unless the Customer requests it from the Supplier's accounts department within thirty (30) days of the date on which Carrenza failed to meet the relevant Service Level for a reason solely due to the fault of Carrenza. A claim for any such Service Credit must be made via email and sent to servicedesk@carrenza.com.
- The calculation of the Service Credit shall be based on Recurring Fees and shall not include any other Fees paid or payable by the Customer to Carrenza.
- Service Credits shall not be paid if the Customer's account is in arrears.