Service Description

Cloud Hosting

IaaS Compute for Legacy Applications

G-Cloud 9

Table of Contents

1 IAAS COMPUTE FOR LEGACY APPLICATIONS OVERVIEW 4
1.1 General 4
1.2 IaaS Services 4
1.3 Compliance 4
1.4 Cloud Deployment Models 4
1.5 OFFICIAL Vulnerability Management & Protective Monitoring 5
1.6 Data Centres 6
1.7 Network & PSN Connectivity 6
1.8 Multi-Cloud 6
2 CARRENZA OFFICIAL IAAS SERVICE 7
2.1 IaaS Services 7
2.2 Compliance 7
2.3 Cloud Deployment Models 7
2.4 OFFICIAL Vulnerability Management & Protective Monitoring 7
2.5 Data Centres 8
2.6 Network & PSN Connectivity 9
2.7 Server Resources 9
2.8 Supporting Government ICT 11
2.9 Resilience 11
2.10 On-boarding and Off-boarding processes 13
2.11 Pricing 14
2.12 Service Management 14
2.13 Service Level Agreement 16
2.14 Commercial Relationship 17
2.15 OFFICIAL Data Management & Handling 17
2.16 Technical Requirements 19
2.17 Trial Service 19
3 CARRENZA COMMERCIAL IAAS SERVICE 20
3.1 Overview 20
3.2 Compliance 20
3.3 Cloud Deployment Models 20
3.4 Data Centres 20
3.5 Network & PSN Connectivity 21
3.6 Server Resources 21
3.7 Supporting Government ICT 23
3.8 Resilience 23
3.9 On-boarding and Off-boarding processes 25
3.10 Pricing 26
3.11 Service Management 26
3.12 Service Level Agreement 28
3.13 Commercial Relationship 29
3.14 Data Management & Handling 29
3.15 Technical Requirements 30
3.16 Trial Service 30

4 AMAZON WEB SERVICES 31
4.1 OVERVIEW 31
4.2 SUPPORT 31
4.3 DATA CENTRE LOCATIONS 31
4.4 SEVERITY DEFINITIONS 31
4.5 SERVICE CONSTRAINTS 31
4.6 ON-BOARDING AND OFF-BOARDING PROCESSES 32
4.7 COMMERCIAL RELATIONSHIP 32
4.8 PRICING 33
5 GOOGLE CLOUD PLATFORM 34
5.1 SUPPORT 34
5.2 DATA CENTRE LOCATIONS 34
5.3 SEVERITY DEFINITIONS 34
5.4 SERVICE CONSTRAINTS 34
5.5 ON-BOARDING AND OFF-BOARDING PROCESSES 34
5.6 COMMERCIAL RELATIONSHIP 35
5.7 PRICING 35
6 VMWARE VCLOUD AIR 37
6.1 SUPPORT 37
6.2 DATA CENTRE LOCATIONS 37
6.3 SEVERITY DEFINITIONS 37
6.4 SERVICE CONSTRAINTS 37
6.5 ON-BOARDING AND OFF-BOARDING PROCESSES 37
6.6 COMMERCIAL RELATIONSHIP 38
6.7 PRICING 38
7 MICROSOFT AZURE 40
7.1 SUPPORT 40
7.2 DATA CENTRE LOCATIONS 40
7.3 SEVERITY DEFINITIONS 40
7.4 SERVICE CONSTRAINTS 40
7.5 ON-BOARDING AND OFF-BOARDING PROCESSES 40
7.6 COMMERCIAL RELATIONSHIP 41
7.7 PRICING 41

1 IaaS Compute for Legacy Applications Overview

1.1 General

Under G-Cloud 9 we are bidding for Cloud Hosting.

1.2 IaaS Services

The Carrenza IaaS compute for legacy applications service is delivered using either the Carrenza OFFICIAL or Commercial IaaS. The service includes VMware X86 hosting, OVM X86 hosting, and Oracle SPARC hosting for non-X86 workloads.

Carrenza provide IaaS and PaaS to support legacy applications for public sector organisations. The service includes legacy application hosting, application and infrastructure automation, and integration services to improve how you deploy, scale, and upgrade your legacy applications and infrastructure environments.

The service supports complex legacy applications requirements, such as applications that run on Oracle database, and our internal DevOps team are available to provide continuous integration and application automation services if required.

The service supports OFFICIAL and OFFICIAL SENSITIVE classified data workloads, offers a choice of both virtual and bare-metal infrastructure, per-hour billing options, and includes a 99.99% service level agreement as standard. Hybrid cloud hosting options are also available.

1.3 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.

1.3.1 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 ONLY applies to Services which 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.

1.4 Cloud Deployment Models

1.4.1 Portal:

The Carrenza VMware vCloud Director Portal provisions software-defined data centre services as virtual data centres that provide virtualized compute, networking, storage and security. Customers are able to make Changes to the environment through the portal as well as create and delete servers as and when required.

1.4.2 API:

Customers can also make use of the vCloud API to utilise the features of vCloud to provision and manage virtual servers.

1.4.3 Carrenza Managed Deployment:

The Carrenza managed deployment model provides the customer with access to the virtual server(s) only, provisioned by VMware vCenter. Requests are submitted through the Carrenza service desk to make changes or service requests for additional servers as and when required.

1.5 OFFICIAL Vulnerability Management & Protective Monitoring

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

Carrenza ensure all 5 key aspects of protective monitoring are conducted on our secure government IaaS platform 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's 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's 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

1.6 Data Centres

Our data centres meet the Uptime Institute Tier 3 requirements for data centres, which includes the following requirements:

- Multiple independent distribution paths serving IT equipment. Generally, only one distribution path serves equipment at any given time.
- All IT equipment is dual-powered and fully compatible within the topology of a site's architecture.

1.7 Network & PSN Connectivity

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

1.8 Multi-Cloud

As part of this service customers are able to leverage Carrenza's partnerships with the leading hyperscale public cloud providers and utilise the services offered by these providers. This includes:

- Carrenza Commercial IaaS
- Carrenza OFFICIAL IaaS
- Amazon Web Services (AWS)
- Google Cloud Platform
- VMware vCloud Air
- Microsoft Azure

2 Carrenza OFFICIAL IaaS Service

2.1 IaaS Services

The Carrenza OFFICIAL IaaS has been built to meet demand for cloud infrastructure that provides high security, enterprise-ready features and the ability to support mission and business critical workloads.

Carrenza's OFFICIAL IaaS services have been built to meet demand for cloud infrastructure that provides high security, enterprise-ready features and the ability to support mission and business critical workloads. Designed from the ground up as an enterprise solution; our IaaS provides high levels of support and guaranteed resource available to you when needed. Our IaaS services make it possible to run just about any enterprise application.

The service supports OFFICIAL and OFFICIAL SENSITIVE classified data workloads, offers a choice of both virtual and bare-metal infrastructure, per-hour billing options, and includes a 99.99% service level agreement as standard.

2.2 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.

2.2.1 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 ONLY applies to Services which 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.

2.3 Cloud Deployment Models

2.3.1 Portal:

The Carrenza VMware vCloud Director Portal provisions software-defined data centre services as virtual data centres that provide virtualized compute, networking, storage and security. Customers are able to make Changes to the environment through the portal as well as create and delete servers as and when required.

2.3.2 API:

Customers can also make use of the vCloud API to utilise the features of vCloud to provision and manage virtual servers.

2.3.3 Carrenza Managed Deployment:

The Carrenza managed deployment model provides the customer with access to the virtual server(s) only, provisioned by VMware vCenter. Requests are submitted through the Carrenza service desk to make changes or service requests for additional servers as and when required.

2.4 OFFICIAL Vulnerability Management & Protective Monitoring

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

Carrenza ensure all 5 key aspects of protective monitoring are conducted on our secure government IaaS platform 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's 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's 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

2.5 Data Centres

Our data centres meet the Uptime Institute Tier 3 requirements for data centres, which includes the following requirements:

- Multiple independent distribution paths serving IT equipment. Generally, only one distribution path serves equipment at any given time.
- All IT equipment is dual-powered and fully compatible within the topology of a site's architecture.

2.6 Network & PSN Connectivity

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

2.7 Server Resources

2.7.1 Compute

The advent of the public cloud has fundamentally shifted the way we think about buying and consuming compute. Where in the past you bought servers to use for a number of years, now you are renting compute by the hour.

Under the hood Carrenza IaaS is built on commodity hardware, which includes several different types of physical hardware. We therefore have defined a unit of compute, a vCPU, which provides you with a consistent amount of CPU capacity regardless of the underlying hardware.

We constantly benchmark and test underlying hardware to ensure the consistency and predictability of the performance of a vCPU.

Our server resources were engineered with enterprise use in mind. Consequentially:

- All of our server resources are elastic.
- We offer reserved resources where guaranteed availability of elastic resources is required.
- All of our storage is persistent.
- We do not contend. The resources you buy are guaranteed to be allocated for you to use.
- Compute can be configured; there are no fixed instance sizes.
- Resources can be deployed as physical (non-virtualised) servers. These devices are billed monthly and cannot be powered off and on in the same way virtual servers can.
- If you require bespoke physical servers these can be provided, but require a direct commitment to the specific resource.

Available Configurations:

Service	Detail
vCPU	Up to 32 vCPUs per server, Changeable while running.
Reserved vCPU	Reserved vCPUs are used to guarantee availability of Compute where it's required in guaranteed form for DR or Scalability. Reserved vCPUs are contended.
RAM	RAM is uncontended and can be delivered in allocations of up to 256GB per server. Maximum RAM:vCPU ratio of 8:1

2.7.2 Storage

Disk: All our servers are SAN backed meaning that the server exists on the SAN and not on local disk, our servers just provide processing and memory which means virtual servers on our cloud infrastructure are hugely resilient.

Disk storage is provided on a per Gigabyte basis with committed total quantities of storage based on the size of the LUNs made available to each server. We have a number of different storage types which are accessible through Carrenza IaaS.

Block Storage: Block storage comes in three types;

- Performant IOPs Pack
- Performant Storage
- Standard Production Storage

Object Storage: Object storage comes in two types;

- Archive Storage
- Public Cloud Object Storage

Available Configurations:

Service	Detail
Performant IOPs Pack	Additional IOPS performance can be configured in units of 1000 IOPS per drive only on Performant Storage.
Performant Storage	PS is delivered from SAN and available per GB with a minimum of 10GB per LUN. Maximum LUN size is 8TB. PS is always delivered using SSD, IOPS are guaranteed between 250 and 1000.
Standard Production Storage	Standard Production Storage is delivered from SAN and available per GB with a minimum of 10GB per LUN. Maximum LUN size is 8TB. When delivered using SSD, IOPS are guaranteed between 125 and 250.
Archive Storage	A low-cost storage service for data archiving, online backup and disaster recovery.
Public Cloud Object Storage	A low-cost distributed Object store for non-compliance affected objects delivered from a Hyperscale public cloud provider.

2.7.3 Network Services

Networking: Every virtual server has access to network services delivered from our core security platform. Designed natively for high-availability Carrenza networking Services can provide for the full range, from Firewalling and load balancing through to VPN termination, dynamic routing and SSL aggregation.

Networking Services are either delivered through our self-service portal or as a managed service. However you choose to work; we allow you to set the security policies; we do not impose any security standards on your service.

Available Configurations:

Standard Networking Service	
Standard Networking	Includes edge firewalling, including High Availability (HA), Network Address Translation (NAT), DHCP, basic load balancing (no SSL termination), site-to-site IPsec VPN and static routing.
Advanced Networking (Standard) Service	
Advanced Networking (Standard)	Includes all Standard Networking features and HA, dynamic routing, advanced Load Balancing (with SSL termination), remote access SSL VPN tunnels (up to 50), site-to-site IPsec VPN (guaranteed up to 512 connections).
Advanced Networking (Premium) Service	
Advanced Networking (Premium)	Includes all Advanced Networking (Standard) features and remote access SSL VPN tunnels (up to 100 guaranteed connections), site-to-site IPsec VPN (guaranteed up to 1600 connections) and guarantees up to 200 routed network segments in a virtual data centre.
DDoS Mitigation	
Layer 3 & 4 DDoS	DDoS mitigation service protecting against flood type attacks (e.g. DNS amplification & SMURF attacks) for all external IP addresses.

Mitigation	Only available in UK datacentres.
Layer 7 / Proxy DDoS Mitigation	Includes all Layer 3 & 4 DDoS Mitigation features and provides application level DDoS protection scrubbing all incoming traffic utilising advanced behavioural analytics.

2.8 Supporting Government ICT

2.8.1 Government ICT

Carrenza's services have been designed to support the government ICT strategy and the Digital by Default Service Standard as published on GOV.UK: https://www.gov.uk/service-manual/digital-by-default. This includes a focus on:

- Understand the user (and customer) needs, underpinned by Carrenza's multi cloud strategy and an emphasis on ensuring our customers use the right cloud for the right workload at the right time.
- Implementing the 14 cloud security principals
- Reducing waste and project failure, and stimulating economic growth
- Using ICT to enable and deliver change
- Strengthening governance
- Using the ITL Framework for IT Service Management
- Supporting agile and providing a flexible service to our customers
- Support open standards
- Provide transparent reporting on service availability and reporting, ensuring the baseline service is fit for purpose

2.8.2 Green IT

Carrenza's 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 the Equinix data centre where we host our most recently provisioned node won the Green Data Centre award from Datacenter Dynamics, and this innovative use of sustainable and renewable energy technology was a key factor in us selecting the facility for our operations.

2.9 Resilience

Our systems are designed to be highly reliable and available, but we recognise that is not always enough to ensure continuous delivery of key services and as a result provide a full range of business continuity and backup services.

2.9.1 Backup & Restore

2.9.1.1 Backup

Our Backup & Restore Service allows you to protect both the essential files necessary for compliance and regulatory purposes and the whole servers required to ensure continuity of delivery of your applications and services to your teams and clients.

Backup: Backup Services are provided using industry leading technologies for both agentless snapshots and agent based granular file and bit-level backup.

Engagement: An engineer will help you to define your backup policies. Together you will consider Data location and replication offsite, the time-to-recover and criticality of each service and the monitoring regime that will ensure that your service is operational and performing as expected.

Requirements: Each Backup Service is specific to a Customer, however there are some common general requirements:

- **Definition;** you will need to define frequency, timing, retention and exclusions governing your backup requirements.
- **Availability;** unless you are taking our remote hands service you will be responsible for ensuring that your server is available to backup and that it has sufficient resources to enable it to perform backup tasks non-disruptively.
- **Agent;** your server may need an agent installed on it, in that event it will need enough resources to support the requirements of the agent and you may need to undertake the agent install.
- **Change Control;** any changes to the backup service, once live, will be done under change control.
- **Cascade;** To take the Backup Service you must have taken the Restore Service.

2.9.1.2 Restore

Backed up data or server snapshots can be restored on demand 24x7. Local backups will be faster, recovery from off-site storage will take longer, your engagement phase will have determined the most appropriate locations for your backups. There are two types of restore:

- **File Level:** Specific Files and/or folders can be retrieved and restored to the last successful backup – or a specific point in time.
- **Server Level:** A complete server image is restored to the state of the last successful backup.

Limitations; there are a few specific limitations to the restore process:

- **Verification;** you will need to verify that a file restore or Server image is correct following a restore.

- **Volume;** the restore process is limited to 4 restores per server per year, additional restores will be charged based on the standard engineer rate.
- **Instruction;** Restores can only be undertaken when Carrenza has received a specific instruction in Writing.
- **Cascade;** To take this Restore Service you must also take the Backup Service.

2.9.2 Disaster Recovery

Our services can be mirrored across multiple infrastructure nodes in the UK (London and Slough) as well as Amsterdam, Netherlands. Multiple nodes can be used to support disaster recovery objectives as well as tactical and business continuity requirements.

2.9.3 Multi-site mirroring

Multi-site resilience is enabled by providing resources in more than one cloud node.

2.9.3.1 Supported Configurations

Supported configurations range from the ability to restore from backups to non-reserved resources in a second node to active-active multi-node operation.

2.9.3.2 Service Summary

The following table provides a summary of the service provided under this Service Description:

Service Area	Service Feature
Disaster Recovery	Server level restore
	Active slave
	Multi-site network

2.9.3.3 Detailed Service Description

Service Feature	Description	Client obligations	Limitations
Disaster Recovery			
Server level restore	The complete server images for a solution will be restored to the state of the last successful backup in an alternative cloud node upon client request.	Clients will have to decide if they are to restore to reserved instances or un-reserved instances when selecting this service feature.	Un-reserved instances are not guaranteed to be available. Reserved instances are guaranteed to be available
Active slave	Permanent committed resources will be made available to support multi-site slave configurations at the platform or application layer.	Clients will have to specify the parameters within which the active slave system needs to operate.	Should low latency be critical for application performance this service can only be guaranteed to be performant with testing.
Multi-site network	Networking available in multiple cloud nodes to support DR and BC requirements.	Clients will need to decide if they are to opt for reserved or committed network resources.	Should low latency be critical for application performance this service can only be guaranteed to be performant with testing.

2.10 On-boarding and Off-boarding processes

2.10.1 On-boarding

Our services are simple to consume requiring only a web browser. New customers are asked to provide us with a list of authorised contacts and permission levels with whom we can engage and those nominated individuals are provided with documentation and if need be training on how to contact us for support, how to access the ticketing and monitoring portals and how to use VMware vCloud.

2.10.2 Off-boarding

The customer is able to take copies of all data it requires at the end of an agreement term. Please see section 2.15.4 for details of the data migration process. Additionally if the customer wishes to have copies of the virtual machines for deployment, for example into another cloud, these can be securely exported in the OVF format via SSL. ISO images can also be securely downloaded via SSL.

2.11 Pricing

Carrenza provide commodity pricing based on resource usage for our OFFICIAL/OFFICIAL SENSITIVE IaaS. Carrenza offer a unique granular pricing model based on resource used (per vCPU, GB RAM and GB Storage) and not per server. This provides increased transparency and means that when environments scale you will only have to pay for the additional resource required and used, and not for the next server size up. This makes it much more cost effective to scale the environment up and down, only paying for the resource you actually use.

The below illustrates the price per hour for some sample server sizing and has been created for illustration purposes. Each server has 60GB data allocated although additional SAN storage is available priced per GB at 16p per GB per month for standard production storage. Hourly billing / pricing is available.

The table below illustrates both the monthly and hourly pricing for the Carrenza IaaS but please see the Carrenza Cloud Services Pricing Guide for a detailed pricing breakdown.

Server Size	vCPU	GB RAM	GB Storage	Monthly Price	Hourly Price
Tiny	1	2	60	£48.41	£0.07
Small	2	4	60	£87.22	£0.12
Medium	4	8	60	£164.84	£0.23
Medium (high memory)	4	16	60	£240.20	£0.33
Large	8	16	60	£320.08	£0.44
Large (high memory)	8	32	60	£470.80	£0.64
Sample App Server 1	8	48	60	£621.52	£0.85
Sample App Server 2	8	64	60	£772.24	£1.06
Sample App Server 3	8	96	60	£1,073.68	£1.47
Large Database Server	16	32	60	£630.56	£0.86
Transactional Server	16	64	60	£932.00	£1.28
High Transactional Server	32	128	60	£1,854.40	£2.54

2.12 Service Management

Carrenza provides service management to its Customers based on the ITIL framework. Service delivery management is delivered by a team of experienced professionals who provide regular reporting, technical account management and a regular review of business objectives to ensure the service is delivering the business value expected. The following sections detail how we monitor and support the environments.

2.12.1 Utilisation monitoring

We use open-source tooling to provide monitoring and reporting.

2.12.2 Support

Support is provided to a Customer to help it derive the best value possible from the Services and is available 24x7 by phone through our service desk and via our ticketing portal.

2.12.2.1 Supported Products

The following table lists currently supported products

Service Description
Server Resources
Network Services
Backup & Restore
Disaster Recovery

2.12.2.2 Detailed Service Description

Service Feature	Description	Client obligations	Limitations
24x7 P1 failure support	24x7 Telephone support for priority 1 issues.	Clients must ensure that contact detail lists are up to date. Priority 1 issues must be reported by Telephone.	Support is limited to P1 infrastructure failures.
9-6 business day support	Business hours telephone and ticket based support for priority 2-4 issues.	Clients must ensure that contact detail lists are up to date.	Support is limited to P2-4 infrastructure failures.
Network Changes	Changes to network services will be carried out in line with the change management procedure	Clients must provide all the details needed to ensure changes can be made.	The number of changes per month is limited; see the Service descriptions in Section 1 for details.
Server Changes	Changes to Server services will be carried out in line with the change management procedure	Clients must provide all the details needed to ensure changes can be made.	

2.12.3 Service Constraints

2.12.3.1 Maintenance

Sometimes it is necessary to undertake maintenance, when that happens it is the job of the support team to help the customer to minimise the impact of any maintenance activity on the delivery of services to end consumers.

Maintenance includes all regularly scheduled error corrections, third party software updates and upgrades to the Carrenza hardware. Some maintenance can be conducted without risk to customer services; Carrenza will undertake this background maintenance at its discretion from time to time.

Occasionally we will need to suspend the service for a planned outage where maintenance cannot be conducted by any other means. Planned outages will be performed between the hours of 12am and 8am and we will provide the customer with 7 days' notice of any planned outage.

In extreme circumstances Carrenza may need to interrupt the Services to perform emergency maintenance, this will only happen where it is unavoidable to ensure the on-going delivery of service or where there is a risk to client data or system integrity.

2.13 Service Level Agreement

2.13.1 Performance

Resources are guaranteed to perform materially in line with the specification.

2.13.2 Availability

Virtualised IaaS services come with a 99.99% uptime guarantee. Physical IaaS services come with a 99.9% uptime guarantee.

2.13.3 Support Hours

Support is provided to a Customer to help it derive the best value possible from the Services and is available 24x7 by phone through our service desk and via our ticketing portal.

2.13.4 Severity Definitions

Priority	Description	Response time	Target resolution time
Priority 1	The Service is "down" and inaccessible or has suffered from failures which degrade service and reduce functionality to users. Priority 1 incidents shall be reported by telephone only.	Within 30 Minutes of completing a call to the Carrenza Emergency support Line. 24x7x365	Four Hours, 24x7x365. Continuous effort after initial response and with Customer co-operation. One Hour for Non-virtualised Infrastructure resolution where a Hot Spare Device has been purchased.
Priority 2	Operation of the Services is severely degraded or Single Points of Failure have resulted from failures. Service to users in not affected. Priority 2 incidents shall be reported by telephone only.	Within 30 Minutes of completing a call to the Carrenza Emergency support Line. 24x7x365	Four hours from the start of the next business day unless an escalation to Priority 1 is requested.
Priority 3	Certain non-essential features of the Service are impaired while all major components of the Service remain functional. Priority 3 incidents are to be reported via the ticketing system.	Within 1 Normal Business Hour.	Within seven Business Days after initial response.
Priority 4	Errors, bugs or inconsistencies that are, not service affecting and clearly have little or no impact on the normal operation of the Services. Priority 4 incidents are to be reported via the ticketing system.	Within 24 Normal Business Hours.	As determined during the investigation of the incident.

2.13.5 Service Credits For Zero Commit Contracts

If availability of a Service falls below the Uptime Service Level in a given calendar month (a "**Service Delivery Failure**"), Carrenza shall credit the Customer's account by an amount calculated as the product of the total cumulative downtime (expressed as a percentage of the total possible uptime minutes in the month concerned) and the total monthly Fee for the provision of the Service owed for that month.

Where a single "**Service Delivery Failure**" persists beyond the "**Target Resolution Time**" (defined in the Service Delivery Failure section) for the failed service Carrenza shall credit the Customer's account by a sum equivalent to 20% of the fees due for the current month for the failed Service.

A table of priorities set out in the Service Definition (Service Delivery Failure) defines the timelines under which support is to be provided. Failure to meet the target response times for responding to a

support call reporting a Priority 1 or 2 failure shall be deemed to be a Service Delivery Failure and shall entitle the client to a credit equivalent to a single days Fees for any Service which had failed and caused that support call to be raised by the Customer.

Each of the credits referred to shall be referred to as a "**Service Credit**". Service Credits accruing in respect of each month shall be applied against the Fees otherwise payable for the following month. The maximum Service Credit allowable in respect of all Service Delivery Failures in a given month is limited to an amount equal to 40% of the total monthly Fee otherwise payable by the Customer to Carrenza for that month. Subject to such monthly maximum, each of the categories of Service Credits listed above shall be cumulative and not mutually exclusive.

2.14 Commercial Relationship

2.14.1 Ordering

Services can be ordered by contacting Carrenza with your requirements. Typically, upon ordering a cool-off contract is issued with a corresponding PO. Following the initial order (for existing customers), 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 our self-service portal.

2.14.2 Use by other suppliers

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

2.14.3 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.

2.14.4 Service Roadmap

None of the services offered as part of this tender will change during the term of G-Cloud 9.

2.14.5 Termination by Customers

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

2.14.6 Termination by Carrenza

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

2.15 OFFICIAL Data Management & Handling

2.15.1 OFFICIAL Data security policy

Carrenza 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:

- 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.

2.15.2 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.

2.15.3 Data Processing

Carrenza 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.

2.15.4 Data Migration

Carrenza 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 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.

2.15.5 Data Storage and Processing locations

Our IaaS services are delivered for G-Cloud 9 from 3 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.

2.15.6 OFFICIAL Data Handling

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

Carrenza IaaS 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 IaaS SyOPS documentation developed by the appropriate service provider. These must conform to Carrenza standing documentation, HMG policy and IAS5 as agreed with the service Accreditor.

Carrenza's IaaS documentation are marked in accordance with their internal Data Handling classification policy (and under the new GSC is likely to be considered OFFICIAL Sensitive at most) with stringent need to know controls applied.

2.15.7 OFFICIAL Hard Disk Destruction

Disks to be sent off-site shall have information removed from them in an approved manner prior to removal, Carrenza uses a degausser that is NCSC approved up to Restricted Level as well as the Blanco v5 application which erases data securely from PCs, laptops, servers and storage environments.

2.16 Technical Requirements

There are no specific technical requirements for consuming this service other than access to a recent browser.

2.17 Trial Service

Our services are available to trial for a two week period on request. Trial services must not be used for production services, and are available in limited volumes. Please contact us to request a trial.

3 Carrenza Commercial IaaS Service

3.1 Overview

Carrenza' s IaaS services have been built to meet demand for cloud infrastructure that provides high security, enterprise-ready features and the ability to support mission and business critical workloads.

Designed from the ground up as an enterprise solution; our IaaS provides high levels of support and guaranteed resource available to you when needed. Resource that was engineered from the ground up to make it possible to run just about any enterprise application.

3.2 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.

3.2.1 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 ONLY applies to Services which 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.

3.3 Cloud Deployment Models

3.3.1 Portal:

The Carrenza VMware vCloud Director Portal provisions software-defined data centre services as virtual data centres that provide virtualized compute, networking, storage and security. Customers are able to make Changes to the environment through the portal as well as create and delete servers as and when required.

3.3.2 API:

Customers can also make use of the vCloud API to utilise the features of vCloud to provision and manage virtual servers.

3.3.3 Carrenza Managed Deployment:

The Carrenza managed deployment model provides the customer with access to the virtual server(s) only, provisioned by VMware vCenter. Requests are submitted through the Carrenza service desk to make changes or service requests for additional servers as and when required.

3.4 Data Centres

Our data centres meet the Uptime Institute Tier 3 requirements for data centres, which includes the following requirements:

- Multiple independent distribution paths serving IT equipment. Generally, only one distribution path serves equipment at any given time.
- All IT equipment is dual-powered and fully compatible within the topology of a site's architecture.

3.5 Network & PSN Connectivity

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

3.6 Server Resources

3.6.1 Compute

The advent of the public cloud has fundamentally shifted the way we think about buying and consuming compute. Where in the past you bought servers to use for a number of years, now you are renting compute by the hour.

Under the hood Carrenza IaaS is built on commodity hardware, which includes several different types of physical hardware. We therefore have defined a unit of compute, a vCPU, which provides you with a consistent amount of CPU capacity regardless of the underlying hardware.

We constantly benchmark and test underlying hardware to ensure the consistency and predictability of the performance of a vCPU.

Our server resources were engineered with enterprise use in mind. Consequentially:

- All of our server resources are elastic.
- We offer reserved resources where guaranteed availability of elastic resources is required.
- All of our storage is persistent.
- We do not contend. The resources you buy are guaranteed to be allocated for you to use.
- Compute can be configured; there are no fixed instance sizes.
- Resources can be deployed as physical (non-virtualised) servers. These devices are billed monthly and cannot be powered off and on in the same way virtual servers can.
- If you require bespoke physical servers these can be provided, but require a direct commitment to the specific resource.

Available Configurations:

Service	Detail
vCPU	Up to 32 vCPUs per server, Changeable while running.
Reserved vCPU	Reserved vCPUs are used to guarantee availability of Compute where it's required in guaranteed form for DR or Scalability. Reserved vCPUs are contended.
RAM	RAM is uncontended and can be delivered in allocations of up to 256GB per server. Maximum RAM:vCPU ratio of 8:1

3.6.2 Storage

Disk: All our servers are SAN backed meaning that the server exists on the SAN and not on local disk, our servers just provide processing and memory which means virtual servers on our cloud infrastructure are hugely resilient.

Disk storage is provided on a per Gigabyte basis with committed total quantities of storage based on the size of the LUNs made available to each server. We have a number of different storage types which are accessible through Carrenza IaaS.

Block Storage: Block storage comes in three types;

- Performant IOPs Pack
- Performant Storage
- Standard Production Storage

Object Storage: Object storage comes in two types;

- Archive Storage
- Public Cloud Object Storage

Available Configurations:

Service	Detail
Performant IOPs Pack	Additional IOPS performance can be configured in units of 1000 IOPS per drive only on Performant Storage.
Performant Storage	PS is delivered from SAN and available per GB with a minimum of 10GB per LUN. Maximum LUN size is 8TB. PS is always delivered using SSD, IOPS are guaranteed between 250 and 1000.
Standard Production Storage	Standard Production Storage is delivered from SAN and available per GB with a minimum of 10GB per LUN. Maximum LUN size is 8TB. When delivered using SSD, IOPS are guaranteed between 125 and 250.
Archive Storage	A low-cost storage service for data archiving, online backup and disaster recovery.
Public Cloud Object Storage	A low-cost distributed Object store for non-compliance affected objects delivered from a Hyperscale public cloud provider.

3.6.3 Network Services

Networking: Every virtual server has access to network services delivered from our core security platform. Designed natively for high-availability Carrenza networking Services can provide for the full range, from Firewalling and load balancing through to VPN termination, dynamic routing and SSL aggregation.

Networking Services are either delivered through our self-service portal or as a managed service. However you choose to work; we allow you to set the security policies; we do not impose any security standards on your service.

Available Configurations:

Standard Networking Service	
Standard Networking	Includes edge firewalling, including High Availability (HA), Network Address Translation (NAT), DHCP, basic load balancing (no SSL termination), site-to-site IPsec VPN and static routing.
Advanced Networking (Standard) Service	
Advanced Networking (Standard)	Includes all Standard Networking features and HA, dynamic routing, advanced Load Balancing (with SSL termination), remote access SSL VPN tunnels (up to 50), site-to-site IPsec VPN (guaranteed up to 512 connections).
Advanced Networking (Premium) Service	
Advanced Networking (Premium)	Includes all Advanced Networking (Standard) features and remote access SSL VPN tunnels (up to 100 guaranteed connections), site-to-site IPsec VPN (guaranteed up to 1600 connections) and guarantees up to 200 routed network segments in a virtual data centre.
DDoS Mitigation	
Layer 3 & 4 DDoS	DDoS mitigation service protecting against flood type attacks (e.g. DNS amplification & SMURF attacks) for all external IP addresses.

Mitigation	Only available in UK datacentres.
Layer 7 / Proxy DDoS Mitigation	Includes all Layer 3 & 4 DDoS Mitigation features and provides application level DDoS protection scrubbing all incoming traffic utilising advanced behavioural analytics.

3.7 Supporting Government ICT

3.7.1 Government ICT

Carrenza's services have been designed to support the government ICT strategy and the Digital by Default Service Standard as published on GOV.UK: https://www.gov.uk/service-manual/digital-by-default. This includes a focus on:

- Understand the user (and customer) needs, underpinned by Carrenza's multi cloud strategy and an emphasis on ensuring our customers use the right cloud for the right workload at the right time.
- Implementing the 14 cloud security principals
- Reducing waste and project failure, and stimulating economic growth
- Using ICT to enable and deliver change
- Strengthening governance
- Using the ITL Framework for IT Service Management
- Supporting agile and providing a flexible service to our customers
- Support open standards
- Provide transparent reporting on service availability and reporting, ensuring the baseline service is fit for purpose

3.7.2 Green IT

Carrenza's 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 the Equinix data centre where we host our most recently provisioned node won the Green Data Centre award from Datacenter Dynamics, and this innovative use of sustainable and renewable energy technology was a key factor in us selecting the facility for our operations.

3.8 Resilience

Our systems are designed to be highly reliable and available, but we recognise that is not always enough to ensure continuous delivery of key services and as a result provide a full range of business continuity and backup services.

3.8.1 Backup & Restore

3.8.1.1 Backup

Our Backup & Restore Service allows you to protect both the essential files necessary for compliance and regulatory purposes and the whole servers required to ensure continuity of delivery of your applications and services to your teams and clients.

Backup: Backup Services are provided using industry leading technologies for both agentless snapshots and agent based granular file and bit-level backup.

Engagement: An engineer will help you to define your backup policies. Together you will consider Data location and replication offsite, the time-to-recover and criticality of each service and the monitoring regime that will ensure that your service is operational and performing as expected.

Requirements: Each Backup Service is specific to a Customer, however there are some common general requirements:

- **Definition;** you will need to define frequency, timing, retention and exclusions governing your backup requirements.
- **Availability;** unless you are taking our remote hands service you will be responsible for ensuring that your server is available to backup and that it has sufficient resources to enable it to perform backup tasks non-disruptively.
- **Agent;** your server may need an agent installed on it, in that event it will need enough resources to support the requirements of the agent and you may need to undertake the agent install.
- **Change Control;** any changes to the backup service, once live, will be done under change control.
- **Cascade;** To take the Backup Service you must have taken the Restore Service.

3.8.1.2 Restore

Backed up data or server snapshots can be restored on demand 24x7. Local backups will be faster, recovery from off-site storage will take longer, your engagement phase will have determined the most appropriate locations for your backups. There are two types of restore:

- **File Level:** Specific Files and/or folders can be retrieved and restored to the last successful backup – or a specific point in time.
- **Server Level:** A complete server image is restored to the state of the last successful backup.

Limitations; there are a few specific limitations to the restore process:

- **Verification;** you will need to verify that a file restore or Server image is correct following a restore.

- **Volume;** the restore process is limited to 4 restores per server per year, additional restores will be charged based on the standard engineer rate.
- **Instruction;** Restores can only be undertaken when Carrenza has received a specific instruction in Writing.
- **Cascade;** To take this Restore Service you must also take the Backup Service.

3.8.2 Disaster Recovery

Our services can be mirrored across multiple infrastructure nodes in the UK (London and Slough) as well as Amsterdam, Netherlands. Multiple nodes can be used to support disaster recovery objectives as well as tactical and business continuity requirements.

3.8.3 Multi-site mirroring

Multi-site resilience is enabled by providing resources in more than one cloud node.

3.8.3.1 Supported Configurations

Supported configurations range from the ability to restore from backups to non-reserved resources in a second node to active-active multi-node operation.

3.8.3.2 Service Summary

The following table provides a summary of the service provided under this Service Description:

Service Area	Service Feature
Disaster Recovery	Server level restore
	Active slave
	Multi-site network

3.8.3.3 Detailed Service Description

Service Feature	Description	Client obligations	Limitations
Disaster Recovery			
Server level restore	The complete server images for a solution will be restored to the state of the last successful backup in an alternative cloud node upon client request.	Clients will have to decide if they are to restore to reserved instances or un-reserved instances when selecting this service feature.	Un-reserved instances are not guaranteed to be available. Reserved instances are guaranteed to be available
Active slave	Permanent committed resources will be made available to support multi-site slave configurations at the platform or application layer.	Clients will have to specify the parameters within which the active slave system needs to operate.	Should low latency be critical for application performance this service can only be guaranteed to be performant with testing.
Multi-site network	Networking available in multiple cloud nodes to support DR and BC requirements.	Clients will need to decide if they are to opt for reserved or committed network resources.	Should low latency be critical for application performance this service can only be guaranteed to be performant with testing.

3.9 On-boarding and Off-boarding processes

3.9.1 On-boarding

Our services are simple to consume requiring only a web browser. New customers are asked to provide us with a list of authorised contacts and permission levels with whom we can engage and those nominated individuals are provided with documentation and if need be training on how to contact us for support, how to access the ticketing and monitoring portals and how to use VMware vCloud.

3.9.2 Off-boarding

The customer is able to take copies of all data it requires at the end of an agreement term. Please see section 3.14.4 for details of the data migration process. Additionally if the customer wishes to have copies of the virtual machines for deployment, for example into another cloud, these can be securely exported in the OVF format via SSL. ISO images can also be securely downloaded via SSL.

3.10 Pricing

Carrenza provide commodity pricing based on resource usage for our IaaS. Carrenza offer a unique granular pricing model based on resource used (per vCPU, GB RAM and GB Storage) and not per server. This provides increased transparency and means that when environments scale you will only have to pay for the additional resource required and used, and not for the next server size up. This makes it much more cost effective to scale the environment up and down, only paying for the resource you actually use.

The below illustrates the price per hour for some sample server sizing and has been created for illustration purposes. Each server has 60GB data allocated although additional SAN storage is available priced per GB at 16p per GB per month for standard production storage. Hourly billing / pricing is available.

The table below illustrates both the monthly and hourly pricing for the Carrenza IaaS but please see the Carrenza Cloud Services Pricing Guide for a detailed pricing breakdown.

Server Size	vCPU	GB RAM	GB Storage	Monthly Price	Hourly Price
Tiny	1	2	60	£48.41	£0.07
Small	2	4	60	£87.22	£0.12
Medium	4	8	60	£164.84	£0.23
Medium (high memory)	4	16	60	£240.20	£0.33
Large	8	16	60	£320.08	£0.44
Large (high memory)	8	32	60	£470.80	£0.64
Sample App Server 1	8	48	60	£621.52	£0.85
Sample App Server 2	8	64	60	£772.24	£1.06
Sample App Server 3	8	96	60	£1,073.68	£1.47
Large Database Server	16	32	60	£630.56	£0.86
Transactional Server	16	64	60	£932.00	£1.28
High Transactional Server	32	128	60	£1,854.40	£2.54

3.11 Service Management

Carrenza provides service management to its Customers based on the ITIL framework. Service delivery management is delivered by a team of experienced professionals who provide regular reporting, technical account management and a regular review of business objectives to ensure the service is delivering the business value expected. The following sections detail how we monitor and support the environments.

3.11.1 Utilisation monitoring

We use open-source tooling to provide monitoring and reporting.

3.11.2 Support

Support is provided to a Customer to help it derive the best value possible from the Services and is available 24x7 by phone through our service desk and via our ticketing portal.

3.11.2.1 Supported Products

The following table lists currently supported products

Service Description
Server Resources
Network Services
Backup & Restore
Disaster Recovery

3.11.2.2 Detailed Service Description

Service Feature	Description	Client obligations	Limitations
24x7 P1 failure support	24x7 Telephone support for priority 1 issues.	Clients must ensure that contact detail lists are up to date. Priority 1 issues must be reported by Telephone.	Support is limited to P1 infrastructure failures.
9-6 business day support	Business hours telephone and ticket based support for priority 2-4 issues.	Clients must ensure that contact detail lists are up to date.	Support is limited to P2-4 infrastructure failures.
Network Changes	Changes to network services will be carried out in line with the change management procedure	Clients must provide all the details needed to ensure changes can be made.	The number of changes per month is limited; see the Service descriptions in Section 1 for details.
Server Changes	Changes to Server services will be carried out in line with the change management procedure	Clients must provide all the details needed to ensure changes can be made.	

3.11.3 Service Constraints

3.11.3.1 Maintenance

Sometimes it is necessary to undertake maintenance, when that happens it is the job of the support team to help the customer to minimise the impact of any maintenance activity on the delivery of services to end consumers.

Maintenance includes all regularly scheduled error corrections, third party software updates and upgrades to the Carrenza hardware. Some maintenance can be conducted without risk to customer services; Carrenza will undertake this background maintenance at its discretion from time to time.

Occasionally we will need to suspend the service for a planned outage where maintenance cannot be conducted by any other means. Planned outages will be performed between the hours of 12am and 8am and we will provide the customer with 7 days' notice of any planned outage.

In extreme circumstances Carrenza may need to interrupt the Services to perform emergency maintenance, this will only happen where it is unavoidable to ensure the on-going delivery of service or where there is a risk to client data or system integrity.

3.12 Service Level Agreement

3.12.1 Performance

Resources are guaranteed to perform materially in line with the specification.

3.12.2 Availability

Virtualised IaaS services come with a 99.99% uptime guarantee. Physical IaaS services come with a 99.9% uptime guarantee.

3.12.3 Support Hours

Support is provided to a Customer to help it derive the best value possible from the Services and is available 24x7 by phone through our service desk and via our ticketing portal.

3.12.4 Severity Definitions

Priority	Description	Response time	Target resolution time
Priority 1	The Service is "down" and inaccessible or has suffered from failures which degrade service and reduce functionality to users. Priority 1 incidents shall be reported by telephone only.	Within 30 Minutes of completing a call to the Carrenza Emergency support Line. 24x7x365	Four Hours, 24x7x365. Continuous effort after initial response and with Customer co-operation. One Hour for Non-virtualised Infrastructure resolution where a Hot Spare Device has been purchased.
Priority 2	Operation of the Services is severely degraded or Single Points of Failure have resulted from failures. Service to users in not affected. Priority 2 incidents shall be reported by telephone only.	Within 30 Minutes of completing a call to the Carrenza Emergency support Line. 24x7x365	Four hours from the start of the next business day unless an escalation to Priority 1 is requested.
Priority 3	Certain non-essential features of the Service are impaired while all major components of the Service remain functional. Priority 3 incidents are to be reported via the ticketing system.	Within 1 Normal Business Hour.	Within seven Business Days after initial response.
Priority 4	Errors, bugs or inconsistencies that are, not service affecting and clearly have little or no impact on the normal operation of the Services. Priority 4 incidents are to be reported via the ticketing system.	Within 24 Normal Business Hours.	As determined during the investigation of the incident.

3.12.5 Service Credits For Zero Commit Contracts

If availability of a Service falls below the Uptime Service Level in a given calendar month (a "**Service Delivery Failure**"), Carrenza shall credit the Customer's account by an amount calculated as the product of the total cumulative downtime (expressed as a percentage of the total possible uptime minutes in the month concerned) and the total monthly Fee for the provision of the Service owed for that month.

Where a single "**Service Delivery Failure**" persists beyond the "**Target Resolution Time**" (defined in the Service Delivery Failure section) for the failed service Carrenza shall credit the Customer's account by a sum equivalent to 20% of the fees due for the current month for the failed Service.

A table of priorities set out in the Service Definition (Service Delivery Failure) defines the timelines under which support is to be provided. Failure to meet the target response times for responding to a

support call reporting a Priority 1 or 2 failure shall be deemed to be a Service Delivery Failure and shall entitle the client to a credit equivalent to a single days Fees for any Service which had failed and caused that support call to be raised by the Customer.

Each of the credits referred to shall be referred to as a "**Service Credit**". Service Credits accruing in respect of each month shall be applied against the Fees otherwise payable for the following month. The maximum Service Credit allowable in respect of all Service Delivery Failures in a given month is limited to an amount equal to 40% of the total monthly Fee otherwise payable by the Customer to Carrenza for that month. Subject to such monthly maximum, each of the categories of Service Credits listed above shall be cumulative and not mutually exclusive.

3.13 Commercial Relationship

3.13.1 Ordering

Services can be ordered by contacting Carrenza with your requirements. Typically, upon ordering a cool-off contract is issued with a corresponding PO. Following the initial order (for existing customers), 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 our self-service portal.

3.13.2 Use by other suppliers

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

3.13.3 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.

3.13.4 Service Roadmap

None of the services offered as part of this tender will change during the term of G-Cloud 9.

3.13.5 Termination by Customers

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

3.13.6 Termination by Carrenza

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

3.14 Data Management & Handling

3.14.1 Data security policy

Carrenza Ltd is an accredited company under ISO/IEC 27001:2013 and as such adheres to the approved security policy noted below:-

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

- 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.

3.14.2 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.

3.14.3 Data Processing

Carrenza 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.

3.14.4 Data Migration

Carrenza 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 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.

3.14.5 Data Storage and Processing locations

Our IaaS services are delivered for G-Cloud 9 from 3 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.

3.15 Technical Requirements

There are no specific technical requirements for consuming this service other than access to a recent browser.

3.16 Trial Service

Our services are available to trial for a two week period on request. Trial services must not be used for production services, and are available in limited volumes. Please contact us to request a trial.

4 Amazon Web Services

4.1 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's Public Sector Hybrid 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's server support or server management services are purchased, access to a Service Desk for reporting incidents and Service Requests.

4.2 Support

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

4.3 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.

4.4 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/.

4.5 Service Constraints

4.5.1 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.

4.5.2 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 and check when planned outages are scheduled. Carrenza are not liable should the customer fail to check and lose data as a result.

4.5.3 Customer Responsibilities

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

4.6 On-boarding and Off-boarding processes

4.6.1 On-boarding

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

4.6.2 Off-boarding

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.

4.7 Commercial Relationship

4.7.1 Ordering

Services can be ordered by contacting Carrenza with your requirements. A call-off contract will need to be executed under the G-Cloud 9 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.

4.7.2 Use by other suppliers

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

4.7.3 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.

4.7.4 Termination by Customers

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

4.7.5 Service Credits

For AWS this is based on standard AWS terms and conditions: https://aws.amazon.com/agreement/.

4.7.6 Termination by Carrenza

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

4.7.7 Minimum Contract Period

The minimum contract period of the service is one hour, other than for dedication Cloud Foundry where it is one month.

4.8 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 will be priced at £100 or 10% of the customers' AWS spend per month.

4.8.1 Monthly Managed Service

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

5 Google Cloud Platform

The Google Cloud Platform provides 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's Public Sector Hybrid Cloud provides a mechanism for customers to procure Google Cloud Platform services. Procuring these services from Google through Carrenza, in combination with other services provided by Carrenza, 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 Google Cloud Platform services listed on the Google website at https://cloud.google.com/products/
- If Carrenza's server support or server management services are purchased, access to a Service Desk for reporting incidents and Service Requests.

5.1 Support

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

5.2 Data Centre Locations

Google Cloud Platform is located in data centres worldwide and the customer can select where their data is held, although we recommend only using Google's 4 EU based data centres in Ireland, Belgium, Finland, and Netherlands.

5.3 Severity Definitions

Google provides support based on the following definitions and the support plan purchased by the customer: https://support.google.com/work/answer/184028?hl=en.

5.4 Service Constraints

5.4.1 Minimum Infrastructure Requirement

There is no minimum infrastructure requirement when using Google. It is recommended for each customer that Carrenza procure Silver or Gold Support as part of the Google Cloud Platform service. This will be priced from £150 per month.

5.4.2 Maintenance and Planned Outage

All Google maintenance and planned outages are published online at: https://status.cloud.google.com/. It is the responsibility of the customer to review this and check when planned outages are scheduled. Carrenza are not liable should the customer fail to check and lose data as a result.

5.5 On-boarding and Off-boarding processes

5.5.1 On-boarding

For customers using Google they must comply with Google's terms at https://cloud.google.com/terms/.

5.5.2 Off-boarding

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

5.6 Commercial Relationship

5.6.1 Ordering

Services can be ordered by contacting Carrenza with your requirements. A call-off contract will need to be executed under the G-Cloud 9 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 Google portal.

5.6.2 Use by other suppliers

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

5.6.3 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.

5.6.4 Termination by Customers

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

5.6.5 Service Credits

For Google this is based on standard Google terms and conditions: https://cloud.google.com/compute/sla?hl=en.

5.6.6 Termination by Carrenza

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

5.6.7 Minimum Contract Period

The minimum contract period of the service is one hour, other than for dedication Cloud Foundry where it is one month.

5.7 Pricing

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

Current Google Cloud Platform pricing is available at: https://cloud.google.com/pricing/.

The Google Cloud Platform Pricing Calculator is available at: https://cloud.google.com/products/calculator/

5.7.1 Monthly Managed Service

Carrenza also provide a Google Cloud Platform Managed Service, starting at £500 per month. This is a bespoke service designed with the specific needs of each customer, with options ranging from basic support and help using the various Google cloud services to delivering a full hybrid service to support workloads across multiple IaaS environments; i.e. using Google for test and dev and Carrenza for PSN OFFICIAL workloads. Full pricing for this service is available on request and is based on requirements.

6 VMware vCloud Air

VMware vCloud Air is a group of secure cloud service offerings operated by VMware, giving IT organizations a VMware-compatible platform to extend their cloud infrastructure and software deployments seamlessly beyond their data centres.

Carrenza's Public Sector Hybrid Cloud provides a mechanism for customers to procure VMware vCloud Air services. Procuring these services from VMware through Carrenza, in combination with other services provided by Carrenza, 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 vCloud Air services listed on the VMware website at http://www.vmware.com/files/uk/pdf/vcloud-air/vcloud-air-Service-Description.pdf
- If Carrenza's server support or server management services are purchased, access to Carrenza's Service Desk for reporting incidents and Service Requests.

6.1 Support

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

6.2 Data Centre Locations

VMware vCloud is located in data centres worldwide and the customer can select where their data is held, although we recommend only using VMware's Europe based data centres in the UK and Germany.

6.3 Severity Definitions

VMware provides support based on the following definitions and the support plan purchased by the customer: https://www.vmware.com/support/vcloud-air/sla.html

6.4 Service Constraints

6.4.1 Minimum Infrastructure Requirement

There is no minimum infrastructure requirement when using VMware vCloud Air

6.4.2 Maintenance and Planned Outage

All Google maintenance and planned outages are published online at: http://vcloud.vmware.com/uk/using-vcloud-air/support-center/status. It is the responsibility of the customer to review this 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 On-boarding and Off-boarding processes

6.5.1 On-boarding

For customers using vCloud Air they must comply with VMware's terms at http://www.vmware.com/uk/support/vcloud-air/terms-of-service.html

6.5.2 Off-boarding

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

6.6 Commercial Relationship

6.6.1 Ordering

Services can be ordered by contacting Carrenza with your requirements. A call-off contract will need to be executed under the G-Cloud 9 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 VMware vCloud portal.

6.6.2 Use by other suppliers

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

6.6.3 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.

6.6.4 Termination by Customers

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

6.6.5 Service Credits

For vCloud Air this is based on standard VMware vCloud Air terms and conditions: https://www.vmware.com/support/vcloud-air/sla.html

6.6.6 Termination by Carrenza

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

6.6.7 Minimum Contract Period

The minimum contract period of the service is one hour, other than for dedication Cloud Foundry where it is one month.

6.7 Pricing

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

Current VMware vCloud Air pricing is available at: http://vcloud.vmware.com/uk/service-offering/pricing-calculator

6.7.1 Monthly Managed Service

Carrenza also provide a VMware vCloud Air Managed Service, starting at £500 per month. This is a bespoke service designed with the specific needs of each customer, with options ranging from basic support and help using the various VMware vCloud Air services to delivering a full hybrid service to support workloads across multiple IaaS environments, for example using vCloud for test and dev and Carrenza for PSN OFFICIAL workloads. Full pricing for this service is available on request and is based on requirements.

7 Microsoft Azure

Microsoft Azure is a growing collection of integrated cloud services – analytics, computing, database, mobile, networking, storage and web – for moving faster, achieving more and saving money.

Carrenza's Public Sector Hybrid Cloud provides a mechanism for customers to procure Microsoft Azure services. Procuring these services from Microsoft through Carrenza, in combination with other services provided by Carrenza, 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 Microsoft Azure services listed on the Microsoft website at https://azure.microsoft.com/en-gb/support/legal/sla/
- If Carrenza's server support or server management services are purchased, access to Carrenza's Service Desk for reporting incidents and Service Requests.

7.1 Support

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

7.2 Data Centre Locations

Microsoft Azure is located in data centres worldwide and the customer can select where their data is held, although we recommend only using Microsoft's Europe based data centres in Ireland and the Netherlands.

A list of datacentre locations is available here: https://azure.microsoft.com/en-gb/regions/

7.3 Severity Definitions

Microsoft Azure provides support based on the following definitions and the support plan purchased by the customer: https://support.microsoft.com/en-us/gp/azuresevdetails

7.4 Service Constraints

7.4.1 Minimum Infrastructure Requirement

There is no minimum infrastructure requirement when using Microsoft Azure

7.4.2 Maintenance and Planned Outage

All Microsoft Azure maintenance and planned outages are published online at: https://azure.microsoft.com/en-gb/status/. It is the responsibility of the customer to review this and check when planned outages are scheduled. Carrenza are not liable should the customer fail to check and lose data as a result.

7.5 On-boarding and Off-boarding processes

7.5.1 On-boarding

For customers using Microsoft Azure they must comply with Microsoft's terms at https://azure.microsoft.com/en-gb/support/legal/

7.5.2 Off-boarding

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

7.6 Commercial Relationship

7.6.1 Ordering

Services can be ordered by contacting Carrenza with your requirements. A call-off contract will need to be executed under the G-Cloud 9 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 Microsoft Azure portal.

7.6.2 Use by other suppliers

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

7.6.3 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.

7.6.4 Termination by Customers

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

7.6.5 Service Credits

For Microsoft Azure this is based on standard Microsoft Azure terms and conditions: https://azure.microsoft.com/en-gb/support/legal/

7.6.6 Termination by Carrenza

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

7.6.7 Minimum Contract Period

The minimum contract period of the service is one hour, other than for dedication Cloud Foundry where it is one month.

7.7 Pricing

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

Current Microsoft Azure pricing is available at: https://azure.microsoft.com/en-gb/pricing/calculator/

7.7.1 Monthly Managed Service

Carrenza also provide a Microsoft Azure Managed Service, starting at £500 per month. This is a bespoke service designed with the specific needs of each customer, with options ranging from basic support and help using the various Microsoft Azure services to delivering a full hybrid service to support workloads across multiple IaaS environments, for example using Azure for test and dev and Carrenza for PSN OFFICIAL workloads. Full pricing for this service is available on request and is based on requirements.