SERVICE ORDER: Kascade Recover

1 KEY TERMS

EFFECTIVE DATE:	AS SET OUT IN THE QUOTE.
INITIAL TERM:	AS SET OUT IN THE QUOTE.
MILESTONES (IF ANY):	AS SET OUT IN THE QUOTE.
SITE(S):	AS SET OUT IN THE QUOTE.
DELIVERABLES (IF ANY):	AS SET OUT IN THE QUOTE
CHARGES AND PAYMENT TERMS:	AS SET OUT IN THE QUOTE.
CUSTOMER EQUIPMENT (IF ANY):	AS SET OUT IN THE QUOTE.
SUPPLIER EQUIPMENT (IF ANY):	AS SET OUT IN THE QUOTE.
PLAN:	AS SET OUT IN THE QUOTE.

1.1 Kascade is a trading name of Computerworld (Systems) Limited. Throughout this Service Order, references to Kascade shall also include Computerworld (Systems) Limited. Computerworld (Systems) Limited and Kascade are used interchangeably to represent our business and services.

1.2 This Service Order is entered into pursuant to the Quote issued by Kascade (the **Supplier**) to the customer as set out in the Quote (the **Customer**), and the Supplier's terms and conditions contained in the Quote (**Terms**).

1.3 This Service Order is dated on signature of the Quote by both parties.

1.4 The Customer receives Microsoft Azure products and/or services from the Supplier (**Microsoft Azure Services**) and the Customer has entered into a separate agreement with the Supplier for the supply of the Microsoft Azure Services (**Microsoft Azure Agreement**).

1.5 The Supplier will supply the Customer with the disaster recovery service (**Kascade Recover**) as per the terms of this Service Order, the Quote and the Terms.

1.6 Unless the context otherwise requires, or otherwise defined in this Service Order, defined terms in this Service Order shall have the same meaning as the defined terms in the Terms and/or the Quote.

1.7 Save as may be varied by or otherwise set out in this Service Order, Clause 4 to clause 32 of the Terms shall apply mutatis mutandis to this Service Order.

1.8 By accepting the Supplier's Quote, the Customer has agreed to accept and be bound by the terms of this Service Order.

1.9 In the event there is conflict between the Terms and this Service Order, the terms of this Service Order will prevail.

1.10 In the event there is conflict between the Service Order and the Quote, the terms of the Quote will prevail.

Proprietary Internal

2 DEFINITIONS

2.1 The following definitions and rules of interpretation apply in this Service Order:

Annual Service Review	the annual review meeting of the Kascade Recover arranged by the Supplier and held between the parties to ensure the Kascade Recover is providing value for money alongside discussing and addressing any service deficiencies or improvements to the service.
AVD Landing Zone	the Landing Zone that will host the AVD Service when taking out a AZDRAVD.
AVD OS	the Azure virtual Desktop Operating system.
AVD Service	a remote desktop service hosted in Azure for providing a remote workspace for users to interact with their business systems in a secure environment.
AZDRAVD	a AVD Service Plan, which does not require a VPN or a jump box to connect as it utilises the AVD Service.
AZDRVPN	a service Plan which does require a VPN or a jump box to connect as it utilises the VPN.
Bastion	a method of providing secure, remote access available natively within the Microsoft Azure platform.
Customer's Active Directory	the database that contains the on-premise security information for the user identities and access to Microsoft systems, hosted across multiple domain controllers.
Customer DC	Microsoft Active Directory Domain Controller.
Kascade Recover Landing Zone	the Landing Zone that the protected VMs will replicate to.
DR Testing	the replicated workloads protected by the Kascade Recover which will be brought live in a test network so the machines can be accessed as if it were an actual live failover to test the

	environment and ensure it is fully functional in the event of an actual disaster.
Failback	the process of failing a disaster recovery environment back to the original location after issues that caused the Kascade Recover invocation are remediated.
FSMO	flexible single master operation.
Indirect CSP	a Microsoft Azure distributer
Intrusion	any intrusion from any third party, malware, exfiltration of Customer Data, malicious code, intrusion through a firewall or virus or physically implemented virus or attack, Trojan, worm and virus, lock, authorisation key or similar device that impairs or could impair the operation of the Kascade Recover.
Jump Box OS	a single server, built on premise by the Customer and replicated with the other protected workloads, that will be used for remote access when running a Test Failover, should the client take out a AZDRVPN.
Landing Zones	an environment in Azure on which to host workloads which consists of a collection of Azure networks, security policies, logging and access controls.
Live Failover	an unplanned outage at the Customer's primary site that means the business cannot function and the Kascade Recover is invoked so the Customer may work from the Azure location until such time the issue on premise is resolved and they can fail back.
Pack	a license granting the Customer the ability to protect up to 5 VMs using the Kascade Recover, as further detailed in clause **Error! Reference source not found.**, and a Pack will be one of the 8 packs set out in clause 6.13.6.1 and 6.13.6.2.
Plans	Standard Plan and Premium Plan, as defined in section 3.1 below.
PS Rate	the Supplier's professional services rate available on request.

Quote	the unified quote template populated with the Customer's details by the Supplier.
Recovery Playbook	The document detailing the priority order of recovery for each VM covered by the Kascade Recover which details inter VM dependencies as well as the order in which VMs are recovered.
RPO	the recovery point objective, being the amount of data loss incurred when failing over to Kascade Recover.
RTO	the return to operation, being the time it takes after Kascade Recover is invoked for the system to be live and running in the Kascade Recover environment.
Service Review	a meeting arranged by the Supplier and held between the parties to review the Kascade Recover following a Failover Test and Live Failover event.
Test Failover	a test of the Kascade Recover which simulates a live failover event to test the consistency of the Kascade Recover.
VMs	virtual machines.
VPN Premium	The VPN plan involves the use of a VPN for connectivity during a Live Failover event and the use of a Jump Box OS in a Failover Test event.

Proprietary Internal

3 SERVICE OFFERING

3.1 All items in this section refer explicitly to the items set out in the Service Schedule available on request.

Standard Plan	The Supplier will provide support for the following components located in the Kascade Recover subscription, available for the Standard Support Hours: - 1 Failover Test - Support of the DraaS infrastructure - Monitoring and proactive support for replication failures (limited to Azure only as set out in clauses 6.8.2– 6.8.4 below) - Minor changes to the replicated VMs during a term - Unlimited unplanned Live Failovers - Activation of AVD Service in Failover Test or Live Failover event (if applicable) - Activation of Bastion in DR Testing or Live Failover (if applicable) - Addition of new VM's to the Kascade Recover (up to current licensed amount) - Removal of VMs from replication (effective immediately) - Changes to the on-premise VPN end point (Supplier will only update the Azure side of the VPN) - Service Review after each Failover Test or Live Failover event - Annual Service Review - Security and feature updates as required
Premium Plan	The Premium Plan includes the same support as the Standard Plan, with the following additional features: - 2 Failover Tests (in place of 1 Failover Test); and - available for the Premium Support Hours.

4 SUPPORT HOURS

4.1 **Standard Support Hours** (10x5) Monday – Friday (excluding bank holidays) 08:00 – 18:00

4.2 **Premium Support Hours for P0 only (available on the Premium plan only for unplanned failovers)** (24x7) Monday – Sunday (including bank holidays, excluding Christmas day)

5 SERVICE LEVELS

5.1 Support process

5.1.1 The Supplier offers two methods of contacting the Supplier's support team – via telephone or email to the following details:

Telephone	0344 833 0601
Email	support@Kascade.co.uk

5.2 Support Service Incident Priority & Response Times

5.2.1 Incident priorities will be recorded as a ticket by the Customer at the time of logging a case, which shall be revised by the Supplier's support team (Tickets).

5.2.2 If the Customer is not satisfied with a revised priority of a Ticket, then this will be a matter for negotiation and escalation as required.

5.2.3 Supplier will use reasonable endeavours to ensure that 98% of Tickets are triaged and prioritised within 1 hour of receipt. If the Supplier fails to comply with this obligation on 3 occasions during a calendar month, the Customer shall have the right to terminate this Service Order under clause 14.1.2 of the Terms if the termination notice is received by the Supplier before the end of the following calendar month.

5.2.4 The Supplier will use reasonable endeavours to ensure that 98% of Tickets are resolved within the timeframes according to the Incident Priority table below. If, during a calendar month, the Supplier fails to resolve 3 P1 and/or P2 Tickets within the timeframes according to the Incident Priority table below, the Customer shall have the right to terminate this Service Order under clause 14.1.2 of the Terms, if such termination notice is received by the Supplier before the end of the following calendar month.

5.2.5 Where Tickets are awaiting third party input, are being monitored to see if the fix is working, or waiting for a client response, this will pause the resolution time until such time as an appropriate response is received.

5.3 Support Service Incident Priority & Response Times

5.3.1 Incident priorities will be recorded by the Supplier at the time of logging a case according to the severity of the request.

5.3.2 The Incident Priority table below summarises the fix time SLA

Incident Priority	Description of Priority and Timeframe	Service Level
P0	Critical Priority: Invocation of DR due to an unplanned event.	1 Business Hour
P1	High Priority: Critical system failure, or Replication ceased.	4 Business Hours
P2	Medium Priority: Minor issue affecting non-critical functionality, RTO/ RPO is impacted, but Failover is possible.	1 Business Day
P3	Low Priority: Change requests to service such as Adding or removing VM's from the service.	3 Business Days
P4	General maintenance: Upgrades and security patching.	5 Business Days

5.4 Incident escalation

5.4.1 Incidents are managed by the Supplier through the IT Service Management solution. Incidents that move outside SLA are automatically escalated to the relevant Service Desk Manager.

5.4.2 SLA performance is reviewed as part of the Annual Service Review, or on an add hoc basis should a valid need arise, by the Service Delivery Manager.

6 ADDITIONAL TERMS

6.1 The following additional terms apply to the provision of the Kascade Recover.

6.2 Costs

6.2.1 There will be additional Azure costs incurred by the Customer for the hosted element of the Kascade Recover. The Supplier reserves the right to increase these costs when the Customer invokes DR for Testing or Live Failover purposes.

6.2.2 These will be billed under a separate consumption invoice as per the terms of the Microsoft Azure Agreement.

6.3 Microsoft Azure Services

6.3.1 The Microsoft Azure Services providing the Kascade Recover, And AVD Landing Zones, must be provided by the Supplier for the Term of the Service Order.

6.3.2 Cancelling, deleting, moving or altering the Microsoft Azure Services or the Kascade Recover subscription in any way will constitute a material breach of this Service Order by the Customer.

6.3.3 The Customer agrees to have the Kascade Recover subscription joint owned and managed by the Customer, Supplier and Indirect CSP provider.

6.3.4 The Customer agrees to be added to and managed by the Suppliers native management platforms.

6.4 Cancellation

6.4.1 Cancellation of this Service Order does not constitute a cancellation of the Microsoft Azure Agreement.

6.5 Support

6.5.1 Monitoring and proactive support is limited to service failures hosted on the Kascade Recover and Microsoft Azure Services.

6.5.2 The Customer is responsible for:

6.5.2.1 any on premise replication elements and any issues affecting or likely to affect the Kascade Recover due to the on-premise infrastructure must be immediately reported to the Supplier on discovery; and

6.5.2.2 all connectivity issues into the Kascade Recover environment and any issues affecting or likely to affect the Kascade Recover must be immediately reported to the Supplier on discovery.

6.5.3 If the Customer fails to immediately report and address known issues with replication to the Supplier on discovery, this will constitute a material breach of the A Service Order by the Customer.

6.5.4 Post deployment issues with replication will be proactively reported to the Customer by the Supplier as relevant.

6.5.5 Customer must grant the Supplier access to the on-premise environment in order for the Supplier to remediate issues with the on-premise replication elements, or to upgrade. Failure to comply with this obligation is a material breach of this Service Order by the Customer.

6.6 Landing Zones and other components

6.6.1 Supplier will implement Landing Zones and associated Kascade Recover components, including AVD (if required) to a comprehensive secure best practice.

6.6.2 Supplier is not responsible for, and has no liability in respect of, any Intrusion relating to the Service.

6.6.3 Remediation of issues due to any Intrusion will be charged at additional cost as per the Supplier's prevailing PS Rates.

6.7 AZDRAVD Plan

6.7.1 Supplier will remediate issues with the AVD Service only.

6.7.2 Where the Customer has a AZDRAVD plan, the Customer is responsible for keeping the AVD OS and applications up to date as per their business requirements.

Proprietary Internal

6.7.3 Where the Customer has a AZDRVPN plan, the Customer is responsible for keeping the Jump Box OS and applications up to date as per their business requirements.

6.7.4 It is also the Customer's responsibility to ensure all relevant Customers are connected to the DR environment via an Azure VPN.

6.7.5 Failure to comply with clauses 6.7.2, 6.7.3 and 6.7.4 will constitute a material breach of this Service Order and will allow the Supplier to suspend the Customer's access to the Kascade Recover.

6.8 Azure VPN

6.8.1 It is the Customer's responsibility to deploy and to ensure that each client device has a functioning Azure VPN connection to the Kascade Recover Landing Zone.

6.8.2 Issues should first be investigated by the Customer. If the Customer is unable to fix an issue with the connection of the VPN to the Kascade Recover Landing Zone, the Customer can report this to the Supplier and the Supplier will use reasonable assistance to investigate and remedy the issue where possible.

6.8.3 Supplier will only fix VPN issues which have originated from the Azure side.

6.8.4 If Azure VPN is proven working by a Customer successfully connecting to the Kascade Recover Landing Zone this will constitute the service working and any further issues will be referred back to the Customer for remediation.

6.9 Software licence and system updates

6.9.1 The Customer shall be responsible for ensuring that all software is correctly licensed and that all software and hardware that is listed in the Service Schedule is currently supported by the Kascade Recover.

6.9.2 The Customer is responsible for updating its systems to be compliant with the Kascade Recover as may be required from time to time.

6.9.3 Supplier will update the Microsoft Azure Services and on premise Kascade Recover components as required from time to time, which may be comprised of security, feature or stability updates.

6.9.4 Kascade will schedule the updates with the Customer to ensure minimal interruption to the Kascade Recover.

Proprietary Internal

6.10 DR Testing

6.10.1 A Customer DC (where present) must be included in the Kascade Recover for DR Testing to be successful.

6.10.2 If FSMO roles are distributed amongst several Customer DCs then all of those Customer DCs must be included.

6.10.3 Any changes to the Customer's Active Directory structure must be immediately reported to the Supplier.

6.10.4 Failure to identify changes to the Supplier, or failure to act on the Supplier's remediation requirements, constitutes a material breach of this Service Order by the Customer.

6.10.5 A Customer DC must also be held permanently live in the Kascade Recover Landing Zone which does not require the provision of any special roles by the Supplier.

6.11 Failback/Failover

6.11.1 Failback to production from the Azure instance is not covered in either Standard nor Premium Plans.

6.11.2 Failback services can be provided but at additional cost as per the Supplier's prevailing PS Rates.

6.11.3 The Customer is responsible for all OS and application remediation prior, during or following a Failover event, be that planned or unplanned.

6.11.4 Supplier will submit a report showing the success of the failover and recovery times (RPO and RTO) after the initial Failover test as part of onboarding as well as every subsequent failover test. This will constitute the validity of the platform until the next Failover test.

6.11.5 Should RTO/ RPO not be met, Supplier will provide the Customer with reasonable assistance to identify the root cause and where possible will re-perform the test where the fault lies with the Kascade Recover.

6.11.6 A Failover, whether Test or Live, can only be authorised by named contacts within the client and the supply of an agreed password. The named contacts

Proprietary Internal

and the password will be agreed and recorded during service onboarding and can subsequently be changed by the client upon written request.

6.11.7 For all Plans, Supplier will perform a Failover Test after initial seeding has taken place and during each other testing window as part of the Kascade Recover. Each additional Failover Test will be performed as per the below;

for the Standard Plan,1 test per year - test will be performed 6 months following the initial Failover Test (10x5) and then every 12 months for as long as the Service Order is renewed;

for Standard Plan, the unlimited unplanned Live Failover (10x5);

for the Premium Plan,1 test per year - test will be performed 6 months following the initial Failover Test (10x5) and then every 6 months for as long as the Service Order is renewed;

for the Premium Plan, unlimited unplanned Live Failover (24x7).

6.12 Recovery Playbook

6.12.1 The Customer is responsible to define and keep the Supplier updated with any changes to the Recovery Playbook.

6.12.2 The Supplier will invoke the Kascade Recover on request, by the order specified in the Recovery Playbook.

6.13 Billing

6.13.1 The Customer may increase the number of VMs protected by the Kascade Recover at any point during the Initial Term (or any subsequent Term) of the Service Order by purchasing an additional Pack.

6.13.2 Each pack including the base pack provides coverage for up to 5 VMs.

6.13.3 The Customer may not reduce the number of Packs below the initial amount as set out in the Quote for the duration of the Term.

6.13.4 The Customer may, on giving the Supplier one months' written notice prior to the end of the relevant Term, request to reduce the number of Packs in use for any agreed Successive Term.

6.13.5 The Customer must ensure they purchase a sufficient amount of Packs to cover the number of VMs protected by the Kascade Recover.

6.13.6 A Customer must buy a Base Pack and then Expansion Packs as required. Details of these Packs are set out as follows:

6.13.6.1 Base Packs: This covers the Kascade Recover Landing Zone components, Azure Site Recovery service and replication of 5 VMs to Azure:

Base SKU	Service
CWC_AZDRAVD_S5B	Standard – AVD Base Pack
CWC_AZDRVPN_S5B	Standard – VPN Base Pack
CWC_AZDRAVD_P5B	Premium – AVD Base Pack
CWC_AZDRVPN_P5B	Premium – VPN base Pack

6.13.6.2 Expansion Packs: covers up to 5 additional VMs for replication:

VM Packs	Service
CWC_AZDRAVD_S5E	Standard – AVD Expansion Pack
CWC_AZDRVPN_S5E	Standard – VPN Expansion Pack
CWC_AZDRAVD_P5E	Premium - AVD Expansion Pack
CWC_AZDRVPN_P5E	Premium - VPN Expansion Pack

6.13.7 Customer may not mix and match Premium Packs and Standard Packs and may not mix and match AZDRVPN and AZDRAVD Packs.

6.13.8 Supplier reserves the right to apply additional Packs to the order should it be discovered the Customer has added additional VMs to the Kascade Recover Landing Zone without informing the Supplier.

6.14 Description of Personal Data Processing

6.14.1 The data processing activities carried out by Supplier are described as follows:

6.14.1.1 Subject matter

Proprietary Internal

For the purposes of providing the Kascade Recover to the Customer.

6.14.1.2 Duration

The Term of the Agreement until the deletion of the personal data in accordance with the Agreement.

6.14.1.3 Nature and purpose

For the purposes of providing the Kascade Recover to the Customer.

6.14.1.4 Data categories

The categories of personal data which are provided by the Customer to the Supplier for the Kascade Recover.

6.14.1.5 Data subjects

The personal data of the Customers' employees and/or authorised users which is provided to the Supplier for the Kascade Recover.

6.14.2 In accordance with clause 2.6 and clause 2.9 of Schedule 1 of the Terms, the Customer consents to the appointment of Binary Fortress Software as a Data Controller. Any personal data processed by Binary Fortress Software will be processed in accordance with Binary Fortress Software's privacy policy (https://www.checkcentral.cc/Privacy/).

Proprietary Internal

7 SERVICE ENHANCEMENTS

7.1.1 The following additional extras can be purchased from time to time by the Customer to assist with other elements of DR or to have additional testing.

7.1.2 All elements are on a time and material basis only and the Supplier does not guarantee either a fix nor workaround for any issue remediation.

7.1.3 Subject to engineering availability, the Supplier will use its best endeavors to provide additional support during a Live Failover event.

Service	Sell	Unit
Support with OS troubleshooting during failover tests 10x5	£200	Per Hour
Support with application troubleshooting during failover tests 10x5	£200	Per Hour
Additional Live Failover test – business hours	£1200	Per Test
Planned DR invocation and Failback – business hours	POA	Project scoped at Kascade prevailing PS Rate
Planned DR innovation and failback – out of hours	POA	Project scoped at Kascade prevailing PS Rate
Unplanned DR Failback consultancy	POA	Project scoped at Kascade prevailing PS Rate