

1. Service Overview

We offer Disaster Recovery as a Service (DRaaS) as a self-service product which replicates your data and offers committed recovery times when your production system is not accessible. DRaaS is a platform only service. You can purchase our DR Management Service separately if you require us to monitor and manage replication of data from your production system into our Disaster Recovery platform.

DRaaS can be delivered on the following destination platforms:

- (a) Enterprise Cloud;
- (b) Public Sector Cloud;
- (c) Microsoft Azure; and
- (d) Dedicated Infrastructure.

Additional information may be included in your Order Form or Statement of Work.

2. Service Features

We offer two resource pool options:

- (a) Virtual infrastructure:
 - (i) Enterprise Cloud and Public Sector Cloud: We will deliver all vCPU and vRAM resources from our shared DR compute platform, which has N+1 resiliency in the event of host failure;
 - (ii) Microsoft Azure: Azure DR will mirror what is in your production area in your chosen Azure data centre.
- (b) Dedicated infrastructure:

We deliver compute resources using one or more blade servers that are dedicated to you and we deliver storage resources from our shared storage array. The dedicated resource pool is provided without N+1 resiliency. The storage is delivered from an enterprise-grade SAN with built-in high availability connected to an N+N storage fabric.

You can select both virtual and dedicated components to meet your workload performance needs.

Both Virtual and Dedicated Infrastructure include the features listed in the table below. Optional items are available for an additional Fee. Your selected resource pool option and optional features will be specified in your SoW.



Feature	Included	Optional
DR Platform Administration and DRaaS Software	•	
Replication and Recovery	•	
Protection and Platform Support	•	
DR managed service ¹		•
Standard Retention (four (4) Hours)	•	
Upgraded Retention (forty-eight (48) Hours)		•

2.2 DR Platform Administration and DRaaS Software

(a) DR Platform

(i) Enterprise and Public Sector Cloud

The DRaaS service is a target platform managed by us providing reserved virtual or dedicated compute and storage resources for you.

(ii) Microsoft Azure

The DRaaS service is a target platform managed by Microsoft.

(b) DRaaS Software

We will select and deliver the DRaaS software depending on the target platform that you choose.

The DR software provided includes the following functionality:

- (i) Support for Windows and Linux applications.
- (ii) Management tools to test and automate failover; and
- (iii) Management tools to provide grouping, templating, and cloning.

For source environments outside our Cloud platforms, you must have sufficient capacity to deploy the DR software within your platform.

Where the source DR environment resides outside our platforms, we will provide the DR software and assist with deployment and configuration on both our platform and/or the platform residing outside of our platforms as part of the onboarding process.

¹ Please refer to our DR Management Service Description.



2.3 Replication and Recovery

We offer multiple DR target sites which will be selected by you after the point of order. The DR software will replicate your data to the target DR site and you will be able to recover such data by ATOT or ATOD.

Our expected RTO's and TPO's are as follows:

- (a) The expected RTO for a full DR recovery is from four (4) hours;
- (b) The RPO achieved will be subject to the bandwidth available between the source and target sites, typically this can be from fifteen (15) minutes.

Please note that these time indications depend on network bandwidth and change rates and are therefore not guaranteed.

We use replication connectivity to replicate data from the source to target (DR platform) for your protected systems. ATOT and ATOD failover connectivity allows users to connect to the target environment upon failover of the protected systems.

The target DRaaS platform requires connectivity between your system and ours. This connectivity may be achieved using:

- (c) Dedicated Internet Access;
- (d) Managed WAN; or
- (e) Virtual Point-to-Point.

Connectivity to the DR platform is your responsibility. Unless you purchase the relevant connectivity service from us, we are not responsible for any issues that arise from or are related to connectivity.

2.4 Protection and Platform Support

We provide reactive support based on our standard operating model for the DRaaS platform defined in this Service Description and you must log any requests following our standard incident logging procedure defined in our Operations Manual.

2.5 DR Managed Service

We offer an additional fully managed DR service, which is optional and chargeable, as detailed in our DR Management Service Description.

2.6 Retention

The standard retention period is four (4) hours. You can upgrade your service to an optional forty-eight (48) hour retention period for an additional Fee, details of which will be included in your SoW. Please note that a longer retention period requires more storage capacity, which will be reflected in your charges.



2.7 Break and Fix Support

We provide proactive support only for the DR infrastructure we monitor and manage, which includes:

- (a) Physical infrastructure;
- (b) Virtualisation layer; and
- (c) Reserved resource availability.

Alerts generated on these monitored services will be raised as Priority 2 level incidents and managed in accordance with our Operations Manual. An automated alert will be sent to your nominated email address.

Incidents alerted will be resolved without notifying you unless our assigned engineer deems that the incident will affect your ability to operate the Service or the incident is re-classified as a Priority 1.

During triage, the incident Priority may be adjusted based on the incident classification as per our Operations Manual.

If you require support outside of what is defined in this Service Description, we will assist you in accordance with our standard support operating procedures as defined in our Operations Manual. Please note that if support is not requested according to our standard escalation procedures, there might be delays in response and resolution times.

Please note that replication and data monitoring is excluded from the scope of this Service. If you require us to perform this activity, please refer to our DR Management Service Description.

3. Service Specific Deliverables

3.1 Enterprise and Public Sector Cloud DR

DR infrastructure resource consumption will only be increased when you order additional resources from us.

We will guarantee the availability of the contracted reserve resources (vCPU, vRAM and storage) on your DR target environment.

3.2 Microsoft Azure DR

To guarantee the availability of your Azure DR resources, you will have to purchase this service in addition to your standard DR resources as part of the Azure DR requirements.

The relevant SLAs are as defined by Microsoft in the applicable Azure DR standard terms and conditions.



4. Service Implementation

4.1 On-Premise

Service Implementation	Us	You
We send you our Welcome Pack and Technical Data Capture form.	•	
You complete and return the Technical Data Capture form to us.		•
We place orders for network connectivity (if you procured connectivity from us).	•	
We confirm projected Ready for Service Date with you.	•	
You provide virtual server resources at source to deploy DR software for Client Host(s).		•
We prepare replication storage and compute platform at target site.	•	
We implement/configure replication and failover network connectivity.	•	
We run internal acceptance tests to confirm the DR environment is ready for you.	•	
We facilitate a training call on using the DRaaS software and admin portal including defining initial protection groups, RPOs and IP addressing schema.	•	
We deliver DRaaS licences and provide technical support.	•	
We demo and test connectivity between DRaaS Client Hosts and DRaaS target platform for one protected server.	•	
We install and undertake initial replication, seeding and testing for the remainder of the servers to be protected.	•	
We configure replication and failover properties for all protected servers.	•	
We provide remote technical support during installation (e.g. using desktop sharing).	•	
We ensure data seeding between source and target are synchronised.	•	
We perform acceptance test (including failover activity) and highlight any issues found.	•	
We work to resolve highlighted issues (may involve working with third-party vendors).	•	
You move to steady-state upon successful replication seeding and failover process.		•

4.2 Cloud Platform

Service Implementation	Us	You
We send you our Welcome Pack and Technical Data Capture form.	•	
You complete and return the Technical Data Capture form to us.		•
We prepare replication storage and compute platform at target site.	•	



Service Implementation	Us	You
We implement/configure replication and failover network connectivity.	•	
We configure initial replication, seeding and testing for all servers to be protected.	•	
We configure replication and failover properties for all protected servers.	•	
We ensure data seeding between source and target are synchronised.	•	
We perform acceptance test (including failover activity) and highlight any issues found.	•	
We work to resolve highlighted issues (may involve working with third-party vendors).	•	
You move to steady-state upon successful replication seeding and failover process.		•

All implementation work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA).

4.3 Ready for Service

The Ready for Service Date is the date when we (acting reasonably and properly) notify you that the implementation steps are complete and that the Service is ready for service. This date may be specified to occur at a later date, if mutually agreed to be so. If you consider that the Service is not ready for service on the date notified, you must notify us within two (2) weeks of our notification, after which the Ready for Service date will be deemed to have occurred regardless of issues or defects of which you may later become aware and notify us about (which will then be dealt with as faults or service issues but will not change the Ready for Service Date).

5. Billing

The Service will be billed as Recurring Fees and Set-up Fees as described in the Billing Guide, using the definition of the Ready for Service Date in Section 4.3 of this Service Description and as indicated in your Order Form.

If you have procured DR for Azure, we will charge you an additional Fee of the Set-up of the infrastructure required for the DR to work. Details of such Fee will be included in your Order Form and/or SoW.

5.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

- (a) Implementation work carried out outside Business Hours; and
- (b) Any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA).



6. Service Operations

5.1 DRaaS Platform Administration

Our Service Operations will be initiated on the Ready for Service date. The key administration activities are listed below.

Enterprise and Public Sector Cloud DRaaS Platform administration:

- (a) We maintain and monitor DRaaS, including storage;
- (b) We maintain, monitor and upgrade DRaaS software; and
- (c) We troubleshoot and resolve DRaaS platform issues.

Azure Platform administration:

- (d) We maintain and monitor the ASR agent ensuring it is up-to-date; and
- (e) We troubleshoot and resolve DRaaS platform issues.

7. Dependencies

We provide DRaaS subject to the following dependencies:

7.1 Client Obligations

- (a) You will either procure network connectivity from source to target from us or provide it in the form of standard internet or dedicated connection;
- (b) You will designate a project lead and technical contacts with the appropriate level of expertise to support the successful implementation and operation of the Service;
- (c) You will provide us all information and configuration details necessary to onboard the Service;
- (d) You will manage any activity involving your third-parties as necessary during Service Implementation and Service Operations;
- (e) You will ensure there is sufficient bandwidth capacity for the data to be replicated and end-user connectivity to failover target ATOT and ATOD;
- (f) You will provide the VM client host in order to enable us to deploy the agentless DR software at the source site;
- (g) For a VMware source platform, you must deploy a VMware vCenter Server within the source environment;
- (h) For a Hyper-V source platform, you must deploy the Hyper-V System Center Virtual Machine Manager within the source environment;



- (i) The initial replication (a.k.a. seeding) must be completed by us for the protected systems before an ATOT or ATOD failover can be initiated; and
- (j) If you are unsure about the supported data sources, it is your responsibility to request from us and review a copy of the full list of capabilities for Windows and Linux workloads or the resource requirements for the agentless software/proxy on your host at the source site. You must review these additional documents in conjunction with this Service Description.

7.2 Service Dependencies

- (a) The RPO capability will only be available after the initial seeding of the replication data is completed. It is also dependent on the network bandwidth in place;
- (b) The RTO is dependent on the recovery plan boot order priorities, which are in sequential order (e.g. priority 2 systems will not start the booting process until priority 1 is completed);
- (c) Any additional VMs outside of the contractual agreement will not be protected unless you specifically request so and it is agreed with us.

8. Exclusions

The excluded items described below are outside the scope of this Service Description:

- (a) DRaaS is not a backup service. It is not designed to provide medium or long-term retention and it will not have any granular level restore (e.g. file or folder). If you require a retention solution, please contact us to discuss our Backup as a Service offering.
- (b) DR Management is not included in this Service. DR Management is sold as a separate service for an additional Fee and is described in DR Management Service Description.

9. Definitions and Acronyms

9.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client. The terms listed have the following meanings:

Term	Meaning
ASR	Azure Site Recovery
Compute	A combination of vCPU and vRAM resources.
GiB	Defined as 1,024MiB.
Initial Seeding	The initial synchronisation of data from the source platform into the target DR platform.
N+1 Resiliency	N+1 redundancy is a form of resilience that ensures system availability in the event of component failure.
N+N	For N + N if 4, 2 will be used, and 2 will be standby (for redundancy).



Storage	Non-volatile media for storing files, databases, applications or virtual servers.
TiB	Defined as 1,024GiB.
vCPU	One or more virtual central processing unit(s) (CPUs) compatible with Intel x86 instruction sets.
Virtualisation Host	A physical host server running server virtualisation software.
vRAM	Virtual random-access memory used for real-time processing.

9.2 Acronyms

Acronym	Meaning
ATOD	At Time of Disaster
ATOT	At Time of Test
DR	Disaster Recovery
OPEX	Operating Expenses
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Storage Area Network
vCPU	Virtual central processing unit
VM	Virtual Machine
VPG	Virtual Protection Group
VRA	Virtual Replication Appliance
vRAM	Virtual random-access memory



10. Operational Targets

We are not responsible for any hardware, software or bandwidth limitations impeding the resolution of the problems.

Type 2	P1	P2	P3	P4
Response	30 mins	30 mins	1 hour	Next Business Day
Fix	4 hours	8 hours	16 hours	3 Business Days
Hours of Support	24x7	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days
Description	A problem in the system being replicated via the service that meets two (2) or more of the following conditions: - It results in the substantial degradation of performance, the loss of data, access to the target DR platform or any other materially adverse effect to the source machine or the replication process; - There is concrete and convincing evidence that our Service is the reason for such problem; - There is no simple workaround, such as the removal of our agent/software that can return the source machine to a normally functioning state.	A problem that meets all the following conditions: - It is not a P1 problem; - It prevents the replication of, or the creation of a replica of, a source machine that should be supported according to the service specification; and - There is no simple workaround that can enable the replication of, and/or the creation of a replica of, the source machine.	A problem that meets all the following conditions: - It is not a P1 or P2 problem; - The target DR platform is accessible and available; - It does not prevent replications; - It does present issues in replication RPO, RTO or retentions due to configuration on the client or server side or changes in the scope environment.	- Service requests; - Non-service affecting work and reports; - A required change or configuration alteration to a service or a technical query.

11. Service Levels and Service Credits

The Service will be delivered at the target level set out below for the percentage level described, against which service credits will be paid (as set out in our Billing Guide).

Service	Measurement	Period	Target	Service Level	Service Credit
DRaaS Availability	Positive TCP port open response on port 902	Calendar Month	99.99%	99.98% - 99.5% 99.49% - 99.0% 98.99 – 98.0% 97.99 – 96.0% Less than 96.0%	5% of monthly value of Recurring Fees 10% of monthly value of Recurring Fees 15% of monthly value of Recurring Fees 20% of monthly value of Recurring Fees 25% of monthly value of Recurring Fees



12. Service Continuity

In the event of a failure, Six Degrees provides the following targets to ensure service continuity. There are no Service Credits applied for the targets for these items.

Service	Measurement	Period
RPO (Recovery Point Objective) average	Per Calendar month	Average < 15 Minutes
RTO (Recovery Time Objective) from point of invocation	Per event	< 4 Hours