Service Description

Managed Disaster Recovery
August 2025

transparity

Contents

1. Service Overview

The Managed Disaster Recovery service provides proactive monitoring of your disaster recovery services within Azure, along with testing of your disaster recovery plan.

2. Service Features

The following is a high-level overview of the functionality available within this service:

KEY:

● Inclusive as part of the standard service offering

◒ Inclusive and as standard when you have purchased the relevant service or if you have requested service(s) that have been documented in your SoW.

○ Available as an optional upgrade for an additional fee.

Feature	Advanced
Proactive Monitoring of Disaster Recovery Services	●
Disaster Recovery Testing	●
Disaster Recovery Playbook Management	●
Service Management	●

2.1 Proactive Monitoring of Disaster Recovery Services

As part of this service, we provide proactive monitoring for disaster recovery services using our monitoring platform.

We will monitor your disaster recovery based on best-practice and our expertise.

Full details of the services monitored are available on request.

2.2 Disaster Recovery Testing

On a bi-annual basis, but no sooner than six (6) months from the Service Commencement Date, we will perform a DR test in conjunction with you at a time and date agreed by both parties. This DR test will follow the DR playbook created for you and we will schedule these DR test(s) with you at a mutually agreed time, but they will only take place two (2) times within a twelve (12) month period.

During the DR test we will record the time each step in the DR playbook takes to complete, issues encountered, remediation necessary to address issues, and any follow-on actions. Following the test we will produce a summary report and share it with you.

2.3 Disaster Recovery Playbook Management

As part of onboarding, after items marked as amber and red in the DR review report have been resolved, or accepted by both parties, we will construct the DR playbook. The DR playbook is a document that identifies: -

- The RPO and RTO for the Disaster Recovery solution,
- Who needs to be involved in each action (from both our and your perspective),
- The definition of a successful recovery, and
- Nominated Contacts from us and you who will sign off on the status of a DR test.

2.4 Service Management Reports

Name	Description	Frequency
DR Test Report	A report summarising a DR test and follow-on actions.	Bi-annual
Service Report	A summary of the service and review of any outstanding activities.	Quarterly

3. Service Operations

Please refer to our Operations Manual for further information on incident management, requests for change and information requests.

4. Billing

4.1 Additional Charges

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

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

5. Dependencies

We will provide the service subject to the following dependencies:

- An existing documented disaster recovery solution and the associated runbooks are in place,
- If an existing disaster recovery solution is not in place a professional services engagement will be required to set up this Service will be subject to separate Statements of Work and Charges.

5.1 Customer Obligations

- Be responsible and accountable for the compliance status of the in-scope cloud environment(s) and all resources they contain.
- Provide named contacts who will be:
  - authorised to submit requests on behalf of your company (“Nominated Contacts”). They will be the designated people with whom all contact is made regarding all requests, and
  - the recipients of service reports and participate in the quarterly service reviews with us.
- Upon request, provide the required information and make available the staff necessary to complete the DR playbook.
- Upon request, provide the required information and make available the staff necessary to maintain the DR playbook.
- Inform your SDM with immediate effect of any changes to the DR solution or personnel identified in the DR playbook as a DR test action owner.
- Inform your SDM with immediate effect of any changes to the DR solution or its management that might have an effect on either the RPO or the RTO.
- Make available the relevant personnel identified in the DR playbook as necessary to perform a DR test using the DR playbook.

- Provide us with:
  - Credentials deemed necessary to carry out our actions during a DR test using the DR playbook.
- Work with us to resolve any issues that arise during a scheduled DR test.
- In the event of any damage or malfunction caused directly by your actions or negligence, you shall be responsible for all necessary repairs or corrections.
- It is your responsibility to comply with your data sovereignty controls, policies and procedures.

5.2 Service Restrictions

- We will provide and support the Service on a reasonable endeavours basis only and will not be subject to any availability targets, if:
  - the OS residing on your VM resources is out of vendor support, or
  - no support contract with the OS provider is in place, or
  - the Supported Public Cloud Environment and or resources are configured in direct contravention of the requirements, best practices, or specific guidelines for support.
- When a ticket is opened with a Public Cloud Vendor the Transparity SLA is paused until a response is received from the respective Public Cloud Vendor

6. Exclusions

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

- DR tests that don't use the DR playbook.
- Recovery during a DR test of any technology, or configuration not documented in the DR playbook.
- We are not responsible for managing or maintaining the security posture for your Cloud Platform(s). If you would like these service(s), for an additional cost they can be procured. Your Account Manager can provide further details.
- We are not responsible for any Public Cloud Platform consumption or licensing costs on an ongoing basis, including those incurred as part of Service Requests in relation to this Service (the Managed Disaster Recovery Service).
- We are not responsible for the support or management of your backup solution, unless provided by another of our Services that you enter into a contractual agreement with us.
- Follow on actions that are identified during or after a DR test unless those actions can be carried out using Service Request from the Service Request Catalogue as part of and when provided by the Azure Managed Service.
- Follow on actions from the DR review that are identified as red or amber status unless those actions can be carried out using Service Requests as part of and when provided by the Azure Managed Service.

6.1 Third Party Related

- Managing incident maintenance for:
  - 3rd party systems,
  - Software, and/or
  - SaaS services
- Specifically, if the above items are not covered by a third party's warranty, support agreement, or terms of use.
- We do not support any service(s) purchased from a Public Cloud Vendor marketplace.
- We do not guarantee the availability, capacity, or performance of the Supported Public Cloud Platform;
- We do not monitor, support, or assure the integrity, functionality, or availability of pipelines, code, applications, or any other processes within your Supported Public Cloud Platform.

- Any software or data deployed, installed, consumed, developed, operated, or generated in the Supported Public Cloud Platform is excluded from this Service;
- Microsoft Entra ID (formerly known as Azure Active Directory) or Microsoft Windows Active Directory either in your Supported Public Cloud Platform or any other location is excluded from this Service;
- Updates to client devices and software are out of scope unless otherwise agreed;
- Certificate management is limited to server endpoints and platform services. Certificate renewals or management on end user devices is not in scope.

7. Definitions and Acronyms

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

7.1 Terms

The terms listed have the following meanings:

Term	Meaning
Statement of Work	This means a document that defines project-specific or Customer-specific activities, deliverables, and/or timelines for providing services to that Customer.

7.2 Acronyms

Acronym	Meaning
CSP	Cloud Solution provider
GDAP	Granular Delegated Access Permissions
OS	Operating System
PAL	Partner Admin Link
PaaS	Platform as a Service
SLA	Service Level Agreement
SSL	Secure Sockets Layer
SoW	Statement of Work
VM	Virtual Machine
VPN	Virtual Private Network
WAR	Well Architected Review

8. Service Level Agreement and Operational Targets

8.1 24*7 Incident Response

	P1	P2	P3	P4
Hours of Support	24*7 Monday – Sunday	24*7 Monday – Sunday	08:00-18:00 Monday – Friday	08:00-18:00 Monday - Friday
Response	15 mins	Four (4) hours	Eight (8) hours	Twelve (12) hours

8.2 Incident Prioritisation

Priority	Severity	Description
P1	Critical	**Business service outage** • System/Service/Application down or unhealthy. Extremely urgent • Very high impact in all business areas, extreme impact on multiple users and disruption is excessive, such as Cloud platform failures, Virtual Machine failures and Cloud networking or connectivity failure • Business critical - work cannot continue
P2	High	**Business service impaired** • High impact on significant business areas or specific users • Individual user cannot complete high priority/business-critical work, or department or group of users unable to continue with routine work • Business-critical work is impaired
P3	Medium	**Group of users affected** • Platform or application problem – user or group priority work cannot be completed • A group of users are experiencing system or business application
P4	Low	**One (1) person affected or minor service fault** • Minor system or application error • Backup or Patching Failure • An individual user is experiencing system or business application problems but is still able to work
P5	Routine	**Non-urgent investigations** • General advice and guidance or agreed scheduled activity