Service Description

Azure Managed Service Advanced
June 2025

transparity

Contents

1. Service Overview

The Azure Managed Service Advanced includes support, monitoring and a range of proactive services for Microsoft Azure based solutions.

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
24*7 Incident Response	●
Proactive Monitoring	●
Well Architected Reviews	●
Azure Virtual Machine Patching	●
SSL Monitoring and Management	●
Backup Management	●
FinOps Recommendations	●
Customer Success Architect	●
Service Requests	●
Service Management	●

2.1 24*7 Incident Response

For Incidents within your Microsoft Azure environment we will provide 24*7 incident response, if the Incident relates to the services provided by Microsoft, we will escalate to Microsoft.

We will follow the Target Response as defined in section 8.1 of this service description.

2.2 Proactive Monitoring

As part of this service we provide proactive monitoring for Azure services using our monitoring platform.

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

Full details of the services monitored are available on request.

2.3 Well-Architected Reviews

We will provide two (2) Well Architected Reviews (WAR) per year. Each WAR will review the public cloud infrastructure that supports one (1) specific application.

Your Service Delivery Manager will present any recommendations from the WAR to you during your monthly service review.

2.4 Azure Virtual Machine Patching

We will configure Azure Update Manager for automated patching of Virtual Machines within your environment.

Patching will be configured monthly based on a schedule agreed with you, the service includes operating system critical, security, definition and service pack updates. Operating system version updates beyond minor release or in cycle updates are not included.

Supporting Operating Systems
Microsoft Windows Server
Red Hat Enterprise Linux

2.5 SSL Monitoring and Management

We will configure proactive monitoring of SSL certificates on virtual machines and PaaS services within your Azure tenant. Where certificates are provided by us we will manage and update the SSL certificates.

Where SSL certificates are provided by you we will alert you of the upcoming SSL certificate expiration date.

2.6 Backup Management

We will configure and monitor backups within for your Azure Virtual Machines and PaaS services. Where backups fail we will investigate the cause and resolve the issue, if the issue relates to 3rd party non-Microsoft software we will notify you.

Where new resources are deployed by a 3rd party, they must be onboarded into our backup monitoring before we monitor backups

Optionally, for an additional charge, we can carry out backup testing.

2.7 FinOps Recommendations

Transparity's Customer Portal provides live access to recommendations for cost optimisation and right sizing.

Your Service Delivery Manager work with you to align these recommendations to develop a workload optimisation planned aligned with your business strategy.

2.8 Service Requests

The managed service includes a defined number of service requests per month based on your Azure consumption, the number of service requests included with your service will be detailed in the statement of work at the point of order.

2.9 Customer Success Architect

You will be assigned a dedicated Customer Success Architect (CSA). The CSA will be an experienced technical consultant or architect with expertise across the Microsoft portfolio.

You will have direct access to your CSA for anything that isn't time sensitive or mission critical such as:

- Expert Consultation: Receive answers to your technical questions from an expert, helping you navigate the complexities of the Azure platform.
- Strategic Guidance: Benefit from strategic advice and best practices to optimise your Azure environment, improve performance, and reduce costs.

2.10 Service Management

As part of your account team, you will be allocated a Service Delivery Manager. They will serve as your primary contact(s) for day-to-day management and interaction for this Service. In addition, the Service Delivery Manager will act on your behalf to ensure we adhere to our processes and standards to meet contracted obligations and provide advice and guidance on your Public Cloud Service.

The responsibilities and/or deliverables of your allocated Service Delivery Manager will include the following as outlined in the table below: -

Name	Description	Frequency	Forum
Operational Risk Management and Tracking	An operational repository (including the Risk Register) will be created for all risks identified and will include information about each risk, e.g., the nature of the risk, reference, and owner, as well as any mitigation measures. This report will be reviewed with you via Service Delivery Manager at your service reviews.	Monthly	Service Review
Detailed Monthly Performance Report	The monthly performance report is comprised of the following sections: • Azure Billing / Spend (for example, the FinOps element) • Recommendations (for example, your security score) • Sustainability and carbon optimisation insights and recommendations • Service Analysis • Housekeeping	Monthly	Service Review
Continual Service Improvement Advice	Strategic advice based on intelligence provided by the Service to investigate how we can potentially increase the quality of products and services at a minimal cost for you. This advice will be tracked in a Continuous Service Improvement plan owned by the Service Delivery Manager. This will be reviewed with you via Service Delivery Manager at your agreed service reviews.	Monthly	Service Review

Name	Description	Frequency	Forum
SLA Breach and Complaints Management	We provide support including graphical information and narrative to you.	As and when an Incident occurs	Service Review
Risk Register	We maintain a register of all known risks for ongoing management – please refer to the Operational Risk and Management Tracking above.	As and when a risk occurs	Service Review

3. Service Operations

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

3.1 Transparity Customer Portal

As part of this service we will provide you with access to our customer portal, the portal includes the following functionality: -

Feature	Description
Overview Dashboard	• Billing summary • Patching status • Backup status
FinOps	• Azure spend dashboard with filters • Hybrid benefit dashboard • Cost anomalies report • New resource dashboard
Sustainability	• Emissions summary dashboard

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:

- All professional services required to set up this Service will be subject to separate Statements of Work and Charges and, where applicable, Service Descriptions.

5.1 Customer Obligations

- You will provide us reasonable assistance in the performance of the Service(s) including, but not limited to, providing all technical and licence information that we may require to perform the Service(s).
- You will provide named contacts who will be authorised to submit support requests on behalf of your company ("Nominated Contacts"). They will be the designated people with whom all contact is made regarding all requests.
- You will provide us with access to the in-scope subscriptions, accounts, and tenants. This access will be used by our support staff and tooling. For example:
    - Microsoft's Partner Admin Link (PAL);
    - Microsoft Granular Delegated Access Permissions (GDAP) relationship;
    - Azure Lighthouse relationship and delegations;
    - Service Principals;
    - Administration break-glass accounts; and
- For Azure subscriptions not purchased through our CSP we will not be able to raise incidents with Microsoft unless you have purchased a separate Microsoft support agreement;
- You will allow us to deploy infrastructure in each public cloud region to handle the collection of activity and diagnostics logs into our monitoring platform.
- You are responsible for having an associated licence (where legally required or contractually required by the vendor to do so) for:
    - Operating System(s) (OS) and software for your applicable Public Cloud Resources.
- You will provide us with reasonable advance notice of any:
    - intent to perform planned maintenance activities (including upgrades, deployments, patching);
    - additional resources that you will deploy into the Supported Public Cloud Platform.
- You will actively work with our operations team to resolve any raised incidents or Service Requests, or any activities relating to patching, that require your input or action. For example, you may be required to make any required changes to an OS running within a VM to which we have no access.
- Some incidents may require user-impacting remediation activity. You are responsible for distributing and coordinating end-user communications and activity unless agreed otherwise during the planning of the activity.
- 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
- PaaS monitoring is for the Microsoft Azure PaaS service and supporting Microsoft Azure infrastructure only. We will not monitor the applications or custom configuration that is deployed to these services.

6. Exclusions

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;
- Management, configuration, maintenance, administration of third-party appliances, Customer applications, and any code used to create, update, or deploy applications from third parties or by the Customer is excluded from this Service;
- Monitoring and support of VPN connections, Microsoft Azure Express Route termination points at the Customer premises or on user endpoints is excluded from this Service;
- Virtual desktop systems including, but not limited to, Microsoft Azure Virtual Desktop endpoints 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

Acronym	Meaning
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	One (1) hour	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

Priority	Severity	Description
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