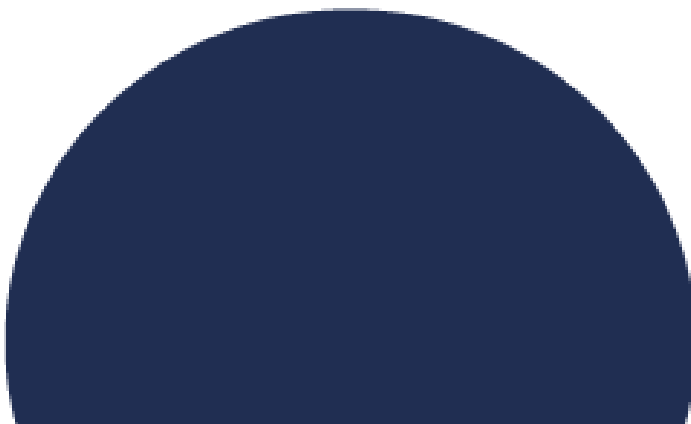




Service Definition

Azure Site Recovery | Managed



1. Operational Services

1.1. Service Description

The Co-Managed Azure Site Recovery (ASR) Service is designed to support the Customer's disaster recovery capability for in-scope Azure Site Recovery protected assets. The Service provides expert guidance, configuration, monitoring, recovery plan management, and support for failover and recovery activities, while the Customer retains responsibility for its wider business continuity and disaster recovery strategy, governance, and decision-making.

1.2. Terms and Definitions

The definitions used in the Terms shall have the same meaning when used in this Service Definition. The additional terms used in this Service Definition are defined as follows:

Term	Definition
Normal Business Hours	9:00 -17:30, Monday to Friday (excluding bank holidays in England and Wales).
Working Day	8.5 Normal Business Hours.
24 x 7	24 hours a day, 7 days a week.
ANS Glass	the portal where the Customer can log/view Service-related tickets, alerts and performance dashboards.
ASR Appliances	on-premises replication appliance required when you use Azure Site Recovery for disaster recovery of VMware VMs or physical servers to Microsoft Azure.
ASR Recovery	the act of failing over to a secondary location from primary as part of an outage or test exercise.
Azure Site Replication Major Version Releases	a release that introduces significant changes, new features, or major enhancements to the Azure Site Recovery service.
Bug Remediation	the process of identifying, analysing, and resolving defects or errors in an IT service, to restore normal functionality and prevent recurrence.
Business Critical Incident	Incidents that cause complete outage or failure of systems or services identified by the Customer as crucial to normal business operations.
CAB Approval	Change approval of the CAB required as part of the Change Management Process for Normal Changes.

Change	the addition, modification, or removal of anything that could have a direct or indirect effect on the Service.
Change Management Process	the Supplier's structured approach to managing Changes.
Change Request Form	template that allows the Customer to submit requested Changes to the Supplier as part of the Change Management Process.
Emergency Change	a change required in order to resolve or implement a tactical workaround for a P1 incident
Enhancement Request	a formal proposal to improve or add new functionality to an existing IT service, system, or process. Submitted when stakeholders identify a desirable change that is not the result of a fault or failure.
Enterprise Monitoring Solution	tools used by the Supplier to monitor and alert on the health of Customer Supported Assets.
Impact Assessment	information the Customer is required to provide as part of logging an Incident with the Supplier.
Incident	an unplanned interruption or the failure of a component of an IT service.
Incident Management Process	the Supplier's structured approach to managing Incidents.
Major Incident	Incidents categorised as P1 using the incident priority table in this document.
Managed Services Handbook	document provided by the Supplier to provide the Customer with key supporting information regarding Managed Service provision.
Microsoft Premier Support	Supplier owned support contract with Microsoft.
Normal Change	Change that is not a Standard or Emergency Change. It goes through the Change Management Process, including assessment, authorisation and scheduling.

Project Change	Change delivered by way of the Supplier's Professional Services.
Root Cause Analysis	a process used to identify the underlying cause(s) of Incidents or problems.
Service Disruption Report	Incident report completed by the Supplier
Service Hours	the applicable hours for provision of the Service as outlined in the column headed Service Hours below.
Service Management Review	regular meeting delivered by the Supplier focused on performance and value of the Managed Services contracted.
Standard Change	a pre-authorised Change that is low risk and follows a documented process for implementation
Security Incident	an Incident that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security.
Sev B	a priority classification from Microsoft Premier Support. Priorities are defined as; A – Critical impact, B – Moderate impact, C – Minimal Impact
Valid Supported Configuration	a configuration of an IT service or component that is formally approved, tested, and supported by the organisation and vendor
WMI	Windows Management Instrumentation.

1.2.1. ANS Service

Service	Service Description	Service Hours
Incident Management	The Supplier is responsible for conducting Incident management via ANS Glass, telephone, teams, email, and remote connection for Priority 2-5 support in Normal Business Hours.	Normal Business Hours
Major Incident Management	The Supplier is responsible for conducting Incident management via telephone and remote connection for Priority 1 scenario support 24x7x365. Priority escalation to Microsoft Premier Support is also included.	24 x 7
Problem Management	The Supplier's problem management processes are adhered to for Enhancement Requests and Bug Remediation and Root Cause Analysis. The Supplier conducts proactive problem management to identify and rectify recurring Incidents triggering and trend analysis. Problems are reviewed during the Service Management Review.	24 x 7
Change Management	The Supplier will take full ownership of the Change Management Process for the Customer Supported Assets.	24 x 7
Root Cause Analysis	Applicable to P1 Incidents only, following a successful resolution of a P1 Incident, the Supplier will perform Root Cause Analysis. In the case of recurring Incidents (regardless of priority) further analysis may be undertaken to identify the underlying cause. Where applicable a Service Disruption Report will be created.	Normal Business Hours
Priority Escalation to Vendor for Faults	High Priority escalation to vendor through partner channels for Priority 1 business critical faults for ASR on relevant public cloud platform.	24 x 7
High Priority Recovery	The Supplier will commit to ASR Recovery of Customer Supported Assets upon a Priority 1 (P1) Incident being raised with the Supplier and Change Request) from the Customer.	24 x 7
Change Guidance & Architecture Validation for Azure Site Recovery	The Supplier provides access to Change advisory for: <ul style="list-style-type: none"> Azure Site Recovery architecture & configuration Azure Site Recovery policy validation Azure Site Recovery design 	Normal Business Hours
Expert Access	The Supplier provides access to qualified Microsoft Azure professionals for question/query service requests.	Normal Business Hours
ASR Setup & Configuration	The Supplier will setup and configure new recovery plans via the Change Management Process to standard	Normal Business Hours

Service	Service Description	Service Hours
	specifications and then customise settings to suit the Customer's requirement.	
Patch Management	The Supplier will install Microsoft released Azure Site Recovery updates on an agreed monthly schedule to ASR Appliances where required.	Normal Business Hours
Recovery Plans	The Supplier will setup recovery plans and help recover/failover on Customer request.	Normal Business Hours
Test Recovery Plans	The Supplier will commit to testing recovery plans of Customer Supported Assets upon a Change Request being submitted by the Customer to the Supplier (max quarterly).	Normal Business Hours
Platform Monitoring	<ul style="list-style-type: none"> ASR Appliance monitoring Azure Site Recovery monitoring Performance monitoring Capacity monitoring <p>Access to the Enterprise Monitoring Solution will be provided to the Customer via ANS Glass and direct monitoring portal access.</p>	24 x 7
Performance tuning and diagnostics	The Supplier will help the Customer identify optimisations, upgrades or changes that can help the Customer's replication achieve better and more consistent performance. Additional licence fees may apply.	Normal Business Hours
Service Reviews	Service Management Review (SMR) reports will be distributed at regular intervals and discussed via a meeting between the Supplier and the Customer. The SMR report will cover the previous period.	Normal Business Hours

1.3. Incident Management

1.3.1. Incident Priority Table

Affect	Business Impact		
	Minor	Moderate	Major
System/Service Down	P3	P2	P1
System/Service Affected	P4	P3	P2
User Down/Affected	P5	P4	P3

1.3.2. Incident Response and Escalation Table

Priority	Response SLA	Specialist Review	Escalation Manager	Escalation Director	Notification Frequency	Target Resolution KPI
P1	30 Minutes	1 Hour	Immediate	Immediate	Hourly Email	4 hours
P2	1 Hour	2 Hours	4 Hours	None	GLASS Portal	1 Day
P3	4 Hours	1 Day	2 Days	None	GLASS Portal	10 Days
P4	1 Day	Never	Never	None	GLASS Portal	30 Days
P5	2 Days	Never	Never	None	GLASS Portal	None

For an Incident, "Response" is the time from when the ticket is first logged within ANS Glass to the time that the Supplier employee responds whether via an email, ANS Glass update, telephone call or in person. For detailed process flow see the Managed Services Handbook. Support to provide a resolution shall be provided within Service Hours from the time of Response until the Incident has been resolved.

From the time of Response until resolution, updates shall be provided to the named contacts and/or escalation contacts on the Customer's account by email or ANS Glass updates at such frequencies as set out in the table above.

1.4. Change Management

All Changes require a Change Request Form to be completed on ANS Glass and submitted detailing the required Change. The Supplier will reject unapproved or incomplete Change Request Forms.

Changes will follow the Change Management Process as defined in the ANS Managed Services Handbook. It should be noted that Emergency Changes will only be carried out in the event of a P1 scenario (either pro-active or reactive) and/or a major Security Incident where the Supplier deems appropriate.

1.4.1. Change Risk Assessment Data

Impact on Service	High	Significant 3 CR3	Major 2 CR2	Critical 1 CR1
	Medium	Minor 4 CR4	Significant 3 CR3	Major 2 CR2
	Low	Candidate for Standardisation 5 CR5	Minor 4 CR4	Significant 3 CR3
		Low	Medium	High
Probability of Negative Impact Until Change is Successfully Completed				

1.4.2. Change Implementation Target Table

Change Type	Implementation Start Date
Normal CR1	1 Working Day from CAB Approval
Normal CR2	2 Working Days from CAB Approval
Normal CR3	3 Working Days from CAB Approval
Normal CR4	4 Working Days from CAB Approval
Normal CR5	5 Working Days from CAB Approval
Normal CR6	Project Changes (Informational and Approval only)
Standard	Change to be completed within 4 Working days from logging on ANS ITSM Tool
Emergency	Change to completed in conjunction with Incident Management Process (P1)

Emergency Changes are dealt with in conjunction with the Incident Management Process; further details of this and all other change types are detailed within the Managed Services Handbook.

Standard and Emergency Changes to the Service within the scope of the Contract will be completed by the Supplier at no additional cost.

2. Service Levels, Key Performance Indicators & Service Credits

Category	Service Level Target	Minimum Service Level	Service Credits
P1 Incidents	100% of Incidents responded to within 30 minutes – 24x7 Service Hours.	100%	1st Incident missed response time – 5% Service Credit 2nd Incident missed response time – 10% Service Credit
P2 Incidents	100% of Incidents responded to within 1 Normal Business Hour.	Service credits apply from 2 nd failure within a calendar month	1 st incident missed response time – 0% Service Credit 2 nd Incident missed response time – 5% Service Credit 3 rd Incident missed response time – 10% Service Credit
P3 Incidents	100% of Incidents responded to within 4 Normal Business Hours.	80%	<80% - 5% Service Credit
P4 Incidents	100% of Incidents responded to within 1 Working Day.	None	No Service Credit
P5 Incidents	100% of Incidents responded to within 2 Working Days.	None	No Service Credit
Root Cause	100% of P1 Incidents to receive a Root Cause Analysis within 10 Working Days of resolution	None	No Service Credit
CR1 Change	100% of Changes start implementation within 1 Working Day from CAB Approval	100%	1 Change missed implementation time - 5% Service Credit 2 Changes missed implementation times - 10% Service Credit

CR2 Change	90% of Changes start implementation within 2 Working Days from CAB Approval	85%	5% Service Credit
CR3 Change	90% of Changes start implementation within 3 Working Days from CAB Approval	None	No Service Credit
CR4 Change	90% of Changes start implementation within 4 Working Days from CAB Approval	None	No Service Credit
CR5 Change	90% of Changes start implementation within 5 Working Days from CAB Approval	None	No Service Credit
Standard Change	100% of Changes implemented within 4 Working Days	90%	5% Service Credit

Service Credits are calculated as a percentage of the monthly Base Charge and in any event, shall not exceed 10% of the monthly Base Charge in the month that the Service Credit arose. Where a Service Credit is due it shall not accumulate with any other Service Credit and only one Service Credit can be offered within the monthly period.

3. Exclusions

The following are listed as exclusions, but this list shall not be considered complete or exhaustive and the applicable Terms should be consulted.

- a. Issues resulting from misconfiguration by the Customer outside of the Customer Supported Assets resulting in impact to the Customer Supported Assets.
- b. Issues resulting from failures in maintenance/administration by the Customer outside of the Customer Supported Assets resulting in impact to the Customer Supported Assets.
- c. Issues resulting from misconfiguration or development by the Customer and/or the Customers chosen 3rd party application provider.
- d. Issues resulting from unauthorised access by the Customer of Customer Supported Assets.
- e. End User or 1st line support.
- f. Technical advice to any persons not listed as a named contact on the Customer's account.
- g. Failure to meet SLA due to Microsoft or AWS outages or local environment factors such as power and cooling.
- h. Normal Changes requiring more than 2 hours of implementation time are excluded from the Service and will be subject to Additional Service Charges.
- i. Project Changes (Normal CR6 – see 4(d)) are excluded from the Service and will be subject to Additional Service Charges. Project Changes are recorded within ANS Glass for informational and approval purposes only.
- j. Emergency Changes that are not a direct output of a Priority 1 Incident may be subject to Additional Service Charges.
- k. Microsoft Azure Site Replication Major Version Releases will be subject to Additional Service Charges as only dot releases and patches are included as part of the Service.

- I. Escalation to Microsoft Premier Support is limited to Major Incidents, subject to Major Incident manager approval. Escalation of Sev B or lower cases is subject to Additional Service Charges.

4. Customer Responsibilities

Including but not limited to:

- a. The Customer shall have an established end user support function that may be validated by the Supplier.
- b. Where required, the Customer shall make available appropriately skilled employees while an Incident is being managed.
- c. The Customer is required to undertake an initial Impact Assessment before logging the Incident with the Supplier. Such Impact Assessment is to include:
 - a. Affected Services
 - b. Business impact
 - c. Number & type of users affected
 - d. Recent changes on Supported Assets (regardless of perceived impact)
 - e. The Customer shall check hardware onsite and ensure the hardware has power and cables are connected as expected (where required)
 - f. The Customer shall check LED status of equipment onsite (where required)
- d. The Customer shall provide full administrative access to the Supplier to all the services outlined in the Impact Assessment and any subsequently identified services or provide persons with adequate access to allow investigations to proceed.
- e. The Customer is required to ensure that all Customer Supported Assets are appropriately licenced and have (where required) Supplier recommended hardware and vendor support in place.
- f. The Customer is responsible for completing a Change Request Form in accordance with the Change Management Process.
- g. The Customer shall ensure that all relevant Customer employees have access to and have read the Managed Services Handbook.
- h. The Customer shall ensure an on-going availability of suitable internet connection (if not provided by the Supplier).
- i. The Customer shall ensure 24x7x365 availability of a suitable escalation contact should the Supplier need to gain approval for an Emergency Change or to engage other aspects of the Customer's support functions.
- j. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the Customer Supported Assets including environmental changes. Failure to do so may result in Additional Service Charges.
- k. The Customer is responsible for 1st line restoration of files and folders.
- l. The Customer is responsible for deployment and updating/patching of Microsoft Azure server agents where required.
- m. The Customer shall request permission from the Supplier in writing in the event that the Customer wishes to change the location of the Customer Assets and/or Supplier Assets from the address specified in the Contract. Any asset that has been moved without notification to the Supplier will be subject to Additional Service Charges.
- n. Where physical hardware support has been purchased, during investigations into a potential hardware or software fault it may be required to reseal certain elements of the device/infrastructure onsite or require a device inspection for LED status. This task sits with the Customer (unless the Supported Asset is located within the Supplier's data centres).
- o. If the Customer requires the Supplier to provide onsite hands and eyes support this will be subject to Additional Service Charges.
- p. It should be noted that the Customer shall report Business Critical Incidents via telephone only. The Supplier cannot offer any Service Levels or Service Credits for Business Critical Incidents raised via email.

5. Assumptions

- a. All Customer Supported Assets and production AWS and Azure accounts within the Customer Supported Assets within the Contract are covered by a valid software maintenance and support agreement in line with applicable Service Levels.
- b. All Customer Supported Assets are in a Valid Supported Configuration at the Commencement Date.
- c. All Customer specific pre-requisites have been completed before the Commencement Date.
- d. The Customer will provide a suitable specification platform, operating system and connectivity for the Enterprise Monitoring collector server.

6. Pre-requisites

- a. On-Boarding health check and documentation.
- b. Deployment of Supplier's monitoring and cloud tooling.
- c. Platform and where applicable WMI access for all monitored services.
- d. Registered Partner of Record (see section 7).
- e. Administrative access permissions for ANS Engineers on supported Cloud Resource Subscriptions/accounts and Customer Supported Assets.

7. Partner of Record

ANS' Managed Cloud for Azure incorporates Microsoft Premier Support for any issues that require escalation to Microsoft. In order for this to be able to be fulfilled, Microsoft leverage information collected from the Partner of Record (PoR) system to assign back-end support rights. As such the Supplier must be registered as the digital PoR on any Cloud Resource Subscriptions that contain or contribute to assets under support or management for the entire duration of the agreement. Consequently, the Customer shall, prior to the Commencement Date arrange for ANS to be registered as the PoR on all Cloud Resource Subscriptions that contain or contribute to assets under support or management for the entire duration of this agreement. The Customer will grant ANS 24 x 7 operational control and management of a Customer's Azure resources via any of the following options:

- Supplier "Global Administrator" permission within Customer's Azure "Active Directory" tenant.
- Azure Lighthouse delegated resources management.
- Directory of guest users or service principals.