Six Degrees

G-Cloud 15

Cloud Managed Services

Service Descriptions

Secure, Integrated Cloud Services

This document includes the following Service Descriptions:

- Azure Manage & Govern.
- Server OS Management Service.
- SQL Server Management Service.
- Active Directory Management Service.
- Backup Management.
- DR Management.
- Cloud Firewall Service.
- Cloud Load Balancer Service.

1. Service Overview

Our Cloud Managed Service encompasses three separate services tiers:

(a) Foundation; and

(b) Manage & Govern.

Our Manage & Govern Services is designed to provide management services for your Managed Subscription(s), including point of escalation to Microsoft for P1 to P4 Azure platform incidents identified utilising our Partner led Azure Support. Our Service includes the provision of financial governance and control through FinOps, reporting.

You can procure a specific Tier of our Cloud Managed Service for one of more of the Azure Subscriptions within your Azure tenant. You can choose to have different Tiers for different Azure Subscriptions.

The Azure Subscriptions for which you have procured the Manage & Govern Service will be set out in your SoW.

2. Service Features

As a standard, the Manage & Govern Service includes the features listed in the table below. The optional features are available upon request and may be subject to an additional Fee.

Your selection will be defined in your Order Form and/or SoW.

Service Deliverable	Azure CSP	Azure Non-CSP
Change Management	●	●
Incident Management	●	●
Microsoft platform support (logging with Microsoft)	●	
Azure Cost Management maintenance and configuration	●	●
Monitoring maintenance and configuration	●	●
Microsoft Defender for Cloud maintenance and configuration	●	●
Monthly FinOps Review*	●	●
OS management	●	●
IaaS and PaaS management	●	●
Azure Backup management	●	●

Azure Site Recovery management	•	•

* If remediation includes activities listed a standard Service Requests (as set out in Section 6.4), you can request us to perform such activities as part of your monthly Service Request Entitlement. If remediation does not relate to a standard Service Request, request for remediation can be completed either via your Flexible Engineering Service or via a separate professional service engagement and subject to an additional Fee.

3. Service Specific Deliverables

3.1 Azure CSP

You may elect to procure your Microsoft Azure directly from us through the Cloud Solution Provider (CSP) licence agreement. In this instance we will invoice you monthly in arrears for all cloud spend. If you have elected to procure Microsoft Azure from us, you agree to:

(a) be bound to the Microsoft Online Subscription Agreement;

(b) providing us with contributor rights to all subscriptions to enable us to deliver the services required; and

(c) allow us to deploy Azure Policies to deliver the Manage & Govern Service. Please note that we will retain ownership of these Azure Policies.

We will raise incidents directly with Microsoft where the fault resides with the Azure platform.

3.2 Azure Non-CSP

You may elect to procure your Microsoft Azure directly from Microsoft or via another provider either through a Cloud Solution Provider (CSP) licence agreement or Enterprise Agreement. If you have selected this option, it is your responsibility to:

(a) maintain the appropriate level of Microsoft Support and contact Microsoft directly for incidents where the fault resides with the Azure platform.

If you have selected this option, you agree to:

(b) provide us with contributor rights and Partner Admin Link (Pal) to all subscriptions to enable us to deliver the services required; and

(c) allow us to deploy Azure Policies to deliver the service. Please note that we will retain ownership of these Azure Policies.

3.3 Change Management

Changes will be managed as a Service Requests in accordance with Section 6.4.

Service Requests can be requested for standard changes and routine management of your Service. We will manage Service Requests in accordance with the response targets for Priority 4 (P4) tickets set out in Section 11.

3.4 Incident Management

We provide proactive support for the Managed Subscriptions included in the scope of the Service.

We will triage alerts generated on your Managed Subscription. If we are unable to resolve the alert, we will raise an incident ticket with the relevant classification. An automated notification will be sent to your nominated email address.

Tickets alerted on from your Managed Subscription will be resolved without notifying you unless our assigned engineer deems that the ticket will affect your ability to operate your Cloud Managed Service or the incident is re-classified as a Priority 1.

During triage, the incident Priority may be adjusted based on the incident classification definition in Section 11.

If you have an issue which generates alerts and you do not resolve it based upon our reasonable advice within 24 hours from being notified to do so, we reserve the right to disable alerting and cannot be held liable for any interruptions to your organisation.

3.5 Microsoft Platform Support (logging with Microsoft)

If you have procured Microsoft Azure from us, we will use our Tier 1 CSP Microsoft Premier Support agreement to raise incidents directly with Microsoft where the fault resides with the Azure platform.

These faults will be confirmed by Microsoft via the Microsoft Service Health information that is available on the Microsoft Azure website. You can raise incidents relating to Microsoft Azure Health directly with us through the Customer Portal.

We will follow the target response and fix times as defined in Section 12.

The Service Level Agreement for the Azure platform (as provided and run by Microsoft platform) can be found here: https://azure.microsoft.com/en-gb/support/legal/sla/.

Please note that the activities listed in this Section 3.5 are outside the scope of your Service where you have procured Microsoft Azure directly from Microsoft or via a third-party provider, in which case you will remain responsible for raising incidents related to Microsoft Azure Health with Microsoft.

3.6 Azure Cost Management Maintenance and Configuration

We will:

(a) Configure according to our standard policies and maintain your Azure Cost Management service;

(b) Configure according to our standard policies and maintain your Azure tagging for billing purposes; and

(c) Manage your RBAC roles and access.

If you require our assistance for remediation activities deemed to be standard Service Requests (as set out in Section 6.4), you can request us to perform such activities as part of your monthly Service Request Entitlement. If remediation does not relate to a standard Service Request, you can place a separate order with us or, if you have procured the Flexible Engineering Service, you can use your Flexible Engineering Pod.

3.7 Monitoring Maintenance and Configuration

We will:

(a) Configure according to our standard policies your VMs and Azure resources for event monitoring; and

(b) Collect and analyse metrics for performance and diagnostic purposes.

(c) Manage your RBAC roles and access.

3.8 Microsoft Defender for Cloud Maintenance and Configuration

We will:

(a) Configure according to our standard policies your Microsoft Defender for Cloud;

(b) Supply appropriate licensing of Microsoft Defender for Cloud;

(c) Configure and maintain the Security baseline for Microsoft Cloud Security Benchmark (MCSB) v1 (please refer to Microsoft Azure website for additional information); and

(d) Manage your RBAC roles and access.

3.9 Monthly FinOps Review

We will evaluate your Microsoft Azure environment once (1) per month and deliver a cost optimisation review. The report will provide you with an overview of your overall spend and recommendations on cost optimisation opportunities identified.

You can implement any suggested remediations following this review. If you require our assistance for activities deemed to be standard Service Requests (as set out in Section 6.4), you can request us to perform such activities as part of your monthly Service Request Entitlement. If remediation does not relate to a standard Service Request, you can place a separate order with us or, if you have procured the Flexible Engineering Service, you can use your Flexible Engineering Pod.

3.10 OS Management

We will provide Operating System (OS) management for Windows and Red Hat Enterprise Linux operating systems deployed by us (provided either as a separate service or as a Service Request) using standard deployment templates, configurations and tools. VMs not provisioned by us are not guaranteed to be enabled for management, and you are responsible for notifying us so that we can appropriately onboard and support them under the terms outlined below.

(a) Managed Patching

We will:

(i) Configure patching, patch groups and patch windows; and

(ii) De-bug and remediate any patching which has been unsuccessfully applied.

You will be responsible for notifying us of assignment of machines into the appropriate patch groups and for ensuring all patches are compatible with your operating systems.

(b) Managed Anti-Virus

We will:

(i) Configure according to our standard policies and maintain anti-virus tagging policies;

(ii) Install, configure and maintain our managed anti-virus solution on your Azure VMs tagged with the correct settings (as agreed with you).

You will be responsible for notifying us of any specific monitoring exclusions that you require.

Please note that we are only responsible for ensuring that the agent is up to date within the acceptable agent version as defined by our preferred tools (Green List). If we have performed our obligations and you are infected by a threat, we will not be liable for any losses, outcome, downtime or remediation activity.

In the event of any infection and where you need us to resolve the issue, we reserve the right to charge you for this service as a professional service, on a time and materials basis.

3.11 Azure Backup Management

We will:

(a) Configure according to our standard policies and maintain Azure Backup service including the management of storage vaults and regional instances (as agreed with you);

(b) Configure a standard set of Azure Backup policies defining standard RPO/RTO goals;

(c) Investigate and resolve repeated backup job failures.

You will be responsible for informing us of which Backup policy you wish to assign to each of your Azure services.

3.12 Azure Site Recovery Management

We will:

(a) Configure according to our standard policies and maintain Azure Site Recovery tagging policies;

(b) At your request, configure replication of VMs from one Azure region to your secondary Azure region;

(c) Monitor replication jobs of VMs and, if any issues are identified, we will raise incidents as described in Section 3.4;

(d) In the event of a P1 Incident, we will fail-over any VMs at your request.

Please note that Azure Site Recovery replication is limited to VMs.

The standard retention period of your replicated data is twenty-four (24) hours (at one (1) hour snapshots), after which the data is automatically deleted.

You may add or remove resources from the scope of your Azure Site Recovery Management at any time by raising a Service Request in accordance with Section 6.4.

If you require a creation of a Disaster Recovery Plan or Disaster Recovery testing, you can request additional professional services subject to a separate Fee.

4. Service Implementation

Depending on your requirements, we will discuss the implementation activities required with you and document them in your SoW. This Service supports the following onboarding scenarios:

(a) Onboarding of an existing Microsoft Azure environment;

(b) Build of new Microsoft Azure environment; and

(c) Migration to Microsoft Azure.

Our Service Implementation team will support you throughout the deployment process and during the transition to a finalised environment into in life support (including support from your Service Delivery Manager if one is assigned to your account).

4.2 Onboarding of existing Microsoft Azure Environment

We will prepare a separate SoW to transition the agreed Microsoft Azure subscriptions onto our Manage & Govern Tier of the Cloud Managed Service

4.3 Build of new Microsoft Azure Environment

We will prepare a separate SoW to perform a CAF (Cloud Adoption Framework) Cloud Implementation to implement the new Microsoft Azure environment. Once deployed to the agreed specification, we will transition the agreed Azure subscriptions onto the Manage &

Govern Tier of the Cloud Managed Service. The CAF Cloud Implementation Service is a separate service subject to an additional Fee, which will be detailed in your SoW and/or Order Form. Please refer to the CAF Cloud Implementation Service Description for further information.

4.4 Migration to Microsoft Azure

We will prepare a separate SoW to perform a CAF Assessment and Migration for any workloads that require migration to a Microsoft Azure environment. Once complete, we will transition the agreed Azure subscriptions onto the Manage & Govern Tier of the Cloud Managed Service. The CAF Assessment and Migration Service is a separate service subject to an additional Fee, which will be detailed in your SoW and/or Order Form. Please refer to the CAF Assessment and Migration Service Description for further information.

After order acceptance, we will deliver the Service as follows:

Service Implementation	Us	You
We will jointly engage in detailed discussion of the Service to ensure accurate scoping.	•	•
We will review your requirements and provide a quote and the associated SoW for Service.	•	
You will approve the quote and associated SoW, and sign-off the Order Form for the Review.		•
We will provide a named Account Manager resource.	•	
We will provide you with details of the scope and the schedule of the Service prior to commencement.	•	
We will set up the kick-off workshop.	•	
You will provide us with information requested in kick-off workshop, including (but not limited to) details of: • Business objectives and current challenges (e.g., migration to Microsoft Azure, refactoring current Microsoft Azure footprint), • Systems SLAs, RO, PPO requirements, and • Procurement, allocation and management of AAD premium licences and features (Basic, P1, P2).		•
You will provide us with details of procurement, allocation and management of AAD premium licences and features (Basic, P1, P2).		•
You will provide us owner/contributor role within your Azure Subscriptions(s).		•
We will jointly review standard policy configuration for Azure services and capture specific policy settings and non-standard requirements.	•	•
We will confirm the date when the Manage & Govern Service is live.	•	

Unless otherwise agreed with you, all implementation work will be carried out during Business Hours.

We reserve the right to charge additional Fees in accordance with your MSA for any change in your requirements occurring after the implementation of the Service and outside the scope of the contract.

4.5 Ready for Service

The Ready for Service Date is the date when we (acting reasonably and properly) notify you that the transition of your Managed Subscription is complete and that the Cloud Managed Service is ready to be actively managed by us.

Please note that if you have procured your Microsoft Azure from us as your CSP, we will bill your for Azure Usage Fees from the date when such charges are first generated by your Azure resources (regardless of the Ready for Service Date).

5. Billing

Subject to Section 5.1, the Service will be billed from the Ready for Service Date as Management Fees monthly in arrears in accordance with the Billing Guide, and calculated as described in Section 5.2 below.

If you have procured your Microsoft Azure from us (Azure CSP), we will also charge you Azure Usage Fees monthly in arrears for your Azure consumption (in accordance with the Billing Guide). The Azure Usage Fee will be calculated from the first instance a resource within your Azure Subscriptions generates consumption charges.

If you are procuring Microsoft Azure from Microsoft or from a third party (non-Azure CSP), you will be charged for your Azure consumption directly from Microsoft or from the relevant third party.

5.1 Minimum Commitment

Unless otherwise agreed in your Order Form or SoW, the Management Fees of your Manage & Govern Service are subject to a monthly minimum commitment of £1,950. On a monthly basis, we will charge you the relevant Azure Usage Fees and the higher of: (i) the monthly minimum commitment of £1,950 (or as otherwise specified in your Order Form or SoW); or (ii) the applicable Management Fees calculated as described in Section 5.3 below.

5.2 Billing Guidelines

The monthly Management Fee of your Manage & Govern Service will be calculated in arrears as a percentage of the total Azure Usage Fees that you have incurred in a specific month for your Managed Subscriptions, regardless of whether you are procuring these from us, from a third party or directly from Microsoft.

We will bill you for the Management Fees from the date when your first Managed Subscription has been through an iteration of service transition (as notified by us). Your order may be small enough that one, or all, of the associated Managed Subscriptions are transitioned together and the management Fee is applied with the conclusion of the order's fulfilment.

The percentage will vary as set out in the table below and depending on: (i) the Band applicable to the usage costs that you have incurred for your Managed Subscriptions in a specific month; and (ii) whether you have procured your Azure Subscriptions from us as your CSP

If, for example, you have incurred total usage costs for your Managed Subscriptions which fall within Band A, we will apply Rate A to such costs to calculate the usage Fee for your Manage & Govern Service.

If the total usage costs of your Managed Subscriptions fall within Band C, we will apply Rate A to the first £15,000 of usage costs, Rate B to the following £24,999, and Rate C to the usage costs in excess of £40,000. We will then calculate the total usage Fee payable for the Manage & Govern Service by adding up the charges payable for each Band calculated at the relevant Rate.

Monthly Azure Usage Fees for Managed Subscription	Band	Azure CSP Rate	Azure Non-CSP Rate
Up to £15,000	A	45%	45%
£15,001 to £40,000	B	35%	40%
£40,001 to £60,000	C	23%	35%
Over £60,001	D	20%	30%

5.3 Additional Charges

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

(a) For time spent during Incident Management where the root cause is identified as outside the scope of our Service;

(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; and

(c) Any Service Request that exceed the Service Request Entitlement within a calendar month (as defined in Section 6.4).

6. Service Operations

6.1 Event Management

We will monitor the Microsoft Azure Service Health and configure our systems to trigger an event when ‘critical’ or ‘warning’ events (as defined by Microsoft) are reported for greater than the time specified within the table below.

Service	Critical Event Trigger	Warning Event Trigger
Microsoft Azure Service Health	5 Minutes	15 Minutes

We will provide 24x7 monitoring for your Managed Subscription and configure our monitoring systems to trigger an event when a condition impacting availability (up/down) capacity or performance persists for greater than a threshold time specified. Details of event monitoring, thresholds and alerts are included in our event management matrix, a copy of which can be provided upon request.

Please note that alerts generated by the monitoring system are internal only. We will review these alerts in accordance with Section 6.2.

6.2 Proactive Break and Fix Support

Alerts generated by our monitoring tools are only for internal alerting purposes to deliver proactive support for your Managed Subscriptions, as defined in Section 3.4. We will triage alert events and open incident tickets if the alerts cannot be resolved, we will raise an incident in accordance with Section 11. We will manage incidents created from monitoring alerts in accordance with the process set out in our Operations Manual.

We will:

(a) Notify you within a reasonable time after we become aware of a potential capacity constraint and provide recommendations on capacity upgrades available;

(b) Seek your approval before upgrading the capacity on your services. Please note this could result in service degradation pending the upgrade, for which we are not responsible. We may switch off further alerting and stop notifications that are repeated when you reach a capacity threshold, pending your approval to the upgrade.

We may offer to upgrade the capacity without first agreeing the associated Fees with you, in which case your approval of the upgrade will be binding. If so, we will act in a commercially reasonable manner in determining the revised price which we will provide you as soon as reasonably practicable afterwards, and which you will be liable to pay.

6.3 Support Portal

You can log and track all of your requests on our client portal. We will provide you registration and login details during the Service implementation phase.

Our support team can be contacted by phone, email or via our client portal and will be able to assist you with the following:

(a) Service Requests;

(b) Technical query requests;

(c) Incidents;

(d) Ticket updates;

(e) Portal logins;

(f) Service reporting; and

(g) General queries.

When you contact our support team, we will issue you with a reference number which acts as your unique reference for your incident or request. We will ask you to quote this reference number when contacting the support team to provide information or an update.

6.4 Service Request Entitlement

As standard, your Manage & Govern Service includes a number of Service Requests in a calendar month free of charge. Your Service Request Entitlement will be calculated based on the Rate applicable to your average spend in the previous calendar quarter. Details of the Service Request Entitlement for each Rate is included in the Service Request Catalogue.

We will confirm your Service Request Entitlement applicable to your first quarter after the initial kick-off workshop.

We can implement Service Requests in additional to your Service Requests Entitlement as and when required for an additional Fee. Information requests will be treated as Service Requests if listed in the Service Request Catalogue.

Any request that is not specifically listed in the Service Request Catalogue available on the Client Portal will be considered a professional services engagement subject to an additional Fee calculated on a time and materials basis. These changes must follow the process covered in our MSA.

We reserve the right to amend the Service Request Catalogue from time to time.

7. Exit Assistance

As a standard, we will perform the following activities shortly before or upon termination of your Service:

(a) We will work with you to remove our access to your Microsoft Azure tenant, Microsoft platform support and associated tools;

(b) We will terminate the creation and distribution of your monthly FinOps reports;

(c) We will remove your access to the Mange & Govern Service from our customer portal;

(d) We will provide instructions on how Azure Lighthouse delegations can be removed by you. We will also remove any additional accounts or permission updates to facilitate the termination of Service; and

(e) Should you have a CSP subscription with us, we will facilitate the transfer of the Microsoft Azure CSP subscription to the new CSP provider, in line with Microsoft guidelines.

Please note that it is your responsibility to provide a valid termination notice in accordance with the terms of your MSA. We reserve the right to charge additional Fees for the performance of the activities listed above if you fail to provide such notice.

If you require us to perform any activities in addition to those listed above, we can provide professional services subject to an additional Fee.

8. Dependencies

We will provide the Service subject to the following dependencies:

8.1 Client Obligations

(a) You agree to provide us with the necessary access, including the provision of Azure Lighthouse with contributor rights and the maintenance of Microsoft Partner Admin Link to all Managed Subscriptions.

8.2 Prerequisites

(a) If you require us to build a new Microsoft Azure environment for you, you must procure our CAF Cloud Implementation Service prior to implementation. Please note that the CAF Cloud Implementation Service is subject to a separate Fee; and

(b) If you wish to migrate to Microsoft Azure, you must procure our CAF Assessment and Migration Service prior to migration. Please note that the CAF Assessment and Migration Service is subject to a separate Fee.

9. Exclusions

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

(a) Monitoring and management of workloads running within your Managed Subscriptions;

(b) Security management for the workloads running within your Managed Subscriptions and compliance with security principles and best practices;

(c) Configuration and management of Azure Sentinel;

(d) Responding to alerts created by Microsoft Defender for Cloud;

(e) Azure Platform patching and platform updates;

(f) We will not perform the activities listed in Section 3.5 if you have procured Microsoft Azure directly from Microsoft or from a third party;

(g) Azure Monitor custom monitors and integration with third party tools;

(h) Disaster recovery:

  (i) Definition of a disaster recovery plan;

  (ii) Disaster recovery testing; and

  (iii) Execution of a disaster recovery plan.

(i) SQL management;

(j) Any activities other than those specifically set out in this Service Description.

Please note that this Service Description sets out what we deliver as a standard. If you require us to perform any bespoke activities, or if you are a reseller and are procuring the Manage & Govern Service for your end clients, additional Fee may be applicable. Any bespoke agreement will be documented in your SoW. Please contact your Account Manager if you wish to discuss your requirements.

10. Definitions and Acronyms

10.1 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
Azure Advisor	Azure product as defined at https://azure.microsoft.com/en-gb/products/advisor/.
Azure Application Insight	An extension of Azure Monitor as defined at https://learn.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview
Azure Change Analysis	An extension of Azure Monitor as defined at https://learn.microsoft.com/en-us/azure/azure-monitor/change/change-analysis
Azure Container Insight	An extension of Azure Monitor as defined at https://learn.microsoft.com/en-us/azure/azure-monitor/containers/container-insights-overview
Azure Cost Management	Azure product as defined at https://azure.microsoft.com/en-gb/products/cost-management/.
Azure CSP	Where you procure your Microsoft Azure directly from us through the Cloud Solution Provider (CSP) licence agreement.
Azure Log Analytic	An extension of Azure Monitor as defined at https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview
Azure Monitor	Azure product as defined at https://azure.microsoft.com/en-gb/products/monitor/#layout-container-uidbbb6.
Azure Non-CSP	Where you procure your Microsoft Azure directly from Microsoft or via another provider either through a Cloud Solution Provider (CSP) licence agreement or Enterprise Agreement.
Azure Policies	Means your business rules used to control your Azure resources.
Azure Subscription	Means all subscription within your Microsoft Azure tenant (whether managed by us or unmanaged).
Azure Usage Fees	Means all Fees associated with the consumption of your Azure Subscriptions that you will incur from the moment we become your CSP provider. If you are procuring Azure Subscriptions from us as your CSP, you will be responsible to pay Azure Usage Fees for the consumption of your Azure resources in addition to the Management Fees of your Foundation Service.
Band	The band applicable to the total usage costs that you have incurred for your Manage Subscriptions in a specific month.
Client Portal	https://6dg.service-now.com/cp/.

Cloud Solution Provider	Means a licensing model for Microsoft where a partner owns a customer's lifecycle and relationship end-to-end on behalf of the customer.
DR Management	The service defined at Section **Error! Reference source not found.**.
Enterprise Agreement	Means a licensing model for Microsoft for a company with 500 or more users or devices to manage licensing and cloud services under one agreement.
Flexible Engineering Service	As defined in the Flexible Engineering Service Description Our Flexible Engineering product which provides you with a pool of annual engineering resources for your Cloud Managed Service.
Flexible Engineering Pod	The pool of resources available to you as part of Flexible Engineering Service.
Managed Subscription	Means your Azure Subscriptions managed by us and included in the scope of the Manage & Govern Service.
Management Fees	Means the Fees associated with the management activities that we will perform in relation to your Managed Subscriptions as described in this Service Description.
Microsoft Azure	Means all your Microsoft Azure Services.
Microsoft Azure Health	Means the health status of Azure including alerts and guidance for any service issues.
Microsoft Defender for Cloud	Azure product as defined at https://azure.microsoft.com/en-gb/products/defender-for-cloud/.
Rate	The rate used to calculate the Management Fees for your Manage & Govern Service based on your applicable Band (as described in Section 5.2).
Ready for Service Date	Means the date when the Initial Service Term of your Service (as defined in the MSA) will commence.
Service Request	One (1) request included in the Service Request Catalogue available on the Client Portal.
Service Request Catalogue	The catalogue available on the Client Portal which lists the Service Request deemed to be standard changes and include details of the Service Request Entitlement for each Rate.
Service Request Entitlement	The number of Service Requests included in the scope of your Service for each calendar month as set out in Section 6.2.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing services to that client.
Tier	Means the Foundation or Manage & Govern tier of your Cloud Managed Service, as relevant.
VM Insight	An extension of Azure Monitor as defined at https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview

10.2 Acronyms

Acronym	Meaning
AAD	Azure Active Directory
CSP	Cloud Solution Provider
DR	Disaster Recovery
DRP	Disaster Recovery Plan

Acronym	Meaning
IaaS	Infrastructure as a service
MSA	Master Services Agreement
NPS	Net Promoter Score
OS	Operating System
PaaS	Platform as a service
RBAC	Role Based Access Control
RPO	Recovery Point Objective
RTO	Recovery Time Objective
OS	Operating System
SoW	Statement of Work
SQL	Structure Query Language

11. Incident Classification and Operational Targets

Incidents affecting the operation of Cloud Managed Service are classified in accordance with the table below.

		Scale			
Business Impact	Impact Description	Business Wide	Department	Team	Individual
	Critical impact – It is not possible to complete key business tasks.	P1	P1	P2	P3
	High impact – Key business tasks are significantly degraded.	P1	P2	P3	P4
	Medium impact – The completion of key business tasks is made more difficult or is taking longer.	P2	P3	P4	P4
	Low impact – Service requests, incidents with no impact on business, or minor incidents where a workaround is available.	P3	P4	P4	P4

The associated response and resolution targets below will apply based on the incident priority assigned.

	P1	P2	P3	P4
Response	30 mins	1 hour	2 hours	4 hours
Fix	4 hours	8 hours	16 hours	40 hours
Hours of Support	24x7	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days
Description	Both response and fix time are calculated from the moment that an incident is raised in accordance with Section 3.3. The response is an acknowledgement sent to your nominated contact that the incident has been received and assigned. Resolution of incidents related to the Azure platform is managed by Microsoft. If you are procuring the Managed License from us, we will escalate the incident to Microsoft in accordance with the Service Description. Microsoft will then manage the incident in accordance with the targets available at https://azure.microsoft.com/en-gb/support/legal/sla/. We will not manage incidents related to the Azure platform where you have procured your Manged Subscriptions directly from Microsoft or from a third-party provider. Please note that these incidents are outside the scope of your Service. If the incident does not relate to the Azure platform and resolution is within the scope of this Service, the incident be deemed fixed when it no longer impacts your Service.			

12. Service Levels

The service levels associated with this service are detailed below:

Service	Service Management Process	Metric	Target
Response	Incident management	Service desk response times	90% within the published response target
Fix	Incident management	Service desk fix times	90% within the published resolution target

1. Service Overview

Our Server OS Management Service offers managed OS (Operating System) solutions for virtual and/or physical servers. The Service includes, but is not limited to, monitoring, patching, backup and regular reporting activities.

Additional information may be included in your Order Form or SoW.

2. Service Features

2.1 Event Management

We offer a 24x7 monitoring and alerting service which includes:

Monitoring KPI	Trigger	Threshold
Service availability	No Ping	15 Minutes
vCPU/CPU	> 95%	15 Minutes
vRAM/RAM	> 95%	15 Minutes
Disk space	< 10%	15 Minutes
Core Windows services	Not Available	15 Minutes
SSL certificate expiry	Alert	28 Days Remaining
Anti-Virus	Infected	Recurring
Backup	Failure	Recurring

Event management alerts are for internal use only and are used to provide proactive break and fix support in accordance with Section 2.2.

For the items listed below, the thresholds within that respective Service Description will supersede the thresholds in this document:

(a) SQL Server Management Service; and/or

(b) Active Directory Management Service.

2.2 Proactive Break and Fix Support

We provide proactive support for the monitored services defined in Section 2.1 of this document.

Alerts generated on your monitored server(s) will be raised internally to our service desk and managed as defined in our Operations Manual. An automated alert will be sent to your nominated email address.

Incidents alerted on from the monitoring service defined in Section 2.1 will be resolved without notifying you unless the assigned engineer deems that the incident will affect your ability to operate the Server OS Management 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.

This document defines what we proactively monitor as a standard. If you require support outside of what is defined in this document, 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.

If you have an issue which generates alerts and you do not resolve it based upon our reasonable advice within 24 hours from being notified to do so, we reserve the right to disable alerting and cannot be held liable for any interruptions to your organisation.

2.3 Change Management

A change is defined as one (1) request of the following items:

Service	Item
Virtual Machines	Resize a Virtual Machine
	Resizing storage within a Virtual Machine
	Adding, deleting or modifying a feature, component or service as defined at https://docs.microsoft.com/en-us/windows-server/administration/server-core/server-core-roles-and-services#features-included-in-server-core
	Adding, deleting or modifying files or network shares
	Modifying network settings
Backup	Modify an existing backup schedule
Anti-Virus	Changes to anti-virus ‘allow listing’ and ‘block listing’
	Regular full system scan timings
OS Patching	Changes to patching schedule
Service Assignment	We can update the original assignment of this managed service to a different Server OS Management Service once per quarter or upon the decommissioning of the original Server OS Management Service

As standard, we offer up to five (5) changes per month. We can implement additional changes as and when required for an additional fee which will be defined in your Order Form or SoW.

Any change request that is not specifically defined in Section 2.3 will be considered a professional services engagement subject to an additional fee calculated on a time and materials basis. These changes must follow the process covered in our MSA.

We will implement standard changes listed in Section 2.3 in accordance with the resolution times listed in our Operation Manual but, in any case, in no less that forty-eight (48) hours from receipt of the request. Please ensure to submit any urgent change, amendment or cancellation request at least forty-eight (48) hours prior the desired implementation date.

2.4 Monthly Reporting

Monthly reporting is delivered through our Client Service Management team and is a chargeable service which can be purchased in addition to this Server OS Management Service. Please contact your Account Manager for more detail.

Report	Breakdown
Backup	Success and failure of backups and why it failed
Anti-Virus	Server status
OS Patching	Patching status over the last thirty (30) days
Virtual Machine	Capacity trends on vRAM, vCPU, storage

2.5 Capacity Management

The following services are subject to capacity constraints and tiers of service:

(a) Virtual servers RAM, vCPU and storage; and

(b) Backup storage.

Typically, we proactively monitor usage and we will be alerted to an impending capacity constraint. However, demand and the rate of change will depend on your usage profile, forecasting and factors within your control, which may limit the amount of notice we receive. So this is provided on a best efforts basis.

We will notify you within a reasonable time after we become aware of a potential capacity constraint, with a recommendation on capacity upgrades available.

We will not upgrade the capacity on your services without your prior approval. This could result in service degradation pending the upgrade, for which we are not responsible. We may switch off further alerting and stop notifications that are repeated when you reach a capacity threshold, pending your approval to the upgrade.

We may offer to upgrade the capacity without first agreeing the price with you, in which case your approval of the upgrade will be binding. If so, we will act in a commercially reasonable manner in determining the revised price which we will provide you as soon as reasonably practicable afterwards, and which you will be liable to pay.

3. Service Specific Deliverables

3.1 Managed Anti-Virus

Our anti-virus agent offers protection against advanced threats, ransomware, and real-time phishing. We will perform the following:

(a) Ensure the agent is operating correctly and is up to date within the acceptable agent version as defined by our preferred tools acceptable agent version Green List; and

(b) Resolve issues related to the use of the antivirus agent software in accordance with our Operations Manual.

Please note that the managed anti-virus service can only be deployed on Windows Servers hosted and managed by us.

If we perform our obligation of keeping the agent up-to-date and within our preferred tool's acceptable agent version (Green List) and you are still infected by any threat, we cannot be held liable for any outcome or downtime this threat may cause on the server/device.

In the event of any infection and where you need us to resolve the issue, we reserve the right to charge you for this service as a professional service, which will be billed on a time and materials basis.

3.2 Patch Management

We will deploy critical and security patches for Windows Operating System (OS), VMware ESXI, VMware vCenter and Red Hat Enterprise Linux according to the table below.

Patch Management	Deliverable
Patching Frequency	Within thirty (30) days from the date a patch is released, unless otherwise agreed with you and documented in your SoW.
Patching Hours	24x7
Patching Days	Monday to Sunday, excluding Public Holidays in UK.
Patch Remediation	Included roll back of services in the case of issues caused by updates.
Runbooks	Pre and post checks and tasks with dedicated engineer inside patching timeframe window.

The table above defines our standard approach. If you require bespoke support, please contact us to discuss your options.

We install the latest available patch rollups for your patching period that will contain security updates.

We are not responsible for any security breaches within your environment or server(s) relating to any patching or lack thereof.

We are not responsible for any effect that the patch updates might have on your applications hosted on your server(s) or the server itself.

If an update affects your server or data, we will triage to resolve the issue and/or roll back if needed, then inform you of the issue.

Please note that database transactions might be affected if updates need to be rolled back.

3.3 Managed Backup

We offer an optional fully managed backup solution as part of our Server OS Management Service.

This optional managed backup service will be charged for the backup software licensing and storage capacity; it will be charged in addition to your Server OS Management Service. Your selection and the related charges will be documented in your Order Form.

If you choose to add this service, we will implement an automated backup schedule as agreed with you and documented in your SoW. Data will be backed up to your preferred target storage (which will be defined in your SoW) and retained, as standard, for a period of seven (7) days. Please contact us to discuss your options if you require a longer retention period.

If you do not have your own specified target storage, we can provide you with backup storage for an additional charge, which will be defined in your SoW or Order Form.

As standard, we will restore the data to the source location three (3) times per month. Any additional restore(s) that you may require will be charged as a professional service engagement.

Our Managed Backup solution includes the following features:

(a) File level backup of all data, including application data and full VM snapshots;

(b) File or folder restoration to a given location; and

(c) Full Server OS restoration from backup.

3.4 Runbook and Automation

A Server OS Management Service runbook is a compilation of the specific automated set of activities to be carried out to restore the virtual machine to OS level following downtime of a server or application.

We will only support the configuration and continuous management of runbooks and schedules developed by us.

Changes or updates to runbooks are outside the scope of the change management service detailed in Section 2.3 and these implementations will be delivered as a professional service and charged on a time and materials basis

Runbooks are limited to one (1) pre-agreed runbook per Server OS Managed Service for the duration of the contract and is not interchangeable. If you require any additional custom runbooks, please contact us to discuss your options. This will be delivered as a professional service and billed accordingly.

Please note that we will not offer any SLA for runbooks that have not been strictly developed by us.

3.5 Log Analytics Performance Data Capture (VMs only)

For virtual servers hosted within Microsoft, we will enable Log Analytics data collection. This tool provides centralised data collection and storage of logs from services running within Microsoft. All data will be stored for three (3) months and is available to be inspected by us using tools such as Monitor.

Please note that we require Log Analytics in order to provide you with reporting and we will not be able to do so if you decline to enable this feature.

4. Service Implementation

After order acceptance, we will implement the Service as follows:

Service Implementation	Us	You
You will provide us the target email address for alerts.		●
We will provide you the runbook template.	●	
You will submit your defined runbooks to us for approval.		●
We will deploy management agents within your infrastructure.	●	
We will configure monitoring and alerting for the resources in scope.	●	
We will send test alert to our Service Desk to confirm receipt.	●	
We will update our CMDB and hand the service over to BAU.	●	
We will implement agreed runbook and automation requirements.	●	
We will implement the anti-virus software onto the server.	●	

4.1 Managed Backup

Server OS Managed Backup Implementation	Us	You
Phase 1: BaaS Infrastructure and Platform Set-up		
We will send you a Welcome Pack and Technical Data Capture form.	●	
You will complete and return the Technical Data Capture form.		●
We will place orders for network connectivity (if required).	●	
We will confirm the projected Ready for Service Date.	●	

You will provide virtual or physical server resources for client host(s).		●
We will implement and configure backup network connectivity.	●	
We will run internal acceptance tests to confirm environment is ready.	●	
We will facilitate a training call on using the backup software and admin portal.	●	
We will deliver backup licences and provide technical support.	●	
You will implement and safely store your BaaS encryption key.		●
You will implement and safely store your encryption key for BaaS.		●
Phase 2: Managed Backup Configuration and Initial Backup		
We will configure your backup schedule and retention for all protected servers.	●	
We will undertake initial backup and testing for you for the remainder of the servers to be protected.	●	
We will perform acceptance test(s) (including restore activity) and highlight any issues found to you (may involve third-party vendors).	●	
We will work to resolve highlighted issues for you (may involve working with third-party vendors).	●	
We will perform initial backup completion and, when successful, we will move to steady state incremental backups.	●	
We will confirm the Ready for Service date and send you the BaaS handover pack before commencing billing.	●	

At the time of service handover, we will review the implementation of the service for you to sign off.

Any further actions that you wish to authorise will be documented and listed as in your SoW.

5. 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).

6. Billing

The Service will be billed as a Set-Up Fee and/or usage-based Fee(s) as defined in our Billing Guide, and as indicated in your Order Form.

6.1 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).

7. Service Operations

OS Service	Deliverable
Patching Operation	Scan of the server to identify missing Windows critical and security patches on a pre-agreed date.
	Request for change raised with you to approve patch installation during a pre-agreed maintenance window.
	Installation of patches during the agreed maintenance window.
Remote Access	The management agent deployed on your server provides us with remote access administration capabilities to support the delivery of this Server OS Management Service. Both the remote password and the remote access administration capabilities are linked.
Password Synchronisation	The management agent deployed on your server provides us with remote password administration capabilities to support the delivery of this Server OS Management Service. Both the remote password and the remote access administration capabilities are linked.

8. Dependencies

We will provide the Server OS Management Service subject to the following dependencies:

(a) The Service is only supported on servers running a version of Microsoft Windows Server covered by Microsoft's Mainstream or Extended support.

8.2 Client Obligations

(a) General:

(i) You will ensure a stable connection is available for all physical servers;

(ii) You must allow us permission to the management agent deployed on your server which provides us with remote access and remote password administration capabilities to support this service;

(iii) For Windows Servers, you must provide us with a domain local user account that has permission to access any virtual and physical servers that are monitored (required to run the monitoring service);

(iv) Windows Servers, the WMI service, SNMP service and Remote PowerShell must be enabled by you;

(v) For Linux workloads, you must provide us a SNMPv3 enabled account and a local or domain account with Sudo privileges/permissions;

(vi) Notifications will be sent to your nominated email address or distribution list that you must supply as part of the service implementation;

(vii) You must submit the runbooks in our specified runbook template which is provided to you during service implementation; and

(viii) Any additional resources required for the full and effective deployment of this service will be billed to you.

(b) Physical Hardware

(i) You will ensure the physical server hardware is covered by vendor support; and

(ii) In the event of any hardware failure, you are required to repair the physical hardware owned by you on our instruction before we can resume our services.

(c) Third-Party Application Management

(i) It is your responsibility to ensure that all applications installed on top of the operating system are patched and up-to-date. If you would like us to patch your applications, please contact your Account Manager to discuss a professional services engagement;

(ii) It is your responsibility to ensure that the applications are functioning and performing as expected after a patching cycle where the application or component support is not provided by us. Testing should be carried out within seventy-two (72) hours of patch implementation; and

(iii) You are solely responsible for all aspects of any application that is installed on top of the operating system unless you take one of our management services relating to that application.

(d) Patch Management

(i) We require seven (7) days' notice in writing to cancel a slot and/or reschedule a new slot for patching. We reserve the right to charge you for rescheduling the patching task should you fail to notify us as described; and

(ii) You are responsible to identify and notify us of any negative effects that patch updates of third-party applications might have on any of their servers prior to any upgrades.

(e) Managed Backup

(i) For Managed Backup, you are responsible to ensure there is sufficient storage space on your chosen source location.

(f) Anti-Virus

(i) If you choose to utilise your own anti-virus, we cannot be held liable of any security breaches on your virtual/physical machine. Please note that this decision must clearly be stated in your SoW.

8.3 Service Dependencies

(a) General

(i) We will deploy a software agent for patching on Windows and Red Hat Enterprise Linux Operating Systems;

(ii) We will install a monitoring probe on a server within your infrastructure to enable us to monitor your system;

(iii) We will deploy backup agents or a backup server for backup management;

(iv) Any operating system not specified in this document needs to be clarified in your SoW and our standard SLA's will not apply as this service will be delivered on a best endeavours' basis;

(v) Operating systems are only supported while in support with the vendor. Once out of vendor support we will not be held responsible for any patching and/or security risks and we will endeavour to work with you to update outdated operating system; and

(vi) We can deliver our Server OS Management Service on physical hardware only where such hardware is reachable remotely.

(b) Monitoring and Alerting

(i) For virtual machines running on Microsoft (e.g. Azure), a Microsoft Monitor Log agent is required to be deployed alongside a corresponding Log Analytics workspace. Additional alerts, their triggers and thresholds will be defined in your SoW.

(c) Change Management

(i) We require written consent from you before any change management can be actioned (as per our Operations Manual).

(d) Runbook and Automation

(i) Once your runbook has been submitted, it must be approved by our support team before it goes live; and

(ii) The runbook and automation capabilities are subject to the limits in the toolset used by us and our operational policies. They will be handled on a case-by-case basis and need to be formally agreed in writing during the implementation stage. We will default to standard monitoring practices for anything that is not agreed before the Ready for Service Date.

9. Exclusions

9.1 General

(a) The Service(s) are for software at the OS level only. The management of the physical hardware is excluded from the scope of the Server OS Management Service;

(b) The Service(s) include support for the following Operating Systems: Windows Server, Red Hat, VMWare ESXI, VMWare vCenter. All other operating systems are excluded unless otherwise agreed in your SoW; and

(c) The Service(s) are for operating systems as set out above. They do not include support for other types of server(s), application(s) or software, such as Microsoft's Exchange Server unless otherwise specifically agreed with you on an Order Form or in your SoW.

9.2 Event Management

(a) The alerts generated by our alerting tools are only for internal alerting purposes to deliver our proactive support services defined in this document; and

(b) The alerts generated by our alerting tools are not client facing.

9.3 Capacity Management

(a) Capacity management does not cover physical servers.

9.4 Application Upgrades

(a) Application upgrades are out of scope. Please contact us to discuss your options if you require our assistance. Any application update (e.g. Microsoft Exchange) will be charged as a professional service engagement.

9.5 Patch Management

(a) The patching service is supported on servers running a version of Microsoft Windows Server that is supported by Microsoft, Red Hat Enterprise Linux, VMware ESXi or VMware vCenter in mainstream or extended support. Any operating system outside of vendor support will not be supported by us;

(b) We are not responsible for any security breaches within your environment/server relating to any patching or lack thereof; and

(c) We are not responsible for any effect that the patch updates might have on your applications hosted on your server/s or the server itself.

9.6 Managed Backup

(a) Managed backup is not included in Server OS Management Service as a standard and all backup related services described in this document are excluded unless you purchase this optional product in addition to Server OS Management;

(b) The data stored on third-party applications will be back up as part of our standard Managed Backup Service. However, the support of such third-party application is excluded from the scope of the Service OS Management Service; and

(c) Backup storage will be charged separately and will be defined in your Order Form.

9.7 Third-Party Applications

(a) Third-party applications are defined as any application(s) installed on top of the operating system of an individual virtual or physical server and are not supported within this Service;

(b) Microsoft applications such as SQL Server, Exchange Server, Active Directory, Remote Desktop Services, MS Office and others similar applications are considered third-party applications. The management of third-party applications is outside the scope of the Server OS Management Service; and

(c) We are not responsible for any security breaches within your environment or server(s) relating to any patching or lack thereof on third-party applications.

9.8 Hardware

(a) Our Server OS Management Service does not cover any hardware failures.

9.9 Anti-Virus

(a) Subject to Section 3.1, we will accept no liability for any security breaches on your platform, physical/virtual servers and/or applications hosted with us.

10. Definitions and Acronyms

10.1 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
Backup Schedule	Times and dates set for backups to occur.
Green List	List of acceptable versions of the agent as per the vendor
No Ping	Checks sent to the device in intervals are not receiving a response.
OS Patching	Updating of your OS software using patches.
Platform	Public or private cloud platform.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing services to that client.
Storage	Non-volatile media for storing files, databases, applications or virtual servers.
Sudo	Linux command for privileged access.

Term	Meaning
Threshold	Time or amount of failures we have defined before a trigger sends an alert
Trigger	Given check we have defined to determine a status
vCPU	One or more virtual central processing unit(s) (CPUs) compatible with Intel x86 instruction sets.
Virtual Machine Disk	File stored on a data store representing each individual disk configured within a virtual machine.
Virtual Server	Virtualised server hosted on a cloud platform comprising of RAM, vCPU and Storage
vRAM	Virtual random-access memory used for real-time processing.

10.2 Acronyms

Acronym	Meaning
BaaS	Backup as a Service
CMDB	Configuration Management Database
KPI	Key Performance Indicator
NIC	Network Interface Card
OS	Operating System
SNMP	Simple Network Management Protocol
SoW	Statement of Work
SPLA	Microsoft Services Provider License Agreement
vCPU	Virtual central processing unit
VHD	Virtual Hard Disk
VMDK	Virtual Machine Disk
vRAM	Virtual Random Access Memory
WMI	Windows Management Instrumentation

11. Operational Targets

We require two maintenance windows per month from 22:00 to 02:00.

Type 1	P1	P2	P3	P4
Response	30 mins	30 mins	1 hour	Next Business Day
Fix	4 hours	6 hours	8 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	• Total loss of service or security breach; • Your service does not function, and you are unable to access it. • EXAMPLES: • Complete loss of access to all VMs through the chosen connectivity option; • Complete loss of access to storage from all VMs; • Total loss of access to the internet.	• Service impaired or degraded; • Performance issues - you are able to access or use your service, but it is performing at an unacceptable level.	• Minor service degradation/warning from monitoring or non-impacting service issue; • A service feature or function is not working; • There is a workaround, or you are able to utilise the service for the majority of its function. EXAMPLE: • Issues relating to a single VM; • Service available with a non-service affecting issue; • Loss of Admin Portal.	• Service requests; • Non-service affecting work and reports; • A required change or configuration alteration to a service or a technical query.

12. Service Levels and Service Credits

Sever OS Management Service aligns to the Service Levels and related definitions for Enterprise Cloud or Public Sector Cloud, so please refer to the Enterprise Cloud or Public Sector Cloud Service Description(s) (where applicable for you and as appropriate) for details.

1. Service Overview

SQL Server Management Service provides you with add-on managed services for Microsoft SQL Server application deployments within the Six Degrees Enterprise Cloud, Public Sector Cloud and Microsoft Azure Public Cloud platforms for IaaS or PaaS deployment. It can apply to both physical and virtual servers and a single SQL Server Management Service supports all Microsoft SQL Server instances on a named server. Where log shipping, failover clustering or an AlwaysOn availability group is deployed, the secondary server is covered as long as it remains passive. If the secondary server is active, it will require its own SQL Server Management Service subscription[1]. A single production SQL Server with up to three (3) instances deployed can be covered by a single subscription. Additional instances on the same server will incur additional Fees.

Test and development SQL Servers require their own SQL Server Management Service subscription, available for a reduced Fee.

All services include notification to you through ServiceNow. Notifications will be sent to your nominated email address or distribution list that must be supplied by you as part of service implementation. Please refer to the Operations Manual for the hours of service coverage and more detail.

2. Service Features

Below is a high-level overview of the functionality available within the SQL Server Management Service:

(a) SQL Server availability monitoring;

(b) SQL Server performance monitoring;

(c) SQL Server patch management;

(d) SQL Server event monitoring;

(e) SQL Server database backup and recovery management;

(f) Database Index and Statistics maintenance;

(g) Capacity management;

(h) SQL Server change management; and

[1] This additional subscription is chargeable.

(i) Third Party Support.

2.2 SQL Server Availability and Event Monitoring

SQL Server Management Service includes monitoring of SQL Server availability using the following metrics:

(a) SQL Server: Offline;

(b) SQL Server Agent: Offline;

(c) SQL Analysis Services Offline;

(d) SQL Server Cluster Failover;

(e) SQL Availability Group Failover;

(f) SQL Log Shipping Failure;

(g) SQL Alert for severity 21 – Fatal Error in Database Process;

(h) SQL Alert for severity 22 – Fatal Error Table Integrity Suspect;

(i) SQL Alert for severity 23 – Fatal Error Database Integrity Suspect;

(j) SQL Alert for severity 24 – Fatal Error Hardware Error;

(k) SQL Alert for severity 25 – Fatal Error;

(l) SQL Alert for Error 823 – Read or Write Request Failure;

(m) SQL Alert for Error 824 – Logical Consistency I/O Error; and

(n) SQL Alert for Error 825 – Read-Retry Required.

All alerts generated by the monitoring system will be raised as P2 incidents, which are a break/fix resolution. Database corruption (correlating to SQL Alerts 22 - 23) or your escalations will be classified as a P2). The restore time for a database corruption is volume driven by data, and not SLA bound.

In the event of Customer or third party invoked P2 incidents, we reserve the right to invoke commercial charges.

Please refer to the Operations Manual in the Customer Portal for prioritisation of Incidents.

2.3 SQL Server Performance Monitoring

Below items are configured with monitoring for use during troubleshooting. Please note that these monitors do *not* raise incidents, and a baseline review will be conducted of your managed SQL instances to allow identification of performance trends.

(a) Physical Disk: Average Disk sec/Read;

(b) Physical Disk: Average Disk sec/Write;

(c) SQL Server: Databases: Log Flushes/sec;

(d) SQL Server: Buffer Manager: Checkpoint pages/sec;

(e) SQL Server: Buffer Manager: Lazy writes/sec;

(f) Processor: % Processor Time;

(g) Memory: System Cache Resident Bytes;

(h) Memory: Available Bytes;

(i) Memory: Pages Input/sec;

(j) Memory: Pages Output/sec;

(k) SQL Server: SQL Statistics: Batch Requests/sec;

(l) SQL Server: Databases: Transactions/sec;

(m) SQL Server: SQL Statistics: SQL Compilations/sec;

(n) SQL Server: SQL Statistics: SQL Re-Compilations/sec;

(o) SQL Server: Access Methods: Probe Scans/sec;

(p) SQL Server: Access Methods: Forwarded Records/sec;

(q) SQL Server: Databases: Backup/Restore Throughput/sec;

(r) SQL Server: Buffer Node: Database Pages;

(s) SQL Server: Plan Cache: Cache;

(t) SQL Server: Memory Node: Free Node Memory (KB);

(u) SQL Server: Buffer Manager: Page reads/sec;

(v) SQL Server: Buffer Manager: Page writes/sec; and

(w) SQL Server Waits.

2.4 SQL Server Patch Management

SQL Server Management Service includes patch management of Microsoft SQL Server.

We will work with you to assess security and product patches as they are released to confirm their compatibility with your environment.

SQL Server patch management includes security and critical patches, but not SQL Server Version or Edition upgrades. If you are interested in these upgrades, please discuss with your Account Manager the possibilities to engage our Professional Services Team.

When patches are identified as required, patching is carried out using the following process:

(a) agreed list of patches to be deployed is signed off by you and your application partner;

(b) all patches are identified patches and are tested within your non-production environment prior to production deployment;

(c) Request for Change raised by us on your behalf. You then need to approve the change request, in order for the patch installation to be done during a pre-agreed maintenance window; and

(d) patches installed during the maintenance window.[2]

The only exception to the above is in the event of a known critical exploit. In such cases, we reserve the right to carry out emergency maintenance on the platform to address the exploit.

2.5 Patching Cancellation

We require seven (7) days' notice in writing to cancel and/or reschedule a slot. We reserve the right to charge you for rescheduling the patching task should they fail to notify as described.

2.6 SQL Server Database Backup and Recovery Management

As part of SQL Server Management Service, we will implement, monitor and manage an agreed backup schedule for named databases per physical or virtual server. Please cross-reference Section 6 for Exclusions.

The standard backup schedule is as follows:

(a) hourly transaction log backups retained for seven (7) days;

(b) daily full database backups retained for fourteen (14) days;

(c) weekly full database backups retained for two (2) months; and

(d) monthly full database backups retained for one (1) year.

We will troubleshoot any backup failures and also provide restore management. Requests to restore a specific database can be made through the Service Request process. Please refer to the Operations Manual for more detail on the Service Request process.

[2] Please refer to the Operations Manual in regards to Maintenance Windows for the SQL Server Management Service.

If you require a custom backup schedule, we will document in the runbook and implement this schedule during the configuration of the SQL Server Management Service.

Please note that sufficient space must be available on the server to store maintenance plan backups and transaction logs prior to backup by the offsite BaaS platform.

2.1.5 SQL Server Database Backup and Recovery Management on Microsoft Azure

All SQL server(s) deployed on Azure VM (IaaS) will be backed up using Azure Backup, unless agreed otherwise.

SQL Backup	IaaS	PaaS
Deployment	SQL Server on Azure VM	Azure SQL Database
Backup Solution	Azure Backup - Manually deployed	N/A – Automatically Enabled
Backup Storage	RA-GRS	RA-GRS
SQL Server versions and regions	As supported by Azure Backup	As supported by Azure SQL Database* *Latest stable version maintained by Azure
Standard Backup Retention Schedule	Hourly transaction log backup – seven (7) days Daily full database backup – fourteen (14) days Weekly full database backup – two (2) months Monthly full database backup – one (1) year	Full Backup – Every Week Differential Backup - Every twelve (12) hours Transaction Log Backup – Every ten (10) minutes Note: Retention period will vary based on model and package purchased.
Long-term Retention	Up to ten (10) years	Up to ten (10) years

2.7 Database Index and Statistics maintenance

SQL Server Management Service includes database maintenance, index maintenance and statistics maintenance to optimise database and query performance.

The standard maintenance tasks are as follows:

(a) daily database integrity check for database corruption;

(b) weekly index maintenance - rebuild or reorganise index dependent on the level of index fragmentation; and

weekly statistics update for query performance optimisation.

The above tasks can be adjusted (for regularity or tuning purposes) through a service request.

2.8 Capacity Management

As part of the SQL Server Management Service, we will monitor key capacity elements of your SQL Server deployment. This monitoring includes:

(a) storage (per logic volume) – customisable alerting above 80% (eighty percent) used disk space for a minimum of thirty (30) minutes; and

(b) database growth trend – to baseline and forecast database growth and adjust capacity accordingly.

Thresholds below this level can be configured in conjunction with a Statement of Work (SoW).

All alerts generated by the monitoring system will be raised as appropriate Priority levels based upon the type of alert. Please refer to the Operations Manual for further details regarding prioritisation of incidents.

2.9 SQL Server Onboarding

Existing SQL Servers being brought under Six Degrees' SQL Server Management Service will be subject to a consultancy review conducted by our Professional Services team. A remediation plan will be provided with appropriate actions. We reserve the right to refuse service if remediation is not funded or actions are not implemented within ninety (90) days. This remediation plan can be discussed on a case-by-case basis.

2.10 SQL Server Change Management

As part of the SQL Server Management Service, we will provide and implement change management within the SQL Server environments, implementing tasks including:

(a) secure regression;

(b) database refreshes;

(c) script execution[3]; and

(d) security access administration.

Change requests are limited to five (5) per month, with no rollover applicable. Change requests can be implemented outside of business hours with commercial agreement on a case-by-case basis.

Information requests will be treated as Change requests, with a consideration that if the change is deemed to take longer than four (4) hours, this change request will require commercial agreement, with up to a one (1) week turnaround after the purchase order has been provided.

Any change request that is not specifically listed above would be chargeable and would be completed by us on a time and materials basis.

2.11 Customer Third Party Support

[3] Reviewed on a case-by-case basis based upon Third Party / Application Partner responsibilities.

As part of the SQL Server Management Service, we will work with your third parties to assist with the troubleshooting and support of applications hosted on the named SQL Server in-line with supported hours and the incident severity level. This exercise is limited to the diagnosis of issues relating to Microsoft SQL Server. Query and index optimisation are outside of scope, and information provided will be on a best endeavours basis.

3. Service Implementation

After order acceptance, we will implement the Service as follows:

Service Implementation	Us	You
You provide the named Microsoft SQL Server instances for us to monitor;		●
We deploy a monitoring probe within your infrastructure;	●	
We configure SQL Server Management Service monitoring and backups;	●	
We carry out the initial SQL Server performance review;	●	
We update our CMDB and hand the service over to BAU.	●	

3.1 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 SQL Server Management 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).

4. Billing

The Service will be billed as Recurring Fees as described in the Billing Guide, and as indicated in your Order Form.

4.1 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).

5. Dependencies

5.1 Prerequisites

The following prerequisites are required to deploy SQL Server Management Service service(s):

(a) the physical or virtual server must have Server OS Management Service[4], unless it is architected as a SQL PaaS service on Microsoft Azure;

(b) a virtual server will be deployed to support the SQL monitoring agent within your infrastructure;

(c) a domain or local user account is required to run the monitoring service. This account must have permission to access all servers that are monitored;

(d) the appropriate firewall ports must be opened to allow Management Service monitoring;

(e) the service must be supported on Microsoft Windows servers running a version of Microsoft SQL Server that is supported by Microsoft;

(f) an account with the appropriate permissions to access and backup Microsoft SQL Server must be provided;

(g) SQL Server Database Backup and Recovery Management - as part of SQL Server Management Service, we will implement, monitor and manage an agreed backup schedule for named databases per physical or virtual server. Please note this service requires that you take the Six Degrees Backup as a Service (BaaS) to provide backup storage - please refer to the Backup as a Service (BaaS) Service Description for further details; and

(h) please note that sufficient space must be available on the Server to store maintenance plan backups and transaction logs prior to backup by the offsite BaaS platform.

5.2 Client Obligations - Patching

(a) It is your responsibility to ensure that the applications are functioning and performing as expected after a patching cycle, where the application or component support is not provided by us. Testing should be carried out by you within seventy-two (72) hours of patch implementation.

(b) We require seven (7) days' notice in writing to cancel and/or reschedule a slot. We reserve the right to charge you for rescheduling the patching task should you fail to notify as described.

6. Exclusions

(a) SQL server patch management - SQL Server Management Service includes patch management of Microsoft SQL Server, unless it is architected as a SQL PaaS service on Microsoft Azure - where Microsoft is responsible for maintaining the patch and version level.

[4] Please refer to the Server OS Management Service Description for more detail.

(b) Multiple backup schedules on the same SQL Server; and

(c) As part of the SQL Server Management Service, we will work with your third parties to assist with the troubleshooting and support of applications hosted on the named SQL Server in-line with supported hours and the incident severity level. This exercise is limited to the diagnosis of issues relating to Microsoft SQL Server. Query and index optimisation are outside of scope, and information provided will be on a best endeavours basis.

7. Definitions and Acronyms

7.1 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
Differential Backup	A type of data backup that saves only the difference in the data since the last full backup.
Geo	A Geo cluster in another geographic location.
GiB	Defined as 1,024MiB.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing services to that client.
Storage	Non-volatile media for storing files, databases, applications or virtual servers.
TiB	Defined as 1,024GiB.
vCPU	Or in the plural “vCPUs”: one or more virtual central processing unit(s) (CPUs) compatible with Intel x86 instruction sets.
vRAM	Virtual random-access memory used for real-time processing.

7.2 Acronyms

Acronym	Meaning
CMDB	Configuration Management Database
IaaS	At Time of Test
PaaS	Recovery Time Objective
RA-GRS	Read Access Geo-Redundant Storage is a storage account type in Microsoft Azure. Please reference here on the Microsoft website for more detail on storage account types.
Sec	second
SoW	Statement of Work
vCPU	Virtual Central Processing Unit
vRAM	Virtual Random-Access Memory

8. Operational Targets

Type 1	P1	P2	P3	P4
Response	30 mins	30 mins	1 hour	Next Business Day
Fix	4 hours	6 hours	8 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	• Total loss of service; or • Your service does not function and you are unable to access it. EXAMPLES: • SQL Server Offline; • SQL Server Agent: Offline; • SQL Analysis Services Offline; • SQL Server Cluster Failover; • SQL Availability Group Failover; • SQL Log Shipping Failure; • Windows: Offline; • SQL Alert for severity 21 – Fatal Error in Database Process; • SQL Alert for severity 22 – Fatal Error Table Integrity Suspect; • SQL Alert for severity 23 – Fatal Error Database Integrity Suspect; • SQL Alert for severity 24 – Fatal Error Hardware Error; • SQL Alert for severity 25 – Fatal Error; • SQL Alert for Error 823 – Read or Write Request Failure; • SQL Alert for Error 824 – Logical Consistency I/O Error; • SQL Alert for Error 825 – Read-Retry Required.	• Service impaired or degraded; • You are able to access or use your service, but it is performing at an unacceptable level. EXAMPLES: • SQL Server or Database performance issue; • Unable to access or use a specific SQL component.	• Minor service degradation; • A feature or function is not working; • There is a workaround, or you are able to utilise the service for the majority of its function. EXAMPLE: • Non-business impacting performance issues.	• Service Requests; • Non-Service affecting work and reports; • A required change or configuration alteration to a service. EXAMPLE: • Development database refresh.

9. Service Levels and Service Credits

SQL Server Management Service aligns to the Service Levels and related definitions for Enterprise Cloud or Public Sector Cloud, so please refer to the Enterprise Cloud Service Description or the Public Sector Cloud Service Description (where applicable for you) for details.

1. Service Overview

Active Directory Management Service is an add-on managed service for the management of your Active Directory. The Active Directory Management Service can be deployed:

(a) on-premise;

(b) within our Enterprise Cloud;

(c) within our Public Sector Cloud; and/or

(d) within Microsoft Azure Public Cloud platforms.

You can choose more than one item or a combination of multiple items from the list above. Your selection and any additional information will be specified in the Order Form. The Active Directory Management Service can be purchased at any time as an add-on to an existing infrastructure (as listed above).

A single Active Directory Management Service provides coverage for a single Active Directory forest.

All services include notification to you. Notifications will be sent to your nominated email address or distribution list that must be supplied when the Active Directory Management Service is implemented. Please cross-reference the Service Implementation section in this document.

2. Service Features

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

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	Essential	Advanced	Premium
Active Directory and DNS Monitoring	●	●	●
Active Directory Troubleshooting	●	●	●
GPO Management		●	●

Annual Active Directory Audit		●	●
Active Directory Continuous Auditing and Assessment			●
Azure Active Directory Connect Continuous Monitoring		◒	◒
ADFS Management		◒	◒
Group Policy Audit	○	○	○
Schema and Domain Functional Upgrades	○	○	○
Domain and Forest Functional Level Upgrades	○	○	○

Active Directory Management Service - Essential

2.1 Active Directory and DNS Monitoring

We monitor key Active Directory and DNS metrics. These metrics are as follows:

(a) **Availability** – Response to a bind request in less than five (5) seconds;

(b) **Service Monitoring** – Critical service failure on any Domain Controller. Monitored services include:

(i) AD DS;

(ii) DNS;

(iii) FRS;

(iv) DFSR;

(v) Windows Time;

(vi) Netlogon, and

(vii) KDC.

(c) **DNS** – DNS response in less than five (5) seconds from any Domain Controller;

(d) **DNS** – Consistent name resolution results across all AD DNS providers;

(e) **Replication Monitoring** – No replication failures on any Domain Controller in the previous twelve (12) hours;

(f) **Group Policy** – Group policy objects consistent across all Domain Controllers in the previous twelve (12) hours; and

(g) **Backup** – Successful Active Directory System State backups completed for seven (7) days.

If the above metrics are not matched, our monitoring system will automatically raise an alert as a Priority 2 incident. We will manage such incidents according to the process documented in our Operations Manual.

We will send notifications to your nominated email address or distribution list that you must supply when the Active Directory Management Service is implemented. Please refer to the Service Implementation section in this document for more information.

2.2 Active Directory Troubleshooting

The Active Directory Management Service includes full access to our Service Desk for troubleshooting Active Directory and DNS issues. You should raise issues through the standard operational process as defined in the Operations Manual. These items will be logged by the system and passed to our technical team for investigation.

Active Directory Management Service - Advanced

The Active Directory Management Service – Advanced includes all of the service features that the Active Directory Management Service – Essential has listed in Section 2.1 and Section 2.2, and the features listed below.

2.3 GPO Management

As an optional professional services engagement, we can complete an audit of your current group policy deployment. Following the audit, our consultants will review the current configuration and highlight areas of concern or recommend improvements. We will provide an estimate of the costs to rectify those areas. Please contact us to discuss your options and to coordinate the delivery of this optional item if you choose it.

2.4 Annual Active Directory Audit

With the annual active directory audit, we will highlight any area of concern and provide recommendations. The audit will cover the following:

(a) Stale user and computer accounts;

(b) OU Structure;

(c) High level Group Policy;

(d) Active Directory site configuration;

(e) Active Directory link configuration;

(f) Active Directory backup and restore process; and

(g) Active Directory change management process.

We will document and provide you with any recommendations arising from the audit. In addition, we will provide an estimate for professional services costs necessary to resolve the highlighted concerns.

Active Directory Management Service - Premium

The Active Directory Management Service – Premium includes all of the service features that both the Active Directory Management Service – Essential (listed in Section 2.1 and Section 2.2) and the Active Directory Management Service – Advanced (listed in Section 2.3 and Section 2.4) have in addition to the features listed below.

2.5 Active Directory Continuous Auditing and Assessment

As part of the Active Directory Management Premium service, we will deploy a tool to provide continuous auditing and monitoring of your Active Directory. We will work with you to define agreed criteria for the audit tool including:

(a) Frequency of Active Directory audits;

(b) Security policy definition;

(c) Compliance requirements;

(d) Audit trail and logging requirements; and

(e) Alert configuration for your notifications.

Once deployed, all alerts generated by the monitoring system will be automatically raised as Priority 2 incidents. We will investigate such alerts in-line with our standard operational process described in the Operations Manual.

This service covers up to ten (10) Active Directory Domain Controllers as standard. If you decide to increase this number, your selection and the relative charges will be documented in the Order Form. Please contact us if you wish to discuss your options.

2.6 Azure Active Directory Connect Continuous Monitoring

Please note that this feature is only available if you have purchased the Azure Active Directory Service, either from us or from another supplier. Please note that Microsoft Azure has different licensing options and, if you purchase it from another supplier, we will require you to select the tier most appropriate for the deployment of the Service features you need. More information about the licensing options can be found here:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect

2.7 AD FS Management

AD FS is an alternative method of providing a single sign-on authentication for Azure Active Directory services. For solutions where AD FS has been deployed, we have defined the following set of monitoring and support services associated with AD FS:

(a) Service Monitoring whether all AD FS services started correctly; and

(b) SSL Certificate due to expire.

Alerts will be raised as a Priority 2 incidents. We will manage such incidents according to the process documented in our Operations Manual.

Optional Items

2.8 Group Policy Audit

As an ***optional*** professional services engagement, we can complete an audit of the current Group Policy deployment. Following the audit, our consultants will review the current configuration and highlight areas of concern or recommendations where improvements can be made. Our professional services team will provide an estimate of the costs to rectify those areas. Please contact your Account Manager, nominated Client Service Manager or Sales Support to coordinate with our professional services team.

2.9 AD Schema and Domain Functional Upgrades

Available as an ***optional*** professional services engagement, we can carry out Active Directory Schema upgrades.

This engagement will be delivered through our standard change control process described in the Operations Manual and with a defined SoW covering the prerequisites required to successfully complete an AD Schema upgrade.

2.10 Domain and Forest Functional Level Upgrades

Available as an ***optional*** professional services engagement, we can carry out Active Directory domain and forest functional level upgrades.

This engagement will be delivered through our standard change control process described in the Operations Manual and with a defined SoW covering the prerequisites required to successfully complete a Domain or Forest functional upgrade.

3. Service Implementation

After order acceptance, we will implement the Service as follows:

Service Implementation - Essential	Us	You
You will provide the Active Directory forest details and connection information.		●
We will configure Active Directory Monitoring.	●	
We will send a test alert to confirm successful configuration of monitoring.	●	
We will update the CMDB and hand the service over to customer for BAU.	●	

Service Implementation - Advanced	Us	You

You will provide the Active Directory forest details and connection information.		●
We will configure Active Directory Monitoring.	●	
We will carry out the initial Active Directory audit.	●	
We will update the CMDB and hand the service over to customer for BAU.	●	

Service Implementation - Premium	Us	You
You will provide the Active Directory forest details and connection information.		●
We will agree the Active Directory auditing parameters with you.	●	
We will deploy enhanced monitoring tools within your infrastructure.	●	
We will carry out the initial Active Directory audit.	●	
We will update the CMDB and hand the service over to you for BAU.	●	

3.1 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 Active Directory Management Service is deployed. 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).

4. Billing

The Service will be billed as a Set-Up Fee and a Recurring Fee as described in the Billing Guide, and as indicated in your Order Form.

4.1 Additional Charges

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

(a) Implementation work carried out outside business hours;

(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);

(c) Multiple AD forests – the charges are per domain and we will charge you according to their number and, therefore, to the number of forests.

5. Dependencies

We will provide the Active Directory Management Service subject to the following dependencies:

(a) The Service is only supported on servers running a version of Microsoft Windows Server covered by Microsoft's Mainstream or Extended support.

5.2 Client Obligations

(a) If you have not purchased our backup service, you will be responsible for maintaining a backup of your AD and we will not be able to recover this data for you if there is an outage;

(b) You will manage any of your end-user administration requests;

(c) You must provide a nominated email address or distribution list for notifications before the Active Directory Management Service is implemented;

(d) You will be responsible for the implementation of split domain DNS configurations; and

(e) You will provide Active Directory administrative account details.

5.3 Prerequisites

(a) A prerequisite of the Active Directory Federation Service is that the current AD FS deployment is operating with no errors;

(b) For Azure AD Connect Service Health Monitoring Azure Premium licensing is required: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect.

6. Exclusions

(a) Custom schema extensions are not covered by this Service; and

(b) Management of Azure Active Directory (AD) Premium features is outside the scope of the Six Degrees Active Directory Management Service.

7. Definitions and Acronyms

7.1 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
Active Directory Forest	Top most logical container in an AD configuration that contains domains, users, computers, and group policies.
Active Directory Schema	Component containing formal definitions of every object class that can be created in an AD forest.

Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing services to that client.

7.2 Acronyms

Acronym	Meaning
AAD	Azure Active Directory
AD	Active Directory
AD DS	Active Directory Domain Services
AD FS	Active Directory Federation Service
BAU	Business as Usual
CMDB	Configuration Management Database
DCDiag	Domain Controller Diagnostic
DFSR	Distributed File System Replication
DNS	Domain Name Service
FRS	File Replication Service
GPO	Group Policy Object
KDC	Key Distribution Centre
OU Structure	Structure Organisational Unit Structure
SLL	Secure Sockets Layer
SoW	Statement of Work

8. Operational Targets

We require two maintenance windows per month from 22:00 to 02:00.

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	• Total loss of service or security breach; • Your service does not function, and you are unable to access it. EXAMPLES: • Unable to access a single or multiple domain' controllers; • Complete failure of Active Directory Authentication.	• Service impaired or degraded; • You are able to access or use your service, but it is performing at an unacceptable level. EXAMPLES: • Single domain controller failure, users are still able to authenticate; • Slow authentication or DNS/replication performance issues.	• Minor service degradation/warning from monitoring or non-impacting service issue; • A service feature or function is not working; • There is a workaround, or you are able to utilise the service for the majority of its function. EXAMPLE: • DNS failure on a single domain controller.	• Service requests; • Non-service affecting work and reports; • A required change or configuration alteration to a service or a technical query.

9. Service Levels and Service Credits

Active Directory Management Service aligns to the Service Levels and related definitions for Enterprise Cloud or Public Sector Cloud, so please refer to the Enterprise Cloud or Public Sector Cloud Service Description(s) (where applicable for you and as appropriate) for details.

1. Service Overview

Our Cloud Back-up Service provides back-up features such as file-level, disk-level application backups. Our Cloud Back-up Service provides back-up features such as file-level and M365 backups.

This Service is offered as a Managed Backup Service or Self-managed Service:

(a) If you procured the Managed Backup Service, Six Degrees will manage

(i) Reschedule or reconfigure backups

(ii) Suspend backups

(iii) Delete or remove backups

(iv) Configure new backups

(v) Restore from backups

(vi) Set-up or change backup configuration

we would also utilise a centralized web dashboard to provide reporting and monitoring.

(b) If you procure the Self-Managed Service, you will retain management responsibilities and self-serve your configuration, scheduling, retention, monitoring, reporting and encryption setup. Should you choose this model, you will be responsible for all activities related to management and recovery of your backups.

Your data will automatically be subject to de-duplication and compression, regardless of whether you are procuring our Self-Managed or Managed Backup Service. Depending on your data, this deduplication can achieve a ratio of up to 10:1 reduction.

All your backup data will be encrypted in transit and at rest using Advanced Encryption Standard (“AES”) with 128, 192, or 256-bit keys, with 256 being the default. This AES requires a user-defined password that we will store for managed customers and employs end-to-end encryption to secure data at the source before transmission and during storage. Please note that if you are procuring our Self-Manged Service, it will be your responsibility to create and safely store your AES password.

As a standard, all backed up data will be stored in a single UK data centre with internal redundancy. Any different region that we may agree with you will be documented in your Statement of Work (SoW).

Details of your Service will be included in your Order Form and/or SoW, including your choice of Managed Backup Service or Self-Managed Service and the associated Fees.

Our Cloud Back-up Service can be procured as a standalone or in conjunction with our Public or Private Cloud Service offering. Please see the relevant Service Description for further details.

2. Service Features

2.1 Cloud Backup Service

Our cloud backup platform includes the features listed in the table below. Please note that these features will be available for both the Managed Backup Service and Self-Managed Service.

Features	Description
File-level, disk-level and application backups.	The backup platform allows for backup and restoration of individual files, applications and folders.
Additional Backup workloads	This Service supports a range of workloads, including Mac, Windows, Linux and Microsoft 365
Local UK / International storage options	By default, data will be secured in UK-based cloud storage locations; however, international storage options may be available if required. Please contact us if you wish to discuss your options.
Flexible recovery options	The backup platform provides flexible recovery options, allowing you to restore to granular files.
Adjustable backup frequency for Microsoft 365	The backup platform offers options for automated daily backups, multiple daily backups, on-demand backups, and automatic new user detection.
Archive/ backup encryption	Encrypts backups using AES with 128-bit, 192-bit, or 256-bit keys, ensuring data security and compliance.
Incremental and differential backups	The backup platform allows you to adjust the frequency and type of your backups.
Immutable backups	Allows users to prevent data from being altered or deleted to mitigate the risk data loss due to accidental or malicious actions.
Deduplication	The backup platform automatically eliminates duplicate copies of repeating data to reduce storage requirements.
Standard monitoring and reporting	You will be able to view standard monitoring activities and reports on your backup service.
Group management for Microsoft 365	The backup platform will allow you to assign policies and tasks to multiple users within your Microsoft 365 environment.

3. Service Implementation

After order acceptance, we will implement the Service as follows:

4. Service Implementation of Cloud Back-up	Us	You
Self-Managed Backup Service		
We will send you a welcome pack.	•	
We will run internal acceptance tests to confirm your environment is ready.	•	
We will facilitate a training call on using the backup software and admin portal.	•	

4. Service Implementation of Cloud Back-up	Us	You
We will confirm the Ready for Service Date, send you the handover pack and commence billing for your Service.	•	
You will install the relevant agents, backup schedules and retention periods.		•
Managed Backup Service		
We will install the relevant agents, backup schedules and retention periods	•	
We will configure the backup schedule and retention for all Protected Servers.	•	
We will undertake initial backup and testing for all the Protected Servers.	•	
We will perform the acceptance test (including restore activity) and notify you of any issues that we identify (this process may involve your third party vendors).	•	
We will perform initial backup and confirm completion to you, then move to steady state incremental backups.	•	
We will confirm the Ready for Service Date, send you the handover pack and commence billing for your Service.	•	

4.1 Delivery phases

We will agree with you the details of the implementation process and the associated key milestones based on your requirements and document this process in your SoW.

3.2 Ready for service

The Ready for Service Date is the date when we (acting reasonably and properly) notify you that the implementation steps and testing 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 a Recurring Fee and Usage Fee from the Ready for Service Date as specified in your Order Form. There will also be a Non-Recurring Fee for each of the service implementation phases.

5.1 Pricing Models

(a) Per Workload model

This is the pricing model that we offer as a standard.

We will charge you a fixed Recurring Fee per Workload, and stored data in GB as specified in your Order.

Within this model, you commit to a monthly quota of storage for your backup data. If the quantity of backed up data exceeds your monthly storage commit, then any additional storage may not be backed up.

You will be notified when you are approaching, and reach your quota, and can increase your commit when necessary.

(b) Microsoft 365 per Seat Model

If you are procuring this Service to back up your Microsoft 356 environments, you can select this optional pricing model to pay a fixed Recurring Fee for each of your Microsoft seats (users).

(c) Per GB Model

We will charge you a fixed Recurring Fee for a specific GB monthly allowance (as specified in your Order Form).

Within this model, you commit to a monthly quota of storage for your backup data. If the quantity of backed up data exceeds your monthly storage commit, then any additional storage may not be backed up.

You will be notified when you are approaching, and reach your quota, and can increase your commit when necessary.

5.2 Additional Charges

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

(a) Any service request in excess of the monthly allowance set out in Section 6 below;

(b) Any change in your requirements occurring after the implementation of the Service and/ or outside the scope of this Service Description, which we will charge as a professional services engagement; and

(c) Any training that you require beyond the initial training courses that we provide as part of the Service implementation activities described at Section 3, which we will charge as a professional services engagement.

6. Service Operations

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

If you are procuring the Self-Managed Service, we will include information on our incident management process in your Welcome Pack.

Service Request Entitlement

A service request for this Service is defined as one (1) request of the following items:

Service Request	Self-Managed Service	Managed Backup Service

Reschedule or reconfigure backup		•
Suspend backup		•
Delete or remove backup		•
Configure new backup		•
Restore from backup		•
Set-up or change backup configuration		•
Portal account administration	•	•
Service availability faults	•	•

As standard, for managed customers we offer 5 services requests per month, with up to 5 changes within each service request permitted. This begins after signoff of initial configuration.

We can implement additional service requests as and when required for an additional Fee which will be defined in your Order Form or SoW. Although we may accept multiple requests on a single support ticket for administrative convenience, we will count each change requested on the same ticket as an individual service request.

We will implement standard service requests listed in the table above in accordance with the resolution times set out in Section 12 but, in any case, in no less that forty-eight (48) hours from receipt of the request. Please ensure to submit any urgent change, amendment or cancellation request at least forty-eight (48) hours prior the desired implementation date.

7. Termination

Upon termination of your Cloud Back-up Service, you have three options regarding your data:

(a) **Data deletion by default**: By default and unless otherwise agreed with you, we will delete your data upon termination of your Cloud Back-up Service, and ensure that no residual data remains on our servers. We will notify you prior to the deletion to give you the opportunity to secure your data before it is permanently removed.

(b) **Transfer to another provider:** Alternatively, you can engage with your replacement partner provider for the transfer and setup of your tenant . If you choose this option, we will use reasonable efforts to facilitate the transfer of your tenant, however you will remain responsible to coordinate with your replacement provider.

(c) **Bespoke professional services engagement:** If you wish to keep and restore some of your existing data, we can provide additional professional services (PS) to assist you with these activities. This option allows for tailored solutions if you have specific data retention and restoration needs. Our PS team will work with you to define the scope of the engagement, including the duration of data retention, specific data sets to be restored, and any additional requirements. Please note that bespoke professional services are subject to a separate Fee which will be based on the complexity and duration of the engagement.

8. Decommissioning Process

The decommissioning of the Service will follow the process below:

Cloud Back-up Platform Administration	Us	You
You will submit a termination request in accordance with your MSA. *Please note that early termination Fees may apply if you wish to cease your service during the Term.*		•
Managed - We will delete all backup agent software/proxy and related components on the source.	•	
Self-Managed - You will delete all backup agent software/proxy and related components on the source.		•
We will delete relevant backup data from our portal, including all backup and recovery schedules, immutable data and backups, encryption keys, and applicable backup data storage. *Please note that this process is irreversible once initiated.*	•	
We will delete your backup account from our Cloud Back-up platform. *Please note that this process is irreversible once initiated.*	•	

9. Dependencies

We provide Cloud Back-up Service subject to the following dependencies:

9.1 Client Obligations

(a) You will ensure that network connectivity from source to target is either procured through us or provided by you in the form of an internet facing connection;

(b) You will designate a project lead and a technical contact with the appropriate level of expertise to support the successful implementation and operation of the service;

(c) You will provide all information and configuration details that we may reasonably require to implement the Service;

(d) You will manage any of your third parties during the implementation and operation of the Service;

(e) For customers not on Six Degrees Enterprise Cloud, you will ensure that there is sufficient bandwidth capacity for the data to be backed up within your chosen backup windows;

(f) If you have selected the Self-Service Backup option, you will be responsible for ensuring that your personnel have the relevant technical skills to manage your backup process. We will only provide the initial training courses online as part of the implementation of the Service. We reserve the right to charge an additional Fee for any bespoke training requirement;

(g) Unless you have selected the Managed Cloud Back-up option, you will be responsible for your own encryption keys. Please note that if you lose your encryption keys, we will not be able to decrypt the backup data;

(h) Throughout the lifetime of the service, you will be responsible to ensure backup targets have sufficient resources (e.g. RAM, CPU, free disk space) for backups to succeed. Where we provide your selected backup target as part of a different service and you require additional capacity, you can increase the scope of that relevant service subject to an additional Fee; and

9.2 Service Dependencies

(a) The restore capability of the Service will only be available after an initial full backup of the data is completed.

(b) Because restores are implemented by the same agent that performs the backups, you will only be able to perform restores on the devices that you have on-boarded to this Service;

(c) The backup platform requires regular updates, during which time some features may be unavailable. We will use reasonable endeavours to minimise downtime as far as reasonably practicable;

(d) Please note that, if you are procuring Self-Managed Backups and you wish to elect for a ‘compliance mode’ deployment (which will provide a hard lockout to our access to your tenant settings and data), you will not be able to reverse this choice;

(e) It is possible to configure a retention period for backups. As a standard, our retention period is fourteen (14) days. This provides a "grace period" to recover deleted backups. Where you have chosen to opt for a retention period, that the Usage Fees associated to the data used for old backups will not decrease until the retention period has expired.

10. Exclusions

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

(a) If you procure our Self-Managed Service, we will not be responsible for any impact to your business due to incorrect configurations, maintenance, or lack of regular monitoring of your backup. We will use reasonable endeavours to escalate any issues that you may experience with the backup platform through 6DG to the relevant vendor, but note that no SLA or operational target will apply.

(b) The provision of full-OS ("bare-metal") restores is outside the scope of this Service. If you require us to provide such a restore, we will use reasonable endeavours to accommodate your request, but please note that no SLA or operational target will apply.

(c) We will not be responsible to perform backups or restores on any of your system that is no longer supported by the relevant vendor. In these instances, we will use reasonable endeavours to work with you to find an alternative resolution, but you remain ultimately responsible for ensuring that your systems are supported by the relevant vendor.

11. Definitions and Acronyms

11.1 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
GB	For the purposes of this document, particularly billing and reporting, a GB is 1,000,000,000 bytes (and does NOT denote a Gibibyte (GiB)).
Protected Server	A server included in the scope of your Service.
Protected Workload	A workload included in the scope of your Service (as set out in you Order Form). Examples of workloads which you may include in your backup plan are virtual machines (VMs), servers, workstations and laptops.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables, and/or timelines for providing services to that client.
Storage	Non-volatile media for storing files, databases, applications, or virtual servers.

11.2 Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
SoW	Statement of Work

12. Operational Targets

Type	P1	P2	P3	P4
Response	30 mins	60 mins	4 hours	Next Business Day
Fix	4 hours	8 hours	16 hours	5 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	An issue with the system being backed up/replicated via the Service that meets one of the following conditions, where there is concrete and convincing evidence that our Service is the reason for such problem: • The Cloud Backup portal is not accessible; or • There is substantial degradation of performance, the loss of data, access to the target backup platform or any other materially adverse effect to the source machine or the backup process.	An issue that meets all the following conditions: • It is not a P1 Incident; • It prevents the backup of multiple source machines, or a single source machine over three or more sequential failed backup attempts; and • There is no simple workaround that can enable the backup / replication of, and/or the creation of a replica of, the source workload.	A issue that meets all the following conditions: • It is not a P1 or P2 Incident; • The target backup platform is accessible and available; and • The service is no longer functioning in the way expected. NB: While data restores are P4 requests, failure to restore data due to technical issues with the server may be uplifted to a P3 Incident (or higher if it meets the other criteria).	• Data Restores • Service Requests • Non-service affecting work and reports • A required change or alteration to a service or a technical query • Account administration requests (including password change issues) • NB: Where a data restore is required to address an incident under a different Service, the restore will be done as part of that incident, not spun off to a P4 request under this Service.

Please note resolution of incidents related to hardware, software or bandwidth limitations is outside the scope of this Service. Any delay caused by your breach of the obligations set out in Section 9.1 or your failure to meet the dependencies listed in Section 9.2 is excluded from the calculation of our Operational Targets.

Please note that there are no Service Levels or Service Credits associated with the Cloud Back-up Service.

1. Service Overview

Our Disaster Recovery Management Service delivers IaaS and PaaS continuity management for onsite, our Enterprise Cloud, our Public Sector Cloud and Microsoft Azure offerings.

We provide managed support services for your geo-redundant DR site environments to recover them upon the failure of your primary infrastructure.

Tools utilized for DR Management Service might differ depending upon your scope and the chosen platform on which you want your disaster site to be located. Your choices will be specified in your DRP.

Detail regarding what is agreed for your site environment(s) is specified in your Disaster Recovery Plan ("DRP") created after order acceptance, please refer to Section 3.1.

2. Service Features

DR management Features	Included
Inter-cloud workload mobility and protection between replication sites.	●
Replication of workloads and failback between sites.	●
Target of standard RPO's of fifteen (15) mins and RTO's of four (4) hours. Shorter RTO's may be defined in your SoW if your architecture supports it.	●

3. Event Management

We include a 24x7 monitoring and alerting service:

(a) Replication

Role	Trigger	Threshold
Service availability	No Ping	Fifteen (15) minutes
RPO	Successful replication of your data to DR site	Twenty-four (24) hours
Capacity	>95%	Recurring

(b) Disaster

Role	Expected State
Disaster Invocation	DR Invocation is for your IT environment only. You cannot invoke DR for a subset of your virtual machines. We will follow the defined notification and invocation workflow as per your DRP. Our time for invoking DR starts if our engineers cannot resolve the issue to the underlying platform within the target resolution time defined in the relevant Service Description.

Event management alerts are for our internal use. Please refer to Section 2.3 (Proactive Break/Fix Support) in this document.

We may decline invocation of a disaster site if the engineer triaging the incident can resolve the issue within the four (4) hour RTO.

In the event that you choose to invoke DR and it is proven that the incident is not platform related, we reserve the right to charge you for the professional services engagement on a time and materials basis (as per our standard charges) to rectify.

3.2 Retention

(a) Private Cloud and Public Sector Cloud

Retention of your replicated data is set for four (4) hours after which the data is automatically deleted. Increased retention is available at an added cost for storage, please contact your Account Manager.

(b) Microsoft Azure

Retention of your replicated data is set for twenty-four (24) hours (at one (1) hour snapshots) after which the data is automatically deleted.

3.3 Proactive Break/Fix Support

We provide proactive support for the monitored services defined in Section 3(a) of this document.

Alerts generated on your monitored server(s) will be raised as Priority 2 level incidents and managed as defined in our Operations Manual. An automated alert will be sent to your nominated email address.

Incidents alerted on from the monitoring service defined in Section 3(a) will be resolved without notifying you unless the assigned engineer deems that the incident will affect your ability to operate the DR 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.

This document defines what we proactively monitor as a standard. If you require support outside of what is defined in this document, 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 within our standard escalation procedures, there might delays in response times and resolution of issues.

If you have an issue which generates alerts and you do not resolve it based upon our reasonable advice, we will disable alerting and cannot be held liable for any interruptions to your organisation.

3.4 Change Management

You may add or remove resources from your DRP at any time (you must contact us to do so). Changes to your DRP will be accompanied by an Order Form reflecting when revised resources are increased.

Any changes to your DRP will be considered out of scope and charged as a professional service on a time and materials basis.

Any additions or changes that may occur on your primary environment will automatically be added to the end of your Boot List until such time as your DRP has been updated.

When requesting new primary resources, you must explicitly ask for these resources to be replicated/added to the DRP.

3.5 Reporting

Following your annual Bubble Test, you will receive an invocation report detailing the results of the Bubble Test and any recommended remediation work required.

3.6 Capacity Management

Any resource adjustment at your primary site must be reflected in your DRP in order to ensure sufficient disaster site resources. We will issue a new Order Form reflecting the adjustment in your resources after you notify us of any changes.

3.7 Microsoft Azure

As Microsoft capacity manages Azure regions, no compute (CPU or RAM) DR resources can be reserved, nor do you pay for these resources in the DR site until invocation.

However, as disks do have a corresponding DR resource, these will be automatically updated when the “live” disk is updated, and we will pass through the corresponding cost to you.

3.8 Service Specific Deliverables

(a) Microsoft Azure

Where PaaS services or appliances are used by us or a third party to support the services in your Azure Platform, we will build an equivalent PaaS resource or appliance within the DR site.

We will ensure that these PaaS DR resources or appliances' configuration mirror their "live" counterparts at the point of service handover. If we make any changes to a "live" PaaS resource or appliance, will also change the DR PaaS service or appliance accordingly.

Where you make changes to these "live" PaaS resources or appliances, it remains your responsibility to ensure that the configuration is updated on the DR PaaS resources or appliances as well.

4. Service Implementation

Service Implementation	Us	You
You provide us target email address for alerts (optional).		●
We jointly complete the DRP.	●	●
We deploy management agents within your infrastructure.	●	
We configure monitoring and alerting for the resources in scope.	●	
We send test alert(s) to our Service Desk and confirm receipt.	●	
We update our CMDB and hand the service over to BAU.	●	
For Azure, we implement the agreed runbook and automation requirements (as indicated on your Order Form).	●	
We will complete a DR Test for implementation.	●	

4.1 Disaster Recovery Plan (DRP)

After order acceptance, we will we share our standard DRP with you. You must complete initial information required in order for us to jointly define it with you. The DRP includes an overview of your disaster recovery plan(s) and the objectives. The final version of the document is shared with you.

4.2 Ready for Service

The Ready for Service Date is the date when we (acting reasonably and properly) notify you that the disaster recovery site has been implemented and that the Service is ready for service. From this date you have fourteen (14) concurrent days to test the underlying DR Platform (which must be purchased separately) and notify us of any issues. If you consider that the Service is not ready for service on the date notified, you must notify us within the fourteen (14) day testing period, 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 Set-up Fees and/or Recurring Fees as defined in our Billing Guide, and as indicated in your Order Form.

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

6.1 Invocation

Invocation	Us	You
System outage ticket will be raised by our monitoring tool.	●	
Our engineers will triage incident for resolution.	●	
Our engineers will declare a disaster requiring DR.	●	
We will begin invocation procedures.	●	
You will start internal DR procedures as per DRP.		●
We will boot all servers to OS level with Boot List as per your DRP.	●	
You will confirm connection to servers.		●
We will execute test plans as per your DRP.	●	

6.2 Roll Back

Roll Back	Us	You
We will prepare the primary site.	●	
We will replicate data back.	●	
We will begin invocation procedures.	●	
You will start internal DR procedures as per your DRP.	●	
We will boot all servers to OS level with Boot List as per your DRP.		●
You will confirm connection to servers.	●	
We will execute test plans as per the DRP.		●

7. Dependencies

We provide DR Management subject to the following dependencies:

7.1 Prerequisites

(a) You must procure our Disaster Recovery Platform Service in order to use the DR Management Service;

(b) With the delivery of this Service, we will require you to complete our standardised DRP. We will provide the document to you as part of the Service Implementation activities.

(c) This service is offered as an additional service in conjunction with your Disaster Recovery Platform services which must be purchased separately.

7.2 Client Obligations - General

(a) We only provide Disaster Recovery Management Service for your full environment. DR target resources must be the same as the primary resources.

7.3 Client Obligations - Plans and Procedures

(a) You shall implement and maintain a response structure in your DRP that will enable timely warning and communication to us. The DRP will be shared jointly between us and you; it shall provide plans and procedures to manage your organization during a disruption. You shall follow the plans and procedures when required to activate business continuity solutions.

7.4 Client Obligations - Response Structure

(a) You shall implement and maintain a response structure, identifying one or more of your teams/persons responsible for responding to disruptions;

(b) The roles and responsibilities of each of your team/persons and the relationships between the teams shall be clearly stated in your DRP and you shall inform us if any of your team members should change.

7.5 Client Obligations - Warning and Communication

(a) You shall document and maintain your own internal procedures for communicating internally and externally to your relevant interested parties, including what, when, with whom and how to communicate.

7.6 Client Obligations - Recovery

(a) You must have documented processes submitted as part of your DRP to restore and return business activities from the temporary measures adopted during and after a disruption.

Please note that:

(i) The time to prepare your primary site is excluded from the calculation of the SLA;

(ii) The time to replicate back and restore a primary site is excluded from the calculation of the SLA; and

(iii) We will schedule failbacks at our discretion depending on our resource availability.

7.7 Testing

(a) You must implement and maintain a programme, agreed with us, of exercising and testing your environment to validate the effectiveness of the business continuity solution.

(b) We shall conduct exercises and tests that:

(i) are consistent with business continuity objectives agreed by both parties;

(ii) are performed once (1) per fiscal year and when there are significant changes within your IT infrastructure. These need to be planned at least one (1) calendar month in advance with us and require use of Runbooks and Boot Lists.

7.8 Service Dependencies - Server or Resource Management

(a) We will not provide any SLA for recovery of any virtual machine, PaaS service or appliance for which you have not contracted a corresponding management service from us.

7.9 Service Dependencies - Microsoft Azure

(a) Where you make changes to “live” PaaS resources or appliances, it remains your responsibility to ensure that the configuration is updated on the DR PaaS resources or appliances as well.

8. Exclusions

8.1 General

(a) Any services that are not listed in your DRP will not be covered as part of your Disaster Recovery Management Service;

(b) The data of any service that you remove from your disaster environment will not be kept and will not be retrievable;

(c) We only provide disaster recovery services for your full environment. DR target resources must be the same as the primary resources; and

(d) RPO’s are not guaranteed and will be affected by data change rate and available bandwidth.

8.2 Applications

(a) We will only guarantee the booting of your device to OS level;

(b) We do not boot any applications above the OS when we invoke your DR site, unless the application is managed by us (e.g. SQL, Citrix) and this must be specified in your DRP as part of your Boot List.

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
Boot List	Lists out all of the items to boot in your DR environment.
Bubble Test	
DRP	A Disaster Recovery Plan document which outlines what will be done for your environments as identified in your SoW when invoking a DR scenario (whether live or test).
DR Target	The target site for where your DR environment lives
Geo-redundant	The physical separation of data centres that span multiple geographic locations.
Invocation	An act of declaring that an organization’s business continuity arrangements need to be put into effect in order to continue delivery of key products or services.
Retention	The time period we keep replicated data
Runbook	A runbook for this Service is a compilation of the specific set of activities to be carried out to restore your services following downtime and must be included as part of your DRP.
Storage	Non-volatile media for storing files, databases, applications or virtual servers.

9.2 Acronyms

Acronym	Meaning
CMDB	Configuration management database
CPU	Central processing unit
DRaaS	Disaster Recovery as a Service
DR	Disaster Recovery
DRP	Disaster Recovery Plan
IaaS	Infrastructure as a Service
LLD	Low level design document
OS	Operating System
PaaS	Platform as a Service
RAM	Random-Access Memory
RTO	Recovery Time Objective
RPO	Recovery Point Objective
VM	Virtual Machine

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 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 or updates to your DRP; • Non-Service affecting work and reports; • A required change or configuration alteration to a service.

11. 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	Period	Target
RPO (Recovery Point Objective) average	Per Calendar month	Target < 15 Minutes
RTO (Recovery Time Objective) from point of invocation	Per event	Target < 4 Hours

1. Service Overview

We offer a cloud deployed, network device for the control of your outbound and inbound network traffic.

We offer three levels of this service: Essential, Advanced and Premium.

Additional information may be included in the Order Form or Statement of Work (SoW).

1.1 Essential Cloud Firewall

The Essential Cloud Firewall is a cloud firewall and an unmanaged NSX Edge based appliance available in the following sizes:

Appliance Size	FW Performance	IPSEC Tunnels	Total Routes
Compact	3Gbps	512	20,000
Large	9.7Gbps	1,600	50,000
Quad Large	9.7Gbps	4,096	250,000
X-Large	9.7Gbps	6,000	250,000

The core features supported by the Essential Cloud Firewall device are the following:

(a) NAT;

(b) DHCP;

(c) Site to Site VPN;

(d) SSL VPN;

(e) Layer 4/7 Load Balancing;

(f) High Availability (Single site); and

(g) Dynamic Routing.

The Essential Cloud Firewall can be managed through the vCloud Director Web interface or API for all configuration changes.

1.2 Advanced Cloud Firewall

The Advanced Cloud Firewall is a fully managed cloud firewall provided by a single vendor.

The appliance is available in the following sizes:

Appliance Size	FW Performance	IPSEC Tunnels	Total Routes
Small	200Mbps	250	5,000
Medium	2Gbps	1,000	5,000
Large	4Gbps	2,000	20,000
X-Large	8Gbps	4,000	64,000

The core features supported by this device are the following:

(a) NAT;

(b) DHCP;

(c) Site to Site VPN;

(d) SSL VPN;

(e) Threat Intelligence;

(f) URL Filtering;

(g) Remote Access VPN;

(h) High Availability (Single site);

(i) Syslog;

(j) App-ID;

(k) Dynamic Routing; and

(l) Managed.

1.3 Premium Cloud Firewall

Like the Advanced, the Premium Cloud Firewall is also a fully managed cloud firewall provided by a single vendor.

Premium includes:

(a) all of the functionality of the Advanced Cloud Firewall (listed above in Section 1.2); plus

(b) an additional second layer of protection from an alternative vendor cloud firewall.

The second firewall will be sized in-line with the sizing guidelines for the Advanced Cloud Firewall and is intended to provide a perimeter-based stateful firewall.

2. Service Features

The Service features are listed in the table below:

Feature	Essential	Advanced	Premium
High Availability	●	●	●
Stateful Inspection firewall	●	●	●
NAT	●	●	●
Site-Site IPSEC VPN	●	●	●
App-ID		●	●
Threat Intelligence		●	●
URL Filtering		●	●
Remote Access VPN		●	●
Perimeter Firewall			●

2.1 High Availability

The High Availability feature we offer with the Essential (or unmanaged) firewall consists of two appliances deployed within the same platform. An affinity rule is created by us to ensure the appliance remains on separate hosts within the cluster.

The two (2) appliances are configured by us as a cluster. In the event that the primary host is unavailable for fifteen (15) seconds, the NSX Edge service will failover to the second appliance.

The Advanced and Premium Firewall Service supports an active/passive high availability configuration, consisting of two (2) appliances deployed as a cluster within a single cloud platform. Once deployed, we configure the devices with High Availability. There are prerequisites for High Availability, including:

(a) An additional /30 link net subnet; and

(b) One interface from each appliance is used for cluster communications.

2.2 Stateful Inspection firewall

All cloud firewalls include stateful inspection capabilities; these ensure that all traffic passing through the firewall is matched against a specific security policy.

The security policies defined within the firewall are evaluated in a top to bottom sequence ensuring that the traffic matching the first rule with the closest definition in the list applies to that session.

2.3 NAT

All cloud firewalls include NAT capabilities that provide a method of remapping an IP address from the Public Internet to a Private IP address within the Cloud platform.

A range of address mapping options are supported, including static and dynamic mapping. These options would be defined in a low-level design document.

2.4 Site-Site IPSEC VPN

All Cloud firewalls support Site-Site IPSEC VPN services. The following IPSEC VPN functions are supported on all virtual firewalls:

(a) IKEv1 and/or IKEv2;

(b) Certificate authentication;

(c) Pre-shared key;

(d) AES (AES128-CBC);

(e) AES256 (AES256-CBC);

(f) Triple DES (3DES192-CBC);

(g) AES-GCM (AES128-GCM);

(h) DH-2 (Diffie–Hellman group 2);

(i) DH-5 (Diffie–Hellman group 5); and

(j) DH-14 (Diffie–Hellman group 14).

The Advanced and Premium Cloud firewalls support the following additional protocols:

(k) DH-19 (Diffie–Hellman group 19); and

(l) DH-20 (Diffie–Hellman group 20).

2.5 App-ID

Application Identification (or App-ID) is a mechanism responsible for identifying applications that traverse the firewalls independently of its port, protocol and encryption (SSL or SSH).

2.6 Threat Intelligence

The Threat Intelligence subscription provides you with integrated protection against network-borne threats (including exploits, malware, command and control traffic, and a variety of hacking tools) through IPS functionality and stream-based blocking of malware samples. This service allows you to monitor security alerts and events.

2.7 URL Filtering

URL Filtering provides you with granular, user-based controls over web activity through URL categories and customizable allow lists and deny lists, as well as protection from web-borne threats through malicious categories like malware and phishing.

The URL Filtering subscription utilizes an Internet-based URL database that automatically categorizes unknown URLs, providing you with the latest URL groupings based on current web page content. The definitions are updated automatically every thirty (30) minutes.

2.8 Remote Access VPN

Remote access VPN extends the protection of a firewall to endpoints both inside and outside a corporate network, in order to deliver consistent security to users in all locations.

Mobile devices can use remote access VPN apps for iOS and Android to connect to the corporate firewall. You can validate the state of the endpoint device as part of the context for your security policy using the Host Information Profile (HIP). You can also deploy Remote Access security subscriptions internally to protect local and wireless networks users.

This service would require a professional services engagement to design and implement the required protection policies.

2.9 Perimeter Firewall

The perimeter firewall option provides a second layer of protection from an alternative vendor cloud firewall outside of the primary Advanced Cloud Firewall. This option is intended to provide a second layer of stateful traffic filtering.

The perimeter firewall will be sized to match the primary Advanced Cloud Firewall deployment.

3. Service Implementation

After order acceptance, we will implement the Service as follows:

3.1 Essential Cloud Firewall

Service Implementation – Essential Cloud Firewall (e.g. Unmanaged Firewall)	Us	You
You sign off initial deployment configuration.		●
You confirm WAN, DMZ and LAN IP address ranges.		●
We deploy the appliance within your virtual network.	●	
We configure the appliance in line with the defined default configuration.	●	
We send you access details for the configured appliance and confirm you are able to connect.	●	
You confirm you are able to connect.		●
Update the CMDB and hand the service over to BAU.	●	

3.2 Advanced or Premium Cloud Firewall

Service Implementation – Advanced and Premium Cloud Firewall	Us	You
You sign off initial deployment configuration.		●

We deploy the Cloud Firewall solution within your virtual network.	●	
We configure the appliance in line with the defined initial deployment configuration.	●	
We confirm the configuration matches the requirements and obtain sign off from you.	●	
You sign off that the configuration matches the requirements.		●
Update the CMDB and hand the service over to BAU.	●	

3.3 Firewall Deployment and Configuration - Essential Cloud Firewall

For the Essential Cloud Firewall (a NSX Cloud Firewall) we will provision the firewall appliance with a default configuration consisting of the following:

(a) WAN Interface configured with the first useable public IP address;

(b) DMZ Interface configured with the first useable DMZ subnet IP address;

(c) LAN interface configured with the first useable LAN subnet IP address;

(d) All incoming traffic blocked; and

(e) Traffic allowed to the management interface from the LAN subnet.

3.4 Firewall Deployment and Configuration - Advanced Cloud Firewall

For the Advanced Cloud Firewall, we will deploy the firewalls based on the agreed initial deployment configuration defined during the post-sale engagement.

This configuration typically includes, but is not limited to, the following:

(a) WAN Interface configured with a public IP address;

(b) DMZ Interface configured with the first useable DMZ subnet IP address;

(c) LAN interface configured with the first useable LAN subnet IP address;

(d) Traffic allowed to the management interface from the LAN subnet;

(e) NAT rules configured as agreed in the initial deployment configuration; and

(f) Firewall policies configured as agreed in the initial deployment configuration.

Once the initial deployment configuration has been completed, you will sign off the initial deployment. Any future configuration changes will follow the standard change management or request for change process defined in the Operations Manual.

Configuration beyond the standard deployment detailed above, in particular for advanced features such as URL filtering or Remote Access VPN's, requires a Professional Services engagement as detailed in your SoW.

3.5 Firewall Deployment and Configuration - Premium Cloud Firewall

For the Premium Cloud Firewall, we will deploy the firewalls based on the agreed initial deployment configuration defined during the post-sale engagement.

This configuration typically includes, but is not limited to, the following:

(a) WAN Interface configured with a public IP address;

(b) DMZ Interface configured with the first useable DMZ subnet IP address;

(c) LAN interface configured with the first useable LAN subnet IP address;

(d) Traffic allowed to the management interface from the LAN subnet;

(e) NAT rules configured as agreed in the initial deployment configuration; and

(f) Firewall policies configured as agreed in the initial deployment configuration.

Once the initial deployment configuration has been completed, you will sign off the initial deployment. Any future configuration changes will follow the standard change management or request for change process defined in the Operations Manual.

3.6 Firewall Management - Essential Cloud Firewall

The Essential (or NSX) Cloud Firewall appliances are fully managed by you and any changes to the configuration can be made through the vCloud Director interface or API. In the event the device becomes unavailable following a configuration change, you can raise a service ticket to request that the issue is investigated by our Support Team. Please refer to the Operations Manual for more information.

3.7 Firewall Management – Advanced and Premium Cloud Firewall

The Advanced or Premium Cloud Firewall are fully managed devices. So, you do not have access to manage or configure these devices. Upon request, you can be granted Read Only access to the web interface of the firewall in order to view the current configuration or any logging information.

If you require a configuration change, please raise a service request following the standard procedures detailed in our Operations Manual. Configuration changes are limited to five (5) changes per month following signoff of the initial configuration. All firewall configuration changes will follow our request for change process and must be submitted by your authorised contact.

As an example, the following list of items defines actions considered as one (1) change:

(a) Adding, deleting, or modifying up to three (3) individual Network Address Translations (NAT) (incoming, outgoing and loop-back) including object creation;

(b) Adding, deleting, or modifying up to two (2) access control list changes (such as permit or deny changes), including the creation of up to six (6) policy objects listed below:

(i) Hosts,

(ii) Groups,

(iii) Networks,

(iv) Ranges, and

(v) Service objects;

(c) Adding, deleting, or modifying up to two (2) individual network routes within the firewall; and

(d) Adding, deleted or modifying URLs for URL filtering.

Standard changes may be comprised of one of the above bullet points.

Any change request that is not specifically listed above would be chargeable and would be completed by us on a time and materials basis. If you wish to upgrade to a higher capacity firewall appliance, please contact us to place a new order and we will work with you to schedule the firewall appliance upgrade at an appropriate time.

3.8 Firewall Monitoring - Essential Cloud Firewall

In the Essential Cloud Firewall, we do not monitor the NSX Edge Firewall appliances for device availability. If the device becomes unavailable, please raise a service ticket as defined in the Operations Manual and your request will be investigated by our support team according to the process detailed there as well.

3.9 Firewall Monitoring – Advanced and Premium Cloud Firewall

The Advanced and Premium Cloud Firewalls are monitored for the following triggers:

(a) Device Status – based on no ping or SNMP response for fifteen (15) minutes;

(b) vCPU/CPU – above 95% usage for fifteen (15) minutes;

(c) vRAM/RAM – above 95% usage for fifteen (15) minutes; and

(d) Disk Space – less than 10% free for one (1) hour.

All alerts generated by the monitoring system are raised as Priority 2 level incidents. Please refer to the Operations Manual for the prioritisation of incidents.

3.10 Software and Patch Management

We will maintain and manage the appliance. Patching of the firewall appliances will be carried out in line with our platform patching patch management policy that is available in your portal at http://my.6dg.co.uk.

In the event of a critical exploit, we reserve the right to carry out emergency maintenance on the platform to address the exploit.

3.11 Edition/Capacity Upgrades

Where you wish to upgrade to a higher capacity firewall appliance, this request should be raised with your Account Manager as a new order. We will then work with you to schedule the firewall appliance upgrade at an appropriate time.

3.12 Managed WAN/MPLS Termination

The Cloud Firewalls listed in the document are intended as gateway appliances for cloud infrastructure. For connectivity to a Managed WAN/MPLS network, clients must purchase a Virtual Point to Point port. Please refer to our Virtual Point to Point Service Description for more information.

For solutions requiring centralised Internet breakout, you must purchase a firewall from our Connectivity portfolio, so please refer to the Next Generation Firewall (NGFW) Service Description for more information.

3.13 Logging

We will maintain the following logs for our Cloud Firewalls:

Item	Platform	Retention
All Logs	Enterprise Cloud	Thirty (30) Days
All Logs	Public Sector Cloud	Three (3) Years
All Logs	Public Cloud	Thirty (30) Days

3.14 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 firewall 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).

4. Billing

The Service will be billed as Recurring Fees as defined in the Payment and Billing Guide, using the definition of the Ready for Service Date in Section 3.14 of this Service Description, and as identified in your Order Form.

4.1 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).

5. Dependencies

We provide Backup as a Service subject to the following dependencies:

5.1 Prerequisites – High Availability

There are prerequisites for High Availability, including:

(a) One interface from each appliance is used for cluster communications.

5.2 Client Obligations

(a) 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;

(b) You will provide us with all of the information needed to complete the configuration of the Service; and

(c) You will need to provide a comprehensive list of business applications, requirements and features to deploy and, where appropriate, a previous firewall configuration document.

6. Definitions and Acronyms

6.1 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
DHCP	Dynamic Host Configuration Protocol is a network management protocol used on Internet Protocol (IP) networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.

Diffie-Hellman	Diffie-Hellman key exchange is a method of digital encryption. It is also called exponential key exchange. It uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted.
NAT	Network Address Translation translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet.
Site to Site VPN	A site to site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network like the internet.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing services to that client.

6.2 Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
DHCP	Dynamic Host Configuration Protocol
IPSEC VPN	Internet Protocol Security Virtual Private Network
NAT	Network Address Translation
SSL	Secure Sockets Layer
SSL VPN	Secure Sockets Layer Virtual Private Network
SNMP	Simple Network Management Protocol
VPN	Virtual Private Network

7. Operational Targets

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	• Total loss of cloud firewall service. • Total loss of access to the Internet	• Performance issues.	• Service Available with a non-service affecting issue.	• Service requests; • Non-service affecting work and reports; • A required change or configuration alteration to a service or a technical query.

8. 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 the Billing Guide).

Service	Measurement	Period	Target	Service Level	Service Credit
Cloud Firewall (Single)	Positive TCP port response on the management interface port 443.	Calendar Month Calendar Month	99.99%	99.89% - 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
Cloud Firewall (High Availability (HA))	Positive TCP port response on the management interface port 443.	Calendar Month 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

1. Service Overview

We provide a range of load balancer services, which we categorise as follows:

(a) Essential: an unmanaged load balancer - an NSX Edge based appliance[1];

(b) Advanced: a managed Advanced load balancer using a single vendor load balancer solution; or

(c) Premium: a managed load balancer using a single vendor load balancer solution with enhanced features and scaling.

The Service we provide you will be as specified on your Order Form. Additional information may be included in the Order Form or a Statement of Work (SoW).

2. Service Features

The Cloud Load Balancer features are listed in the table(s) below for each respective variant. Optional items are available for an additional fee. Your selection will be specified in the Order Form.

Feature	Essential	Advanced	Premium
Layer 4-7 Load Balancing	●	●	●
Server Health Checking	●	●	●
Reverse Proxy		●	●
SSL Offload		●	●
Global Server Load Balancing		●	●
Compression and Caching		●	●
High Availability		●	●
Web Application Firewall		●	●
Application DDoS Protection			●
Single Sign-on			●
Managed		●	●
Unmanaged	●		

[1] This offering is an option for Six Degrees' Public Sector Cloud and is not applicable to Six Degrees' Enterprise Cloud.

2.1 Essential Load Balancer

The Essential load balancer is available in a range of sizes and is provided as an unmanaged appliance. The Essential load balancer is deployed using a feature of the underlying NSX Edge based firewall appliance. The sizing of this appliance is aligned with the deployed NSX Edge firewall appliance.

Appliance Size	Application Service per Load Balancer	Pools per Load Balancer
Compact	64	64
Large	64	64
Quad-Large	64	64
X-Large	1,024	1,024

The core features supported by this device include:

(a) Layer 4-7 load balancing; and

(b) Server Health Checking.

The Essential load balancer can be managed through the vCloud Director Web interface or API for all configuration changes.

2.2 Advanced Load Balancer

The Advanced load balancer appliance is a scalable virtual appliance. As standard the appliance is deployed with the following specifications:

(a) vCPU - 2;

(b) RAM – 2GB; and

(c) Storage – 25GB.

The appliance supports up to eight (8) network interfaces. The core features supported by this device include:

(a) Layer 4-7 load balancing;

(b) Server Health Checking;

(c) Reverse Proxy;

(d) SSL Offload;

(e) Global Server Load Balancing;

(f) Compression and Caching;

(g) High Availability; and

(h) Web Application Firewall (Optional).

2.3 Advanced Load Balancer - Layer 4-7 Load Balancing

The core feature of the Advanced load balancer is providing Layer 4-7 load balancing. This functionality includes the following features:

(a) IP and port-load balancing rules including a wide range of criteria;

(b) Server pools;

(c) Application specific (Layer 7) redirection rules;

(d) Inline content rewrite;

(e) User authentication; and

(f) Geo-location detection.

2.4 Advanced Load Balancer - Server Health Checking

As part of the load balancing functionality the Advanced load balancer can perform server health checks of the target servers to ensure availability.

Based on the response to these checks the appliance can redirect traffic to alternative servers.

2.5 Advanced Load Balancer - Reverse Proxy

The Advanced load balancer includes Reverse Proxy functionality, this enables incoming client connections to be terminated on the appliance whilst separate connections are sent to the back-end servers.

In this scenario the clients never connect directly to the internal back-end servers.

2.6 Advanced Load Balancer - SSL Offload

The Advanced load balancer provides the ability to decrypt SSL traffic within the appliance and send unencrypted traffic to the back-end servers, this reduces the load on the servers delivering applications services.

2.7 Advanced Load Balancer - Global Server Load Balancing

In addition to the core load balancing functionality, the Advanced load balancer also supports Global Server Load Balancing across multiple geographically diverse platforms. This provides a DNS based system that can support resiliency for platforms across multiple geographic locations as well as the ability to route traffic based on the source location.

2.8 Advanced Load Balancer - Compression and Caching

The Advanced load balancer supports optional content compression and caching, this can optionally compress Web content during deliver to the end point providing improved performance.

The Content Caching functionality uses configurable profiles to cache content within the Load Balancer appliance reducing the load on back-end servers.

2.9 Advanced Load Balancer - High Availability

The Advanced load balancer supports both Active-Active and Active-Passive clustering solutions to support highly available load balancing solutions.

2.10 Advanced Load Balancer - Web Application Firewall

The Advanced load balancer incorporates optional Web Application Firewall capabilities. This includes the following features:

(a) HTTP protocol protection;

(b) Real-time deny list lookups;

(c) HTTP denial of service protections;

(d) Generic web attack protection; and

(e) Error detection and hiding.

2.11 Premium Load Balancer

The Premium load balancer appliance is a scalable virtual appliance, as standard the appliance is deployed with the following specifications:

(a) vCPU - 1;

(b) RAM – 2GB; and

(c) Storage – 10GB.

The core features supported by this device include:

(a) Layer 4-7 load balancing;

(b) Server health checking;

(c) Reverse proxy;

(d) SSL offload;

(e) Global server load balancing;

(f) Compression and caching;

(g) High Availability;

(h) Web application firewall;

(i) Application DDoS protection; and

(j) Single sign-On.

The core features are identical to the Advanced Load Balancer with the addition of the following functionality outlined in the sub-sections below.

2.12 Premium Load Balancer - Application DDoS Protection

The Premium Load Balancer includes capability to provide Application level DDoS protection, this functionality is designed to protect against DDoS based attacks that mimic legitimate applications requests but are designed to overload the target CPU or memory.

2.13 Premium Load Balancer - Single Sign-On

The Premium Load Balancer incorporates identity federation to support multi-factor authentication and single-sign with external identify services. Support identity services include:

(a) Microsoft Azure AD and Active Directory;

(b) Okta;

(c) Cisco; and

(d) Gemalto.

2.14 Advanced and Premium Load Balancer - 24x7 Monitoring and Alerting

For the Advanced or Premium Load Balancer, by default we offer a 24x7 monitoring and alerting service[2]. Your selection will be specified in your Order Form.

In the event an alert requires additional resource or other items authorised by you, we reserve the right to disable alerting for that threshold if the recommended solution is not authorised. If you have an issue which generates alerts, if you don't resolve it based upon our advice, we will disable alerting.

Alerts generated by the monitoring system will be raised as Priority 2 level incidents and triaged by our support team, during triage the incident Priority may be adjusted subject to the incident classification as per the Operations Manual.

The service includes the following monitoring and alerting:

[2] 24x7 Monitoring and Alerting is not available with our Essential Load Balancer as it is an unmanaged service.

(a) Appliance Status – based on no ping or WMI response for five (5) minutes;

(b) vCPU/CPU – above 95% usage for fifteen (15) minutes;

(c) vRAM/RAM – above 95% usage for fifteen (15) minutes; and

(d) Disk Space – less than 10% free for one (1) hour.

3. Service Implementation

After order acceptance, we will implement the Service as follows:

3.1 Essential Load Balancer Implementation

Service Implementation of an Essential Cloud Load Balancer	Us	You
Send Welcome Pack and Technical Data Capture form to you.	●	
Complete and return Technical Data Capture form to us.		●
Confirm projected Ready for Service Date.	●	
Configure Essential Cloud Load Balancer appliance as per agreed deployment configuration	●	
Provide access to the Essential Cloud Load Balancer via vCloud Director	●	
Confirm you have access to the Essential Cloud Load Balancer		●
Confirm 'Ready for Service', send Cloud Load Balancer handover pack and billing commences.	●	

3.2 Advanced or Premium Load Balancer Implementation

Service Implementation – Advanced and Premium Cloud Firewall	Us	You
Send Welcome Pack	●	
Finalise initial configuration as per the SoW	●	
You to sign off the initial configuration		●
Confirm projected Ready for Service Date.	●	
Configure Advanced or Premium Cloud Load Balancer appliance as per agreed deployment configuration	●	
Confirm 'Ready for Service', send Cloud Load Balancer handover pack and billing commences.	●	

4. Service Operations

4.1 Load Balancer Deployment and Configuration - Essential

For the Essential Load Balancer, we will provision the appliance with a default configuration as follows:

(a) WAN Interface configured with the 1st useable public IP address;

(b) LAN interface configured with the 1st useable LAN subnet IP address; and

(c) Traffic allowed to the management interface from the LAN subnet.

4.2 Load Balancer Deployment and Configuration - Advanced and Premium

For the Advanced or Premium Load Balancer, we will deploy the load balancers based on the agreed initial deployment configuration defined in the high-level design.

This configuration would typically include, but is not limited to, the following:

(a) WAN Interface configured with a public IP address,

(b) LAN interface configured with the 1st useable LAN subnet IP address, and

(c) Traffic allowed to the management interface from the LAN subnet.

Once the initial deployment configuration has been completed, you will sign off the initial deployment. Any future configuration changes will follow the standard change management process as defined in the Operations Manual.

4.3 Load Balancer Management - Essential

In the Essential Load Balancer, NSX load balancer appliances are fully managed by you. Changes to the configuration can be made through the vCloud Director interface or API.

In the event the device becomes unavailable following a configuration change, you can raise a service ticket to request that the issue is investigated by our Support team. Please refer to the Operations Manual for more information.

4.4 Load Balancer Management - Advanced and Premium

The Advanced Load Balancer or the Premium Load Balancer are both fully managed devices; therefore, you do not have access to manage or configure these devices.

Configuration changes for Cloud load balancers should be raised as Service Requests following the standard operational procedures and our change management process – please refer to the Operations Manual. Configuration changes are limited to five (5) changes per month following signoff of the initial configuration.

The following are examples that will be treated as one (1) change:

(a) Modify a single load balancing rule; and

(b) Modify a single Web Application firewall rule.

Standard changes may be comprised of one or more of the above bullet points. Any change request that is not specifically listed above would be chargeable and would only be completed by us on a time and materials basis.

4.5 Software and Patch Management

We provide ongoing maintenance and management of the appliance. All patching is carried out according to the following process:

(a) Scan of the device to identify missing Critical and Security patches;

(b) All patches are identified patches that are tested within our lab environment prior to production deployment;

(c) A Request for Change (RFC) is raised internally - to approve patch installation during a pre-agreed maintenance window; and

(d) Patches are installed during the maintenance window.

The only exception to the above list will be in the event of a known critical exploit. In the event of a critical exploit being identified, we reserve the right to carry out emergency maintenance on the platform to address the exploit.

4.6 Edition/Capacity Upgrades

Where you wish to upgrade to a higher capacity Cloud load balancer appliance, this request should be raised with your Account Manager as a new order. We will then work with you to schedule the appliance upgrade at an appropriate time.

4.7 Logging

We will maintain the following logs for our Cloud Load Balancers:

Item	Platform	Retention
All Logs	Enterprise Cloud	Thirty (30) Days
All Logs	Public Sector Cloud	Three (3) Years
All Logs	Public Cloud	Thirty (30) Days

4.8 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 your Cloud Load Balancer 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 as defined in the Billing Guide, using the definition of the Ready for Service Date in section 4.8 of this Service Description and as identified in your Order Form.

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. Dependencies

We provide Backup as a Service subject to the following dependencies:

6.1 Client Obligations

(a) You will designate a project lead and a technical contact with the appropriate level of expertise to support the successful implementation and operation of the service;

(b) You will provide all information and configuration details to onboard the service. We reserve the right to amend the fees and/or contract should you require any changes from the initially agreed contract; and

(c) You will manage any third-party activities during the implementation and operation of the service.

7. Exclusions

(a) 24x7 Monitoring and Alerting is not available with our Essential Load Balancer as it is an unmanaged service. If you want 24x7 Monitoring and Alerting, please purchase and refer to our Advanced Load Balancer or Premium Load Balancer in Section 2.14.

8. Definitions and Acronyms

8.1 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
NAT	Network Address Translation translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet.
NSX	VMware NSX is a virtual networking and security software product family created from VMware's vCloud Networking and Security (vCNS) and Nicira's Network Virtualization Platform (NVP) intellectual property.
Site to Site VPN	A site to site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network like the internet.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing services to that client.

WMI	Windows Management Instrumentation (WMI) is a set of specifications from Microsoft for consolidating the management of devices and applications in a network from Windows computing systems. WMI provides users with information about the status of local or remote computer systems.

8.2 Acronyms

Acronym	Meaning
DHCP	Dynamic Host Configuration Protocol
IPSEC VPN	Internet Protocol Security Virtual Private Network
NAT	Network Address Translation
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
SSL VPN	Secure Sockets Layer Virtual Private Network
VPN	Virtual Private Network
WMI	Windows Management Instrumentation

9. Operational Targets

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	• Total loss of load balancer service	• Performance issues.	• Service Available with a non-service affecting issue.	• Service requests; • Non-service affecting work and reports; • A required change or configuration alteration to a service or a technical query.

10. 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 the Billing Guide).

Service	Measurement	Period	Target	Service Level	Service Credit
Cloud Load Balancer (Single)	Positive TCP port response on the management interface port 443.	Calendar Month Calendar Month	99.99%	99.89% - 99.5%	5% of monthly value of Recurring Fees
				99.49% - 99.0%	10% of monthly value of Recurring Fees
				98.99 – 98.0%	15% of monthly value of Recurring Fees
				97.99 – 96.0%	20% of monthly value of Recurring Fees
				Less than 96.0%	25% of monthly value of Recurring Fees
Cloud Load Balancer (High Availability (HA))	Positive TCP port response on the management interface port 443.	Calendar Month Calendar Month	99.99%	99.98% - 99.5%	5% of monthly value of Recurring Fees
				99.49% - 99.0%	10% of monthly value of Recurring Fees
				98.99 - 98.0%	15% of monthly value of Recurring Fees
				97.99 - 96.0%	20% of monthly value of Recurring Fees
				Less than 96.0%	25% of monthly value of Recurring Fees