Microsoft Cloud Proactive Care

Powered by Umbrellar Cloud Operations

Service Description

Contents

1 Description

1.1 What is a Service Description?

The Umbrellar Service Description defines the services offered and specific conditions for each of these Services. This document forms part of our General Terms and Conditions. The overall terms comprise:

a) Sales Proposal including a Schedule of Services purchased or a signed Master Services Agreement
b) Umbrellar Service Descriptions detailing the conditions of Services purchased
c) General Terms and Conditions

1.2 Service Descriptions

The below service descriptions define the elements delivered as part of the contracted products. This will include the inclusions, exclusions, service levels, product options and associated support model.

2 Document Information

2.1 Document History

This document has been through these revisions:

Date	Status	Version	Edited by	Description for Changes
26/09/2018	Approved	1.0	ILK/DG	Initial version
19/11/2018	Updated	1.1	ILK	New Branding, minor changes to Account Review
04/12/2018	Updated	1.2	ILK	Removed “The Parties” section
17/05/2019	Approved	2.0	ILK	Merged Azure and Umbrellar Cloud Proactive Care and updated to align with Azure Managed Services Practise
21/05/2019	Updated	2.1	ILK	Added section 5.1.2.3 and section 4.1.3
06/08/2019	Updated	2.2	ILK	Incorporated SLA’s into Proactive Care
13/08/2019	Updated	2.3	ILK	Proactive Care Basic Offering
30/10/2019	Updated	2.4	DH	SLA Update and Formatting
26/08/2021	Updated	2.5	AV	Update and refresh content
10/05/2022	Updated	3.0	AV	Branding and content refresh
11/05/2022	Updated	3.1	AV	Redesign of Criticalities for IaaS

3 Microsoft Cloud Proactive Care

3.1 What is Microsoft Cloud Proactive Care?

1. Umbrellar's Microsoft Cloud Proactive Care is a proactive service level agreement for Azure and Umbrellar Cloud powered by Azure Stack Services.
2. The Service Level Agreement applies on an account basis.
3. Microsoft Cloud Proactive Care applies on a per solution / subscription basis. A solution can include one or more subscriptions.
4. A server, solution or subscription can either be managed or unmanaged. NOTE: Unmanaged devices need to be placed in a separate subscription in Azure.

Support Level Tasks	Detail
Support	
Umbrellar Portal (mycsp.io)	✓
Customer Service	Business hours access to Customer Service
Technical Support	Business hours access to Support Engineers via email, phone and online 24x7 access to Support Engineers via call-out
Microsoft Premier Support (Critical and Essential SLA)	✓
Who Can Open Cases	unlimited contacts / unlimited cases
Third-Party Software Support	Interoperability & configuration guidance and troubleshooting
Incident Priority & Initial Response time SLAs	✓
Managed Services Onboarding	
Documentation	✓
Resource Classification	✓
Ongoing Service Management	
Network Management (Azure platform networking)	✓
Managed Firewall Service	Selected from approved list of Sophos, Azure WAF or FortiGate virtual devices
Platform monitoring and alerting	✓

Virtual machine monitoring, alerting and uptime	✓
Advanced Monitoring – Application level	Optional
Backup management (monitoring & alerting)	✓
Backup restores	Optional
Managed Antivirus	Optional
Azure Advisor Recommendations	Optional (SDM Module)
Operating System patching	✓
SSL Certificate Management	✓ (Refer to Section 7.10)
Incident Management	✓
Change Management	✓
Umbrellar Expertise	
Service Delivery Manager	Selectable as a module

1. Call Out is defined as our teams being available outside of Business hours for response. Our call out team are raised by system alerting or inbound incidents being raised through available phone channels. Support requests that qualify for call outs are defined as part of service criticality entitlements.
2. Umbrellar requires full access to the environment in order to provide any of the above proactive care plans.
3. Umbrellar will not be responsible for any changes made by the customer.
4. Umbrellar must be informed of any changes made by the customer that could affect the stability of the environment or could result in system alerts.

4 Umbrellar Support

4.1 Umbrellar Portal

As an Umbrellar CSP customer, everything related to Azure subscription(s) purchased through Umbrellar can be accessed via the Umbrellar Portal:
https://portal.mycsp.io

The Umbrellar Portal provides:

- Access to manage linked azure subscription(s)
- Purchase new subscriptions and services
- Manage users and view invoices and payment history

4.2 Premier Support

As part of signing up as an Umbrellar CSP customer, Umbrellar is the sole point of contact for supporting Umbrellar Cloud powered by Azure Stack and Azure platform. Umbrellar has a strategic relationship with Microsoft. The customer will be able to leverage this relationship for any reactive and/or proactive technical escalations to Microsoft. Umbrellar will do so on the customers behalf by leveraging Umbrellar's Microsoft Partner Premier Support agreement.

4.3 Priority Levels & Response Times

The following table sets out Umbrellar's priority level definition as well as Umbrellar and Customer expected responses.

Priority	Customer's situation	Expected Umbrellar Response	Expected Customer Response
1	**Critical business impact:** • Customer's business has significant loss or degradation of services • Needs immediate attention	**Initial response:** • 30 minutes • Continuous effort all day, every day	• Allocation of appropriate resources to sustain continuous effort all day, every day • Accurate contact information on case owner • Expectation is that Customers notify Umbrellar via a telephone call
2	**Moderate business impact:** • Customer's business has moderate loss or degradation of services, but work can reasonably continue in an impaired manner. • Needs attention within 2-4 business hours	**Initial response:** • 30 minutes (Business Hours) • Business hours effort.	• Allocation of appropriate resources to sustain continuous business effort • Accurate contact information on case owner
3	**Minimum business impact:** • Customer's business is substantially functioning with minor or no impediments of services. • Needs attention within 4-8 business hours	**Initial response:** • 1 business day	• Accurate contact information on case owner

4	**Requests:** • No material impact to services. E.g. MACD's	**Initial response:** 2 business days	• Accurate contact information on case owner • Reasonable notice to Umbrellar for requests that fall in this category.

Umbrellar may (acting reasonably) reclassify any issues misclassified as falling into one of the emergency categories listed above, and such issues will not qualify for emergency treatment.

5 Service Level Exclusions

Any downtime incurred from incidents as a result of the non-recommended use of non-warranted Supported Hardware or Supported Software is excluded from the Service Level tables above.

These include but are not limited to;

- Any infrastructure component or service that has gone end of life from a vendor.
- Any infrastructure component or service that has no suitable vendor warranty applied.
- OS that are deemed outside of mainstream support by the vendor (Windows 2008 etc.)
- Unlicensed software or component.

- Any infrastructure component or service noted by Umbrellar or vendor technical resources as non-compliant.

Such infrastructure component or service will be supported under a "best efforts" basis whereby our team will react and support as stated in the agreement however will not be held by any SLA or KPI measures until such time as the hardware/software is approved to be supported under full support.

Such components or service will be noted to Umbrellar when known.

- Any downtime incurred as a result of jobs carried out during specific agreed maintenance windows are excluded from the Service Level tables above.

- Any jobs resulting from accident, negligence, abuse or misuse by the consumer of Umbrellar services are excluded from the SLA. However, Umbrellar will do everything possible to minimise and avoid unnecessary downtime during any situation of this nature. Any issues of this nature will also be reported to Umbrellar accordingly and appropriately.

- Umbrellar cannot control the actions of any of the consumers designated 3rd parties and therefore cannot include 3rd Party jobs within our SLA terms. However, Umbrellar will do everything possible to minimise and avoid unnecessary downtime during any situation of this nature. Any significant 3rd Party issues, that result in disruption will also be reported to Umbrellar accordingly and appropriately.

- In the event of an attack of a malicious nature, e.g. if an external party initiates a "Denial of Service" or other form of disabling attack against your website, your servers, or major portions of your network, Umbrellar will do everything in its power to stop the attack but cannot guarantee a resolution time.

- Any Incident that requires additional information from the consumers staff or other 3rd parties and is deemed vital to carrying out a resolution/delivery of request/alert will be put on hold pending the receipt of this information.

6 Managed Services Onboarding

6.1 As Built Documentation

During the managed services onboarding, Umbrellar will work with the customer to create a customized monitoring response runbook. This runbook defines the Umbrellar Cloud Operations team's standard operating procedures for working with the customer and any authorised third party on monitoring alerts and includes custom escalation procedures in accordance with best practices. These customer runbooks are designed to present the right information at the right time to Umbrellar's success and services teams. This is important in order to respond quickly and effectively to any incidents. Providing relevant and focused documentation to Umbrellar's success and services teams helps to maintain the availability of customer solutions and keep the business impact to a minimum.

6.2 Resource Classification

In order for Umbrellar to understand the business impact of the customer resources, Umbrellar suggests the below resource classification. Each service will be categorised during the onboarding to ensure the best outcome for the customer.

	Business Critical	Business Essential	Non-Production
Business Impact in the event of an incident	Critical	Medium	Low
Incidents being attended to (as per SLA)	24/7 (P1-P2) Business Hours (P3) *	24/7 (P1) Business hours (P2-P3) *	Business Hours (P3 only) *
Suggested Resource Type	Customer facing or core Line of Business applications	Secondary business applications (the business can still operate)	Tertiary business applications, UAT, test and development resources

*Support will be provided but is chargeable after-hours, on a case-by-case basis and a minimum 4-hour block will be charged.

6.2.1 Resource Classification Requirements

For a resource to be able to be classified as Business Critical, Business Essential or Non-Production the following requirements need to be met.

Classification	Requirements
Business Critical	• Inline/Snapshot based Backup • Escalation support agreement with vendors, and aligned Return To Operation (RTO) • Technology is current (within n-1 of current release)
Business Essential	• Industry standard Backup regime • Technology is not end-of-life • Technology is within a current warranty (if appropriate) • Vendor warranties have aligned RTO
Non-Production	• No minimum criteria

6.3 Technical Contact

The technical contact is our primary point of contact for all issues that may arise with your Managed Services and need to be discussed with you. This contact is also the person who can open any change requests via a support case.

6.4 Management Host

For Proactive Care Advanced customers, Umbrellar reserves the right to require the deployment of a management device(s) in a separate subscription, which will be included in the managed services fee. This host is used to enable secure Umbrellar remote access to the customer environment. Access is restricted to known and secured Umbrellar management endpoints using RDP or SSH. Umbrellar engineers will then access customer virtual machine using RDP or SSH from the management host. One management server will be created per region containing managed customer virtual machines.

6.5 Management Tools

Deployment of management tools required by Umbrellar to provide Operating System Support and patching are pre-approved changes and as such will be built into platform automation to be automatically deployed to any new builds/rollouts in the Microsoft Cloud infrastructure.

6.6 Service User

For Proactive Care Advanced customers, Umbrellar reserves the right to require the customer to grant an Umbrellar service user access to the environment. If a customer requires Umbrellar to have named accounts to access the environment, additional charges may apply.

7 Ongoing Service Management

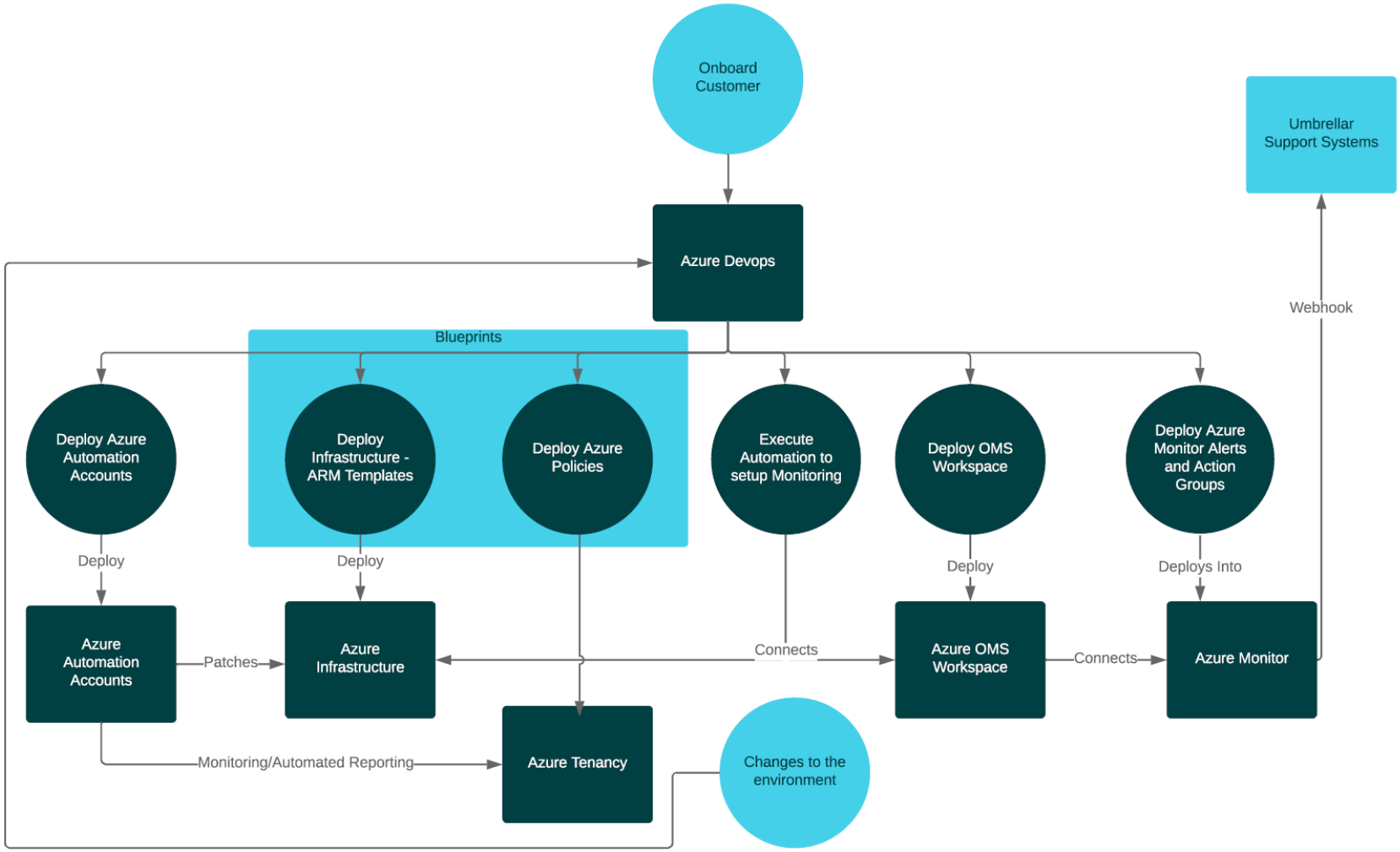
7.1 Azure Cloud Practice leveraging DevOps Principles

Once a customer has been onboarded to Managed Services, a pre-defined set of assets are deployed with built in automation using Azure DevOps or Terraform pipelines.

This includes:

- **Automation Accounts** - These are utilized to ensure deployments are consistent and are not only deployed but maintained to an agreed desired state.
- **Infrastructure** - –Standardised templates are used for deployment and can be customized to the requirements of the customer. These are especially useful to stitch together multiple resources and automating the deployment as required.
- **Azure Policies** – Umbrellar's deployments adhere to simple policies relevant for the monitoring solution being deployed, these are further augmented by custom policies that define a wide range of aspects. This may include allowed VM's and Storage SKU's as well as resource tagging to aid with reporting and billing.
- **Operations Management Suite (OMS) Workspace** – Umbrellar has adopted a hybrid model to leverage Log Analytics. This ensures any customer data that is sensitive stays within the customer's tenancy, while only surfacing generalized data to Umbrellar's central Log Analytics workspace. A number of workspaces can be deployed depending on the customer's needs.
- **Automated OS patching (Optional – Refer to Cloud Operations Rate Card)** – Along with Log Analytics workspaces, Automation accounts are leveraged to run automated patching of workloads within the tenancy. This information is fed back into an Management dashboard for visibility.
- **Monitoring Dashboards** - All the automation setup above is presented via pre-built dashboards. Any alerts generated by the monitoring solution are configured to the customer's needs.

7.1.1 Azure DevOps Lifecycle for Support (for Azure DevOps – ADO)



7.1.2 Azure Monitoring & Alerting

Umbrellar can monitor the underlying Microsoft Cloud platform as well as individual virtual machine instances.

7.1.2.1 Platform Monitoring

Umbrellar will check and generate notifications for, platform-related events such as service or region incidents on public Azure.

7.1.2.2 Environment Monitoring

Umbrellar will work with the customer to implement and configure monitoring for services under scope of management.

This offering consists of monitoring and alerting for CPU, Memory and Disk utilisation and backup status and backup status. Additionally, specific monitors and alerts for PaaS services will be implemented upon agreement with the customer.

7.1.2.3 Advanced Monitoring

Advanced customers can purchase additional application endpoint monitoring. Umbrellar will monitor agreed application endpoints to ensure the application is accessible from the internet. Umbrellar will carry out pre-approved remediation checks, if agreed during the Managed Services onboarding, before alerting the customer.

7.1.2.4 Backup Management

Umbrellar will monitor backups 24/7 and attend to any backup alerts and change management requests during business hours. Data restoration requests are not included in the Proactive Care plan and are subject to additional charges as per Umbrellar's published rates unless superseded by a customer specific Managed Services Agreement. The customer may request to restore data (file level or full server instance) by submitting a service request.

The customer acknowledges that Umbrellar shall not be held responsible or liable for the validity or quality of such data contained within the backup.

7.2 Antivirus

Customers have the option to subscribe to Umbrellar's Proactive Care Managed Antivirus service.

7.3 Deployment Template Library

Umbrellar has several proprietary and best-practice templates that will be available to Proactive Care customers as well as access to custom template specific for the customer. Templates can be created during a project or through Professional Services.

7.4 Azure Advisor Recommendations

Umbrellar team work on recommendations and intelligence provided covering areas such as Cost Management, Security and other operational intelligence.

7.5 Configuration Management

Umbrellar will assist and manage configuration and modification of Azure and/or Umbrellar Cloud resources. This may include subscription level actions such as configuring Role Based Access Control (RBAC), Resource Group advise and creation as well as resource actions such as updating of network security groups, resizing of instances, establishment of site-to-site VPN tunnels and configuration changes for the virtual machine operating system (IaaS VM).

7.6 End-of-Life Support

Umbrellar will provide management services up to the date of the operating system going end-of-life. After the end-of-life date any provided services are on a best effort basis and Umbrellar will not guarantee any SLA's. Additional charges may apply upon end-of-life of the operating system.

7.7 Operating System Patching

Umbrellar will apply operating system updates in line with the patching process and schedule defined within this document. Umbrellar will ensure the updates are applied in line with vendor recommendations. Patching will end, if the installed operating system is end of life. Umbrellar will not patch customer applications or other 3rd party software as part of this service.

7.7.1 Windows based operating system Patching

1. Any available updates from the Microsoft Update Catalogue relevant to the installed operating system.
2. Any available updates from the Microsoft Update Catalogue for other installed Microsoft products if the option “Give me updates for other Microsoft products when I update Windows” is enabled. This will be discovered during the managed services onboarding.

7.7.2 Linux based operating system Patching

1. Security updates and minor version updates for any operating system packages with dependencies as required.

7.7.3 Maintenance

Umbrellar will undertake Managed Patching that may require an interruption to the Service during specified periods. Umbrellar will work with the customer to agree a patching schedule during the managed services onboarding.

7.8 Incident Management

Incident management refers to the management of incidents where restoration of the services is the primary objective.

1. Umbrellar applies a consistent approach to all incidents as per Umbrellar's standard operating plan, except where a customer specific approach has been previously agreed with the customer and documented in the customer as built documentation. Incidents can only be initiated by:
    a. Authorised technical contacts on the customer account. This can be a customer employee and/or a 3rd party contact.
    b. Umbrellar employees
    c. Monitoring management tools
2. The Umbrellar Support team will investigate the incident in accordance with your purchased Cloud Care plan, once the case has been logged.
3. Umbrellar will communicate with the customer and 3rd parties, named and authorised by the customer, where and as needed to resolve the incident.
4. If an Umbrellar Engineer requires assistance to resolve an incident that is outside of scope of Umbrellar standard manages service support, Umbrellar will engage with 3rd party vendors to seek resolution. Authorisation for 3rd party engagement may be sought out as required.
5. Corrective action in the form of a Post Incident Review (PIR) will be supplied for Priority 1 critical service impacting event and will include engagement with other parties as required.

7.9 Change Management

1. Change management includes a standardized set of procedures that enables Umbrellar to deliver efficient and prompt handling of all changes in an organized manner to help ensure minimum impact on the customer services.
2. For any change requests raised by the customer, the customer has to use the Umbrellar RFC template, which will be provided during the onboarding phase.
3. Umbrellar will raise a case, that is owned or initiated by Umbrellar. Customers can raise a case for situations where Umbrellar support is required for any changes owned and initiated by such customer.
4. All changes will be managed through the Umbrellar case and change management systems. This supports long-term tracking of all information and the best delivery of services through the various lifecycle processes of deployment, change management, incident management, etc.
5. Umbrellar will organize the best suited engineer, with experience in the specific change, to manage the change as scheduled, keeping the customer fully informed on progress.

7.10 SSL Certificate Management

Umbrellar Provides SSL Certificate management as part of our managed service offering, included in VM or PaaS management, if the below criteria are met:

1. Umbrellar procures the certificates on behalf of the customer via our preferred provider (Digicert)
2. Service or VM requiring the certificate is under monthly management
3. The client conducts internal testing to ensure application compatibility with the SSL certificate.

Umbrellar will, if the above criteria are met, provide a quote to the customer for procuring/renewing SSL Certificates, purchase/renew SSL certificates and assist with installation and validation. The process to quote, purchase/renew and issue/install SSL certificates will be presented to the customer as a MACD (Move, Add, Change, Delete) which will include the cost of the certificate as well as engineering effort required.

Should the customer use their own SSL Certificate provider, Umbrellar will monitor and notify the customer of certificate expiry, but not manage the process on behalf of. Installation assistance will be a MACD for engineering effort.

8 Umbrellar Expertise

8.1 Third-Party engagements

Umbrellar will also work with any third parties nominated by the customer. As part of the managed services onboarding, Umbrellar will work with the customer to establish and document the level of engagement with any third parties.

8.2 Service Delivery Manager (SDM)

The SDM is an optional shared resource available to Proactive Care Advanced customers. The SDM will provide monthly reviews in order to analyse the performance of a customer's Azure and/or Umbrellar Cloud environment and provide recommendations for optimizations. This includes recommendations around the use of various types of resources, root causes of alerts and investigation for service improvements. The review will be based on the following agenda:

- Support Cases
- Alert trends
- SLA Measurement
- Cost Optimization
- Service Improvements and recommendations

8.3 Architectural Guidance

Under this agreement, customers can have access to Umbrellar Architectural expertise. Where required, Umbrellar will leverage our partner ecosystem to provide best of breed architectural services including Microsoft Architectural services. Additional costs will apply, and these engagements will be managed under separate engagement documents.

8.4 Additional Professional Services

Services	Professional Service	Pricing Model
Detailed Solution Design	✓	Refer to Cloud Operations Rate Card
Migration Assistance	✓	Refer to Cloud Operations Rate Card
Deployments	✓	Refer to Cloud Operations Rate Card
Architecture Guidance	✓	Refer to Cloud Operations Rate Card
Workshops (e.g. Dev Ops training)	✓	Refer to Cloud Operations Rate Card

9 Appendix

9.1 Roles and Responsibilities

Service Level Tasks	Umbrellar	Customer
Support and Subscription Management		
Provide named technical contact	C/I	R/A
Keep technical contact up to date	C/I	R/A
Purchase subscriptions in the Umbrellar Portal	C/I	R/A
Grant Umbrellar tenant/subscription/resource access	C/I	R/A
Monitoring		
Provide monitoring alerting response based on purchased Proactive Care plan	R/A	C/I
Configure standard monitoring alerting	R/A	C/I
Custom event logging and alerting	R/C	A
Operating System		
Break-fix and troubleshooting	R/A	C/I
Configuration Management	R/C	A
Patching		
Patching Windows based operating system during agreed Patching Window	R/A	C/I

Patching Linux based operating system during agreed Patching Window	R/A	C/I
Install agent for patching	R/A	C/I
Apply any major software version updates including but not limited to Microsoft SQL, MySQL, PHP, NGINX, IIS	C/I	R/A
Keep Application up to date	I	R/A
Provide and maintain pre and post patching checks (if required)	C/I	R/A
Provide and maintain server patching order (if required)	C/I	R/A
Provide and maintain Umbrellar's access to the server's operating system for patching related tasks and troubleshooting	C/I	R/A
User Management		
Create and manage new users and groups	I	R/A
Platform-As-A-Service (PAAS) Administration		
Deployed connectivity objects e.g., VNET, NSG, App Gateway	R/A	C/I
Web App/ App Service maintenance	R/A	R/C
Database Server Administration (MSSQL, MySQL)	C	R/A
Database Server Configuration (MSSQL, MySQL)	R/C	R/A
Database Monitoring	R/A	C/I
Any 3rd party application (Installation, configuration and administration)	I	R/A

SSL Certificates		
Purchasing and maintaining SSL certificates (Infrastructure)	R/A	C/I
Installing SSL certificates (Infrastructure)	R/C/I	R/A
Backups & Disaster Recovery		
Optional - Testing of BCP/DR functionality (Pre-Existing plan/architecture)	R/A	C/I
Configuration and Management of Backup Policies	R/A	C/I
Monitoring of Backup Schedule & Status	R/A	C/I

R – Responsible A – Accountable C – Consulted I – Informed