MANAGED AZURE SERVICE

SERVICE DESCRIPTION SD053

DOCUMENT CONTROL

Version	Completed by	Date
5.2	Megan Creed	07 February 2024
5.3	Megan Creed	03 July 2024
5.4	Megan Creed	23 October 2024
5.5	Megan Creed	TBC

The version history has been recorded and archived and is available upon request should these be required.

PREPARED BY

Name	Job title
Megan Creed	Service Development Programme Manager
Emma Fox	Service Development Programme Manager

CONTENTS

1. SERVICE OVERVIEW

All bold and capitalised terms throughout this Service Description are described in the Glossary and definition of terms.

1.1 SERVICE SUMMARY

The Managed Azure Service provides Customers with management, Support, and delivery of their Microsoft Azure environment(s) from Softcat's UK based 24x7x365 Operations Centre.

The Service comprises:

- Pre-assessment of the Customer's Microsoft Azure environment ("**Pre-Qualifying Questionnaire**")
- 24x7x365 access to log Support Cases ("**Softcat Support**")
- High level guidance from Softcat's Cloud Solution Architects with up to two (2) hours per month of workshops to ensure the most efficient use of cloud-based solutions ("**Cloud Architect(s)**")
- Access to Softcat's Cloud FinOps capabilities, including Platform access, set-up and monthly optimisation recommendations delivered through reports and workshops ("**FinOps**")
- Access to Softcat's Innovation Points programme ("**Innovation Points**")
- Onboarding, training, and access to the Cloud Management Platform to provision, orchestrate and manage Microsoft Azure Resources ("**Cloud Management Platform**")
- Microsoft Azure monitoring, patching, security posture management, Microsoft Azure governance & back up and Operating System (OS) Management ("**Systems Management**")
- Standardised methods, processes and procedures which are used for all changes ("**Change Management**")
- Management of high impacting events that affect a large number of users, depriving the business of one or more critical services ("**Major Case Management**")
- Root Cause Analysis to identify, track and resolve recurring incidents and ultimately prevent these from occurring ("**Problem Management**")
- Providing a named Service Delivery Manager, service reviews and service reporting ("**Service Delivery Manager**")

Optional Add-Ons are chargeable extras, and where required will be quoted and confirmed on the Work Order:

- The Enhanced Cloud Optimisation Service provides additional analysis, monthly optimisation recommendations and high level guidance from a Softcat Cloud Architect with up to four (4) hours of their time per month ("**Enhanced Cloud Optimisation**") (**Optional Add-On**)

Together, the above comprise the "**Managed Azure Service**", referred to as the "**Service**" within this document.

The Service is delivered in accordance with the following ISO standards:

- ISO 21001
- ISO 20000
- ISO 9001
- ISO 22301

Unless otherwise stated in the Work Order, and in addition to any terms set out in this Service Description, the following applies to the delivery of the Service set out in this Service Description:

- Softcat Terms and Conditions: T&Cs
- The Data Processing Agreement: DPA
- CloudHealth End-User License Agreement (EULA): EULA
- Softcat Customer Success Manager (CSM) EULA: EULA

1.2 SERVICE FEATURE TABLE

	Managed Azure Service	Enhanced Cloud Optimisation (Optional Add-On) [1]
Pre-Qualifying Questionnaire		
Initial assessment of Customer's Azure environment	✓	
Softcat Support		
Log Support Cases 24x7x365 [2]	✓	✓
Online Support portal to track and log calls	✓	✓
A minimum of two (2) Customer Contacts	✓	✓
P1 response Service Level	15 minutes	15 minutes
Cloud Architects		
Cloud solution and best practice workshop and summary write up	Two (2) hours	Four (4) hours
Cloud Solution Architect technical optimisation advice and documentation		
FinOps		
Onboarding: initial optimisation of environment against core best practice policies	✓	✓
Onboarding: initial discovery with stakeholders and comprehensive report back on findings	✓	✓
Onboarding: set up perspectives and policies for Customers	Five (5) perspectives and five (5) policies	Ten (10) perspectives and thirty (30) policies
Access to Softcat's FinOps Platform, including cost, performance, governance and security reports	✓	✓
Recommendations for security and governance	Single monthly report and workshop	Multiple reports, tailored by persona/business unit
FinOps Analyst Support, including updates to the policies, perspectives and customer dashboards within the FinOps Platform		✓
Ongoing tracking of savings made through recommended improvements, and potential further savings to be made		✓
Annual FinOps maturity assessment		✓
Implementation of recommendations by the CloudOps team	✓	✓
Innovation Points		
Access to menu of additional services [3]	✓	✓
Cloud Management Platform		

	Managed Azure Service	Enhanced Cloud Optimisation (Optional Add-On) [1]
Monthly spend on cloud Resources	✓	✓
Case information	✓	✓
Display Azure Resource health status	✓	✓
Display AWS Resource health status	✓	✓
System Management		
Monitoring and alerting (Microsoft Azure infrastructure and Virtual Machine (VM) OS metrics/logs)	✓	
Security posture management (Microsoft Azure Security Benchmark)	✓	
Regulatory compliance and governance (Microsoft Azure Policy)	✓	
Backup and restore (Microsoft Azure Resources)	✓	
Windows and Linux server OS critical/security patching	✓	
Management via infrastructure as code (IaC) or console	✓	
Change Management		
Standard Change requests	✓	
Normal Change requests	✓	
Retrospective Change requests	✓	
Emergency Change requests	✓	
Customer performed maintenance	✓	
Major Case Management		
Major Case management process applies	✓	
P1 notifications	✓	
Service Delivery Manager		
Named Service Delivery Manager	✓	✓
Service reports and reviews [4]	✓	✓

[1] Optional and Optional Add-On means a chargeable extra. Where an optional extra is chosen by a Customer, this is confirmed on the Work Order.
[2] Requests are acted upon within contracted coverage hours, as confirmed in the Work Order. Cases that are raised to FinOps will be progressed during UK Working Hours.

[3] Customer will have access to a full menu of services that the Innovation Points can be used towards.

[4] Service reports are provided on a monthly basis only, and the frequency of the service review is at the Customer's request.

2. SERVICE DETAIL

2.1 PRE-QUALIFYING QUESTIONNAIRE

The Pre-Qualifying Questionnaire is carried out between the Softcat Account Team and the Customer. This will provide Softcat with a high-level overview of the Customer's Microsoft Azure Environment, capturing essential details required for the ongoing solution.

Softcat may recommend and require reasonable and industry-standard changes be completed within the Customer's Microsoft Azure environment before the Activation Date.

Softcat can manage and implement these upgrades in collaboration with the Customer at an additional charge; the delivery will be via Softcat Cloud Architects. Any quotes required for Softcat Cloud Architect work will be provided via the Customer's Softcat Account Manager. The pre-qualifying questionnaire is carried out between the Softcat Account Manager and the Customer.

2.2 SOFTCAT SUPPORT

Customer Contacts have access to Softcat Support around the clock and on any day of the year ("24x7x365").

Customer Contacts should raise Cases via phone, email or from the Cloud Management Platform ("CMP")[5].

Customer Contacts should raise a Case primarily via the Support portal, where the Case type will be assessed, defined and communicated and the priority level will be agreed with the Customer. Where Service Levels apply to the management of a Case, these will be confirmed on the Work Order. For any Case which the Customer believes to be urgent, the Customer Contact must report to Softcat by telephone.

[5]The CMP is continuously evolving with new features.

2.3 CLOUD ARCHITECT

The Service provides the Customer with a monthly workshop which is delivered by a Softcat Cloud Architect. The Cloud Architect will provide guidance to the Customer in two (2) key areas:

- Architectural guidance for the implementation of optimisations that originate either from the Customer or from Softcat's FinOps teams.
- Architectural guidance and/or peer review for the Customer's existing or planned cloud initiatives, for example, how to ensure the most efficient use of cloud-based solutions and/or making existing solutions more cloud native.

In fulfilment of these activities, the Customer will benefit from up to two (2) hours of time per month with a Softcat Cloud Architect. The hours used will be tracked by Softcat each quarter. Beyond the two (2) hour time allotted, the aligned Softcat Cloud Architect can attend monthly service reviews, however for further needs driven by Customer requirements, additional charges may apply.

2.4 FINOPS

FinOps provides the Customer with analysis, reporting, and recommendations regarding the commercial governance of their Cloud solutions. There is a pre-requisite to ensure that the Customer's Microsoft Azure CSP (Cloud Solutions Provider) resides with Softcat, or suitable contracts are in place directly with Microsoft in order for Softcat to deliver the Service. Further guidance can be provided by the Customer's Softcat Account Manager.

High level information is displayed in the Softcat CMP, from which access is also provided to the FinOps Platform.

Customers will be assigned a FinOps Analyst, who will run workshops to set up reports, dashboards, perspectives and policies, as well as provide an overview of the Support that will be offered. The FinOps Analyst will send the Customer an initial questionnaire, to understand the key areas they would like to focus on and Support them during these workshops. This will also include agreeing on plans for actioning the outlined insights to improve the relevant areas. It will be the responsibility of the Customer to then implement the outlined recommendations.

As part of the Service onboarding process, Softcat's FinOps Analysts will also create up to five (5) policies and five (5) perspectives for the Customer in the FinOps Platform, as well as running initial optimisation workshops to examine the areas where cost savings and efficiencies could be made.

Customers will also take part in the FinOps 'clean the house' workshop, which focuses on identifying and implementing immediate improvements and optimisation opportunities, to enhance cost efficiency and security posture in the cloud environment(s). The FinOps analyst will provide actionable insights and strategies to streamline their cloud operations and maximise resource utilisation.

For Brownfield Customers, the accuracy of FinOps is dependent on aspects such as cloud Resource tagging. If such tagging is not in place, Softcat will provide recommendations around defining these and in scenarios where extensive work is required (which cannot be fulfilled by a Change Request) additional costs will apply.

Additionally, all associated Subscriptions within the Customer's Microsoft Azure tenant will automatically be onboarded into Softcat's FinOps tool and a monthly reoccurring charge will be incurred. Any widgets in the CMP relating to the Customer's Microsoft Azure cloud spend will show all Subscriptions in the Customer's Microsoft Azure tenant.

Where a Customer is onboarding multiple Microsoft Azure tenants into the Service, the Customer is responsible for ensuring they are onboarded in a timely manner to get the most from the Service. Softcat will guide the Customer through the onboarding activities, however where there is a delay to onboarding due to the Customer, data and information may be restricted and optimisations / recommendations will be limited, and additional charges may apply.

2.5 INNOVATION POINTS

As part of the Service, Customers will accrue 'Innovation Points' which is a way Customers can generate loyalty points, providing them with the option to spend them from a menu of complementary project-based capabilities.

Points are accrued as a percentage of the Customers' ongoing Service spend and are automatically calculated as part of the billing process. One (1) pound (£) is equivalent to one Innovation Point and Customers will receive a sign-up bonus to begin utilising the points straight away.

The Innovation Points menu has been designed to cover a range of capabilities and skills that Customers may benefit from and to provide them with a layer of additional value from the Service.

The Innovation Points menu includes:

- Advisory services
- Design/architectural reviews
- Deployment of new workloads and migration delivery
- Accelerator services
- Training
- DevOps

2.6 CLOUD MANAGEMENT PLATFORM

The Cloud Management Platform is a key feature of the Service. It is a Platform which provides access to areas including [5]:

- **Case management –** Management of Cases, requests and changes.
- **Provisioning/orchestration/automation –** Of various cloud tasks including start/stop of Resources and deployments.
- **Monitoring and alerting –** To view cloud native dashboards, utilising Microsoft Azure Monitor for Resource health and status.
- **Security and compliance –** To view live compliance data from cloud native Platforms.
- **Commercial intelligence –** To view dashboards regarding cloud spend and savings.
- **Service management –** During the onboarding process, a number of pre-agreed Customer Contacts will be created to ensure they have access to the relevant insight and/or where necessary can interact with the Service, for example to manage Cases and view monitoring data and cost optimisation dashboards.

For users of the CMP, the following EULA applies: Softcat CSM EULA

[5] The CMP is continuously evolving with new features.

2.7 SYSTEM MANAGEMENT

The Service provides Customers with a secure, feature-rich, and optimised environment for their Workloads. Additionally, the Service manages the Customers' Azure environment from the OS layer down, removing the complexity from the Customer and enabling them to focus developing and operating their Applications and business services.

Customers will have the choice of being either ("Infrastructure as Code (IaC)-Managed") or ("Console-Managed"). The distinction refers to the way that Customers are managed and supported within the core Service on a day-to-day basis.

2.7.1 IAC-MANAGED

IaC-Managed Customers are provided with the features and capabilities listed below:

- Version-controlled environments providing the Customer with an audit trail.
- Deployment consistency across environments.
- Automated scanning of code for misconfigurations that may lead to security and compliance issues using the following tools:
    - **Microsoft Azure**: Customer can choose the geographic location.
    - **GitHub states**: GitHub will abide by the requirements of applicable European Union, European Economic Area, United Kingdom and Swiss Data Protection Law, and other Data Protection requirements, in each case regarding the transfer of Personal Data to recipients or jurisdictions outside such jurisdiction.
    - **Checkov**: Customer data is not stored. Scans code in place.
    - **Inspec**: Customer data is not stored. Queries infrastructure deployed and confirms deployed as expected.
- Automated deployment of Azure Resources to the Customer's environment(s).
- Automated quality checks of environment(s) deployed.
- If an issue occurs as the result of a change via IaC, the change can be rolled back as each change will be versioned.
- New environments will benefit from being deployed with best practices applied from the outset, using a combination of code analysis and Softcat's IaC modules. These consist of both Softcat and Microsoft Azure best practices.

Softcat fully manage the Customer's environment up to the OS layer. For IaC-Managed Customers, should the Customer require certain permissions into the environment in order to complete day to day tasks, the level of permissions will be agreed between Softcat and the Customer during the sales cycle.

2.7.2 CONSOLE-MANAGED

Console-Managed Customers are provided with following features and capabilities listed below:

- Any changes made to the environment are applied directly via the Microsoft Azure Portal.
- Changes will be planned and reviewed before deployment manually.
- Changes will not be version controlled.
- Changes are not automatically analysed for misconfigurations and best practices.

2.7.3 MONITORING AND ALERTING

Microsoft Azure Monitor allows for the monitoring and alerting of multiple metrics and logs within a Customer's environment. The Service is delivered from our UK-based 24x7x365 Operations Centre. For supported Microsoft services, the monitoring features of the Service are made up of:

- Automated deployment and management of the monitoring infrastructure.
- Granular assignment of alert rules to Resources.
- Prescribed set of Microsoft and Softcat best practice alert rules.
- Customisation of default alert rules.
- Bespoke alert rules – on request alert rules for metrics/logs not covered by the default/custom alert rules.

- Failed backup and service health monitoring.
- Automatic Case creation from alerts utilising Softcat's ITSM tool.
- Investigation and resolution of alerts.
- Continual improvement of automation and alert rule scope.

As part of the deployment of the monitoring infrastructure, the automation requires for tags to be created and then added to the Customer's Resource(s). Only necessary monitoring Resources are deployed to ensure no additional costs are incurred.

The Service provides Microsoft and Softcat best practice default alert rules for supported Resources in the Customer's environment e.g. high central processing unit ("CPU") utilisation on a VM. If required, Softcat can make adjustments to the configuration of the default alert rules e.g. change alert threshold from ninety-eight (98%) percent to ninety-five (95%) percent. Any change to a default alert rule results in it being classed as custom. The alert rule scope is set to only the Resources that require monitoring.

Softcat can create bespoke alert rules if the Customer requires monitoring of a metric/log which is not covered by the default alert rules. In this instance, the Customer will be the sole recipient and responsible for the alerts.

2.7.4 SECURITY AND GOVERNANCE

Microsoft Azure Defender allows for monitoring of the Customer's environments against the Microsoft Azure Security Benchmark compliance framework. This includes the following:

- Automated enrolment of the Customer's environment(s) into Microsoft Azure Defender for cloud.
- Monitoring of supported Resources against the Microsoft Azure Security Benchmark regulatory compliance framework.
- Automatic service Case creation for un-compliant Resources.
- Investigation and resolution of un-compliant Resources.
- Exclusion of un-compliant Resources if required.

Microsoft Azure Defender provides Customers with a 'free' tier, which enables the Microsoft Azure Security Benchmark with no additional cost. Customers will also have the option to enable the 'standard' tier if required, which will incur further charges in their environment. For more information, the Customer should contact their Softcat Account Manager.

2.7.5 WINDOWS OS MANAGEMENT

The Service includes Support for the Microsoft server OS and covers all versions in accordance with Microsoft's Product lifecycle.

The Operations Centre will troubleshoot and remediate issues with server roles and features necessary for the stability of the OS.

2.7.6 LINUX OS MANAGEMENT

The Service includes Support for three (3) major Linux distributions which covers versions listed in Microsoft's supported distribution list and the official Support channels set out by the distributor(s) developer. These distributions include:

- Ubuntu

- Red Hat Enterprise Linux
- CentOS (Brownfield Customers only, for more information please see Customer exclusions)

2.7.7 ENVIRONMENT ACCESS AND SECURITY

As part of onboarding and ongoing delivery, Softcat will require a certain level of access to be provided into the Customer's Microsoft Azure environment. The type of access and permissions that must be configured are outlined below:

- **Microsoft Entra Multi-Tenant Application Registrations** – each Customer will have a unique set of app registrations created in Softcat's partner account which they will need to accept into their tenant. These application registrations will contain permissions at the tenant level and require Customers to provide permissions at the Subscription level to allow for programmatic access to the environment.
- **Reader Application** – information is pulled from the Customer's tenant(s) and Resources into the CMP. The application will require 'reader' permissions at both the tenant and Subscription level.
- **Management Application** – used to deploy infrastructure and changes to the environment and to allow ongoing management of the Customer's environment monitoring. This application will require 'reader' permissions at the tenant level and 'owner' permissions at the Subscription level.
- **Microsoft Azure Lighthouse Offer** – each Customer will need to accept a Microsoft Azure Lighthouse offer into their tenant and provide this offer with delegation at the Subscription level. The offer contains both permanent and eligible permissions to ensure just in time (JIT) access is available to the Softcat engineer who provides the Service. The permanent permissions allow the Softcat engineer to have sufficient access to review the environment and to log Support Cases with Microsoft when required. The eligible permissions allow the Softcat engineer to elevate their permissions to make any required changes to the infrastructure when needed. To elevate permissions, the Softcat engineer must go through a Microsoft Azure Privileged Identity Management (PIM) workflow. This requires another Softcat engineer to approve the elevation request before the individual will be granted the elevated permissions. This elevation is also limited to a specific maximum time frame of four (4) hours.
- **Microsoft Azure Bastion** – if a Customer's environment contains VMs, a Microsoft Azure Bastion must be deployed and configured into the environment. This gives the Softcat engineer providing the Service secured and auditable connectivity into the VM(s), through the Microsoft Azure portal and access provided by Microsoft Azure Lighthouse. In addition, Customers will need to provide Softcat with credentials to log into the VM(s) where applicable.

2.7.8 UPDATE MANAGEMENT

Update Management provides automated monthly patching for Supported Linux and Windows servers hosted within the Customer's Microsoft Azure environment. The Service is delivered from Softcat's UK-based 24x7x365 Operations Centre. For the Supported Products, Update Management includes:

- Installation of the required Agents to each supported server.
- Monthly updates applied to the supported servers.
- Linux kernel, critical and security OS updates, as released by the Linux distribution developers to their official repositories.
- Critical and security package updates as released by Microsoft to the supported Customer environment.
- Scheduled updates at a time and date agreed with the Customer as part of the upfront onboarding process.
- Communication to the Customer and remediation of any failed updates or exclusions.

- Change Management process for initial patching run. Any subsequent changes to the agreed patching schedule will also require a change to be raised.
- Reboot of Supported Products as required through the downtime period.

In the scenario a server becomes unreachable because of an applied patch, the Customer will be contacted before Softcat carry out a full restore of the server from backup.

In the scenario a server is reachable, but the Customer experiences performance or availability issues with its Applications or services running, then Softcat can carry out a full restore. This will be based on a last known working state or uninstall of the patch following an Agreement with the customer as part of the Case management process.

2.7.9 AZURE BACKUP

Microsoft Azure allows for the backup and recovery features of many Resources within a Customer's environment. While specific policies (e.g. frequency, retentions, and regional protection) will be agreed with each Customer during the design process (for new systems) or onboarding process (for existing systems), the below summarises the typical features:

- Microsoft Azure VM backup and recovery via Microsoft Azure Recovery Services Vault.
- Microsoft Azure backup and recovery e.g. point in time restore ("PITR") for the following:
    - SQL server in Microsoft Azure VM via Microsoft Azure Recovery Services Vault.
    - Microsoft Azure Disks via Microsoft Azure Backup Vault.
    - Microsoft Azure Blobs (Azure Storage) via Microsoft Azure Backup Vault.
    - Microsoft Azure Database for PostgreSQL servers via Microsoft Azure Backup Vault.
    - Kubernetes Services via Microsoft Azure Backup Vault.

For the purpose of assurance to the Customer during critical and security OS patching only, each server within scope will have a daily Bare Metal recovery backup taken. This ensures recoverability of the server's OS should it be required. As part of this Service, any VM included will be set up for daily backups which will be configured within a Microsoft Azure Recovery Services Vault contained within the Customer's Subscription.

2.8 MAJOR CASE MANAGEMENT

As part of the major Case process, initial P1 email communications are sent to the Customer Contact list within fifteen (15) minutes of receiving the escalation.

Updates will be communicated hourly, unless there is a specific reason for a delay (e.g. a restore job is running and is expected to take two (2) hours). In such circumstances, the Customer's expectation will be set in the previous communication.

When Softcat has determined that the impact of the P1 Case on the Customer has been mitigated, the P1 Case will be 'resolved'.

Following the resolution of the Case, if the Customer is still running at a loss of redundancy, or at a reduced but acceptable capacity, then the Case will be reassessed, and priority determined and reflected accordingly.

Upon resolution, a report will be compiled and provided to the Customer.

If the reason for the outage has not been established, a problem record will be raised and managed by Softcat.

2.9 PROBLEM MANAGEMENT

Softcat will use its Problem Management process to identify the root cause and make recommendations to the Customer to help to prevent further such incidents arising.

This Problem Management process captures information about problems and resolves them, according to Softcat standards and policies.

The process identifies, documents, analyses, tracks and resolves all problems as follows:

- Problems are logged in a standardised format.
- The impact of problems and number of incident reoccurrences is minimised.
- Where possible, recommendations on how to prevent further reoccurrence will be made. Any costs associated with such recommendations will be discussed with the Customer prior to implementation.
- Problems are routed and managed in accordance with ITIL-aligned processes.
- Problem status is accurately reported.
- Quality assurance on all problem records is provided.
- Problems are prioritised and handled in the appropriate sequence.
- Incident review meetings after major incidents and P1s generate reports which the Service Delivery Management team share with Customers.
- Trend analysis and root cause analysis is completed, and the output shared with Customers.
- Productivity of resources is maximised.
- The Service is monitored and measured.
- Resolutions or workarounds are implemented in accordance with ITIL guidelines.

2.10 CHANGE MANAGEMENT

Softcat's Change Management process caters for activities such as patching, fixes, best practice upgrades or any other recommended change to an existing item deployed in Microsoft Azure. Such changes can be for Softcat-recommended items or for Customer-initiated items e.g. a requirement to make a configuration change by raising a Case via email, telephone call or the CMP.

Change requests, including changes to configuration, will be managed under the Softcat Change Management process with the Customer approving all changes. During the Service onboarding process, the Customer will nominate named Customer Contacts who have the authority to approve these changes. The Customer can also initiate a change e.g. a requirement to make a configuration change.

In certain cases, a change may be re-classified by Softcat as a project, at which point additional charges [6] and timelines will apply, based on but not limited to the following principles:

- Any request to build a new item will be viewed as a project. In some examples e.g. building a single item from a pre-defined template, Softcat may agree this as a change.
- Any request for work that requires more than four (4) hours effort to be actioned will be viewed as a project.

[6] For more information, the Customer should contact their Softcat Account Manager.

2.10.1 STANDARD CHANGES

Standard changes are pre-approved changes that are determined as carrying extremely low risk. These changes have defined roll out, back out and test plans associated with them. Standard changes will complete within one (1) Working Day of the request being logged unless the Customer specifies a later date.

2.10.2 NORMAL CHANGES

Normal changes are not pre-approved and will require a Softcat technician to complete a roll out, back out and test plan. Under the Change Management process, these plans will be approved by the Customer and Softcat Change Management. If the change is expected to be actioned on a repeated basis, Softcat and the Customer can mutually agree that it is recorded as a standard change.

2.10.3 RETROSPECTIVE CHANGES

Retrospective changes are only permitted if the change was implemented to resolve or immediately prevent an outage on a business-critical system. For a retrospective change to be actioned, the Customer and Softcat's Change Management approval will be tracked against the Case of the related issue.

2.10.4 EMERGENCY CHANGES

Emergency changes are raised when the implementation window is required in a time prior to the next available Change Advisory Board meeting (CAB). If a Customer requests an emergency change, then it is implemented entirely at their own risk. If the change is not successful, it will be rolled back, if possible. No ad-hoc trouble shooting will be completed.

2.10.5 CUSTOMER PERFORMED MAINTENANCE

These changes are designed to allow Softcat Support to record when a Customer or a Customer's supplier advises that they are performing maintenance work. These changes they will automatically progress through to an 'open' and then a 'closed' state when the scheduled window begins and expires.

2.10.6 PROJECT-RELATED WORK

In certain cases, a change may be re-classified by Softcat as a project, at which point additional quotes and timelines may apply.

Here follows examples which can guide the Customer on whether a request is a business-as-usual ("BAU") change which follows one of the Change Management processes noted in the sections above, or whether it is a chargeable project.

BAU change examples:

- Change of Resource settings; increase or decrease in disk/CPU/memory or firewall policy change.
- Recovery of a backup for a non-service-impacting incident.
- Management of administrative permissions, including Identity & Access Management admin roles and network access.
- Deploying a new environment based on an existing fully templated/code-based environment.

- Minor version updates, e.g. service pack installation or any update which can be completed in-situ/in-place upgrade.
- Adding or decommissioning singular Components, e.g. a new VM (unless it represents a redesign, e.g. adding a Microsoft Azure Firewall to replace a third-party appliance with an audit of rules and series of changes to implement will be out of scope and classed as a chargeable project).

Chargeable change and project examples:

- Design/build of a new solution or new environment within an existing solution.
- Disaster Recovery testing unless otherwise agreed in the contract as an in-scope activity.
- Re-writing/reverse engineering the code-base of an existing solution to the agreed standard, e.g. from Python, ARM or CloudFormation to Terraform.
- Deploying a new environment which is partially or not fully templated/code-based.
- Major version updates including any update which cannot be completed in-situ/in-place but instead requires a new build/rebuild and migration.
- Reverse engineering any Customer-executed console changes to an environment that is agreed as in scope for code-based management.

Please note – this is not an exhaustive list of examples but rather categories of request that are used for illustrative purposes only.

2.11 SERVICE DELIVERY MANAGER

Customers will be assigned a named Service Delivery Manager who will act as a point of contact and escalation for the Service during standard UK Working Hours.

The aligned Service Delivery Manager will produce service reports and deliver service reviews as agreed. As part of the service review, they will run through the report in more detail and discuss and capture any other Service-relevant actions.

Reporting provided will detail performance against pre-defined KPIs and Service Level targets, with various Case details.

2.12 ENHANCED CLOUD OPTIMISATION (OPTIONAL ADD-ON)

The Enhanced Cloud Optimisation Optional Add-On provides Customers with additional levels of analysis from Softcat's FinOps Analysts. The FinOps Analysts produce tailored reports based on the Customer's needs and requirements, as well as holding regular workshops with a subset of stakeholders with the Customer's organisation.

2.12.1 CLOUD ARCHITECTS

Customers will receive a more detailed workshop with Softcat's Cloud Architects to provide technical perspectives on the Customer's infrastructure as well as documentation that outlines Microsoft and Softcat best practices for governance and cost management optimisation. These include:

- Recommending the use of more cost-effective cloud services, or tighter governance policies.
- Architectural guidance and/or peer review for the Customer's existing or planned cloud initiatives, as well as an output document to capture such recommendations.

In fulfilment of these activities, the Customer will benefit from up to four (4) hours per month with a Softcat Cloud Architect. The hours used will be tracked by Softcat each quarter. Beyond the four (4) hours' time allotted, the aligned Softcat Cloud Architect can attend monthly service reviews, however for further needs driven by Customer requirements, additional charges may apply.

2.12.2 FINOPS

Customers will receive a higher level of service and reporting with the Enhanced Cloud Optimisation Service, as outlined below.

Each Customer will have an aligned FinOps Analyst who will review insights from the FinOps Platform and aggregate recommendations into multiple[7] monthly reports and workshops for review. These reports and workshops can be tailored for Customer's business units or pre-defined personas; these requirements will be agreed with the Customer upfront as part of the Service onboarding process. One of these reports will be a senior leadership level summary report including top level KPIs and summary findings.

Customers will also take part in the FinOps 'clean the house' workshop, which focuses on identifying and implementing immediate improvements and optimisation opportunities, to enhance cost efficiency and security posture in the cloud environment(s). The FinOps Analyst will provide actionable insights and strategies to streamline their cloud operations and maximise resource utilisation.

In addition, Softcat's FinOps Analysts will create up to thirty (30) policies and ten (10) perspectives for the Customer in our FinOps Platform, as well as running initial optimisation workshops to examine the areas where cost savings and efficiencies could be made.

The monthly review workshops will include the agreement of plans for actioning the outlined insights to improve areas such as cost and security posture. Softcat's Engineers will action these recommendations following the Change Management process. The FinOps Analysts will track the ongoing savings made through implementation of the optimisations recommended and will highlight the potential further savings to be made if outstanding recommendations are implemented.

The FinOps Analysts will update dashboards, Policies and the financial groups of cloud Resources within the FinOps Platform as required. Customers should request these updates by raising a Case via the CMP.

As part of the Service, Customers will receive a FinOps Maturity Assessment. This assessment will serve as an educational tool covering various topics and starts with an initial questionnaire (as described in section 2.3). A follow up workshop will be conducted, providing an overview of various FinOps capabilities and their respective maturity levels, selected by Softcat's FinOps Analysts. This session will give Customers a clear understanding of their current state and the steps needed for progression.

Following the workshop, the FinOps Analyst will collaborate with the Customer to select the capabilities they wish to focus on as part of their FinOps journey. These selected capabilities will be targeted on a quarterly basis to help the Customer advance in their FinOps maturity. The FinOps Analyst will work closely with the Customer to continuously educate, improve and maximise the value Customers receive from their cloud investments.

For Brownfield Customers, the accuracy of FinOps relies on factors such as cloud Resource tagging. If such tagging is not in place, Softcat will provide recommendations defining these tags. In cases where extensive work is required beyond what can be fulfilled by a Change Request, additional charges will apply.

[7] Up to three (3) reports and workshops are included, with any additional scope subject to further agreement.

3. SERVICE LEVELS

3.1 SOFTCAT SUPPORT

Softcat offers a response Service Level target, which is Softcat's commitment to raise a Case within a given time from when the request is made to Softcat Support.

In the table below, the Service Level target column shows the percentage of requests responded to within the response metric, for example: 95% of Cases logged as a P1 are responded to within fifteen (15) minutes.

The response metrics for Cases are shown in the table below:

Priority	Description	Service coverage hours	Response metric	Service Level target
Priority 1 (P1)	Business impacted or imminent impact expected within four (4) hours; full Customer Site outage; a business-critical system or Supported Product is not working; Customer cannot perform business critical functions; loss of revenue; risk of severe reputational damage; all End-Users unable to perform business critical roles.	24/7	<15 minutes	95%
Priority 2 (P2)	Partial Customer Site outage; loss of redundancy; a non-business-critical system or Supported Product is down; Customer experiencing a high degradation in Service; risk to revenue generation; multiple End-Users unable to perform business critical roles.	24/7	<30 Minutes	95%

Priority	Description	Service coverage hours	Response metric	Service Level target
Priority 3 (P3)	Single End-User issue that prevents them from performing business-critical elements of their role; multiple End-Users affected by an identical issue that does not prevent them from performing their roles; reduction in redundancy for business-critical systems.	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	95%
Priority 4 (P4)	Single user issue that does not prevent them from performing their role or a critical operation; reduction in redundancy for non-business critical systems.	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	95%

Category type	Description	Service coverage hours	Response metric	Fulfilment target	Service Level target
Request 8	Request – Working Hours only	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	Five (5) Working Days	95%

[8] Unless specified otherwise, any requests are subject to the above metrics.

The Service Level target may be reviewed at any point, by mutual Agreement. The document may also be reviewed where changes to the requirements warrant an amendment.

3.1.1 DIRECT MICROSOFT CUSTOMER AGREEMENTS

In respect of Customers who have direct support agreements with Microsoft, the Softcat Service Level target for the respective Case will be paused while the Customer handles any communication with Microsoft. Softcat will continue to manage the Case in accordance with the Service Level parameters, for example, P1 and P2 Cases will continue to be managed by Softcat 24x7x365, but depending on the availability of the Customer and their Working Hours.

Softcat will liaise directly with Microsoft where permitted or via the Customer in the diagnosis and resolution of the Case.

In scenarios where Softcat is the Microsoft Azure billing partner, Softcat will by default also be the Microsoft Azure Break-Fix Support partner (as opposed to Microsoft directly). In such scenarios the Softcat Service Level target will apply as normal.

3.2 CHANGE MANAGEMENT

The Service Level is determined by the type of Change. The Change Management process ensures that standardised methods and procedures are used for efficient and prompt handling of all Change Requests, in order to minimise the impact of change-related incidents upon Service quality, and consequently improve day-to-day operations of the organisation. The Service Level starts from when the Customer supplies Softcat with all of the information that is required by Softcat for the completion of the work. Any time spent determining the Customer's expectations or requirements will not be included in the Service Level.

Category Type	Description	Service coverage hours	Response metric	Service Level target
Standard Change	A pre-approved procedural change with minimum risk and impact to service.[9]	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	95%
Normal Change	A change, which requires authorisation, is complex and / or requires down time for a related service.	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	95%
Emergency Change [10]	A change required to restore service or protect / mitigate a threat to the environment where it is not acceptable to restore under the related Case.	Applied in line with a Major Case (Priority 1)		

[9] This is dependent on all required information being received to complete the request.

[10] Softcat reserve the right to disable users, services, or devices which are found to present an immediate threat to the Customer or Softcat environment without authorisation. This also excludes project related tasks where scope has deviated from agreed design

4. CUSTOMER RESPONSIBILITIES

4.1 PRE-QUALIFYING QUESTIONNAIRE

The Customer must complete all questions within the pre-qualifying questionnaire. These will be sent to them by the Softcat Account Manager.

4.2 SOFTCAT SUPPORT

a. The Customer should ensure that Customer Contact(s) are skilled in or knowledgeable of the Customer's Operating Environment, have sufficient access rights and are of a sufficient proficiency to apply the recommendations that are provided as part of this Service.
b. Prior to Service commencement the Customer should provide:
    i. The Customer's admin on Softcat's ticketing Platform must maintain at least two (2) Customer Contacts for the purposes of Support and continuity; and
    ii. Any relevant Key Information e.g., models, serials, tenancy, Subscriptions.
c. When raising a Case, the Customer Contact should provide, when requested by Softcat:
    i. Reasonable visibility of system logs, configuration files and error messages;
    ii. A description of the symptoms and other services impacted;
    iii. Confirmation of when the issue first occurred and if it has occurred before (where possible provide previous Case references);
    iv. Details of any recent changes or projects implemented prior to the issue being raised;
    v. Details of all fixes, configuration amendments and updates already performed to attempt to resolve the issue prior to raising the Case;
    vi. To what extent the issue is affecting operation of the Customer's business;
    vii. The number of End-Users impacted and their location;
    viii. Contact details of the Customer Contact; and
    ix. Details of any trouble-shooting steps already undertaken.
d. It is the Customer's responsibility to ensure that the Service is made highly available, which may result in additional charges.
e. Direct Support for End-Users. Customers should ensure the Customer's engineer are trained to refer all Cases to the Customer Contact in the first instance, and not permit persons other than a Customer Contact to approach Softcat to register Cases.
f. Use the Service only for the business purposes of the Customer and keep all access credentials and certificates, which Softcat may provide to allow access to the Service, safe and secure, and not share them with any third party without Softcat's prior written consent.
g. Not use or attempt to use or misuse the Services in any way that is criminal or otherwise unlawful in any relevant jurisdiction.
h. In scenarios where Microsoft Azure Agreements are purchased directly with Microsoft, the Customer will be responsible for ensuring any Cases escalated by Softcat are raised with Microsoft for Support.
i. The Service can only be delivered where the Customer purchases Microsoft Azure via Softcat's Cloud Solution Provider (CSP) program or directly from Microsoft. For the avoidance of doubt, the Service cannot be provided where the Customer purchases Microsoft Azure via another partner's CSP program.

4.3 CLOUD ARCHITECT(S)

a. The Customer is required to participate in agenda setting for the quarterly workshops so that Softcat can deliver the content and outcomes the Customer requires.
b. The Customer is required to ensure the appropriate technology stakeholders from their organisation attend the monthly workshops. Relevant attendees may vary depending on the topics selected.
c. The Customer can utilise Softcat capabilities to implement some or all of the optimisation recommendations as part of a separate, paid-for engagement and can take advantage of Innovation Points that may already have been accrued to contribute towards the time and effort required. Where the Customer has in-house capabilities to deliver upon some of those recommendations, this should be discussed and agreed with Softcat to ensure that the changes are well-understood, managed and do not impact any other services.
d. Where additional hours are required with a Softcat Cloud Architect, the Customer is responsible for ensuring they have reviewed and signed any additional documentation provided, such as the Statement of Work and separate quote.

4.4 FINOPS

a. Where applicable (should the Customer have Reserved Instances (RI(s)) in place), Softcat will be reliant on the Customer providing the reservation order so that Softcat can provide the Service outlined in this Service Description.
b. Purchasing of RI(s) where applicable.
c. Provide the necessary Microsoft Azure Portal information to allow Service initiation.
d. Notification of new public cloud account creation for linking to the existing account.
e. Complete onboarding activities aligned to the Customer, to ensure optimisations and recommendations can be provided as part of the Service.
f. The Customer is responsible for reviewing and approving the implementation of the optimisation recommendations identified via Softcat's Change Management process.

4.5 INNOVATION POINTS

a. Engage their Softcat Account Manager when they want to utilise their Innovation Points against an additional service.
b. The Customer is required to have a nominated Customer Contact in order to Call-Off Innovation Points.

4.6 CLOUD MANAGEMENT PLATFORM

Prior to Service commencement the Customer should provide:

i. A minimum of two (2) nominated Customer Contacts; and
ii. The Customer should ensure that the Customer Contacts are available at the start of onboarding and are skilled in and have knowledge of the Customer's Operating Environment, have sufficient access rights and are of a sufficient proficiency to apply the recommendations that are provided as part of this Service.

4.7 SYSTEM MANAGEMENT

4.7.1 IAC-MANAGED

a. The Customer is responsible for ensuring they remove any owner and/or contributor permissions not assigned directly to Softcat, in order for Softcat to manage the environment successfully.

4.7.2 MONITORING AND ALERTING

a. Prior to the Service commencement the Customer should provide:
   i. Connectivity to the Customer estate to make it available to the Softcat Operations Centre; and
   ii. The required passwords for each server covered.
b. The Customer is to ensure that tags or Resources associated with Softcat's Monitoring solution in their environment are not changed or removed.
c. The Customer is required to allow Softcat's Operations Centre the ability to promptly resolve issues highlighted by alerts.
d. The Customer is to accept that alert rules will be suppressed if they do not provide the Softcat Operations Centre approval to resolve the underlying issue or resolve it themselves.
e. The Customer is required to provide a resolver group for bespoke alert rules.
f. The Customer is required to participate in the Change Management process, including approval.

4.7.3 SECURITY AND GOVERNANCE

a. Ensure adherence to all regulatory compliance frameworks available in Microsoft Azure Defender for cloud.
b. Management of Microsoft Azure Arc enabled devices.
c. Management or maintenance of, or Software associated to:
   i. End-User devices (other than the Supported Devices);
   ii. Network devices (other than the Supported Devices); or
   iii. Any other part of the Customer's Operating Environment.
d. Direct Support of End-Users.
e. Support where vendor best practice recommendations have not been implemented by the Customer.
f. Customer data management.
g. Resolution of any application issues.
h. Management of Data Loss Protection (DLP).
i. Customers must not use or attempt to use or misuse the Service(s) in any way that is criminal or otherwise unlawful in any relevant jurisdiction.
j. Any changes that are made to the environment(s) by the Customer that could cause problems/risks/security breaches are the responsibility of the Customer. Caveats will be called out in the relevant Customer documentation.
k. Customers are responsible for defining and maintaining their Role-Based Access Control ("RBAC") roles and security groups.

4.7.4 WINDOWS AND LINUX VM OS MANAGEMENT

a. Connectivity to the Customer Operating Environment to make it available to the Softcat Operations Centre.
b. Providing the required passwords for each server covered.

c. Providing sufficient notification in writing to Softcat Support of the requirement to opt out of automated patching at least five (5) Working Days prior to the patching services commencing. Where no such notification is received, servers will automatically be scheduled for patching.
d. The Customer is responsible for keeping their Windows and Linux Operating Systems updated to the latest Supported versions.

4.7.5 UPDATE MANAGEMENT

a. Prior to Service commencement the Customer should provide:
   i. Connectivity to the Customer estate to make it available to the Softcat Operations Centre;
   ii. The required passwords for each server covered;
   iii. Confirmation that servers can connect to a valid update source.
b. Thirty (30) days' Notice to the Operations Centre of any requested addition(s) or change(s) to the Supported Device inventory or update management schedules.
c. Provide Notice, in line with Softcat's Change Management process, of any required configuration changes.
d. Participate in Change Management process including approval.
e. Have in place a suitable method to restore servers in the event of significant failure.
f. Providing sufficient notification in writing via Softcat Support of the requirement to opt out of automated patching at least five (5) Working Days prior to the patching services commencing. Where no such notification is received, servers will automatically be scheduled for patching.

4.7.6 DISASTER AND RECOVERY

The Service will deploy the Recovery Service Vault (for Microsoft Azure Site Recovery) and the target Microsoft Azure Virtual Network (VNET) if the Customer requires it. Any failover playbooks or testing are the Customer's responsibility. The Service will initiate a failover on their behalf, but the Customer will need to test the target Resources to ensure that the failover was successful.

4.7.7 AZURE BACKUP

a. Customer is responsible for the transfer of any files after a VM restore (new VM or new disk).
b. Customer is responsible for testing the validity of restore data.
c. Customer is responsible for requesting restores via Softcat's Support portal.

4.7.8 ENVIRONMENT ARCHITECTURE

Customers will require a resilient and highly available environment. This will be addressed during onboarding by the Cloud Architects and build team. In the instance that the Customer is unable to change the architecture of their environment to achieve this, the resulting redundancy and resilience risks will need to be included and accepted by the Customer in a risk/decision log.

4.8 CHANGE MANAGEMENT

a. The Customer has a responsibility to ensure that their Customer Contact list is maintained accurately. This determines who is a change approver and who is a commercial approver. In the instance that the approver does not respond, then the next Customer Contact will be contacted to check whether the change is still needed and/or approve it. If no contact can be made within three (3) consecutive days via email/telephone, then the request will be closed.
b. Change Requests to the IaC configuration will enter Softcat's automated testing and deployment pipeline. The Change Request will be scanned for potential security issues, reviewed by Softcat's

engineers, deployed and quality checked. During the Service onboarding process, the Customer will nominate named individuals who have the authority to approve the changes.

c. The Customer is responsible for ensuring they follow the Change Management process for any BAU related activities.
d. Where the Customer requires additional project work outside of BAU activities, they are responsible for ensuring they have notified Softcat via their Softcat Account Manager and/or aligned Service Delivery Manager to begin scoping.

4.9 MAJOR CASE MANAGEMENT

The Customer has a responsibility to ensure that their Customer Contact list is maintained accurately.

4.10 SERVICE DELIVERY MANAGER

a. Provide email distribution list for any service reports or communication.
b. Keep Customer Contact list up to date in the ticketing Platform to allow Service Delivery Manager(s) to provide the Service effectively.
c. Provide advanced notification to Softcat Support of any planned maintenance that could have an impact on any hardware or Software that Softcat provide Services for.
d. Provide advanced notification to Softcat Support of any planned decommissioning of Softcat-related equipment or Software.

4.11 ENHANCED CLOUD OPTIMISATION (OPTIONAL ADD-ON)

a. The Customer is responsible for joining the 'welcome' call with the FinOps Analyst for onboarding and for agreeing the date and scope of the workshop(s).
b. The Customer is responsible for reviewing and approving the implementation of the optimisation recommendations identified by Softcat's FinOps Analyst via Softcat's Change Management process.
c. The Customer must align the appropriate person to attend the 'clean the house' workshop. The workshop can be scheduled at a time that is convenient for the Customer during the Contract period and will be facilitated by the FinOps Analyst.
d. As part of the FinOps Maturity Assessment, the FinOps analyst will identify and advise on security posture. Softcat's Engineers will review the recommendations and action changes via Softcat's Change Management process.
e. Where additional hours are required with a Solution Architect, the Customer is responsible for ensuring they have reviewed and signed any additional documentation provided, such as the Statement of Work and separate quote.

4.12 GENERAL RESPONSIBILITIES

Where the Customer has a Microsoft Unified Support agreement on Subscriptions that require this Service, the Customer is responsible for removing the Subscriptions from the support agreement. The Service cannot commence until such migration has completed. Softcat will guide the Customer through the migration process where required.

5. NOTABLE EXCLUSIONS

5.1 PRE-QUALIFYING QUESTIONNAIRE

The Pre-Qualifying Questionnaire is limited to information required for the selected tenants and Subscriptions only, which will be onboarded to the Service.

5.2 SOFTCAT SUPPORT

At an additional cost the Customer can request project and design work, including Professional Services by contacting their Account Manager for a quote.

5.3 CLOUD ARCHITECT(S)

a. Any type of implementation activities.
b. Creations of Statements of Work or other documentation not specifically highlighted as in scope within this Service Description.

5.4 FINOPS

a. No services other than the FinOps service itself.
b. Performance management of cloud-based assets.

5.5 INNOVATION POINTS

Innovation Points can only be used for services which are listed on the Innovation Points menu. They can be used to purchase these services outright, or to pay for part of the cost of that service. They cannot be used towards any other service or managed/support services and cannot be called off as a cash rebate or discount against this Service.

5.6 CLOUD MANAGEMENT PLATFORM

a. Access to AWS via Single Sign on (SSO) is currently not available.
b. Resource deployment, automation and orchestration is not currently available.

5.7 SYSTEM MANAGEMENT

Under the System Management feature, the following are classed as excluded from the Service:

5.7.1 MONITORING AND ALERTING

a. Custom metrics.
b. Custom log sources.
c. Operating Systems not listed as supported by the vendor.
d. Microsoft Azure Arc enabled devices.
e. Management or maintenance of, or Software associated to:
    i. End-User devices (other than the Supported Devices);
    ii. network devices (other than the Supported Devices); or

iii. any other part of the Customer's Operating Environment.

f. Direct Support for End-Users.
g. Support where Microsoft and Softcat best practice recommendations have not been implemented by the Customer.
h. Customer Data management.
i. Resolution of any Application issues.
j. Management of DLP.
k. Provision of the Service outside of the UK.
l. Any non-Azure-native network troubleshooting/Support/management.

5.7.2 WINDOWS OS MANAGEMENT

a. Support for free of charge Microsoft Online Services.
b. Telephone or remote technical Support of Cases or changes relating to any server or Applications not covered by this Service Description.
c. Support for any changes made to the environment which have been modified against the vendor's specifications and recommendations.
d. Support directly to any End-Users.
e. Any failover testing measures required in automatically or manually failing over the environment from production to disaster recovery and back again.
f. Documentation of the as-built environment.
g. Reinstallation and configuration of the OS in the event of failure. Only a Bare Metal recovery from the latest backup is included as part of the Microsoft OS Backup and Recovery.
h. Reinstallation of any Applications running within the OS.
i. Technical Support required from Softcat to remediate incidents created intentionally or unintentionally by Customer personnel or a third-party making changes to the environment that degrade the Service availability.
j. Any additional Windows server roles, role services and features that are installed as additions to the default items included as part of the base OS installation or as part of a selected optional Application.
k. Migration of a selected optional Application to a newer version. Additional Services engagement can be provided by Softcat should this be required and will be on a time and materials basis at the agreed rate.
l. Essential patches outside the critical and security OS patches installed by the automated monthly patching provided by Softcat.
m. Support for VM versions that are no longer supported by the vendor.
n. Only Microsoft Azure native Resources will be supported, including troubleshooting and escalation to Microsoft as required. No third-party virtual appliances will be supported.
o. Softcat will ensure that the OS is ready to support Applications, but management of the Applications themselves will not be provided.
p. Microsoft Windows server core and or Microsoft Windows client versions.
q. Any Microsoft Windows server versions outside of Microsoft's End of Sale (EOS) date.

5.7.3 LINUX OS MANAGEMENT

a. CentOS Linux – distribution is now End-of-life (EOL) and supported for Brownfield Customers only. In this case a migration path to a supported Linux distribution will be conducted as part of the initial

onboarding assessment. Temporary Support for servers running CentOS Linux during migration period will be given on a best-effort basis.

b. Older Linux distribution versions not currently listed as in the Support period by their respective developer.

5.7.4 SECURITY AND GOVERNANCE

a. Management of Microsoft Azure Defender standard.
b. OS not listed as supported by the vendor.
c. Any liaison with third parties.
d. The Support of third-party code.
e. Any transfer or manipulation of Customer data.

5.7.5 DISASTER RECOVERY

a. Failover playbooks and/or testing.
b. Testing of target Resource to ensure failovers have been successful.

5.7.6 AZURE BACKUP

a. Backup and recovery via the Microsoft Azure Recovery Services (MARS) Agent.
b. VM file level restores. Softcat will restore to a new VM or restore to new disks to attach to an existing VM.

5.7.7 UPDATE MANAGEMENT

a. Microsoft Azure VM Scale Sets.
b. OS not listed as supported by the vendor or the Microsoft Azure update management solution.
c. Microsoft Azure Arc enabled devices.
d. Custom scripting or any pre/post commands.
e. Management or maintenance of, or Software associated to:
    i. End-User devices (other than the Supported Devices);
    ii. Network devices (other than the Supported Devices); or
    iii. Any other part of the Customer's operating environment.
f. Direct Support of End-Users.
g. Support where best practice recommendations have not been implemented by the Customer.
h. Customer Data management.
i. Resolution of any Application issues.
j. Management of DLP.
k. Provision of the Service outside the UK.
l. On demand patching excluding zero-day vulnerabilities.

5.8 SERVICE DELIVERY MANAGER

a. Any bespoke reporting or service reviews. [11]
b. Service Delivery Managers will not act as a project manager or in any other capacity outside of the activities described in this Service Description.

[11] This is available, but subject to an additional charge. Customers can request a quote by contacting their Softcat Account Manager.

5.9 GENERAL EXCLUSIONS

a. The use of Microsoft Azure 'Classic' Resource providers e.g. Azure Service Manager within Microsoft Azure.
b. The Support of any non-Microsoft Products or services purchased via the Microsoft Marketplace.
c. The Support of any non-Microsoft Products or services running on the Microsoft Azure Platform.
d. The Support of third-party code.
e. Only Microsoft Azure native Resources will be supported, including troubleshooting and escalation to Microsoft as required. No third-party virtual appliances will be supported.
f. Any transfer or manipulation of Customer data.
g. Softcat cannot log Cases to Microsoft if the Customer's Subscriptions reside with an alternative partner.

6. SERVICE ACCEPTANCE AND ONBOARDING

Following the acceptance of the Contract, the Onboarding Period will begin. This is the period in which any prerequisite dependencies for the Service are completed, for example:

- Customer sign-off of the onboarding assessment report (delivered under an SOW).
- Access to the Customer's Microsoft Azure environment to commence build.

During the Onboarding Period [12], the Customer will have an aligned onboarding team to ensure key activities are completed throughout. Key activities may include:

- Kick off call between Softcat and the Customer.
- Appropriate reporting / documentation as agreed between Softcat and the Customer.
- Management of Softcat personnel directly connected to onboarding.
- Any project Change Requests required will be managed by Softcat.
- Ensuring Acceptance into Service document is signed.

[12] Where applicable, an SOW will be written to detail the specifics of the Customer's Onboarding Period and additional charges may be incurred.

At the end of the Onboarding Period, the Customer will be provided with an Acceptance Into Service (AIS) document which is required to be signed by the Customer within five (5) days of receipt. The Activation Date for the Service will be the day on which the Onboarding Period ends and is signed off as complete by the Customer or, in the event of no response, five (5) days after the Onboarding Period has completed and the AIS document has been provided (which is the sooner). Where any Key Information requested by Softcat is outstanding at the Activation Date, Softcat's obligation to deliver the Service shall be subject to reasonable endeavours.

Shortly after the Work Order is signed, the Customer will receive a 'Softcat Services Welcome Pack' document, which includes key contact details for Softcat, an overview of the escalation process, and other useful information.

7. SERVICE BILLING AND CONTRACT TERM

The billing frequency and the Initial Term will be agreed with the Customer and confirmed in the Work Order.

Before the end of any existing Contracts, Softcat will contact the Customer at least thirty (30) days prior to expiry with a quote for renewal. Customers will need to provide a minimum of three (3) months' Notice, should they wish to terminate the Contract. In addition, Customers have the option of renewing the Service at any time prior to the renewal date by obtaining a quote from their Softcat Account Manager.

8. TERMS AND CONDITIONS

8.1 OVERVIEW OF TERMS AND CONDITIONS

The delivery of the Service to the Customer shall be governed by this Service Description, the Work Order and Softcat's Terms and conditions and the other Agreements listed below.

- Softcat Terms and conditions: https://www.softcat.com/general-terms-and-policies/terms-and-conditions-uk.

  Capitalised terms in this document shall have the meaning set out here https://www.softcat.com/9916/3785/7176/Softcat-Glossary-and-Definition-of-Terms.pdf

In the event of any discrepancy or conflict between the Softcat Terms and conditions, Service Description and the Work Order, the conflict shall be resolved with the later-listed document taking precedence over those documents listed earlier.

For the purposes of the relevant Work Order and this Service Description, the term "Service" shall be interpreted as an "Annuity Service".

8.2 DATA PROCESSING AGREEMENT AND ACCEPTANCE OF THE CONTRACT

By signing the Work Order, in addition to agreeing to the Service Description, the Customer agrees to the Data Processing Agreement (DPA), available here: https://www.softcat.com/2816/1288/2265/Softcat-Services-DPA2019.pdf.

The DPA shall be a separate agreement to the Contract (and no liability shall arise (i) under this Contract in respect of the Processing, or (ii) under the Data Processing Agreement in respect of the remaining aspects of providing or using the Annuity Services).

If, in the absence of a signed Work Order but following receipt of this Service Description, the Customer provides a purchase order for the Services and/or instructs Softcat to provide the Services, the Customer shall be deemed to have accepted the terms and conditions of the Contract, including the Service Description and the DPA.

8.3 END-USER LICENSE AGREEMENT

End-User's use of the CloudHealth Offerings shall be in accordance with the End-User Agreement located at https://docs.broadcom.com/doc/end-user-agreement-english. By accepting the Work Order, CloudHealth agrees that it shall at all times comply with the EULA.

8.4 SOFTCAT CSM EULA

The Softcat Cloud Management Platform is a Platform that collects and consolidates Customer's cloud environment data by gathering data and metadata related to Customer's use of cloud-based services. It does this through direct integration with the Customer's cloud environment as well as extraction of data via third party solutions, which in turn directly integrate with the Customer's cloud environment.

Softcat CSM EULA:

8.5 FRAUD PREVENTION

Softcat strongly recommend that every Customer implements rigorous fraud prevention and detection risk mitigation controls. To effectively prevent fraudulent activity or misuse it is important to understand potential risks and establish policies and practices that minimise exposure. Some examples of violation and abuse of service include:

- Crypto mining
- Spamming
- Hacking
- Distributed denial of service ("DDoS") attacks
- Malware distribution
- Resale of pirated Subscriptions

Each cloud and service provider makes recommendations to End-Users concerning security, fraud and risk mitigation. It is responsibility of the Customer to review and implement those recommendations. In addition, Softcat recommends using the following policies and practices to reduce exposure to online transaction risks:

- Monitor and secure tenants using tools such as multi-factor authentication ("MFA").
- Enable MFA for privileged accounts/users.
- Regularly monitor usage of cloud spend.
- Set budget alerts and make use of budget control tools.
- Take quick action when suspicious activities are detected.
- Implement a process to quickly receive, review, act on, and respond to Softcat security notifications.
- Manage and track identities using services (such as digital identity services).
- Secure and manage user access keys.
- Restrict the use of root/global admin users for general administration.
- Grant least privilege access to users.
- Decommission redundant accounts and permissions.
- Ensure audit trail/logging is enabled.

It is the Customer's responsibility to secure and protect infrastructure and systems, including tenant(s) and Cloud Platform(s). Softcat does not monitor the Customer's use of cloud or related services, nor who accesses it. Softcat does not accept any responsibility, duty to monitor, or investigate usage.

The Customer is responsible for maintaining security and utilising the available tools to control and monitor usage and spend. Softcat does not accept liability or responsibility for fraudulent, unauthorised access or usage of the Customer's cloud Platform. The Customer is responsible and will be required to pay for such fraudulent or unauthorised use regardless of how it occurs.

8.6 ISO STANDARDS

The Service is fully compliant with the following ISO standards, ensuring the highest levels of quality, security and continuity:

- **ISO 20000 –** Focuses on IT service management, ensuring that services are aligned with business needs and adhere to best practices. By following ISO 20000, the Service guarantees that the IT service

management processes are efficient, effective, and continually improving to meet Customer evolving demands.

- **ISO 27001 -** Dedicated to information security management systems. It helps organisations protect data and manage security risks systematically. Compliance with ISO 27001 ensures that robust security measures are in place to safeguard sensitive information mitigate risks and respond promptly to security incidents.
- **ISO 9001 –** Addresses quality management systems. It ensures that the Service consistently meets Customer requirements and strives for continuous improvement. By adhering to ISO 9001, the Service demonstrates commitment to delivering high-quality services that enhance Customer satisfaction and operational excellence.
- **ISO 22301 –** For business continuity management systems, helping organisations prepare for a respond to disruptive incidents. Compliance with ISO 22301 ensures that the Service has comprehensive plans and procedures in place to maintain business operations during unforeseen events, thereby minimising downtime and ensuring service continuity.

SOFTCAT PLC, FIELDHOUSE LANE, MARLOW, BUCKS, SL7 1LW