PROACT

G-Cloud 14

Proact Monitoring or Managed Service for Public Cloud Service Definition

PROACT

Document control

Document type	Public - Freely Distributable		
Company	Proact IT UK		
Address	Proact IT UK Grayson House, Venture Way, Chesterfield, Derbyshire, S41 8NE		
Telephone	01246 266 300		
Primary contact	bids@proact.oc.uk	Role	N/A

Revision history

Issue date	Author	Version	Revision description
04/04/2024	Colin Abram	V1	Document Upload

PROACT

Proact Monitoring or Managed Service for Public Cloud Service Definition

Proact's Monitoring as a Service provides a 24x7x365 remote monitoring and support solution for a range of device hardware, software, and systems. All monitoring and support activities are performed remotely via secure internet connectivity. Monitoring as a Service provides the following deliverables:

- 24x7x365 Proact Service desk
- 24x7x365 automated monitoring of devices
- Self-service support and self-service monitoring portals
- Break-fix fault co-ordination and resolution
- Event and Incident management.

Proact provide the option for Monitoring to also be consumed as a platform service which can be managed directly by the customer.

Proact's Service Management provides management in addition to monitoring for device hardware, software and systems. All monitoring, support and management activities are performed remotely through secure internet or WAN connectivity.

- 24x7x365 Proact Service desk
- 24x7x365 automated monitoring of devices
- Self-service support and self-service monitoring portals
- Break-fix fault co-ordination and resolution
- Incident management and resolution
- Problem management
- Change and configuration management
- A named Service Delivery Manager to co-ordinate delivery and provide regular customer reports

Proact provide support for the following technology areas as part of the Monitoring and Service Management services:

- Storage systems and associated software
- Hypervisors
- Server Operating Systems
- Network appliances and devices (Firewalls, Switches, Routers, Load Balancers)
- Backup software and associated hardware platform
- Public Cloud
- Azure Virtual Desktop
- Workspace software

This document contains the following appendices detailing the service definitions for the Monitoring and Service Management services:

PROACT

Appendix 1 - Monitoring as a Service (MaaS) Service Definition

1.1 - Service Overview

Proact's Monitoring as a Service (MaaS) provides a 24x7x365 remote monitoring and support solution for a range of hardware, firmware, software and systems.
All monitoring and support activities are performed remotely through secure internet connectivity.
The deliverables of Monitoring as a Service are:

- 24x7x365 Proact Service desk
- 24x7x365 automated monitoring of devices
- Self-service support and self-service monitoring portals
- Break-fix fault co-ordination and resolution
- Event and Incident management.

1.2 - Service Types

Monitoring as a Service is delivered as a Proact managed service.
The following options are applicable to Monitoring as a Service (MaaS). The table below sets out the options available, and in terms of the Service Options provided and the services charging table shown in Section 3 list the Service Options chosen by the customer.

Service Type	Service and component summary
MaaS-Storage	Proact delivers enterprise-class remote monitoring and support of the customer's storage estate.
MaaS-Server	Proact delivers enterprise-class remote monitoring and support of server operating systems, running as physical or virtual servers, on customer site or in a public cloud provider's datacentre.
MaaS-Hypervisor	Proact delivers enterprise-class remote monitoring and support of the customer's hypervisor estate.
MaaS-Hyper-converged	Proact delivers enterprise-class remote monitoring and support of the customer's hyperconverged estate
MaaS-Network	Proact delivers enterprise-class remote monitoring and support of the customer's network estate, including switches, firewalls and routers located on customer site(s).
MaaS-Backup	Proact delivers enterprise-class remote monitoring and support of the customer's backup hardware appliances and backup software infrastructure located on the customer's site(s).
MaaS-Public Cloud	Proact delivers enterprise-class remote monitoring and support of the customer's public cloud estate, which may comprise one or more public cloud networks (that is, Virtual Private Clouds, VPCs or provider-equivalents).
MaaS-Database	Proact delivers enterprise-class remote monitoring and support of SQL databases, running on physical or virtual servers, on customer sites or in a public cloud provider's datacentre.
MaaS-Custom monitoring	Proact delivers enterprise-class remote monitoring with predefined probe definitions for customer's devices that support ICMP, SNMP Trap or HTTP(S).

1.3 - Monitoring as a Service - Architecture

This appendix covers detail on deliverables that are specific to the service. This service also includes the deliverables defined in the **Common Service Deliverables** labelled as 'Monitored'. This architecture is applicable to all service options listed above.

The responsibility for each deliverable is defined below and colour-keyed for easy review:

Proact Responsibility	Customer Responsibility	Joint Responsibility

1.3.1 - Platform

Deliverable	Description and content summary	Responsibility
Monitoring Platform	The Proact Monitoring platform collects, collates and processes statistics, events and alerts. It comprises: ▪ A Remote Monitoring Application at each customer site to collect monitoring information from each Configuration Item (CI). ▪ A central monitoring platform collating statistics, events and alerts from the remote monitoring applications over secure tunnels.	**Proact**
Monitoring Portal	Proact provides the customer with access to the Proact monitoring portal showing monitoring metrics for in-scope systems, to allow customer administrators to view trends and configuration items.	**Proact**
Remote Access	The Proact Remote Access Platform enables engineers to access the customer devices in scope in order to provide support. For all support traffic, Proact operate a VPN or reverse tunnel over the Public Internet or other dedicated WAN link between Proact and each of the customers' sites.	**Proact**

1.3.2 - Components

Deliverable	Description and content summary	Responsibility
Monitoring Application Server	The customer provides one or more virtual or physical servers (Windows or Linux), along with the *operating system* licenses and ongoing management, patching and security of the servers. Whenever Windows systems are to be monitored, the monitoring application server must run Windows itself.	**Customer**
Monitoring Application	Proact will deploy the Remote Monitoring Application on the Monitoring Application Server(s) provided by the customer.	**Joint**
Remote Access	Proact support specialists use a remote management session from a Proact device to connect to devices in scope either directly or via a gateway server at the customer's site.	**Proact**
Support utility	In the event of unavailability of the normal remote management mechanism, a customer-assisted remote support utility session will be used to connect.	**Customer**

1.3.3 - Continuity

Deliverable	Description and content summary	Responsibility

Maintenance – Customer resources	The customer must inform Proact of any planned maintenance or other changes at their premises that may impact any element of the service or generate monitoring alert(s). The customer will work with Proact to remediate any loss of connectivity that occurs as a result of such changes.	**Customer**

1.3.4 - Connectivity

Deliverable	Description and content summary	Responsibility
IP-Address	Monitoring requires an external public static IPv4 address on the customer's (or a third-party or public cloud provider's) firewall; dynamic IP addressing is not supported.	**Customer**
Bandwidth usage	Proact and the customer will both maintain sufficient internet bandwidth to accommodate Monitoring and Support traffic.	**Joint**
Device Access	Remote support is provided using customer-hosted remote support utility.	**Customer**
Internet routing	The communication between the central platforms and the monitoring applications within the customer environment relies on working internet routing between the sites. Proact uses different upstream providers but cannot influence, in general, a variety of hops on the path from the customer to the datacentre(s).	**Out of Scope**
On Demand Access	It may be that one of the devices under monitoring is the routing entry point by which Proact access the environment. In such cases a customer-assisted On-Demand session can be used to assist Proact to investigate the potentially faulty device. This connection is encrypted between the customer administrator's PC/laptop, and a PC/laptop used by a Proact-assigned engineer.	**Joint**
Jump Host	A jump-host or reverse tunnel will be created to enable Proact network engineers' remote access to the devices under monitoring. The IP address of the device will be permitted routed access to all relevant devices.	**Joint**
Log Collection	Devices under monitoring will be configured to send system logs to a collector managed by the customer. This may be located locally or off-site but must be accessible by Proact engineers in the event of an incident to enable troubleshooting.	**Joint**

1.3.5 - Security

Deliverable	Description and content summary	Responsibility
Data encryption	All monitoring and support traffic traverses the public Internet using encrypted tunnels.	**Proact**
Support location	All support is delivered remotely from a secured Proact NOC	**Proact**

1.3.6 - Licensing

Deliverable	Description and content summary	Responsibility

Monitoring Software	Full licensing for monitoring software for the selected option(s) in scope is provided by Proact.	**Proact**

1.3.7 - Hardware Support

Deliverable	Description and content summary	Responsibility
Support Contract(s)	Any CI which is not covered by Proact Premium Support must have a break-fix contract provided by a third-party.	**Customer**
Licenses	Any CI which is not provided by Proact must have maintained and adequate licenses for all used features and/or configurations.	**Customer**

1.4 - Service Deliverables

This section covers the deliverables within “Monitoring as a Service”.

1.4.1 - Service Monitoring

This section gives examples of the items that are included in every Monitoring as a Servicesolution. The exact monitoring configuration may vary according to the particular environment and is subject to change by Proact.

Deliverable	Description and content summary	Responsibility
Monitoring Profiles	The actual implementation of monitoring profiles including alerting thresholds are to be defined in the start-up workshop. These are based on Proact standards and are subject to modification according to changing requirements during the contract term.	**Joint**
Dial-home services	Compatible devices with dial home diagnostics capability may be configured to report to the Proact Service Desk for investigation. This includes errors and system faults which are logged and escalated to customer escalation contacts for investigation. Only reported errors and faults from dial home diagnostics are logged and escalated. This does not include performance, utilisation and misconfiguration reports.	**Customer**

1.4.2 - Operational Activities

The operational activities which are common to all Monitoring as a ServiceOptions are listed in the common section above.

1.5 - Service Upgrades

Deliverable	Description and content summary	Responsibility

Upgrades and new features	This service is a standard service, based on a multi-tenant platform provided by Proact. All upgrades, or enablement of new features, is at the sole discretion of Proact.	**Proact**

1.6 - Acceptance Criteria

Below are the defined service acceptance criteria for Monitor. Invoicing for the service(s) will commence once the following criteria have been met.

Deliverable	Description and content summary	Responsibility
Monitoring	Proact are monitoring successfully the state of CIs in scope, and alerts related to those CIs are being sent to Proact's Service Desk for investigation, except for those where any of the following apply: ▪ The customer has not provided valid and working credentials for monitoring in the required time period The customer has not provided required network access to those CIs from the Monitoring Application as appropriate in the required time period	**Proact**

1.7 - Applicable Service Levels

Response	Applicable Levels
Applicable Service Levels (Incident)	Defined with Common Service Level Agreement (See 1.12), as part of this service, Proact will endeavour meet the following Incident Service Levels: ▪ P1 ▪ P2 ▪ P3
Applicable Service Levels (Changes)	Defined with Common Service Level Agreement (See 1.12), as part of this service, Proact will endeavour meet the following Change Service Levels: ▪ Standard ▪ Normal ▪ Emergency

1.8 - Vendor Terms

The services described in this Services Specification will be subject to all or part of the vendor terms set out in the table below.
These terms are available in full at https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/.

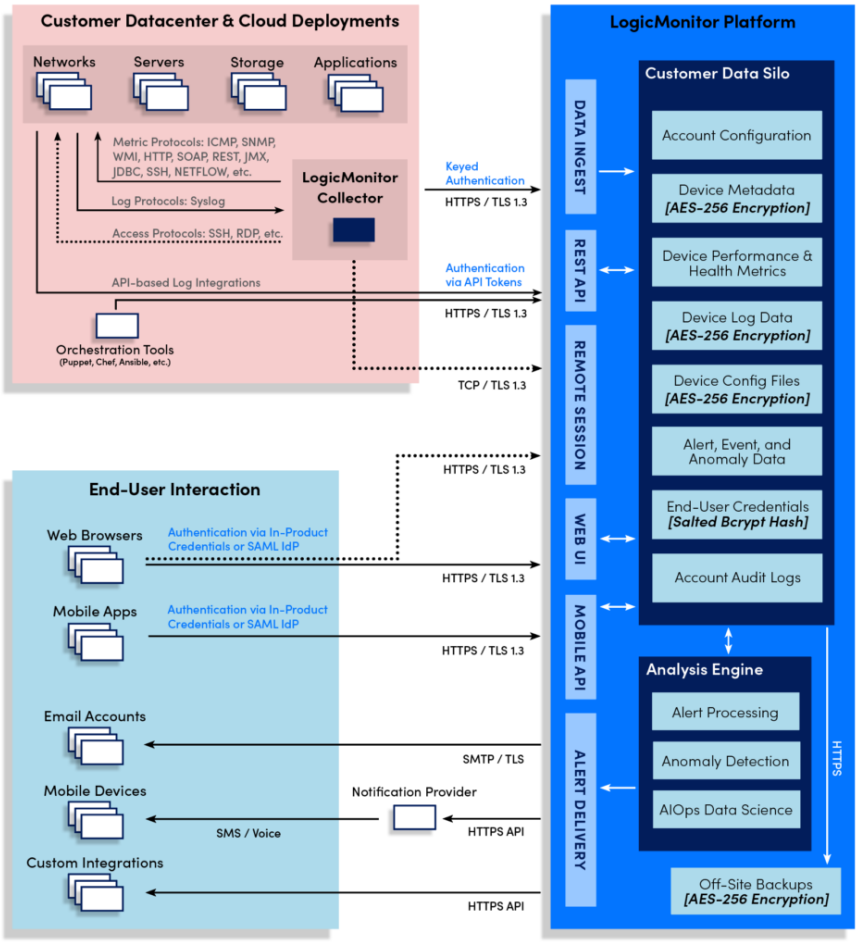
Vendor Name
LogicMonitor

Appendix 2 – Monitoring Platform as a Service (MPaaS) Service Definition

2.1 - Service Overview

Proact's Monitoring Platform as a Service (MPaaS) provides a monitoring solution for systems and services running on-premises, in Proact's and other datacentres, and the public cloud. Proact will deliver a fully managed cloud service that provides an independent monitoring and alerting solution and is configurable by the customer.

The following diagrams shows connectivity and data transfer:



2.2 - Service Types

The Monitoring Platform as a Service is delivered with the following service types:

Service type	Service type summary
MPaaS shared	Proact provide a managed platform for monitoring and alerting. The customer receives an administrative account within Proact's shared platform (https://proact.logicmonitor.com) along with the ability to add and configure monitoring for the devices in his dedicated environment within the shared platform.
MPaaS dedicated	Proact provide a dedicated platform for monitoring and alerting. The customer receives an administrative account within their own dedicated platform (https://[CUSTOMERNAME].logicmonitor.com) along with the ability to add and configure collectors, integrations and monitoring for the devices in this dedicated environment.

2.3 - Service Options

The table below sets out the service options available within MPaaS.

The services provided by Proact are referenced in the charging tables in section 3 of this contract.

Option name	Option description
MPaaS-Enterprise	Proact to provide customer with LogicMonitor Enterprise licenses for a defined number of devices (Configuration Items).
MPaaS-Cloud	Proact to provide customer with LogicMonitor Cloud licenses for a defined number of cloud resources.
MPaaS-Containers	Proact to provide customer with LogicMonitor Container licenses for a defined number of containers.
MPaaS-Logs	Proact to provide customer with LogicMonitor Logs licenses for a defined amount of log data to be ingested, stored and processed (GB).

2.4 - Specific Architecture

This appendix covers detail on deliverables that are specific to Monitoring Platform as a Service (MPaaS). This service also includes the deliverables defined in the **Common Service Deliverables** labelled as 'Managed'.

The responsibility for each deliverable is defined below and colour-keyed for easy review:

Proact Responsibility	Customer Responsibility	Joint Responsibility

2.4.1 - Platform

Deliverable	Description and content summary	Responsibility
Platform	A secure, cloud-based multi-tenant platform for the monitoring of (multi-cloud) IT-environments.	**Proact**
Retention	Raw data ingested is stored within the platform for a 24-month period from the date of saving. All customer specific data will be deleted at the end of the contract.	**Proact**

2.4.2 - Connectivity

Deliverable	Description and content summary	Responsibility
Monitoring traffic	Connectivity for the solution will be via the internet. All monitoring traffic will be directly from the customer's infrastructure to the platform. Customer will maintain sufficient internet bandwidth to accommodate the monitoring traffic.	**Customer**
Customer credentials	An 'admin account' with sufficient privileges to allow administration within the platform will be sent during the service start-up.	**Proact**
Proact admin credentials	During service start-up, Proact will create an additional 'service account' and API token with sufficient privileges to allow support, billing and administration within the platform. This account will be maintained, by Proact, for the length of the contract. The customer must inform Proact prior to changing the password for this service account and provide Proact with the new password.	**Joint**

2.4.3 - Security

Deliverable	Description and content summary	Responsibility
Data encryption	All monitoring data will be encrypted in-flight using standard security protocols (TLS encryption).	**Proact**

2.4.4 - Licensing

Deliverable	Description and content summary	Responsibility
LogicMonitor licensing	Proact to provide customer with an adequate number of licenses of the different types throughout the contract.	**Proact**

2.5 - Configuration

2.5.1 - Service Capabilities

Deliverable	Description and content summary	Responsibility
Monitoring Methods available	Proact to provide the customer with current licensing and versions of the underlying platform, including the full scope of available LogicModules and protocols for data collection.	**Proact**
Monitoring configuration	Customer will configure monitoring within the platform, deploy and connect collectors and amend thresholds as required.	**Customer**
Alerting Methods integration	Proact will provide standard integration capabilities of the platform with external systems to enable the outbound messaging.	**Proact**
Alerting configuration	Customer will configure alerting within the platform, configure integrations and amend thresholds as required.	**Customer**
Active Directory Integrations	Where is MPaaS dedicated service type is purchased, Proact will provide customer with single sign on integration to customer's active directory.	**Proact**

Deliverable	Description and content summary	Responsibility
CMDB/ITSM Integrations	Where is MPaaS dedicated service type is purchased, Proact will provide customer with additional, specific integrations to customer's systems like e.g. ServiceNow. This covers solely the ability to connect, the actual implementation is an onboarding task and not in scope of this service.	**Customer**

2.6 - Service Deliverables

2.6.1 - Operational Activities

Deliverable	Description and content summary	Responsibility
Collector upgrade (Customer)	Where is MPaaS shared service type is purchased, the Customer will upgrade collector versions according to its preferred schedule.	**Customer**
Collector upgrade (Proact)	Where is MPaaS shared service type is purchased, Proact will from time to time automatically upgrade the collectors deployed out of and connected to the shared platform, to ensure collectors remain on supported versions	**Proact**

2.6.2 - Service Monitoring

The following provides an overview of the specific monitoring provided for MPaaS. Proact's standard monitoring deliverables are provided in the Common Service Deliverables appendix.

Deliverable	Description and content summary	Responsibility
Monitored items	▪ Platform status ▪ Device count by type	**Proact**

2.6.3 - Service Upgrades

Deliverable	Description and content summary	Responsibility
Upgrades and new features	This service is a multi-tenant platform provided by Proact. All upgrades, or enablement of new features, is at the sole discretion of Proact.	**Proact**

2.7 - Acceptance Criteria

Below are the defined service acceptance criteria for MPaaS. Invoicing for the service(s) will commence once the following criteria have been met:

Deliverable	Description and content summary	Responsibility
Portal access	Proact will provide a primary account for the customer's monitoring environment and verified functionality of those accounts.	**Proact**
First collector provisioned	Customer has provisioned and connected one or more collectors.	**Customer**

2.8 - Vendor Terms

The services described in this Services Specification will be subject to the vendor terms set out in the table below.

These terms are available in full at https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/.

Vendor Name
LogicMonitor

2.9 - Service Level Agreement

2.9.1 - Availability Service Levels

This service level agreement sets out what levels of uptime availability Proact will endeavour to provide. Availability is monitored using Proact's software platform and is measured continuously. The SLAs will be measured in units of a month; however, service reports will be provided to the customer quarterly.

Service	SLA	Monthly SLA Description	Measurement
MPaaS	99.9%	The service will be available for at least 99.9% of each month	The service will be available if the Portal-URL assigned to the customer responds to Proact's monitoring software's requests.

PROACT

Appendix 3 - Service Management Service Definition

3.1 - Service Overview

Proact's Service Management provides a 24x7x365 remote monitoring, support and management solution for a range of hardware, firmware, software and systems.
All monitoring, support and management activities are performed remotely through secure internet or WAN connectivity.

- 24x7x365 Proact Service desk
- 24x7x365 automated monitoring of devices
- Self-service support and self-service monitoring portals
- Break-fix fault co-ordination and resolution
- Incident management and resolution
- Problem management
- Change and configuration management
- A named Service Delivery Manager to co-ordinate delivery and provide regular customer reports

3.2 - Service Types

Service Type	Service and component summary
SM-Storage	Proact delivers enterprise-class remote monitoring, support and management of the customer's storage estate.
SM-Server	Proact delivers enterprise-class remote monitoring, support and management of server operating systems, running as physical or virtual servers, on customer site or in a public cloud provider's datacentre.
SM-Hypervisor	Proact delivers enterprise-class remote monitoring, support and management of the customer's hypervisor estate.
SM-Hyper-converged	Proact delivers enterprise-class remote monitoring, support and management of the customer's hyperconverged estate
SM-Network	Proact delivers enterprise-class remote monitoring, support and management of the customer's network estate, including switches, firewalls and routers located on customer site(s).
SM-Backup	Proact delivers enterprise-class remote monitoring, support and management of the customer's backup hardware appliances and backup software infrastructure located on the customer's site(s).
SM-Public Cloud	Proact delivers enterprise-class remote monitoring, support and management of the customer's public cloud estate, which may comprise one or more public cloud networks (that is, Virtual Private Clouds, VPCs or provider-equivalents).
SM-Database	Proact delivers enterprise-class remote monitoring, support and management of SQL databases, running on physical or virtual servers, on customer sites or in a public cloud provider's datacentre.

3.2.1 - Platform

Deliverable	Description and content summary	Responsibility
Monitoring Platform	The Proact Monitoring platform collects, collates and processes statistics, events and alerts. It comprises: ▪ A Remote Monitoring Application at each customer site to collect monitoring information from each Configuration Item	**Proact**
Monitoring Portal	Proact provide the customer with access to the Proact monitoring portal showing monitoring metrics for in-scope systems, to allow customer administrators to view trends and configuration items (CIs).	**Proact**
Remote Access	The Proact Remote Access Platform enables engineers to access the customer devices in scope in order to perform health checks, implement changes and resolve incidents. For all support and service management traffic, Proact operate a VPN or reverse tunnel over the Public Internet or other dedicated WAN link between Proact and each of the customers' sites.	**Proact**
Communication system usage	All requests should be by telephone to Proact's Service Desk or via Proact's Service Portal.	**Customer**

3.2.2 - Components

Deliverable	Description and content summary	Responsibility
Monitoring Application Server	The customer provides a virtual or physical server (Windows or Linux), along with the *operating system* license and ongoing management, patching and security of the server.	**Customer**
Monitoring Application	Proact will deploy the Remote Monitoring Application that is required to be run within the customer environment. Whenever Windows systems are to be monitored, the application has to be installed on a Windows server.	**Joint**
Remote Access	Proact support specialists use a remote management session from a Proact device to connect to devices in scope either directly or via a gateway provided by the customer.	**Proact**
Support utility	In the event of unavailability of the normal remote management mechanism, a customer-assisted remote support utility session will be used to connect.	**Customer**

3.2.3 - Continuity

Deliverable	Description and content summary	Responsibility
Maintenance – Customer resources	The customer must inform Proact of any planned maintenance or other changes at their premises that may impact any element of the service or generate monitoring alert(s). The customer will work with Proact to remediate any loss of connectivity that occurs as a result of such changes.	**Customer**
Maintenance - Public Cloud	The customer must advise Proact of any planned maintenance or other changes to their cloud environment that may impact on Proact's ability to connect to resources hosted there. The customer will work with Proact to remediate any loss of connectivity that occurs as a result of such changes.	**Customer**
Customer-managed systems	Where devices and/or services under Proact Service Management interact with any system, application or environment not managed by Proact, it is the customer's responsibility to ensure that it remains compatible with any Proact-managed systems/applications at the hardware, firmware, OS, and application version levels – as recommended by Proact or its vendors as best practice.	**Customer**
Business Impacting Scheduled Maintenance	Proact must advise the customer of any scheduled maintenance it is performing on the devices under management that may impact the customer's business and ensure that there is an communicated maintenance window within which the work occurs.	**Proact**

3.2.4 - Connectivity

Deliverable	Description and content summary	Responsibility
IP-Address	Monitoring and management requires an external public static IPv4 address on the customer's (or a third-party or public cloud provider's) firewall; dynamic IP addressing is not supported.	**Customer**
Bandwidth usage	Proact and the customer will both maintain sufficient internet bandwidth to accommodate Monitoring and Support traffic.	**Joint**

Deliverable	Description and content summary	Responsibility
Device Access	Customer will create Proact user accounts on devices under management at super-user/administrator/root level to permit full device management.	**Customer**
Internet routing	The communication between the central platforms and the monitoring applications within the customer environment relies on working internet routing between the sites. Proact uses different upstream providers but cannot influence, in general, a variety of hops on the path from the customer to the datacentre(s).	**Out of Scope**
Proact Access	Access by Proact network engineers to devices under management must be enabled by the customer and be available at all times. In the event of apparent device failure, or during device upgrades when normal connectivity may not be available, an alternate connection method must be provided, including access to the device serial port.	**Customer**
On Demand Access	It may be that one of the devices under management is the routing entry point by which Proact access the environment. In such cases a customer-assisted On-Demand session can be used to assist Proact to investigate the potentially faulty device. This connection is encrypted between the customer Administrator's PC/laptop, and a PC/laptop used by a Proact-assigned engineer.	**Joint**
Jump Host	A jump-host or reverse tunnel will be created to enable Proact network engineers' remote access to the devices under management. The IP address of the device will be permitted routed access to all relevant devices.	**Joint**
Log Collection	Devices under management will be configured to send system logs to a collector managed by the customer. This may be located locally or off-site but must be accessible by Proact engineers in the event of an incident to enable troubleshooting.	**Joint**

3.2.5 - Security

Deliverable	Description and content summary	Responsibility
Data encryption	All monitoring and support traffic traverses the public Internet using encrypted tunnels.	**Proact**
Support location	All support and management is delivered remotely from a secured Proact NOC	**Proact**

3.2.6 - Licensing

Deliverable	Description and content summary	Responsibility
Remote Monitoring Software	Full licensing for monitoring software for the selected option(s) in scope is provided by Proact.	**Proact**
Remote Management Software	Full licensing for remote management software for the selected service option(s) in scope is provided by Proact. Access licenses to devices in scope are provided by the customer.	**Joint**

3.2.7 - Hardware Support

Deliverable	Description and content summary	Responsibility
Support Contract(s)	Any CI which is not covered by Proact Premium Support must have vendor support or a vendor backed break-fix contract provided by a third-party.	**Customer**
Licenses	Any CI which is not provided by Proact must have maintained and adequate licenses for all used features and/or configurations.	**Customer**

3.2.8 - Service Monitoring

Deliverable	Description and content summary	Responsibility
Monitoring profiles	The actual implementation of monitoring as well as associated thresholds are to be defined in the start-up workshop. These are based on Proact standards and are subject to modification according to changing requirements during the contract term.	**Joint**
Dial-home services	Compatible devices with dial home diagnostics capability are configured to report to the Proact Service Desk for investigation. This includes errors and system faults which are logged and escalated to customer escalation contacts for investigation. Only reported errors and faults are logged and escalated from dial home diagnostics. This does not include performance, utilisation and misconfiguration reports.	**Customer**

3.2.9 - Operational Activities

Deliverable	Description and content summary	Responsibility
Incident Management	Proact will provide hardware break-fix, critical alert fault and vendor coordination as well as incident support and resolution. Response time SLA are applicable.	**Proact**
IT Service Continuity Management	Proact will participate in *DR* documentation, contingency testing and in any actual recovery activity, in line with contractual scope.	**Proact**
Change Management	Proact will perform standard, approved normal and emergency changes following change requests (CRs) in line with the response time SLA, limited to specified CIs and Options. All CRs are performed under the Proact Change Management process, which will interact with the customer's change processes as required, including submission of CRs to the customer's *CAB*	**Proact**
Health checks	Proact perform yearly health checks on all managed systems to review performance, ensure sound configuration, review capacity, and identify any risks and recommended updates. The findings of these health-checks will be included in the technical sections of Service Review reports.	**Proact**

3.2.10 - Service Upgrades

Deliverable	Description and content summary	Responsibility
Upgrades and new features	This service is a standard service, based on a multi-tenant platform provided by Proact. All upgrades, or enablement of new features, is at the sole discretion of Proact.	**Proact**

3.2.11 - Acceptance Criteria

Deliverable	Description and content summary	Responsibility
Monitoring	Proact are monitoring successfully the state of CIs in scope, and monitoring alerts for those CIs are being sent to Proact's Service Desk for investigation, except for those where any of the following apply: ▪ The customer has not provided valid and working credentials for monitoring in the required time period ▪ The customer has not provided required access to those CIs as appropriate in the required time period	**Proact**
Initial Health Check	Prior to service commencement Proact will conduct a health check to identify deviations from Proact's configuration best practices. It is the customer's obligation to remediate any of these deviations prior to any SLA being applicable or operational activities to be carried out.	**Joint**
Remote Access	Proact engineers can access devices under management using the agreed method.	**Joint**
Out-of-band console access	The customer will provide out-of-band console access to all physical devices under management, and this connectivity is tested as working.	**Joint**

3.3 - Applicable Service Levels

Response	Applicable Levels
Applicable Service Levels (Incident)	Defined with Common Service Level Agreement (See 1.12), as part of this service, Proact will endeavour meet the following Incident Service Levels: ▪ P1 ▪ P2 ▪ P3
Applicable Service Levels (Changes)	Defined with Common Service Level Agreement (See 1.12), as part of this service, Proact will endeavour meet the following Change Service Levels: ▪ Standard ▪ Normal ▪ Emergency

3.4 - Service Management for Storage Service Definition

3.4.1 - Service Options

Service Option	Option Number	Service and component summary
SM-Storage Controller	1	Covers the basic functionality of storage controllers. (mandatory)
SM-Storage Data Protection	2	Selected when an in-scope controller is either in a replication relationship or being used to drive backups
SM-Storage Hosts	3	Selected when SAN-connected hosts connect into the controller(s) ▪ Manages the storage element of the host only ▪ Does not extend to management of the server as a whole ▪ Covers the storage vendor's software installed on the servers to take application consistent backups and connectivity software to manage LUNs presented to the hosts.
SM-Storage NAS	4	Selected when an in-scope controller is used as a NAS and performs file serving activities.
SM-Storage SAN	5	Selected when an in-scope controller is part of a SAN and performs block based activities.
SM-Storage S3	6	Selected when an in-scope controller performs object based activities.
SM-Storage Switches	7	Selected when in-scope Storage and/or SAN switches connect to controllers. ▪ This option manages the switch's basic element and any port or zoning required to connect controllers to the SAN. ▪ If this option is associated with a Fibre Channel over Ethernet switch, it only covers the Fibre Channel element of the switch.

3.4.2 - Operational Activities

Deliverable	Applicable Options	Description and content summary	Responsibility
Logical Unit Management	1	Proact creates, modifies, deletes and assigns logical storage units across the available tiers on the managed controller(s).	**Proact**
Efficiency	1, 4-6	Proact configures and manages vendor provided storage efficiency features on in scope devices.	**Proact**
Physical Components (Proact)	1	Proact remotely manages the configuration of physical components including discs and other system components.	**Proact**
Physical Components (Customer)	1	It's the customers responsibility to replace Customer Replaceable Units as per vendor's definition.	**Customer**
Snapshots	4-5	Proact will create and make available clones and snapshots using the vendor provided disc management and data protection features.	**Proact**

Deliverable	Applicable Options	Description and content summary	Responsibility
Replication	6	Proact will create information lifecycle policies and/or erasure coding for cross site replication and redundancy.	**Proact**
Management Applications	1	Vendor or Proact provided management and reporting toolsets are used and supported as defined during the start-up workshop	**Proact**
Networking	1, 4-6	Proact manages the network configuration of in scope devices through vendor provided tools.	**Proact**
Performance	1	Proact manages performance related configurations of in scope devices through vendor provided tools.	**Proact**
Data Protection	2	Proact manages synchronous and asynchronous replication between in scope devices through vendor provided tools.	**Proact**
System Contingency Testing	2	In conjunction with the customer's wider DR procedures, Proact will perform any storage controller related commands and tasks necessary to make the data available on a replicated storage system. Tests must be performed within Proact's normal business hours.	**Joint**
Backup	3	Proact manages storage vendor provided backup tools and replication to storage systems on in scope hosts.	**Proact**
Host Connectivity	3	Proact manages storage specific access configuration to in scope storage systems along with vendor provided tools on in scope hosts.	**Proact**
Authentication	4,6	Proact manages OS provided authentication and file locking mechanisms on devices in scope.	**Proact**
Management	4-6	Proact manages integration with supported tooling on hosts, licensing, quotas and statistics on in scope devices.	**Proact**
Namespace	4	Proact manages distributed file systems and replication within those using tooling provided by the vendor with the base OS.	**Proact**
Security	1	Proact manages the in-scope devices encryption features through vendor provided management tools.	**Proact**
Connectivity	7	Proact manages connectivity between in scope switches and connected in scope devices.	**Proact**
FCP/FCoE Switch	7	Proact manages Port configuration, grouping and zoning on in scope devices.	**Proact**

3.5 - Service Management for Servers Service Definition

3.5.1 - Service Options

Service Option	Option Number	Service and component summary
SM-Base	1	Covers the basic functionality of the Server operating system and includes routine items common to every server.
SM-Server Physical	2	Selected when the server operating system is running directly on physical hardware. It also covers items associated with the physical server.
SM-Server Clustering	3	Selected when the server is in a local high-availability cluster where resources may move between servers to increase the availability of the resources
SM-Server Patching	4	Selected when the server's operating system is kept up to date with regular patching to keep in-line with the operating system manufacturer's best practice. The patching feature set extends to *centralised patching*.
SM-Server Security	5	Selected when the server has *Anti-Virus* (*AV*) software or agents installed. The Security option extends to centralised AV management servers.
SM-Server File/Print	6	selected where the server is offering file and-or print services using the operating system's native file and-or print capabilities.

3.5.2 - Operational Activities

Deliverable	Applicable Options	Description and content summary	Responsibility
Connectivity	1	Proact manages interaction between the devices in scope and central user authentication systems as well as remote client access configurations.	**Proact**
Manage-ment	1	Proact manages the in-scope devices through vendor provided management tools including logging and, where appropriate, licensing configuration	**Proact**
Networking Config	1	Proact manages the network client configuration of in scope devices including routing configuration and packet encapsulation where provided by the base OS.	**Proact**
Access Security	1	Proact manages the basic user and group access, encryption and certificate configuration of in scope devices.	**Proact**
Local Storage	1	Proact manages local file systems using tooling and features provided by the vendor with the basic OS.	**Proact**
Hypervisor Tools	1	Proact manages hypervisor related tools running inside VMs in scope where it is not supported from central hypervisor level.	**Proact**
Network Connections	2	Proact manages Fiber Channel over Ethernet and associated encapsulations to achieve lossless transport.	**Proact**
IPMI Management	2	Proact manages the integrated IPMI (Intelligent Platform Management Interface) configuration of in scope devices.	**Proact**
Physical Networking	2	Proact manages physical network adapters and native features of these as well as the network connection to the servers blade chassis.	**Proact**

Deliverable	Applicable Options	Description and content summary	Responsibility
TPM Management	2	Proact manages the in scope devices Trusted Platform Module (TPM).	**Proact**
BIOS	2	Proact manages the pre-boot configuration and manageable, vendor provided, hardware including blade-centers of in scope devices.	**Proact**
Boot Storage	2	Proact manages internal storage and network boot of in scope devices.	**Proact**
Backup	3	Proact manages the backup and synchronisation of clustering configuration between in scope devices.	**Proact**
Load Balancing	3	Proact manages the native built-in network load balancer functionality of the in scope devices OS.	**Proact**
Disaster Recovery	3	Proact ensures a proper failover of services running on in scope devices at an OS level.	**Proact**
OS Clustering	3	Proact manages the actual OS clustering functionality of in scope devices.	**Proact**
Cluster Networking	3	Proact manages the clustering related networking configuration of in scope devices.	**Proact**
Cluster Storage	3	Proact manages the storage clustering functionality of in scope devices on an OS level.	**Proact**
Centralised patching service	4	Proact will provide centralised multi-tenant patching system(s) to which the customer can register their servers for patching.	**Proact**
Dedicated patching system (existing)	4	Where the customer requires an existing customer-owned dedicated patching system to be used on-premise, this must have been specified within the contract and must be configured to meet Proact's best practices. Proact shall perform a health check of any such existing system and the customer shall be responsible for remediating current configuration to meet best practice according to the result of the health check, prior to service commencement.	**Joint**
Dedicated patching system (new)	4	Where the customer requires a new dedicated patching system to be used on-premise, this must have been specified and costed within the service agreement. Any requirements not declared in the service agreement shall be scoped and priced as a separate Professional Services engagement, at the customer's cost.	**Out of Scope**

Deliverable	Applicable Options	Description and content summary	Responsibility
Local server / central configuration management	4	The customer must configure all servers in scope for patching (directly or via a central configuration management tool) to point towards Proact's centralised patching services via URL, and to be registered against one of the available patch approval time groups, details of which shall be provided by Proact during Service Transition. If the customer requires Proact to advise on patch groupings, timings or centralised management configurations, this shall be scoped and priced as a separate Professional Services engagement, at the customer's cost.	**Customer**
Initial server patch levels	4	The customer is responsible for making sure all systems in scope of patching are **no more than 90 days out of date** with vendor critical and security patches before go-live. Systems that are outside this timeframe may still be able to be patched by Proact but may not behave optimally or as expected. Where this occurs, it remains the customer's responsibility to remediate these issues. Proact reserve the right to levy additional professional services charges for any work required by Proact to assist the customer in remediation of these issues.	**Customer**
Patch frequency and selection	4	Proact will review and process vendor patch releases on a monthly basis, and to deliver approved patches within 30 days of release. By default, Proact will mark for approval all patches classified as "Critical" and/or "Security" by the vendor. The Customer may request that Proact use different or additional selection criteria, within the capabilities of the technologies being used for patching.	**Proact**
Adding or excluding patches from selection	4	It is the customer's responsibility to notify Proact at least 8 working hours prior to the scheduled patching if they wish to request any particular patches to be excluded, or for any specific non-critical / non-security patches to be installed in addition to the patches announced.	**Customer**
Patches for applications	4	Patching covers the base operating system and associated built-in components only. Patches for applications will not be installed unless those applications are separately contracted for Service Management (for example, Active Directory)	**Out of Scope**
Patch approval groups	4	Customer may select to assign in-scope CIs to separate patching groups for which patches are approved on a consecutive week basis each month. Up to 3 groups may be utilised. If no groups are specified, Proact will assign all customer systems to the first weekly patching group	**Customer**

Deliverable	Applicable Options	Description and content summary	Responsibility
Patch status reporting	4	Wherever a centralised patching system is utilised, Proact will provide patch status as according to that system to the customer on regular intervals within scheduled Service Review reports.	**Proact**
Anti-Virus (Proact)	5	Proact manages supported Anti-Virus products installed, including scanning for and quarantining of infected files.	**Proact**
Anti-Virus (Joint)	5	The scope of this element of the service is the recommendations provided by the AV tools and depending on the recommendation will either be actioned by the software directly or escalated to the customer's administrator to resolve.	**Joint**
OS Security	5	Proact configures the system's security settings according to tooling provided by the vendor with the base OS.	**Proact**
OS Tools	5	Proact manages operating system security using tooling provided by the vendor with the base OS.	**Proact**
Authentication Security	6	Proact manages OS provided authentication and file locking mechanisms on devices in scope.	**Proact**
SMB/NFS	6	Proact manages OS provided SMB and NFS connectivity on devices in scope.	**Proact**
Document Management	6	Proact manages print server configuration and connectivity to network printers using tooling provided by the vendor with the base OS.	**Proact**
Quota Management	6	Proact manages file server and quota configuration using tooling provided by the vendor with the base OS.	**Proact**
DFS Namespace	6	Proact manages distributed file systems and replication within those using tooling provided by the vendor with the base OS.	**Proact**
Access Control	6	Proact manages access control to file services using tooling provided by the vendor with the base OS.	**Proact**
Physical Server IPMI	2	The customer must ensure each physical server has a separate out-of-band management interface conforming to the *IPMI* standard and central management software. Proact require access to this interface to work on the servers, associated devices and firmware.	**Customer**
Hardware alerts	2	For physical servers, hardware alerts are dealt with by automated alerts where the hardware has a separate out-of-band management interface that supports both IPMI and SNMP.	**Proact**
Cluster Management	3	Proact manage clustered servers using the native OS clustering software or native OS network load balancer (NLB).	**Proact**
File services	6	Proact manages the File Server functionality, limited to the services provided by the Server's OS.	**Proact**
Print Services	6	Proact manages the Print Server functionality, limited to the services provided by the Server's OS.	**Proact**

3.6 - Service Management for Hypervisors Service Definition

3.6.1 - Service Options

Service Option	Option Number	Service and component summary
SM-Hypervisor Base	1	Covers the basic functionality of the hypervisor OS including features common to most hypervisor systems: names, IP addresses, data store management (for example: volume expansion) and VM resource allocation.
SM-Hypervisor Management	2	Selected when the hypervisor hosts are managed through a central management application (for example: VMware vCenter or Microsoft Virtual Machine Manager) to enhance the capabilities of the Hypervisor.
SM-Hypervisor Dataprotection	3	Selected when the hypervisor host is a replication relationship (for example: for DR or Backup) using native hypervisor-based replication applications.
SM-Hypervisor Backup and Restore	4	Selected when native hypervisor OS capabilities are being used as the primary method of backing up and restoring data
SM-Hypervisor Hyperconverged	5	Selected when the hosts is from a hyper-Converged manufacturer or is running a hyper-converged OS

3.6.2 - Operational Activities

Deliverable	Applicable Options	Description and content summary	Responsibility
Hypervisor Server Manage-ment	ALL	The customer must ensure each hypervisor server has a separate out-of-band management interface conforming to the *IPMI* standard and central management software. Proact require access to this interface to work on the servers, associated devices and firmware.	**Customer**
Hardware alerts	ALL	For hypervisor systems, hardware alerts are dealt with by automated alerts where the hardware has a separate out-of-band management interface that supports both IPMI and SNMP.	**Proact**
Integration software updates	ALL	Proact rolls out updates to the hypervisor related tools running inside VMs where it is supported from central hypervisor level.	**Proact**
Provisioning of new VMs	ALL	Proact provision new VMs either by cloning existing VMs or by deploying them from existing templates.	**Proact**
Hypervisor updates	2	Proact update the associated central management application (and separate database if applicable) used to administer multiple hosts, as part of the update of the Hypervisor environment.	**Proact**
DR updates	3	Proact upgrade the DR application used to perform system contingency testing as part of hypervisor environment upgrades	**Proact**

Deliverable	Applicable Options	Description and content summary	Responsibility
Datastore Manage-ment	ALL	Proact manage the data store capacity of hypervisors based on threshold breaches, and growth predictions based on historical trend reports. This is only possible when sufficient spare capacity for growth is provided by the customer throughout the contract term.	**Joint**
VM backup and restore	4	Proact restore VMs as requested by the customer using the native SnapShot and-or Backup capabilities of the hypervisor	**Proact**

3.7 - Service Management for Network Service Definition

3.7.1 - Service Options

Service Option	Option Number	Service and component summary (where supported by Vendor and device capability)
SM-Network Access Switch	1	covers the basic functionality of the Ethernet switching
SM-Network Distribution Switch	2	selected for switches with basic L3 functionality, QoS and/or internal dynamic routing protocols
SM-Network Core Switch	3	selected for switches with extended L3 functionality, IPv6, MPLS and/or external dynamic routing protocols
SM-Network Branch Router	4	covers the basic functionality of routers
SM-Network Enterprise Router	5	selected for routers with multihoming and/or additional features
SM-Network Branch Firewall	6	covers the basic functionality of firewalls
SM-Network Enterprise Firewall	7	selected for firewalls with multihoming and/or additional features

3.7.2 - Operational Activities

Deliverable	Applicable Options	Description and content summary	Responsibility
Basic Ethernet Manage-ment	ALL	Proact manages ethernet functionality of covered devices, limited to: ▪ Ethernet connectivity only (not FibreChannel nor FibreChannel over Ethernet) ▪ Configuration of access and trunk (dot1q) ports to connect to endpoints, including use of aggregated ethernet (port-channel) ▪ Configuration of uplink ports to other network devices	**Proact**
Access and Log Manage-ment	ALL	Proact manages basic access and logging functionality of devices in scope, limited to: ▪ Device access management using AAA ▪ Syslog to external collector	**Proact**
Basic Switch Manage-ment	1-3	Proact manages basic common switching functionality of devices in scope, limited to: ▪ Configuration and management of VLANs and STP across the network, including support for Voice VLAN ▪ Port protection eg BPDU Guard, Root Guard or vendor equivalent ▪ Switch Stacking and power-redundancy where available	**Proact**
Common L3 Features	2-7	Proact manages basic routing and tagging on devices in scope, limited to: ▪ DHCP, including DHCPv6 and DHCP-Snooping or vendor equivalent where applicable ▪ IPv4 and IPv6 interface addressing and static routes ▪ VLAN interfaces and VLAN-tagged subinterfaces	**Proact**
Additional L2 Features	2-5	Proact manages additional Ethernet features on devices in scope, limited to: ▪ QoS ▪ Next-Hop resolution protocols (HSRP, VRRP or vendor equivalent)	**Proact**
Dynamic Routing Protocols	2-5,7	Proact manages dynamic routing on devices in scope, limited to: ▪ IP routing protocols RIP, OSPF, EIGRP (where applicable)	**Proact**
Border Gateway Protocol	3-5,7	Proact manages dynamic routing via BGP (Border Gateway Protocol) on devices in scope. This is only valid for a table with a limited number of routes and a maximum of two (2) neighbours.	**Proact**

Deliverable	Applicable Options	Description and content summary	Responsibility
Additional L3 Features	3,5	Proact manages additional Ethernet features on devices in scope, limited to: ▪ IPv6 Tunnelling ▪ MPLS (LDP and RSVP) ▪ L3-VPN and L2-VPN ▪ IP-Fabric, including eVPN and VXLAN ▪ VRF	**Proact**
Distribution Switch Features	2-3	Proact manages additional features typical to distribution switches in scope, limited to: ▪ Policy routing and Route-Maps ▪ Port Security ▪ MACSec ▪ IGMP and PIM Snooping	**Proact**
Core Switch Features	3	Proact manages additional security features typical to core switches in scope, limited to: ▪ 802.1x Identity-based management ▪ PIM Sparse Mode or Bidirectional PIM	**Proact**
Branch Router Features	4-5	Proact manages additional features typical to routers on devices in scope, limited to: ▪ Simple ACL/firewall ruleset ▪ DMVPN or Vendor equivalent ▪ NetFlow ▪ IGMP and PIM Snooping ▪ VRF-lite	**Proact**
Enterprise Router Features	5	Proact manages additional features typical to enterprise routers on devices in scope. This is aiming at Multiple Full Feeds and additional security, limited to: ▪ Multihoming ▪ BGP full internet routing table ▪ PIM Sparse Mode or Bidirectional PIM	**Proact**
Branch Firewall Features	6-7	Proact manages additional features typical to firewalls on devices in scope, limited to: ▪ High Availability ▪ DNS ▪ NTP client ▪ ACLs (Firewall Rules and NAT) ▪ IPS ▪ Remote Access (SSL) and site to site VPN – where device supports this	**Proact**
Enterprise Firewall Features	7	Proact manages additional features typical to Enterprise Firewalls on devices in scope, limited to: ▪ Support for Multicast ▪ NTP server ▪ LDAP support for user-defined firewall rules ▪ NGFW anti-malware, deep protocol inspection (ALG), IPS and antivirus ▪ URL filtering ▪ SSL proxy and Certificate management ▪ Multi-context and virtual instances	**Proact**

Deliverable	Applicable Options	Description and content summary	Responsibility
Health Check	ALL	Proact will conduct a yearly health-check on the service, covering: ▪ Device health ▪ Firmware ▪ Bug reports from Vendors* Vulnerabilities*	**Proact**
Vulnerability Reports	ALL	* Proact collects vulnerability and bug reports from Vendors on an ongoing basis and will respond to serious and critical issues as they arise. Critical vulnerabilities are addressed within 10 days, and Major issues within 30 days.	**Proact**
Utilisation Checks	ALL	▪ Interface Utilisation (Bandwidth) ▪ Number of free ports ▪ Port Errors	**Proact**

3.8 - Service Management for Backup Service Definition

3.8.1 - Service Options

Service Option	Option Number	Service and component summary
SM-Backup Application	1	Covers the basic functionality of backup software and includes routine items, which every backup and archive product has.
SM-Backup Backup and Restore	2	Selected when the software is configured to perform backup and restore tasks.
SM-Backup Archive	3	Selected when the software is configured to perform archive tasks.
SM-Backup Data Protection	4	Selected when the infrastructure is configured with additional resilience, such as: ▪ Disaster recovery of backup master servers ▪ Clustered media servers ▪ Clients configured with Continuous data protection (CDP).
SM-Backup End User Devices	5	Selected when the infrastructure is configured to allow the backup and restore of end-user devices (for example: laptops or tablets)
SM-Backup Tape	6	Selected when the infrastructure has tape media or a virtual tape library as part of the solution.

3.8.2 - Operational Activities

Deliverable	Applicable Options	Description and content summary	Responsibility
Management	ALL	Proact manages the in scope devices through vendor provided management tools including logging, alert configuration, service infrastructure configuration, storage configuration, data replication, client configuration, reporting configuration and licensing configuration.	**Proact**
Backup Software Access	ALL	Proact will be provided with full administration rights to the backup software interface.	**Customer**
Backup Software Users	ALL	Proact will manage the backup software's internal user authentication. Including the creation/deletion and modification of backup software users and their backup service privileges. This excludes administration of Active Directory or any other external user authentication administration.	**Proact**
New client deployment (Customer)	ALL	To enable new client deployment, the customer will, with Proact's assistance: ▪ Install, customised and test the remote deployment route, including configuration onto the network and patching of operating systems to appropriate level ▪ Make any required pre-built software packages available to Proact.	**Joint**
New client deployment (Proact)	ALL	Proact will perform the routine remote installation of new backup clients where: ▪ The software vendor supports remote deployment ▪ A working remote deployment method exists ▪ Appropriate pre-built software packages (configuration and binaries) are available in the central management console.	**Proact**
Infrastructure software upgrade	ALL	Proact will perform software upgrades to the backup infrastructure (master servers & media servers) in scope, from time to time.	**Proact**
Client software upgrade	ALL	Proact will perform backup software upgrades to the software installed on clients from time to time. This excludes updating firmware on underlying infrastructure (for example: disk arrays or tape libraries)	**Proact**
Backup capacity (Proact)	ALL	Proact extend storage capacity where storage volumes reach certain thresholds to ensure that they do not run out of space.	**Proact**
Security	ALL	Proact manages the in scope devices encryption and authentication features through vendor provided management tools.	**Proact**
Data archive	3	On the customer's request, Proact perform administration of archive tasks, within the operating parameters of the product used, including; creation, deletion and modification of archive tasks, schedules and data retention policies.	**Proact**

Deliverable	Applicable Options	Description and content summary	Responsibility
Data restores	2	Proact perform data restores on receipt of the appropriate approved customer request, within the operating parameters of the product used. Any target server must have an existing OS, be fully configured onto the network and be in a state to accept the restore.	**Proact**
Data recovery	3	Proact will manage self-service recovery of archive data, through the use of stubs, allowing file and email data to be recovered directly by the customer.	**Proact**
Archive compliance	3	Proact will provide users with the ability to erase selective content from the archive storage system, within the operating parameters of the product used.	**Joint**
System contingency testing	4	As part of System Contingency Testing and in conjunction with the customer's wider DR procedures, Proact will perform any backup software related commands and tasks necessary to make the backup data available on a replicated backup system. Tests must be performed within Proact's normal business hours.	**Joint**
System contingency failover	4	As part of System Contingency Failover and in conjunction with the customer's wider DR procedures, Proact will perform any backup software related commands and tasks necessary to make the backup data available on a replicated backup system. The actual failover, whenever it is not automated, is taken care of within the emergency change management process on customer request.	**Joint**
CDP agents	4	Proact perform administration of continuous data protection tasks including; creation, deletion, modification and failover.	**Proact**
End user management	5	The customer will be responsible for the administration of user authentication, user administration and end user device administration	**Customer**
End user backup	5	Proact will provide backup for a customer's end user devices via the internet, to allow for backup from remote locations, within the operating parameters of the product used.	**Proact**
End user restore	5	Proact will, on customers's reasonable request, provide the customer's end user with an interface to perform self-service restore, where available within the product used. End users are not permitted to log calls with Proact directly to perform restore tasks.	**Joint**
Physical media (Customer)	6	Where tape media is in use, the customer will perform physical media (including cleaning tapes) handling tasks or appoint a third party business to perform these tasks.	**Customer**
Physical media (Proact)	6	Proact interact with the software to allow vaulting to be performed and make requests for either the customer or a third-party (if appropriate) to perform physical handling of devices and media.	**Proact**

Deliverable	Applicable Options	Description and content summary	Responsibility
Tape capacity	6	Where tape is used, the customer will provide sufficient storage and cleaning media and replace used media as it ages and to accommodate for growth.	**Customer**

3.9 - SM for Public Cloud Service Definition

3.9.1 - Service Types

Service Type	Service and component summary
SMfPC – Landing Zone	Management of infrastructure resources within a Customer landing zone. Azure operations conducted by a combination of Infrastructure-as-Code (DevOps) and manual configuration (ClickOps). Infrastructure-as-Code (IaC) is delivered either fully, or up to a specific demarcation point to facilitate the desired level of IaC and co-delivery options.

3.9.2 - Operational Activities

Deliverable	Description and content summary	Responsibility
Health Checks	Proact will perform periodic technical health checks, which checks a landing zone against the latest best practice.	**Proact**
Base Advisor Cost Control	Proact will perform a quarterly review of recommendations provided by Azure advisor to reduce Azure cost.	**Proact**
Health Alerting and Maintenance	On a continual basis, Proact will inform the Customer and, where possible, take preventative actions to limit production downtime for Azure maintenance.	**Proact**

3.9.2.1 - Service Options

Service Option	Option Number	Service and component summary
SMfPC – Advanced Cost Control	1	Perform quarterly investigations and provide recommendations on deployed Azure services, including other systems under Proact Service Management, to reduce overall Azure spend.

3.9.3 - Platform

Deliverable	Description and content summary	Responsibility
Public Cloud Platform	A valid subscription(s) and maintained for the period of the contract.	**Customer**

Deliverable	Description and content summary	Responsibility
Management access	Provide Proact with access to the Public Cloud platform and subscriptions for management. Proact requires access to Customer environment with sufficient permissions via Azure Lighthouse.	**Customer**
Management Platform	Management of the (Public) Cloud Platform(s), including changes, is to be performed by Proact with either with Infrastructure as Code (IaC) principles, or Click Operations.	**Proact**
Resource Management (General)	Upon Customer request, Proact creates, modifies, and deletes resources, identities and roles already defined with the landing zone.	**Proact**
Resource Management (General)	Requests for new business systems, regions, updates or Azure features require a PS engagement to design, plan and execute the implementation.	**Out of Scope**
Resource Management (Storage)	Management of Azure storage account related features (such as Azure Files and Blob) and services within the Customers' Public Cloud infrastructure.	**Proact**
Access Control (Storage)	Management of file/directory level permissions via access control lists (ACL's) within file shares.	**Customer**
Resource Management (Network)	Management of the network subnets, network security groups (NSG's) and virtual networks to allow access to required resources. Manage private or public endpoint configured for accessibility or connectivity of the resource(s) in scope	**Proact**
Resource Configuration	Responsible for all configuration within the resources. (Unless covered by additional service management options e.g. Service Management for Servers)	**Customer**
Code Configuration Monitoring	Proact identifies deviations from the agreed IaC standard within the Customer's Public Cloud Tenant. Where significant drift is detected, a plan will be agreed with the Customer. This may be subject to acceptance of Professional Services quote.	**Proact**
Code resources	Customer will provide resources to deploy required agents within the landing zone for monitoring and management of the environment.	**Customer**
Code Agents	Proact will deploy agents within the Customer landing zone for monitoring and management of the environment.	**Proact**
Key management	Creation of Customer Managed Keys (via keychains, keystores etc.) upon creation of the resources.	**Proact**
Support Accounts	Customer to provide Proact with user accounts, as required, for technical case logging and escalation to Microsoft for Incident resolution.	**Customer**
Intellectual property	All code is intellectual property (IP) of Proact and will be developed and maintained centrally in a repository by Proact for quality improvements, ease of management, reuse of code and Change Control Processes. Upon termination of contract, Proact can transfer Code to the Customer, subject to acceptance of Professional Services quote.	**Out of Scope**

3.9.4 - Connectivity

Deliverable	Description and content summary	Responsibility
Administrative Connectivity	Management access for Azure is achieved via Azure Lighthouse from Proacts Azure management tenant. An arm template and parameters file will be supplied by Proact. The Customer will need to execute the template within their environment to facilitate access.	**Joint**
Testing devices	Where the Customer requires Proact to test using Customer-specific testing devices, the Customer is responsible for the provision of required testing hardware and the creation of user accounts for Proact on those devices.	**Customer**
All other network connectivity	Provide the network connectivity and services required to connect to workloads outside of Azure (including, but not limited to) Customer premises, external applications and other (public cloud) providers.	**Customer**
IP-Address Connectivity	Where monitoring and or management requires an external public static IPv4 address, the Customer will provide on their firewall, dynamic IP addressing is not supported.	**Customer**

3.9.5 - Security

Deliverable	Description and content summary	Responsibility
Administrative Access via Lighthouse	User access will be secured via conditional access policies and MFA applied via the Proact Azure Management domain.	**Proact**
Key Vault	Responsible for the defining or agreeing the access policy and third party access to keys stored in the key vault.	**Customer**
Administrative Access via Customer domain	Access required into virtual machines or applications secured by the Customer will require local or application accounts within that security domain.	**Customer**
Tenant Security	While Proact may manage the configuration of certain security features and resources within the Customer's Azure tenant, the overall security of the tenant is the responsibility of the Customer.	**Customer**
Identity and Access Management (IAM)	For secure access that does not utilise Lighthouse, all sign-in activity to the Public Cloud management portal(s) to be secured with conditional access, either secured based on verified and limited public IP address ranges or with multi-factor authentication.	**Joint**

3.9.6 - Licensing

Deliverable	Description and content summary	Responsibility
Public cloud licensing	The Customer must have a valid subscription and licenses to allow for Proact to connect to the Customers resources hosted in the Public Cloud. The Customer must maintain the subscription and licenses for the period of the contract, to allow Proact to perform management.	**Customer**
Remote Monitoring licensing	Full licensing for standard monitoring software is provided by Proact.	**Proact**

3.9.6.1 - Service Monitoring

The following provides an overview of the specific monitoring provided for SMfPC. Proact's standard monitoring deliverables are provided in the Common Service Deliverables appendix.

Deliverable	Option	Description and content summary	Responsibility
Monitored items	ALL	The resources in scope of this contract will be monitored by Proact where Azure provides the required output. For example, ▪ Overall resource health status utilisation and availability. ▪ Maintenance notifications from Microsoft.	**Proact**
Monitoring profiles		In addition to Azure monitoring, improvements can be deployed. These are based on Proact standards and are subject to modification according to changing requirements during the contract term. The actual implementation of monitoring as well as associated thresholds are to be defined in the start-up workshop.	**Joint**

3.9.6.2 - Additional Complementary Services *(not included within Service Management for Public Cloud)*

Service Option	Service and component summary
SMfStorage	Add-on for Azure NetApp files.
SMfBackup	Add-on for Azure backup or BaaS-E or BaaS-V
SMfServers	Add-on for Server OS Management.
SMfWorkspace	Add-on for DaaS / AVD / Citrix / Nerdio
SMfFirewall	Add-on for Firewall Management, Azure or Palo
SMfNetworking	Add-on for Enterprise networking, including advanced connectivity (Express route, VPN, VWAN) into, out of, and within Azure.
SMfSecurity	Add-on for Management of Sentinel and Defender

3.10 - SM for Public Cloud Service Definition

3.10.1 - Service Management for Nerdio Service Definition

This appendix covers detail on deliverables that are specific to Service Management for Nerdio. This service also includes the deliverables defined in the **Common Service Deliverables** labelled as 'Managed'.

3.10.1.1 - Operational Activities

Deliverable	Description and content summary	Responsibility
AVD Services	Monitoring the health status and operational availability of NME-managed AVD services, including host pools and file shares used for the NME-managed AVD environment	**Proact**
Image Health	▪ Perform user density and load balancing checks to ensure optimal performance ▪ Perform image optimisations for performance and scale	**Proact**
Host pool management	Deploy host pools based on the defined virtual workspace images	**Proact**
Advanced Advisor Cost Control	Proact will perform a quarterly review of recommendations provided by Azure advisor & NME to reduce Azure cost	**Proact**
Maintenance Notifications	Proact will inform the Customer of Azure maintenance affecting the NME-managed AVD environment	**Proact**
Scaling	Adjust scaling policies where applicable to optimize environment. This can include: ▪ Scale Out / In & Scale Up / Down Hosts ▪ Just In Time VM Creation ▪ Disk Conversion Policies ▪ Azure Files Scaling	**Proact**
Suspended user sessions reset	Reset suspended user sessions within the customer environment reported by the customer	**Proact**

Deliverable	Description and content summary	Responsibility
Inactive user profiles	Provide information which users profiles within the customer environment are now inactive	**Customer**
Inactive user profile removal	Remove inactive user profiles within the customer environment reported by the customer	**Proact**
Operating System / VDA	Maintain Microsoft Windows virtual workspace images by installing updates for: ▪ Microsoft Windows ▪ Microsoft Azure Virtual Desktop Agent (VDA)	**Proact**
Image Requirements	Define the requirements for virtual workspace images, including the applications to install in the image(s)	**Customer**
Base Applications: Installation	Install in Microsoft Windows virtual workspace images any of these Base Applications that are required: ▪ Google Chrome ▪ Adobe Acrobat Reader	**Proact**
Base Applications: Updates	Schedule and implement the installation of updates to Base Applications installed in Microsoft Windows virtual workspace images	**Proact**
Non-Base Applications: Installation	Install in Microsoft Windows virtual workspace images any required non-Base Applications	**Joint**
Non-Base Applications: Update / Removal Scheduling	Schedule and request Proact update or remove non-Base Applications in Microsoft Windows virtual workspace images	**Customer**
Non-Base Applications: Update Installation / Removal	Update or remove non-Base Applications in Microsoft Windows virtual workspace images when requested by the Customer	**Proact**
Non-Base Applications: Pre-requisites	Provide to Proact the following pre-requisites for non-Base Applications: ▪ Original installation / update / removal files ▪ Detailed procedures for installation / updating / removal that do not require specialist skills, hardware or software to use	**Customer**
Non-Base Applications: Vendor Support	Collaborate with application vendors to install, update or remove non-Base Applications	**Joint**
Acceptance Testing	Responsible for acceptance testing of changes made to AVD	**Customer**
Image Creation	Creation of new virtual workspace images requires a separately-chargeable Proact professional services engagement	**OUT OF SCOPE**

3.10.1.2 - Platform

Deliverable	Description and content summary	Responsibility
Platform Management	Management of AVD and NME, including changes, is to be performed by Proact	**Proact**

Deliverable	Description and content summary	Responsibility
Platform Management Code	Develop and maintain all code centrally in Proact's dev-ops environment for ease of management, reuse of code and change control purposes	**Proact**
Nerdio Appliance	Manage these configuration items related to NME's management of AVD: ▪ Nerdio Manager Azure App Service Plan ▪ Azure SQL Database ▪ Azure Key Vault ▪ Storage Account ▪ Azure Automation Account ▪ Log Analytic Workspace ▪ Application Insights	**Proact**
Policy Management	Change policies within the environment as requested by the customer or following advice from vendor support	**Proact**
Profile Management	Manage Microsoft FSLogix profiles used by the NME-managed AVD environment	**Proact**
Storage Management	Manage Azure Storage account related features used to host AVD / Nerdio platform and associated profiles	**Proact**
Storage Management	Manage file / directory level permissions via access control lists (ACLs) within file shares	**Customer**
Management Access	Provide Proact access to the AVD platform and NME subscriptions for management. Proact requires access to Customer environment with sufficient permissions via Azure Lighthouse.	**Customer**
Devices	Manage & configure end user devices and peripherals, ensuring that they are compatible with AVD	**Customer**
Proact Professional Services	Requests for new business systems, regions, updates or Azure features require a separately-chargeable Proact professional services engagement to design, plan and execute the implementation	**OUT OF SCOPE**

3.10.1.3 - Connectivity

Deliverable	Description and content summary	Responsibility
AVD Networking	Manage the Network Security Groups (NSGs), VNETs and IPs within the AVD platform	**Proact**
All Other Network Connectivity	Provide and manage all other network connectivity, including from end user devices to AVD and from AVD to applications and services used by AVD	**Customer**
Administrative Connectivity	Management access for Azure is achieved via Azure Lighthouse from Proact's Azure management tenant. An arm template and parameters file will be supplied by Proact. The Customer will need to execute the template within their environment to facilitate access.	**Joint**

Deliverable	Description and content summary	Responsibility
Testing Devices	Where the Customer requires Proact to test using Customer-specific testing devices, the Customer is responsible for the provision of required testing hardware and the creation of user accounts for Proact on those devices	**Customer**
IP Address Connectivity	Where monitoring and or management requires an external public static IPv4 address, the Customer will provide this on their firewall. Dynamic IP addressing is not supported	**Customer**

3.10.1.4 - Security

Deliverable	Description and content summary	Responsibility
Authentication and Authorisation	Define and manage the Azure Entra conditional access and MFA policies	**Customer**
Administrative Access via Lighthouse	User access will be secured via conditional access policies and MFA applied via the Proact Azure Management domain	**Proact**
Key Vault	Responsible for the defining or agreeing the access policy and third party access to keys stored in the key vault	**Customer**
Administrative Access via Customer Domain	Access required into virtual machines or applications secured by the Customer will require local or application accounts within that security domain	**Customer**
Subscription Security	While Proact may manage the configuration of certain security features and resources within the Customer's Azure subscription, the overall security of the tenant and subscriptions is the responsibility of the Customer	**Customer**
Identity and Access Management (IAM)	For secure access that does not utilise Azure Lighthouse, all sign-in activity to the Microsoft Azure management portal(s) to be secured with conditional access, either secured based on verified and limited public IP address ranges or with multi-factor authentication	**Joint**

3.10.1.5 - Licensing

Deliverable	Description and content summary	Responsibility
Subscriptions	Have a valid Microsoft 365 or Windows 10 / 11 Enterprise subscription and maintain this for the period of the contract	**Customer**
Subscriptions	Maintain the NME subscription for the period of the contract	**Customer**
Application Licensing	Responsible for licensing applications installed in virtual workspace images	**Customer**

3.10.1.6 - Service Monitoring

Deliverable	Description and content summary	Responsibility
AVD Services	Monitor the resources in scope of this contract where Azure provides the required output. For example: ▪ Overall resource health status utilisation and availability ▪ Maintenance notifications from Microsoft	**Proact**
Monitoring Profiles	Identify and define customised monitoring thresholds using Proact's standard monitoring toolset	**Joint**

3.11 - Service Management Service Transition Process

In addition to the Common Service Transition Process, the table below details specific deliverables related to Service Management.

Deliverable	Applicable Options	Description and content summary,	Responsibility
Creation of dedicated management server	All	There are two options: ▪ Management server is located on customer premises. ▪ Management server is located in Proact Datacentre The former is preferred and can operate jointly as the monitoring application server. The management server must have network access on all relevant ports to the devices under management so that Proact designated personnel can log on to them.	**Joint**

3.12 - Vendor Terms

The services described in this Services Specification will be subject to the vendor terms set out in the table below.
These terms are available in full at https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/.

Vendor Name
LogicMonitor

Appendix 4 - Service Management for Citrix

4.1 - Service Overview

Service Management for in scope Virtual Desktop service will be provided based on the following service description/

The responsibility model is appended to each function as either **-Proact, -Customer** or **-Joint.**

4.2 - Core Platform Management

Management of Core Platform services

Deliverable	Description and content summary	Responsibility
Citrix	▪ Policy Configuration ▪ Service availability monitoring ▪ License Management	**Proact**
Hosting Platform (VMWare)	▪ Management (covered under Service Management for Hypervisors) ▪ Performance and capacity trending	**Proact**
Federated Authenticati on Service	▪ Perform configuration changes ▪ Perform maintenance and environment upgrades and patching ▪ Service availability monitoring	**Proact**
StoreFront	▪ Perform configuration changes ▪ Perform maintenance and environment upgrades and patching ▪ Service availability monitoring	**Proact**
NetScaler Gateway/A DC	▪ Perform configuration changes ▪ Perform maintenance and environment upgrades and patching ▪ Service availability monitoring	**Proact**
NetScaler ADM	▪ Perform configuration changes ▪ Perform maintenance and environment upgrades and patching ▪ Service availability monitoring	**Proact**
Citrix Related GPO	▪ Creation of new GPO ▪ Updating existing GPO ▪ Retiring obsolete GPO	**Joint**
AppSense Policy	▪ Creation of new Policy ▪ Updating existing Policy ▪ Retiring obsolete Policy ▪ Perform configuration changes ▪ Perform maintenance and environment upgrades and patching ▪ Service availability monitoring	**Proact**
ShareFile Control Plane	▪ Policy Configuration ▪ Service availability monitoring	**Proact**

Deliverable	Description and content summary	Responsibility
Published Resources	▪ Perform the creation and management of published applications ▪ Perform the creation and management of published desktops ▪ Monitor availability of Delivery Groups and Worker servers	**Proact**

Resource Location

Management of Resource Location specific components:

Deliverable	Description and content summary	Responsibility
Profile Storage Locations	▪ Perform configuration changes ▪ Perform maintenance and environment upgrades and patching ▪ Service availability monitoring ▪ Perform capacity management ▪ Perform optimisation and clean-up activities	**Proact**
Remote Access	▪ Monitor Remote Access infrastructure uptime for end-to-end service availability	**Proact**
Provisioning Services	▪ Perform configuration changes ▪ Perform maintenance and environment upgrades and patching ▪ Service availability monitoring	**Proact**
UniPrint	▪ Perform configuration changes ▪ Perform maintenance and environment upgrades and patching ▪ Service availability monitoring	**Proact**
ShareFile Storage Zone Controllers	▪ Perform configuration changes ▪ Perform maintenance and environment upgrades and patching ▪ Service availability monitoring ▪ Perform capacity management	**Proact**

Master Image

Management tasks for each Master Image

Deliverable	Description and content summary	Responsibility
Application Updates/Changes	▪ Perform configuration changes ▪ Update Base Applications ▪ Office ▪ Browser(s) ▪ Anti-Virus ▪ Adobe Reader ▪ Citrix VDA	**Proact**
Application Updates/Changes	▪ Collaborate with application vendors to update non base applications ▪ Collaborate with application vendors to deploy new applications ▪ Collaborate with application vendors to remove obsolete applications	**Joint**

Deliverable	Description and content summary	Responsibility
Software Updates	▪ Apply Windows and base application updates to master image ▪ Rollout updates following UAT process ▪ Update and maintain supported VDA versions	**Proact**
Image Health	▪ Perform User density and load balancing checks to ensure optimal performance ▪ Perform image optimisations for performance and scale	**Proact**

User Experience
Management tasks to ensure optimal user experience.

Delivery of User Experience Index Monitoring and Response is only conducted in standard business hours of 08:00 – 18:00.

Deliverable	Description and content summary	Responsibility
Perform Profile Management optimisation tasks	▪ Log on Time Optimisations ▪ Profile size Optimisations	**Proact**
Platform and licence capacity trending	▪ Monitor and trend Workspace licence usage for in scope products	**Proact**
3rd line support for user platform related issues	▪ Respond to proactive alerts impacting end user access and performance ▪ Respond to ticket escalation from the Customer's Service desk	**Proact**