

SCHEDULE A: SERVICE DEFINITION FOR ENHANCED OPERATIONAL MANAGEMENT LEVEL – OS MANAGED

The Enhanced Operational Management Level – OS Managed provides operational management of the Supported Items within virtual server environments on Hyper-V and VMWare hypervisors, as well as physical environments, up to the Operating System (OS) level. This Enhanced Operational Management Level provides a fully-maintained Operating System environment, based on systems listed in the Functional Capability section below, and configured by the Service Desk to the Customer's requirements.

The OS Managed Enhanced Operational Management Level provides the following components:

- Installation of the OS managed environment based on Vysiion's standard OS build specification, for the OS configurations listed in the Functional Capability section of this Schedule A;
- Decommissioning of the OS managed environment based on Vysiion's standard, ITIL compliant decommissioning process;
- Installation and configuration of the required software needed to support Vysiion's service delivery of the OS (including AV, backup, monitoring software, and the setup of VM tools, where applicable);
- Configuration and management of the OS environment, excluding any OS options, features, or applications installed onto the OS;
- Provisioning of the OS license where purchased by the Customer through Vysiion;
- Vysiion's standard AV solution installed and configured for the OS and application workloads, and managed as set out in this Schedule A;
- Continuous (24x7x365) OS monitoring and alerting;
- Backup management of the OS environment, including configuring daily backups, monitoring the backups daily, picking up backup faults, and remediating them for OS issues to Vysiion's standards detailed in this Schedule A;
- Carry out full system and file level restores from backup for the OS environment as requested by the Customer;
- Automated analysis and resolution of incidents raised for configured OS alarms and warnings;
- Manual analysis and resolution of incidents raised for OS alarms and warning that cannot be automatically resolved;
- Manual changes raised for OS changes recommended by Vysiion;
- Delivery of approved changes raised by Vysiion and the Customer;
- Patch Management of OS patches in line with Vysiion's standard, ITIL compliant patching process as detailed in this Service Document; and
- Vysiion administration account and Vysiion test user account management.

Functional Capability

Vysiion manages and supports the Supported Item OS to Vysiion's standard build specification for the vendor's products under Mainstream Support, as detailed in the following location and amended from time to time:

<https://www.vysiion.com/operating-systems-support>.

Vysiion's responsibilities with respect to the OS Managed Enhanced Operational Management Level are as follows, to the extent relevant to the Supported Items. The Customer is responsible for all management not included within Vysiion's responsibilities.

Aspect	Vysiion's Responsibilities
Anti-virus ("AV") Agent	• Set up and manage AV configuration settings including recommended vendor exclusions for the OS. • Identify new AV signature updates and approve these updates to be made to agents automatically on an hourly schedule.

Aspect	Vysiion's Responsibilities
	• Monitor and manage AV signature downloads and AV application. • Identify eligible AV product and agent software (including upgrades) that apply to all Supported Items. • Notify the Customer of eligible AV product and agent upgrades via new change ticket, and the time when these upgrades will be carried out. • Carry out product and agent upgrades at the time agreed by the Customer. • Install and configure agent software on new Supported Items. • Monitor and notify the Customer of any detected virus infections. • Remove virus infections from Supported Items once detected and where possible. • Produce and maintain a document in the CMDB detailing the Vysiion AV process and the processes the Customer must follow to report new virus infections, request AV version updates, request AV product changes etc.
Asset Management	• Management of OS licenses, including arranging Customer renewals and keeping up to date OS license records. • Maintain a valid software library for OS software owned or leased by the Customer as provided by the Customer. • Maintain a valid software library for OS software provided by Vysiion to the Customer. • Retain hardware information for Supported Items in the CMDB regarding their specification, warranty and configuration. • Maintain a full and up to date asset management register for Supported Items that is available to the Customer in the CMDB.
Backup	• Configuring daily backups of all Supported Item Operating Systems to include the ability to restore individual files as well as whole Operating Systems, and the data it contains. The Customer is responsible for ensuring the restored data is reviewed and to confirm to Vysiion that it operates as required. • Monitoring backups daily. • Test application specific backups and restores during the On Boarding activity to prove the recoverability of backed up data. • Use reasonable endeavours to detect backup faults and remediate them for OS issues. • Carry out full system restores from backup as requested by the Customer. Each Supported Item includes one full system restore event per annum without additional charge. Additional full system restores can be completed at additional charge. • Carry out OS file level restores from backup as requested by the Customer. Each Supported Item includes sixty (60) file system restore events per annum without additional charge. Additional file level restores can be completed at additional charge. • Produce and maintain a document in the CMDB detailing the backup settings used to back up Supported Items, and the processes the Customer must follow to back up and restore Supported Item data.

Aspect	Vysiion's Responsibilities
Certificate Management	• Manage certificate renewals for OS functionality with Customer approved providers for Supported Items on behalf of the Customer. • Keep up to date certificate records available in the CMDB. • Link OS level certificates to the OS for Supported Items. • Manage bespoke certificate provider authorisation licenses on Supported Items.
Disaster Recovery and Business Continuity	• Provide the Customer with a standard format Disaster Recovery and Business Continuity document for the Supported Items. • Request sign off from the Customer stakeholders for the standard format Disaster Recovery and Business Continuity document for the Supported Items. • Participate in isolated DR exercises for the Supported Items once a year (to support DR failover exercises delivered remotely on a sample and isolated environment as detailed in the Disaster Recovery and Business Continuity document, unless agreed otherwise in writing by the Parties). • Participate in chargeable Disaster Recovery simulations with the Customer on Supported Items if requested by the Customer. This is subject to a minimum of five (5) Working Days' notice provided to the Service Desk by the Customer. • Coordinate with the Customer's representatives to execute DR processes in line with the Customer's IT Disaster Recovery and Business Continuity Plan, at the Customer's request. Vysiion is responsible for carrying out all activities agreed for completion by Vysiion in the Customer's IT Disaster Recovery and Business Continuity Plan. • Participate with the Customer on an annual basis to review and improve the Disaster Recovery and Business Continuity document.
Documentation	• Maintain solution design documentation for Supported Items in the CMDB. • Maintain solution configuration documentation for Supported Items in the CMDB. • Maintain solution testing documentation for Supported Items in the CMDB. • Ensure that the CMDB includes the day-to-day operational procedures for the OS Managed Enhanced Operational Management Level. • Produce and maintain a document detailing the configuration of the standard OS images available from Vysiion's VDC and private cloud environments. • Implement and maintain version control for all above documentation.
End of Life Management	• Advise the Customer at least three (3) months in advance of upcoming End of Life dates of any Supported Items. • If the Customer is not able to upgrade the OS by the End of Life date, Vysiion will use reasonable endeavours to continue to deliver the OS Managed Enhanced Operational Management Level in accordance with this Schedule however the Flex Manage service level agreement shall not apply to any Supported Items that have reached their End of Life date.

Aspect	Vysiion's Responsibilities
Licensing	• Vysiion is responsible for licensing management under the Contract to cover: ○ Application agents for AV as applicable for the Supported Items. ○ Application agents for backup as applicable for the Supported Items. ○ License management to ensure the Supported Items have OS licenses and utilisation CALs/SALs. ○ RMM monitoring agents as applicable for the Supported Items. For the avoidance of doubt, this covers management of licences, not the provision of those licences.
Monitoring	• All Supported Items will be configured with a RMM method that will be used to proactively monitor the health and availability of the Supported Items. • Configuring and maintaining standard, automated OS monitors for Supported Items to notify Vysiion of OS issues and outages. • Document all monitoring settings for all Supported Items during the On Boarding activity and make this information visible to the Customer in the CMDB. Update the documentation when monitoring changes are made. • Proactive monitoring of Supported Item CPU, RAM, disk space, and network utilisation if access to this information is provided by the Supported Item, and storing this information for thirty (30) days. • Proactive monitoring of all Supported Items at regular intervals (as agreed during On Boarding) to collect standard OS metrics. • Carrying out Vysiion standard automated health check and performance monitoring for Supported Item Operating Systems. • The Customer may choose up to five (5) additional OS monitors from Vysiion's list of available additional OS monitors that Vysiion will monitor for Supported Items. • Logging issues uncovered by OS monitoring within the management platform. • Process issues uncovered by OS monitoring to remediation (where possible). • Management and maintenance of the monitoring agent software.
Operating System Minor Upgrades	• Minor upgrades include all updates to the OS of the Supported Items that can be performed on the existing system. These upgrades do not require the existing supported OS environment or the applications running on it to be rebuilt to perform the upgrades. The following upgrades are included alongside the OS-level minor upgrades: ▪ Hardware firmware upgrades ▪ All OS RMM agent upgrades ▪ All backup software agent upgrades ▪ All anti-virus software agent upgrades Major upgrades (including all updates to the OS or other parts of the Supported Items that require a new physical or virtual OS to be built) are not included with the OS Managed Enhanced Operational Management

Aspect	Vysiion's Responsibilities
	Level and if required, will be undertaken by Vysiion subject to additional Charges. • All upgrades to Supported Items will be subject to the change management process, and the Customer will be required to approve all upgrade changes before the Service Desk will carry them out.
Patch Management	• Provide a list of critical, security, and non-critical OS updates (as identified by Vysiion's third party patching solution) to the Customer on a monthly basis, at least five (5) days prior to the scheduled installation date. The Customer must confirm to Vysiion in writing which of the identified critical and security updates are to be installed during the next patching event onto Supported Items. • Install Customer approved critical and security OS updates onto Supported Items on a monthly schedule. • Install Customer approved non-critical OS updates onto Supported Items on a monthly schedule, or less frequently (as agreed by the Parties during the Supported Item On Boarding process). • Provide a list of critical and performance updates for Supported Item hardware to the Customer on a quarterly basis, at least five (5) days prior to the scheduled installation date. The Customer must confirm to Vysiion in writing which of the identified critical and performance updates are to be installed during the next patching event to Supported Items. • Install Customer approved critical and performance updates onto Supported Item hardware on a quarterly schedule. • Provide a list of non-critical and firmware updates for Supported Item hardware to the Customer on a semi-annual basis, at least five (5) days prior to the scheduled installation date. The Customer must confirm to Vysiion in writing which of the identified non-critical and firmware updates are to be installed during the next patching event to Supported Items. • Install Customer approved non-critical and firmware updates onto Supported Item hardware on a semi-annual schedule. • Install critical and performance updates onto Supported Item hardware on a quarterly schedule. • Install non-critical and firmware updates onto Supported Item hardware on a semi-annual schedule. • Notify the Customer of proposed OS and hardware updates to the Supported Items at least three (3) Working Days prior to the scheduled update. • Configure all Supported Items for automated update installation by the Service Desk. Supported Items that are not compatible with the Vysiion automated update process will be updated manually. • Invoke the Emergency Patch Procedure when updates are identified by the vendor, Customer or Vysiion as urgent. This procedure is a variation of the Standard Patch Procedure and aims to expedite the installation of the OS update for the Supported Items. This procedure is documented in the CMDB.

Aspect	Vysiion's Responsibilities
	• Create the Standard Patch Procedure and the Emergency Patch Procedure jointly with the Customer and document these procedures in the CMDB and schedule Patching in line with the Procedures. • Patch management excludes any item that would in Vysiion's reasonable opinion cause significant impact to the existing Supported Item. For example, a patch that may require a full rebuild of the Supported Item. This will be a chargeable Professional Services engagement. • Patch Management excludes security hardening of the Supported Item required by regulatory or compliance purposes. This will be a chargeable Professional Services engagement.
Reporting	• Delivering the following performance and management reports for Supported Items covering a thirty (30) day period: ○ Performance Review ○ Computer Audit ○ Patch Compliance ○ Anti-virus Health ○ Software List
Server Replication	• Installation and configuration of Server Replication software agent on Vysiion provided virtual servers that are Supported Items. • Installation and configuration of Server Replication software agent on public cloud provided servers that are Supported Items. • Monitor and alert on the availability and performance of the Server Replication software applied to Supported Items. • Provide proactive remediation of Server Replication issues generated through the monitoring and alerting toolsets for Supported Items. • Identify new Server Replication software updates via a new change ticket for the software updates, and the time when these updates will be carried out. • Carry out product and agent updates at the time agreed by the Customer.
Standard Installation Activities	• Installation of Vysiion RMM agents on Supported Items. • Configuration of Vysiion standard monitoring on Supported Items.
Standard Operational Activities	• Configuration of remote access to the OS. SSH is configured for Linux, and ScreenConnect is configured for Windows systems. • Configuration of management accounts for Vysiion engineering staff. • Server reboots when required to keep OS functionality working, and when required by the Customer. • Service restarts for OS services. • Clearing temporary files and logs to release available OS space. • Identification of high risk OS issues. • Monitoring and delivering monthly Customer reports on the Flex Manage service level agreement.

[Pre-requisite Requirements](#)

To start OS management of a Supported Item, Vysiion requires the following pre-requisites to be fulfilled by the Customer during the On Boarding period.

- Provision of an OS license for the Supported Item if this is not provided by Vysiion.
- Provision of an AV license for the Supported Item if this is not provided by Vysiion.
- Provision of a Backup license for the Supported Item if this is not provided by Vysiion.
- Conducting the Customer On Boarding activities (as identified by Vysiion during the On Boarding process) including providing information needed by Vysiion to correctly manage and support the Supported Items.
- Provision of design documentation for currently running Supported Items, where this exists.
- Provision of Configuration documents or CMDB information for currently running Supported Items, where it exists.

Customer Dependencies

For Vysiion to deliver the OS Managed Enhanced Operational Management Level, the following Customer dependencies exist. Failure of the Customer to meet these Customer Dependencies may affect the service Vysiion is able to deliver to the Customer, and Vysiion's obligations under the Flex Manage service level agreement.

- The Customer shall provide documented naming conventions for all Supported Items.
- The Customer shall provide documented active Customer IT policies for all Supported Items at the time of starting the On Boarding process.
- The Customer shall provide Vysiion with advice in advance of any peculiar, special, or particular modifications made to the Supported Item. This includes advice on the Vysiion OS base level configuration as well as Vysiion's standard OS Managed practices.
- The Customer shall be responsible for documenting and maintaining any differing configuration and build requirements pertaining to the OS environment that is peculiar, special, or has had particular modifications applied.
- The Customer shall provide, in accordance with the timelines defined during the On Boarding activity, approval for patching events, the approved list of updates to be installed, and approved list of firmware to be installed on physical Supported Items.
- The Customer shall undertake application and pre-deployment compatibility testing before authorising Vysiion to deploy recommended patches to Supported Items.
- The Customer shall review the compatibility of all custom and non-standard applications or line of business applications with the OS and service packs to be used.
- The Customer shall ensure that Customer endpoints and management environments are secured, patched, and maintained in accordance with Good Industry Practice.
- The Customer shall ensure that Customer applications layered on top of the OS are secured, patched, and maintained in accordance with Good Industry Practice.
- The Customer shall assess in advance the application suitability for virtualisation of their applications, and for use with the hypervisor used for VMs.
- The Customer shall work with Vysiion to replace all End of Life Supported Items before the arrival of the End of Life date.
- The Customer shall review the compatibility and suitability of the selected Supported Item configuration for its intended application usage.
- The Customer shall provide Vysiion with administrative rights on the Supported Items in order to provide the OS Managed Enhanced Operational Management Level on Supported Items.
- The Customer shall perform Application installation or updates for all OS Managed Supported Items. Details of application installations or updates shall be notified to Vysiion by the Customer prior to their application via the change management process.

- The Customer shall be responsible for provisioning, administration, and management of the applications installed on the Supported Items and the application technical requirements that are not OS related for these applications to function/operate.
- The Customer shall be responsible for all Supported Items being protected by AV software. Supported Items not deployed with AV software are not covered by the OS Managed Enhanced Operational Management Level for virus infections free of charge.
- The Customer shall be responsible for all Supported Items being protected by backup software. Supported Items not deployed with backup software are not covered by the OS Managed Enhanced Operational Management Level for rebuild by Vysiion free of charge.

Service Education

Vysiion will provide education to Customer staff about the details of the service provided, and how to make use of the provided OS Managed Enhanced Operational Management Level. Vysiion will provide the following service education.

Education	Timeline	Method
Raising incidents for faults/issues	On Boarding	Face-to-face CMDB document
Raising changes for system changes	On Boarding	Face-to-face CMDB document
Reporting	On Boarding	Face-to-face CMDB document
Requesting the creation of new Supported Items	On Boarding	Face-to-face CMDB document
Requesting the addition of Supported Item resources	On Boarding	Face-to-face CMDB document
Disaster Recovery and Business Continuity design and process	On Boarding	Face-to-face CMDB document
Solution design documentation for Supported Items	First 3 months of BAU	CMDB document
Solution configuration documentation for Supported Items	First 3 months of BAU	CMDB document
Solution testing documentation for Supported Items	First 3 months of BAU	CMDB document

Accountabilities and Responsibilities

RACI

A responsibility assignment (RACI) matrix showing whether Vysiion, the Customer or any relevant third parties are Responsible, Accountable, Consulted or Informed in respect of a particular aspect will be drawn up to ensure a joint understanding. The RACI is bespoke to the Customer, is formalised during the On Boarding phase, and is documented in the CMDB.

The following table details who is responsible for high level ITIL-level RACI activities for the OS Managed Enhanced Operational Management Level. Some activities are shared between Vysiion and the Customer, where the Customer will be responsible for activities such as raising or approving change requests. Specific details are documented within the CMDB.

ITIL Process	Vysiion	Customer
Asset Management	RA	CI
Change Management	RA	RACI
Configuration Management	RA	CI
Event Management	RA	CI
Incident Management	RA	CI
Patch Management	RA	CI
Release Management	RA	CI
Request Management	RA	RACI

The Customer is responsible for all RACI activities for areas that Vysiion is not responsible for. During the On Boarding activity the Customer shall identify key internal and 3rd line primary and back-up contacts to the Service Desk and promptly inform the Service Desk of any changes during the term of the Contract.

Service Requests

Service Requests are requested changes to a Supported Item or a request for an operational task made by the Customer.

Types of Service Requests may include those set out in the table on the following pages.

Where a Quantity and Frequency are specified in the table on the following pages, this is a maximum allowance included free of additional Charges over the corresponding timeframe. Service Requests in excess of this allowance will be accepted by Vysiion but shall be invoiceable in arrears in accordance with Vysiion's then-current Professional Services rates. For the avoidance of doubt, allowances apply on a "use it or lose it" basis and unused portions of any allowance cannot be rolled-over or the subject of any credit. Where the Quantity is designated as N/A, there is no maximum allowance and no additional charges shall apply.

All Service Requests that are designated in the table on the following pages as PR and any other Service Requests of a type not listed in the table are not included within the Charges for the Flex Manage Services and will be invoiceable in arrears in accordance with Vysiion's then-current Professional Services rates plus any additional charges that apply as agreed in writing at the time of Service Request acceptance.

All Service Requests will be reviewed, verified and subject to approval by Vysiion and Vysiion will confirm if additional charges apply.

Service Requests will be subject to the applicable Target Time to Complete (if any) set out in the table on the following pages. Vysiion shall use reasonable endeavours to complete the Service Request within this timeframe. The Customer may request the delivery time for all Service Requests to be scheduled for a future date/time in which event, the Target Time to Complete will commence at the relevant date/time.

Service Requests will be carried out by Vysiion during the Hours stated in the table on the following pages. Should the Customer request that they be carried out outside of the applicable Hours, additional charges in accordance with Vysiion's then-current rates for Professional Services shall apply.

ID	Request Description	Method of Submission to Service Desk		Type *	Hours	Target Time to Complete	Quantity	Frequency
		Email	Phone					
SROSM 01	Shut down OS	Yes	Yes	OSR	24 x 7 x 365	1 hour	10	Per month
SROSM 02	Reboot OS	Yes	Yes	OSR	24 x 7 x 365	1 hour	10	Per month
SROSM 03	Request new physical SI	Yes	Yes	PR	Normal Business Hours	7 Working Days following hardware delivery	N/A	As required
SROSM 04	Request new virtual SI	Yes	Yes	PR	Normal Business Hours	1 Working Day	N/A	As required
SROSM 05	Change IP address	Yes	Yes	OSR	24 x 7 x 365	1 hour	1	Per quarter
SROSM 06	Change hostname	Yes	Yes	OSR	24 x 7 x 365	1 hour	1	Per quarter
SROSM 07	Complete emergency patching	Yes	Yes	OSR	24 x 7 x 365	8 hours	1	Per quarter
SROSM 08	Complete emergency AV scanning	Yes	Yes	OSR	24 x 7 x 365	8 hours	1	Per quarter
SROSM 09	Complete additional backups of the SI	Yes	Yes	OSR	24 x 7 x 365	8 hours	5	Per quarter
SROSM 10	Restore the full physical OS from backup	Yes	Yes	OSR	24 x 7 x 365	1 Working Day	1	Per annum
SROSM 11	Restore the full virtual OS from backup	Yes	Yes	OSR	24 x 7 x 365	1 Working Day	1	Per annum
SROSM 12	Restore individual files from backup	Yes	Yes	OSR	24 x 7 x 365	1 hour	60	Per annum
SROSM 13	Test restore files from backup to test backup validity	Yes	Yes	PR	Normal Business Hours	2 Working Days	N/A	As required
SROSM 14	Fail over the virtual SI to another location	Yes	Yes	OSR	24 x 7 x 365	1 hour	1	Per month
SROSM 15	Adjust the physical resources allocated to the SI upon Customer request	Yes	Yes	PR	Normal Business Hours	2 Working Days following hardware delivery	N/A	As required
SROSM 16	Adjust the virtual resources allocated to the SI upon Customer request	Yes	Yes	OSR	24 x 7 x 365	1 Working Day	1	Per month
SROSM 17	Create and format physical disk volumes	Yes	Yes	PR	Normal Business Hours	2 Working Days following hardware delivery	N/A	As required

ID	Request Description	Method of Submission to Service Desk		Type *	Hours	Target Time to Complete	Quantity	Frequency
		Email	Phone					
SROSM 18	Create and format virtual disk volumes	Yes	Yes	OSR	24 x 7 x 365	1 Working Day	1	Per month
SROSM 19	Create fault tolerant physical disk systems	Yes	Yes	PR	Normal Business Hours	2 Working Days following hardware delivery	N/A	As required
SROSM 20	Create fault tolerant virtual disk systems	Yes	Yes	OSR	24 x 7 x 365	1 Working Day	1	Per month
SROSM 21	Complete one-time performance trend analysis of SI environments (CPU, RAM, disk space, network utilisation)	Yes	Yes	OSR	24 x 7 x 365	2 Working Days	1	Semi annually
SROSM 22	Review DR and BC plan	Yes	Yes	OSR	Normal Business Hours	5 Working Days	1	Per annum
SROSM 23	OS patch installation	Yes	Yes	OSR	24 x 7 x 365	8 hours	1	Per month
SROSM 24	Hardware firmware installation	Yes	Yes	OSR	24 x 7 x 365	2 hours	1	Semi annually
SROSM 25	Reset SI management account password	Yes	Yes	OSR	24 x 7 x 365	1 hour	1	Per quarter
SROSM 26	Review OS audit logs	Yes	Yes	OSR	24 x 7 x 365	2 Working Days	1	Per annum

* PR = Project Requirement, OSR = Operational Support Request