vysiion™

AN EXPONENTIAL-E GROUP COMPANY

MANAGED AZURE CLOUD – Service Definition

RM1557.15 G-Cloud 15: Lot 3 – Cloud Support

ISO 9001 QUALITY MANAGEMENT

ISO 27001 INFORMATION SECURITY MANAGEMENT

ISO 14001 ENVIRONMENTAL MANAGEMENT

ISO 45001 HEALTH & SAFETY MANAGEMENT

HM Government G-Cloud

Crown Commercial Service Supplier

Constructionline Gold Member Verified Member

CYBER ESSENTIALS CERTIFIED PLUS

SafeContractor APPROVED

Audited RISQS

Achilles UVDB VERIFIED

Contents

Service

Service Type

Lot 3: Cloud Support

Service Name

Managed Azure Cloud

Service Description

The Azure Managed enhanced operational support level provides management and support to the Customer on CSP based Microsoft Azure environments on a 24x7x365 basis. This enhanced operational support level provides support for all Azure resources within the Customer's Azure tenancy ("Supported Items").

Vysiion will provide management of the Customer Virtual Machines within Azure as set out below. The service is designed to operate as an "IT to IT" model where the Customer IT Management Team will be approved to interact with Vysiion Managed Services team through the Service Desk. End Users will not be permitted to contact the Vysiion Managed Services team.

Vysiion will undertake the following management tasks within the Azure Managed enhanced operational support level:

Service	Tasks
Azure Backup (if used)	Configuring daily backups of all Supported Items to include the ability to restore individual files and whole Operating System environments and the data they contain. Limitations of Azure backup are listed in the "Backup Support Matrix" provided by Microsoft which is updated regularly. https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix The following checks are included as part of the Vysiion Service: • 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 and remediate backup faults for OS and application issues of Supported Items • 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 an additional charge • Carry out OS and application 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 an additional charge • Produce and maintain a document in the CMDB detailing the backup settings used to back up Supported Items and the processes to do this.

Azure Site Recovery (if used)	• Provide the Customer with standard Disaster Recovery and Business Continuity process document(s) for the Supported Items • Request sign-off from the Customer stakeholders for the standard format Disaster Recovery and Business Continuity process document(s) 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 process document(s), unless agreed otherwise in writing by the Parties) • Participate in chargeable Disaster Recovery simulations with the Customer on Supported Items if the Customer requests. This is subject to a minimum of ten (10) Working Days' notice provided to the Service Desk by the Customer • Coordinate with the Customer's representatives to execute DR processes per the Disaster Recovery & Business Continuity process document(s). Vysiion is responsible for carrying out all activities agreed for completion by Vysiion in the Disaster Recovery and Business Continuity process document(s) • Participate with the Customer annually to review and improve the process document(s) for Disaster Recovery and Business Continuity.
Azure Service Monitoring	• Vysiion will monitor Azure services with existing Vysiion ITSM integrations • 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 or via customer request.
Virtual Machine monitoring	• All Supported Items will be configured with an Remote Monitoring and Management ("RMM") method that will be used to monitor the health and availability of the Supported Items proactively • Configuring and maintaining standard, automated OS and application monitors for Supported Items to notify Vysiion of OS and application 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. It is customer responsibility for ensuring the identified list of Resources is complete and accurate • Proactive monitoring of Supported Item CPU, RAM, disk space, and network utilisation if the Supported Item provides access to and stores this information for thirty (30) days • Proactive monitoring of all Supported Items at regular intervals (as agreed during On-Boarding) to collect standard OS and application metrics

	• Carrying out Vysiion standard automated health check and performance monitoring for Supported Item Operating Systems and applications • The Customer may choose up to five (5) additional OS monitors from Vysiion's list of available additional OS and application monitors that Vysiion will monitor for Supported Items • Logging issues uncovered by OS and application monitoring within the management platform • Process issues uncovered by OS and application monitoring to remediation (where possible) • Manage and maintain the monitoring agent software.
Azure Management Tasks	**Global Azure Management** • Manage the Azure tenancy and its configuration settings on behalf of the Customer • The cost anomaly detection will be agreed with the Customer and Vysiion will notify the Customer if anomalies are detected. It is the Customer's responsibility to review all costs and ensure they are as expected, and any Reserved Instances ("RI") or Savings Plans are correctly applied • Quarterly cost optimisation report • Quarterly performance review of service recommendations • Annual Review of the Azure Environment • Decommissioning of Azure services if requested by the Customer, based on Vysiion's ITIL-compliant decommissioning process • Configuration and management of the Azure tenancy environment, including any Azure options, features, or supported applications installed onto Azure. **Access and Rights** • Manage Azure Lighthouse integration with the Customer's Azure tenancy • Manage Microsoft Single Sign On ("SSO") authentication using the Azure AD tenant. • Manage Azure AD Connect to provide the following features to the Customer correctly: password hash synchronisation, pass-through authentication, federation using AD FS, synchronisation of AD objects with Azure, and robust health monitoring of on-premise identity infrastructure. • Manage the management of users created in the Azure tenancy for Exponential administrative, Customer administrative, data access, and Azure end user services purposes. • Manage the management groups created in the Azure tenancy for Vysiion and the Customer. • Configure and manage Azure AD Multi Factor Authentication ("MFA") policies for Azure administrators and users for access to supported hardware, operating systems, and applications.

	• Configure and manage Azure AD conditional access policies to Customer information on Microsoft 365 and Office 365 • Configure and manage Azure AD Self-Service Password Reset. **Commercial** • Configure and manage Azure budgets and spending threshold notifications as requested by the Customer. **Health** • Monitor Azure Service Health and notify the Customer of detected health problems. **Monitoring** • Configure Azure Monitor for required resources within the tenancy • Raising incidents in the event of Azure infrastructure health and availability problems • Remediating Azure infrastructure health and availability problems • Aspect Vysiion's Responsibilities • Installation and configuration of the required software needed to support Vysiion's service delivery of the managed services (including monitoring software and the setup of VM tools where applicable).
Cost Optimisation – Quarterly Review and Recommendations for performance optimisation (i.e. resizing)	• Undertake a quarterly review of cost optimisation and recommendations within Azure with the Customer • At Customer request, discuss impact of change and propose recommendations to Customer for resizing Azure Virtual machines. • Review recommendations relating to Reserved Instances • Review previous two (2) quarters Azure spend to identify cost change trends.
Patch Management – if applicable Vysiion will manage patching on Azure VMs for the Customer	• Schedule the delivery of patches in line with the Vysiion standard patching process: The following Patch management policy shall apply in respect of the Service(s). not withstanding anything to the contrary in the Schedules of this Service Document. Software/Firmware patches shall be applied when deemed necessary by the Vysiion Operational Centre. Patching could be triggered under various conditions: ○ A remotely exploitable security vulnerability is identified and the vendor releases a patch for the vulnerability. Vysiion software release management function conducts a regular review of new vulnerabilities and assesses the functional and security risk to platforms under its remit. It is often the case that vulnerabilities are only applicable if certain configuration is present on the device in question, and if certain features are enabled. If the net effect is that no vulnerability is exposed, then the patch would not be applied. If vulnerability is

exploitable but it is feasible to amend configuration in such a way as to prevent the vulnerability being exploited, then the patch would also not be applied – however in this case the work-around configuration would be introduced under the normal change control procedures;

- A normal end of lifecycle upgrade may be triggered when vendor support of the technology in question is no longer available. In certain circumstances a hardware refresh or upgrade would be required, which falls outside the scope of this patch management policy;
- A bug is identified which is adversely affecting the reliable operation of the device. It is frequently the case that bugs are triggered only under certain specific conditions which are not present in all environments. Under these circumstances Vysiion will assess whether the bug potentially has widespread impact (in which case the patch would be rolled out to all similar devices under Vysiion management), or the condition is isolated (in which case only the particular affected device would be patched).
- Patch Management excludes security hardening required for regulatory or compliance purposes. This will be a chargeable Professional Services engagement.
- The following Release management policy shall apply in respect of the Service(s). Only software updates relating to the operating system supported by the vendor shall be implemented by the Vysiion Operational Centre. Software is managed within the following guidelines:
- Vendor announcements and vulnerability announcements are continually reviewed by Vysiion in order to identify new software vulnerabilities;
- In case a vendor announces a new remotely exploitable vulnerability and releases a patch to address the vulnerability for which no workaround exists, an upgrade will be initiated by Vysiion. In many cases a particular vulnerability requires a specific configuration to be present. Vysiion will analyse the impact of the vulnerability on Vysiion managed devices, as covered by the Contract, and propose either an upgrade or a workaround if the vulnerability is remotely exploitable;
- A release of software becomes end of support due to the end of lifecycle as determined by the vendor;

	○ A specific bug is identified that impacts the Customer environment in terms of performance or stability of the platform. ○ The Customer may request an upgrade to a version of the operating system software fully supported by Vysiion as part of the Service through a service request. If none of the above scenarios are met, Vysiion will not proceed to release a new software revision. ○ VYSIION SHALL HAVE NO LIABILITY FOR ANY SECURITY INCIDENTS OR SERVICE FAULTS/ERRORS/FAILURES TO THE EXTENT DUE TO THIRD PARTY SOFTWARE. • Vysiion carry out patch tests in a lab environment where possible to ascertain whether patches are safe to deploy and look to notify customers where known issues apply. Customers are required to schedule 2-4 weeks behind vendors' release cycles so that faults identified are corrected before installation in this scenario. • All patching is carried out in line with the agreed Change and Release processes during scheduled windows. Where possible, automation is used.

Service Hours

Vysiion will provide the Azure Managed enhanced operational support level on a 24x7x365 basis.

Azure Service Exclusions

Vysiion does not maintain technical skills for all Azure services in-house. However, customers leveraging non-supported services can still log incidents with Vysiion, and Vysiion will escalate with Microsoft on the Customer's behalf through Vysiion's Premier Support Agreement with Microsoft to provide the Customer with Microsoft based support for Azure related issues and support requirements.

The services Vysiion does not support directly includes, but is not limited to:

Azure Orbital	Load Testing
Internet Analyzer	Managed Grafana
Vnet Manager	Microsoft Dev Box
Avere vFXT	SignalR Service
Azure Elastic SAN	Visual Studio App Center
Azure NetApp Files	Energy Data Services
Confidential Ledger	Health Data Services
Data Share	Notification Hubs
HPC Cache	Web PubSub
Managed Lustre	Azure Maps
StorSimple	Azure Sphere
Azure Batch	Defender for IoT
Azure Quantum	Digital Twins
Azure Red Hat OpenShift	IoT Central
Cloud Services	IoT Edge
Azure AD EI (MS Identity)	IoT Hub
Kubernetes Fleet Manager	Object Anchors
Managed Apps	Remote Rendering
Apache Cassandra MI	Spatial Anchors
Database for MariaDB	Time Series Insights
Database for PostgreSQL	Azure Comms. Gateway
Redis Cache	Media Services
Data Catalog	Azure Chaos Studio
Data Explorer	Azure Spring Apps
Operator Insights	Lab Services
Applied AI Services	Open Datasets
Bot Service	Project Bonsai
Microsoft Genomics	

Service Onboarding

The Supported Items will undergo the following technical gates during On-Boarding:

Acceptance into Service 1 (AIS 1)

AIS 1 is achieved once the Azure Services have been enabled by Vysiion or a combination of Vysiion and the Customer. During this phase, the Azure Managed enhanced operational support level is not delivered to the Customer by Vysiion.

Acceptance into Service 2 (AIS 2)

AIS 2 is achieved once the Azure Services have been enabled and configured by Vysiion or a combination of Vysiion and the Customer and any migration activities have been completed. During this phase, the Azure Managed enhanced operational support level is not delivered to the Customer by Vysiion.

Early Life Support (ELS)

ELS is achieved once the Onboarding activity has been completed and Vysiion commences delivering the Azure Managed enhanced operational support level. The period for ELS is agreed on an individual basis with the Customer during the On-Boarding activity and is at least one (1) month following the On-Boarding completion date. The Azure Managed enhanced operational support level is provided during the ELS phase, and the Service Level Agreement (SLA) will apply, but no Service Credits shall be payable.

Business as Usual (BAU)

BAU is achieved once the ELS period has elapsed and once all projects, programmes and expected activities that might introduce change have been concluded. During the BAU phase, Vysiion will deliver the Azure Managed enhanced operational support level, the SLA will apply, and Service Credits will be payable thereunder.

The Service Commencement Date for the Supported Items is the date that the Supported Item has been On Boarded by the Vysiion Service Desk and Early Life Support has commenced.

Service Education

Vysiion will provide information to the Customer about the service's details, and how to effectively interact with the Azure Managed enhanced operational support levels. Vysiion will provide the following service information during onboarding.

Information/Process	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
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

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 managed resources within the Azure 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	ACI	R
Configuration Management	RA	CI
Event Management	RA	CI
Incident Management	RA	CI
Patch Management	RA	CI
Release Management	RA	CI
Request Management	ACI	R

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 Features and Benefits

Key Features

- **Microsoft Azure Expertise**: Skilled in deploying and managing Azure-based solutions, including migrations and custom builds
- **Comprehensive Services**: Offers Azure foundational services, virtual servers, backup solutions, domain controllers, and managed services, such as mobile device management with Intune
- **Secure Backup**: Azure Backup secured with TLS encryption
- **Flexible Resources**: Provides flexible Virtual Data Centre (VDC) resources, including vCPU, vRAM, and storage
- **Unified Communications**: Includes services like Teams Calling as a Service (TCaaS)
- **Licensing Support**: Microsoft 365 E3 and E5 licensing with bolt-on security
- **Customised Solutions**: Supports tailored designs to meet specific organisational goals and requirements.

Key Benefits

- **Enhanced Security**: Stringent security measures and compliance with high-security standards
- **Improved Business Continuity**: Reliable backup services and disaster recovery options ensure operational continuity
- **Cost-Effective Solutions**: Reduces reliance on on-premises hardware and optimises IT operational activities
- **Scalability**: Facilitates workload flexibility and resource scaling to meet varying demands
- **Expert Support**: Access to a 24/7 ITIL-accredited service desk and skilled technical teams
- **Simplified IT Management**: Streamlined remote working models and reduced complexity in IT operations.

Service Constraints

Service Dependencies

- Vysiion must be the Azure Cloud Services Provider (CSP) for the services under Azure Managed enhanced operational support levels
- The Service is underpinned by Microsoft Premier Support
- Vysiion will use Azure Lighthouse for access to the Customer Azure environment.
- Note: The service cover only applies to Microsoft Azure products under general release/support by Microsoft

Customer Dependencies

The following Customer dependencies exist for Vysiion to deliver the Azure Managed enhanced operational support level. Failure of the Customer to meet these Customer Dependencies may affect the service Vysiion can deliver to the Customer and Vysiion's obligations under the service levels.

- The Customer shall provide documented active Customer IT policies for all Supported Items when starting the On-Boarding process
- The Customer shall provide Vysiion with advice in advance of any peculiar, special, or particular modifications made to the Azure Managed enhanced operational support levels
- The Customer shall be responsible for documenting and maintaining any differing configuration and requirements pertaining to the Azure Managed enhanced operational support levels that are peculiar, special, or have had particular modifications applied
- The Customer shall ensure Customer endpoints and management environments are secure, patched, and maintained in accordance with Good Industry Practice.
- The Customer shall ensure that any Customer-managed Azure Managed enhanced operational support levels are secured, patched, and maintained in accordance with Good Industry Practice
- The Customer shall work with Vysiion to replace all End-of-Life Supported Items before the End-of-Life date arrives
- The Customer shall provide Vysiion with appropriate rights on Azure Managed enhanced operational support levels to provide appropriate support
- The Customer must use Vysiion as Azure CSP
- The Customer will permit the use of Azure Monitor to be used for the purposes of monitoring an alerting against configured Azure services
- The Customer will permit the use of Azure Lighthouse for Vysiion Management Services
- The Customer shall review the Cost Optimisation Report on a quarterly basis, and notify Vysiion of any wish to make changes to existing services
- The Customer will permit the deployment of additional services required to deliver enhanced service capabilities, and associated charges. For example, Azure VMs to run additional collectors, bastion hosts, jump servers etc.
- The customer must agree to providing Vysiion with all relevant Admin privileges for the tenancy through GDAP, this must include but not be restricted to Azure role-based access control (RBAC) role assignments with *Microsoft.Support/supportTickets/write* permissions, all additional roles can be found

here: GDAP role guidance https://learn.microsoft.com/en-us/partner-center/gdap-least-privileged-roles-by-task

Supplier Type

Service Levels

Service Level Agreements

Vysiion will use all reasonable endeavours to meet the "Target Response Time", “Target Assignment Time” and “Target Fix Times” set out in the following table:

Priority Level	Target Response Time	Target Assignment Time	Target Fix Time
P1	15 minutes to respond	1 hour	4 hours
P2	15 minutes to respond	2 hours	8 hours
P3	30 minutes to respond	4 hours	4 days
P4	30 minutes to respond	8 hours	7 days

Response Time covers the time for Vysiion to acknowledge the incident report. Assignment Time covers the time for Vysiion to indicate to the Customer likely timescales for dealing with the fault and allocate and communicate to the Customer the appropriate personnel. Fix Time covers the period after the incident has been acknowledged (i.e. a ticket has been raised) during which a temporary or permanent fix is put in place. In all Priority 1 and 2 situations, the Customer will be updated hourly on the progress of the fix by email. In the event that the Target Response Times set out in the table above are not met other than due to Excused Reasons (as set out below), the Customer shall be entitled to claim a Service Credit calculated in accordance with the following table:

Time to Respond - Critical (P1)	Time to Respond - High (P2)	Total Number of Incidents per Month Where Time to Respond Exceeded	Service Credit*
15 minutes or less	30 minutes or less	0 – 9%	No Service Credit
Greater than 15 minutes	Greater than 30 minutes	10% – 19%	5% of the current monthly Flex Manage charge
Greater than 15 minutes	Greater than 30 minutes	20% - 25%	10% of the current monthly Flex Manage charge
Greater than 15 minutes	Greater than 30 minutes	Greater than 25%	15% of the current monthly Flex Manage charge

** monthly charge is the Annual Charge divided by 12.*

The maximum amount of Service Credits payable pursuant to the above table in any calendar month shall be limited to fifteen percent (15%) of the then-current monthly Flex Manage charge.

Excused Reasons

Vysiion shall have no liability for any failure to meet any target service levels due to, or as a result of, any of the following reasons (“Excused Reasons”):

- Any Force Majeure Event;

- Suspension of service in accordance with the Contract;
- Customer default or delay, or any negligent, wilful or reckless act, fault or omission by the Customer (or users of the Service for whom the Customer is responsible pursuant to the Contract), or any of their representatives, employees, agents or sub-contractors;
- the Customer not being contactable via the contact details provided by the Customer;
    - the Customer's failure to meet the stated Customer Dependencies; and/or
- Supported Items being End of Life.

Service credit claims must be submitted to customerservices@vysiion.co.uk within thirty (30) calendar days of the end of the calendar month in which the failure to meet the target service level occurred. Any service credit claims not raised by the Customer within this period are irrevocably waived. If service credits claimed are rightly due, they shall be calculated in accordance with this section (such service credits being a genuine pre-estimate of loss, not unconscionable and not a penalty) and shall be applied to the Customer's account. Service credits are the Customer's sole and exclusive remedy with respect to any failure to meet the Flex Manage target service levels.

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 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 Professional Services rates will apply.

ID	Request Description	Availability		Type*	Hours	Time to Complete	Quantity	Frequency
		Email	Phone					
SROAM01	Shut down OS	Yes	Yes	OSR	24 x 7 x 365	1 hour	10	Per month
SROAM02	Reboot OS	Yes	Yes	OSR	24 x 7 x 365	1 hour	10	Per month
SROAM03	Request new physical SI	Yes	Yes	PR	Normal Business Hours	7 Working Days following hardware delivery	N/A	As required
SROAM04	Request new virtual SI	Yes	Yes	PR	Normal Business Hours	1 Working Day	N/A	As required
SROAM05	Change IP address	Yes	Yes	OSR	24 x 7 x 365	1 hour	1	Per quarter
SROAM06	Change hostname	Yes	Yes	OSR	24 x 7 x 365	1 hour	1	Per quarter
SROAM07	Complete emergency patching	Yes	Yes	SO	24 x 7 x 365	8 hours	1	Per quarter
SROAM08	Complete emergency AV scanning	Yes	Yes	SO	24 x 7 x 365	8 hours	1	Per quarter
SROAM09	Complete additional backups of the SI	Yes	Yes	SO	24 x 7 x 365	8 hours	5	Per quarter
SROAM10	Restore the full physical server from backup	Yes	Yes	OSR	24 x 7 x 365	1 Working Day	1	Per annum
SROAM11	Restore the full virtual server from backup	Yes	Yes	OSR	24 x 7 x365	1 Working Day	1	Per annum
SROAM12	Restore individual files from backup	Yes	Yes	SO	24 x 7 x365	1 hour	60	Per annum
SROAM13	Test restore files from backup to test backup validity	Yes	Yes	PR	Normal Business Hours	2 Working Days	N/A	As required
SROAM14	Fail over the virtual SI to another location	Yes	Yes	OSR	24 x 7 x 365	1 hour	1	Per month
SROAM15	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
SROAM16	Adjust the virtual resources allocated to the SI upon	Yes	Yes	SO	24 x 7 x 365	1 Working Day	1	Per month

	Customer request							
SROAM17	Create and format physical disk volumes	Yes	Yes	PR	Normal Business Hours	2 Working Days following hardware delivery	N/A	As required
SROAM18	Create and format virtual disk volumes	Yes	Yes	OSR	24 x 7 x 365	1 Working Day	1	Per month
SROAM19	Create fault tolerant physical disk systems	Yes	Yes	PR	Normal Business Hours	2 Working Days following hardware delivery	N/A	As required
SROAM20	Create fault tolerant virtual disk systems	Yes	Yes	OSR	24 x 7 x 365	1 Working Day	1	Per month
SROAM21	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
SROAM22	Review DR and BC plan	Yes	Yes	SO	Normal Business Hours	5 Working Days	1	Per annum
SROAM23	OS and application patch installation	Yes	Yes	SO	24 x 7 x 365	8 hours	1	Per month
SROAM24	Hardware firmware installation	Yes	Yes	SO	24 x 7 x 365	2 hours	1	Semi annually
SROAM25	Reset SI management account password	Yes	Yes	SO	24 x 7 x 365	1 hour	1	Per quarter
SROAM26	Review OS and application audit logs	Yes	Yes	OSR	24 x 7 x 365	2 Working Days	1	Per annum
SROAM27	Restart applications	Yes	Yes	OSR	24 x 7 x 365	1 hour	10	Per month

** PR = Project Requirement, OSR = Operational Support Request*

User Support

Vysiion's Service Desk is manned 24 x 7 x 365 by engineers for the reporting and remediation of incidents. The Service Desk is aligned to ITIL and industry best practices and it is underpinned by Vysiion's ITIL-based management platform. Details on how to contact the Vysiion Service Desk reporting can be found in the "Customer Support Handbook", a copy of which is available upon request from customerservices@vysiion.co.uk. Where Vysiion becomes aware of a fault with Supported Items, the Customer will be alerted as soon as Vysiion's Service Desk becomes aware of the fault and an incident ticket has been raised by Vysiion. When it is the Customer who first detects the fault, it should be reported by telephone or email to Vysiion's Service Desk. For all logged incidents a priority will be set in accordance with the following table. This is automatically set for incidents raised by Vysiion's Remote Monitoring and Management (RMM) tool and will be set by the Vysiion Service Desk for faults detected by Vysiion outside of the RMM tool. For incidents logged to the Service Desk, the impact for the incident will be set by Vysiion in line with the priority table below. Therefore, when the Service Desk logs an incident the priority of the incident will be set to the corresponding value as in the priority table below. When the Customer raises an incident or wishes to escalate the priority of an incident logged by the Service Desk, the urgency will be defined by the Customer, acting reasonably, after consulting the priority table below. Vysiion will allow incidents to be escalated by one priority level upon reasonable request by the Customer or as deemed reasonable by Vysiion.

Priority Level	Description*
P1	A critical business service is: • non-operational, thus impacting the Customer organisation, multiple users or multiple sites; or • subject to severe functional error or degradation affecting production, demanding immediate attention. Business impact is high, with immediate financial, legal or reputational impact.
P2	The Customer or Supported Item is experiencing: • failure or performance degradation that severely impairs operation of a critical business service; or • failure or degradation although a workaround may exist; or • degradation or loss of functionality; or • degradation that impacts significant number of users or a whole site. Business impact is high.
Priority Level	**Description***
P3	The Customer is experiencing a problem that causes moderate business impact. The impact is: • limited to a single user or a small group of users ; or • moderate, not widespread; or • non-existent. Business impact is low.
P4	Standard service request (e.g. User Guidance); or updating documentation. Low or minor localised impact.

** The incident priority consists of a combination of two items that are detailed for each incident in the Vysiion's management platform:*

- ***Impact.*** *The importance of the incident to the infrastructure at a technical level.*
- ***Urgency.*** *The importance of the incident to the Customer.*

Vysiion understands the necessity of ensuring the uptime and availability of your cloud services. For complete peace of mind, Vysiion's Support Desk provides a fully managed 24/7/365 Cloud Connectivity Monitoring service for all your cloud services. We provide bespoke levels of support packages to suit your business needs.

Our Cloud Connectivity Monitoring Service enables you to extend your existing IT services without increasing your headcount, removing the significant expense of customers setting up their own internal Support Desk provision.

- **Alert**: our Support Desk utilises the most advanced event detection to proactively monitor our customers' infrastructures 24/7/365, raising alerts when pre-defined thresholds are met. The Support Desk's monitoring and alerting systems are configured to each customer's requirements. Alerts will either be passed directly to the customer's service team or integrated with our own service management tool, triggering the ITIL aligned Event and Incident Management processes as appropriate
- **Inform:** our Support Desk team provides customers with information on Capacity and Performance, as well as access to the Vysiion online portal. Here, customers can retrieve real time monitoring data, ticket status updates and allows them to track the progress of any Incidents online
- **Resolve:** when an Incident arises, the Support Desk team resolves or escalates to the relevant Vysiion/customer Resolver groups or third-party suppliers. In all cases, the Vysiion team will manage the Incident until it has been resolved to the customer's satisfaction, and the ticket closed.

The Vysiion Support Desk provides the focal point for proactive and reactive network activities 24/7/365 including monitoring, performance tuning, software distribution and updating, router and domain name management, and coordination with affiliated networks.

Connecting to your infrastructure securely and seamlessly, our Support Desk uses industry leading monitoring tools to provide detailed metrics and visibility.

Change Management

Vysiion will operate an ITIL-based change management process for all planned and unplanned changes to the Supported Items.

Problem Management

Vysiion will operate an ITIL-based problem management process to initiate root cause analysis following repetition of a critical (P1) incident. A problem is defined as an unknown cause of one or more critical incidents.

Service Acceptance Criteria (SAC)

Vysiion will operate a SAC process which enables the controlled delivery of a live Flex Manage Service that satisfy its own expectations and requirements as well as those of the Customer. The SAC process measures the flow of information and subsequent On Boarding activities that the Service Desk completes to ensure the provided Flex Manage Service meets its functionality and quality requirements, and that Vysiion is ready to operate the Flex Manage Service for each Supported Item.

Third Party Administration Rights

Vysiion will provide access rights to Supported Items for the Customer or any Customer nominated third party, if explicitly authorised by the Customer in writing. Vysiion will not be liable for any problems caused by the execution of third-party administration rights against any Supported Items.

Support Methods

Vysiion provides multiple contact methods from its 24/7/365 Service Desk, ensuring accessibility and efficient support for its customers. These methods include:

- **Email**: Customers can report incidents or raise support requests by emailing servicedesk@vysiion.co.uk. This ensures a clear and traceable communication route for managing support needs
- **Phone**: A dedicated support telephone line is available 24/7, allowing customers to speak directly with Vysiion experts. This ensures immediate response for critical issues
- **Support Portal (Ticketing System):** Vysiion utilises an ITIL-aligned Service Management Platform, ServiceNow, branded as the Service Centre, accessible through an online portal. Customers can log incidents, submit service requests, and monitor ticket progression. The Service Centre is configured to align with specific service levels and KPIs, ensuring efficient workflows and consistent communication
- **Onsite Support:** Vysiion provides robust onsite support through its Smart Hands solution, delivering 24/7/365 assistance via SC-cleared engineers. These engineers handle a range of activities such as remote IT infrastructure management, equipment troubleshooting, installation services, and maintenance tasks. With formal Service Level Agreements (SLAs) tailored to individual requirements, we ensure rapid response times, including the ability to be onsite within 15 minutes. This ensures efficient and secure operations for organisations across high-compliance sectors.

Support Levels

Vysiion provides multiple levels of support tailored to meet specific customer requirements. These levels include:

- **Standard Support**: Covers basic operational support such as incident management, proactive monitoring, and maintenance activities during defined working hours, typically 08:00–18:00 on weekdays
- **Enhanced Support**: Includes 24/7 support for incident resolution, proactive monitoring, and escalations to ensure critical systems remain operational
- **Customised Support**: Tailored packages designed in collaboration with customers to meet unique business needs, including managed services, system administration, and application support.

Cost of Support Levels

The cost of support services varies based on the level selected:

- **Standard Support**: Included in the base service agreement if within predefined thresholds. Any additional requests are charged per the agreed rate card
- **Enhanced Support**: Fees are typically based on 24/7 availability and include time-related charges for on-site support, along with travel and subsistence costs
- **Customised Support**: Bespoke pricing based on the scope of requirements, based on a per unit per day for consultancy and tailored support.

Technical Account Manager or Cloud Support Engineer

- Vysiion provides **dedicated Account Managers** such as a Service Delivery Manager (SDM) and Sales Account Manager. The SDM ensures service reviews, reporting, and escalations are handled effectively, while the Sales Account Manager oversees additional service discussions
- **Cloud Support Engineers** are available as part of enhanced operational support packages. Their responsibilities include managing Microsoft public cloud environments, monitoring, troubleshooting, and maintaining security configurations.

Security Clearance

Vysiion's employees are screened to the Baseline Personnel Security Standard (BPSS) as a minimum, with many holding Non-Police Personnel Vetting (NPPV) Level 3 or Security Check (SC), and a subset holding Developed Vetting (DV). Vetting is conducted by Warwickshire Police under NPPV procedures and includes identity verification, BPSS checks, internal records checks, security questionnaires, criminal record checks, credit reference checks, and security service checks.

Our pre-employment screening covers the core control areas specified in BS7858:2019 by performing identity verification, criminal record checks, credit checks, and security service checks through the NPPV process, and we retain auditable records of screening and approvals within our ISO 27001 Information Security Management System. All staff undergo BPSS/NSV screening prior to employment, with additional clearances granted based on role and access to customer data and assets. All operational staff are vetted and cleared to work in high-security environments, enabling on-site delivery for Defence, Blue Light, and CNI customers.

We operate at scale with an Operations team of around 80 people; 26 are responsible for Secure Operations and Support and all hold security clearances. This provides assured 24/7/365 service coverage in restricted environments and an auditable trail for starters, movers, and leavers to manage access across systems and locations.

Why Vysiion?

Vysiion provides integrated turnkey solutions, delivering critical infrastructure and comprehensive managed services into a broad range of sectors including central government, utilities, defence, and the emergency services.

Our customers have come to rely on us for the delivery of Critical National Infrastructure (CPNI) and business systems alike ranging from WAN and Operational Networks, Fibre and Cabling in the field and datacentre, to Cloud, Managed Services and consultancy for IT networks and Infrastructure for the delivery of key applications and compute environments.

Having built a reputation in delivering and supporting critical infrastructure (communications and IT), over the past 30 years, through a combination of organic and acquisitive growth, Vysiion has built on this foundation and undergone a period of accelerated growth. This culminated in Vysiion becoming an 'Exponential-e Group Company' following the acquisition of all Vysiion shareholding in February 2020.

Vysiion and the Exponential-e group have a combined annual turnover of c.£200m, employing 850+ staff, and are recognised as one of the fastest growing private companies in the UK. We are a Customer First organisation, committed to the delivery of customer service excellence, demonstrated by 99% of customers renewing annually and a sector leading NPS score of 88.

The Group provides customers with a variety of IT managed services, leveraging Exponential-e's core network infrastructure to provide a backbone of network connectivity services, with additional/standalone Cloud, Communications, Infrastructure, Security & Managed Services. By leveraging group resources and expertise, Vysiion ensures its clients receive best-in-class service.

Proven Expertise

Vysiion is a trusted provider of cloud solutions with proven expertise in delivering tailored, secure, and scalable cloud deployments across a wide range of sectors including central and local government, utilities, defence, and emergency services. Our solutions are designed to meet the unique requirements of enterprise-level organisations, providing the foundation for seamless digital transformation and operational efficiency.

Vysiion offers a full suite of cloud services, including Public Cloud, Private Cloud, and Hybrid Cloud solutions. These services are designed to optimise performance, scalability, and security, ensuring organisations can transition their workloads to the cloud with confidence. Our team works closely with clients to design bespoke solutions tailored to their goals, compliance requirements, and existing infrastructure.

Vysiion specialises in designing and managing cloud environments for sectors with complex requirements, including CNI, Defence, and Central Government. Our solutions provide isolated development environments optimised for testing, development, and production, ensuring security and compliance are always maintained.

Experience

Vysiion's combination of industry expertise, robust methodology, and strong vendor partnerships makes us the ideal choice for organisations seeking reliable and efficient cloud services. Our cloud solutions are designed to maximise cost savings and scalability. By utilising intelligent automation, we deliver faster deployments and ensure organisations can scale resources up or down based on changing demands, reducing operational overheads and improving efficiency.

A range of G-Cloud services and complementary capabilities are available from Vysiion. These can be procured alongside this service to support an organisation's transition towards more commodity-based ICT.

Partnerships with Leading Providers

We have established strategic partnerships with key vendors such as Microsoft Azure, AWS, VMware, Cisco, and Ark Data Centres. These partnerships allow us to leverage cutting-edge technologies to deliver robust cloud environments that meet the stringent compliance and security standards required for enterprise applications.

Robust Security and Accreditation

Vysiion demonstrates robust capabilities in delivering secure cloud solutions, ensuring compliance and accreditation with industry-recognised standards. Our cloud solutions are built on stringent security frameworks, including ISO 27001, Cyber Essentials, Cyber Essentials Plus, and ISA/IEC 62443 certifications. These certifications confirm Vysiion's commitment to maintaining high standards in information security management systems and mitigating vulnerabilities in critical infrastructure design and operation. Vysiion also adheres to the NCSC's Cyber Assessment Framework (CAF) and Secure by Design principles, ensuring the comprehensive protection of customer infrastructures from cyber threats and unauthorised access.

We integrate security as a fundamental aspect during the design phase of business applications. A 'Secure by Design' approach ensures infrastructure and assets are protected from initial concept through ongoing operations, validated against applicable regulatory frameworks. This includes proactive measures informed by the latest threat intelligence to mitigate risks across IT and OT environments. Access controls such as multi-factor authentication and role-based permissions further enhance the security of internal systems used in pre-sale, design, delivery, and support processes.

Vysiion employs security-cleared engineers and operates a UK-based Cyber Security Operations Centre (CSOC) that provides 24/7 real-time security monitoring and alerting services. This approach ensures organisational cyber resilience and minimises risks associated with cybercrime. Additionally, Vysiion engages CREST-approved third-party vendors for penetration testing to validate the security of IT infrastructures.

Hosting solutions are delivered through Tier 3+ Data Centres, offering high levels of physical and cyber security. These data centres are equipped with multi-layered security measures, biometric access controls, and environmental monitoring systems, ensuring compliance with Cabinet Office and NCSC standards.

Our Accreditations

We support the security and compliance standards of the Public Sector by embedding our compliance certifications into our Business Management Systems. These include:

- ✓ **ISO9001 -** Quality Management
- ✓ **ISO2000 -** IT Service Management
- ✓ **ISO27001 -** Information Security
- ✓ **ISO14001 -** Environmental Management
- ✓ **ISO45001 -** Health & Safety Management
- ✓ **Cyber Essentials Plus**