vysiion™

AN EXPONENTIAL-E GROUP COMPANY

TEAMS CALLING AS A SERVICE – Service Definition

RM1557.15 G-Cloud 15: Lot 2b – SaaS

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 2b: Software as a Service (SaaS)

Service Name

Teams Calling as a Service

Service Description

The Teams Calling as a Service provides PSTN connectivity over the Vysiion network and processes inbound and outbound call traffic to/from the Customer's Microsoft Teams environment to/from the PSTN using Session Initiation Protocol (SIP), presented at a user level. The Teams Calling user calls are delivered to the PSTN via the Vysiion carrier grade TCaaS Platform, utilising its dedicated carrier interconnects. The Teams Calling Service is a customisable Service using the following components:

Mandatory Components

Component	Overview
User License	This is the provision of dial-tone to Microsoft (MS) Teams users. The TCaaS Platform will accept outbound calls from and route incoming calls to MS Teams users. In order for calls to be placed to and from the PSTN, it will be necessary to associate a DDI with the Microsoft Teams environment.

Optional Components

Component	Overview
Managed User	User license for Customers where Vysiion is responsible for the management of the Customer's Microsoft Office 365 tenant for all elements relating to Teams Direct Routing and external PSTN calling. Includes Microsoft TCaaS User License. Please note, support does not include elements outside PSTN calling such as user to user calling or any collaboration items within Microsoft Teams / Office 365.
Calling Bundle	Inclusive UK Calling bundle allocated on a per user license
Endpoint Management	Technical support for Endpoints to be used by Microsoft Teams users. Support covers the fault resolution of Endpoints used in conjunction with the Vysiion TCaaS service for configuration and service issues. Please note, this component is only available in conjunction with 'Managed User' and supported Endpoint must be purchased from Vysiion.

Optional Hardware

Component	Overview
Endpoints	A range of Microsoft Teams supported Endpoints. Please note, if endpoints are to be supported, Endpoint Management must be purchased.
Session Border Controller	A range of Session Border Controller to be used in conjunction with the Vysiion TCaaS service if dedicated devices are required. Use of these devices may include support for international offices or analogue support.

The following chargeable Professional Services units are available:

Professional Services	Description (Info)
Consultation	Consultation to work with the customer to define business outcomes
Project Management	Project Management, Customer Kick Off or Low-Level Design Workshops
Implementation	Architect / Design, Engineering Build or Quality Assurance and Testing
Adoption	Admin and User Training, Documentation

The following table defines what is included with each Professional Services unit:

Professional Services	Breakdown	Items Provided
Consultation	Consultation	Consultation to work with the Customer to define business outcomes. The output is an updated scope of works. The amount of Days will be specified on the Order Form.
Project Management	Project Management	Project Management to support project delivery and setup. The amount of Days will be specified on the Order Form.
Professional Services	**Breakdown**	**Items Provided**
	Customer Kick Off	Project Management to provide the Customer kick off meeting. The amount of Days will be specified on the Order Form.
	Design Workshops	Design workshop to finalise the detailed solution design to be performed on site or remotely. The output is a low-level design. The amount of Days will be specified on the Order Form.
Implementation	Architect/Design	Professional services from a design architect to be performed remotely. The output is the sign-off of the implementation design. The amount of Days will be specified on the Order Form.
	Pre-Build Engineer	Engineering to perform the service build to be performed on site or remotely. The amount of Days will be specified on the Order Form.
	Quality Assurance and Testing	Professional services to complete the solution testing and make any required amendments before go-live. To be performed on site or remotely. The amount of Days will be specified on the Order Form.
Adoption	Admin Training	Admin training to be delivered on site or remotely. The amount of Days will be specified on the Order Form.
	Agent Training	Agent training to be delivered on site or remotely. The amount of Days will be specified on the Order Form.
	Go Live/Floor walk	Go-live support to be delivered remotely or on-site with a floor walk. The amount of Days will be specified on the Order Form.

TCaaS Customer Premises Equipment (CPE) (optional)

Any routers, Endpoints and Network Termination Equipment (NTEs) provided will remain the property of Vysiion. Unless agreed otherwise in the Contract, it is the Customer's responsibility to connect any CPE on their premise(s).

Calling Bundle

The TCaaS Service may be purchased with an inclusive call bundle. Where a call bundle has been purchased this will be specified on the Order Form. Where purchasing a call bundle, the Customer must purchase the same call bundle for all users. Vysiion offers the following minutes bundle on a monthly basis:

Bundle Name	National/local Calls*	Mobile calls*
Calling Bundle	2,000 minutes	1,000 minutes

** National/Local calls are defined as those calls to UK 01/02/03 numbers. Mobile calls are defined as calls to FM1, FM3, FM4, FM5 and FM6 tariffs. Bundled minutes are aggregated for national/local and mobile across all of the Customer's TCAAS users. If the aggregated usage for national/local and/or mobile exceeds the relevant aggregated bundle allowance then Usage Charges in accordance with the current rate card shall apply. Any unused monthly minutes cannot be rolled over.*

TCaaS Service Demarcation Point (SDP)

The TCaaS SDP is the point up to which Vysiion's TCaaS service obligations apply and is the point up to which the TCaaS Service Level Agreement covers. The Microsoft Office 365 tenant will be the default SDP, unless Vysiion is providing 'Managed User' or 'Endpoint Management' as part of the TCaaS Service, in which case the PSTN calling elements of the Microsoft Teams users will be the SDP. For instances where Vysiion is proving 'Endpoint Management', the IP handsets will also be covered.

Service Features and Benefits

Key Features

- Have a single app for all communication and collaboration needs including inbound/ outbound calling, IM, chat, video, file share and more with full integration with the Microsoft ecosystem
- Drive productivity and responsiveness using highly available Session Border Controllers (SBCs) – within geographically diverse data centres
- Use TCaaS with an O365 E3 with Microsoft Phone System licence or an O365 E5 license for each end user, enabling enterprise calling features and functionality within the Microsoft Teams interface for a rich user experience
- Our on-going 24/7 management and support from UCC specialists completely removes the IT burden from the customer's internal team to make more effective use of resources
- Option for full management of the customer's MS Teams and Office 365 environment, refocusing internal resources on driving developments instead of firefighting
- Replace your systems with on-premise or hosted telephony platforms, with our Cloud-based direct routing service for built-in resilience and anywhere, anytime access across end-user devices
- Use voice quality metrics to ensure the best possible user experience (UX) and drive user adoption to deliver faster time-to-value on the customer investment
- Supported through in-country SBC deployments for international projects offering the ability to extend the UCC estate across further sites
- Self-Serve Portal: Cloud-native platform-as-a-service that centralises the automation of unified communications lifecycle management. Using a single-pane view, users have access to zero-touch provisioning, call routing, number management, and add-on services. Using the portal, customers can deploy Teams Voice through either Direct Routing or Operator Connect
- Provide users with the flexibility of choosing how they want to work – with monitoring overlaid to continually manage call quality.

Key Benefits

- Save time and reduce costs
- Always-on calling functionality
- Leverage existing investment into Microsoft
- Delivers an end-to-end solution
- Fully managed solution
- Replace older systems
- Performance monitoring
- Bring Your Own-PSTN
- Certified endpoints.

Cloud Deployment Model

The service is deployed using the following Cloud Deployment Model:

- Private cloud.

Service Constraints

- Any routers, Endpoints and Network Termination Equipment (NTEs) provided will remain the property of Vysiion
- Unless agreed otherwise in the Contract, it is the Customer's responsibility to connect any CPE on their premise(s).

System Requirements

To utilise Vysiion's Teams Calling as a Service, the following system requirements must be met:

- **Hardware and Software Requirements**
  - **Microsoft Licenses**:
    - Users require one of the following Microsoft licenses:
    - Microsoft Teams Phone Standard
    - During initial synchronisation, Call2Teams requires two additional Microsoft licenses:
    - Microsoft 365 Business Basic or equivalent Business Licenses (Microsoft E3 or E5 licenses)
    - Common Area Phone or Microsoft Teams Phone Standard licenses
  - **Devices**:
    - Each user must have a Direct Dial-In (DDI) number available in the number pool
    - A primary device configured as the Microsoft Teams Calling Trunk – C2T – Direct Routing device with a "zero rate" tariff
- **Session Border Controllers (SBCs)**:
  - Managed SBCs are supported via AudioCodes OVOC (One Voice Operation Centre) for proactive troubleshooting and quality monitoring.
- **Network Requirements**
  - **Private Interconnects:** Vysiion maintains multiple private interconnects with Tier 1 carriers for secure PSTN traffic and SIP session delivery
  - **Direct Routing**: Configuration of central SBCs to bridge platforms and enable controlled migrations.
- **Administration and Management**
  - **Global Administrator Details:** A Microsoft 365 Global Administrator account is required to receive synchronisation emails and perform "Sync Now" tasks in the Call2Teams portal.
  - **Call2Teams Portal:** Administrators must perform initial synchronisation and assign the *Microsoft Teams Calling Integration Business Service*.
  - **Teams Admin Centre (TAC):** Number porting, new number allocation, and management of numbers are handled through TAC or Vysiion's Multi-UC automation platform.

Service Levels

TCaaS Availability

The TCaaS Service availability is defined, for each particular Customer Site, as the ability to make/receive calls to/from the PSTN from the SDP.

	Target Availability
TCaaS	99.99%

In the event an access method other than an uncontended Vysiion private Ethernet over Fibre connectivity service is used to access the TCaaS Platform (e.g. Ethernet over Copper or Broadband or 3rd party Ethernet over Fibre) the SLA will not apply in the event of a connectivity failure or impairment.

Service Credits

	Measure	Service Credit*
Availability	>0.1 Below Target	5%
	>0.5 Below Target	10%

** The service credit is applied as a percentage of the fixed Monthly Charge for the TCaaS for the affected Customer Site only (not including variable call spend).*

User Support

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.

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.

These contact options are designed to provide a single point of contact for all support needs, ensuring issues are logged, tracked, and resolved efficiently.

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.

This structured approach ensures flexibility, scalability, and alignment with customer-specific goals.

Onboarding and Offboarding

Onboarding Process

Vysiion ensures a seamless onboarding experience for users of its Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) solutions. The process begins with a comprehensive consultation to understand the customer's requirements and existing infrastructure. Following this, Vysiion delivers managed implementations, including in-house design and testing of the proposed solution, ensuring it aligns with the customer's operational and security needs.

Training and Documentation

Vysiion provides both online and onsite training, tailored to the customer's needs. Bespoke documentation is created as part of this process, detailing system configurations, user guides, and operational manuals. This ensures users are equipped to fully utilise the capabilities of the service. Documentation includes high-level designs (HLDs) and low-level designs (LLDs), structured reviews, and step-by-step guides for managing the service.

Initial Setup

Vysiion’s cloud experts assist with the setup, enabling a stress-free transition. This includes provisioning secure access for end-user devices, integration with existing systems, and deployment of hybrid solutions where required.

Offboarding Process

When the contract ends, Vysiion ensures the secure and compliant extraction of customer data. Data stored within the IaaS and PaaS platforms is exported in formats agreed upon during the contract initiation. Vysiion supports customers in securely migrating their data to alternative platforms or storage solutions.

Data Extraction

Vysiion uses encryption and secure transfer protocols to prevent data loss or breaches during extraction. Customers can request additional services for bespoke migration needs, which may incur extra costs.

Account and Access Management

Access to the system is revoked upon contract termination to prevent unauthorised use. Vysiion provides detailed offboarding reports, outlining actions such as account deactivation and system audits.

Pricing Structure

The contract price typically includes:

- Access to Vysiion's multi-tenant IaaS and PaaS cloud platform
- Standard onboarding services including consultation, training, and documentation
- 24/7 operational support from Vysiion's ITIL-accredited service desk.

Additional costs may apply for:

- Bespoke training or documentation requests beyond the standard provisions
- Data migration services during offboarding if unique requirements are specified
- Advanced features such as encryption at rest, hybrid cloud solutions, or bespoke connectivity setups.

Vysiion's structured onboarding and offboarding processes ensure smooth transitions while maintaining security and compliance at every stage.

Data Exporting

Vysiion provides users with a structured and secure approach to data export within its software services. The company's approach ensures compliance with data protection regulations, operational efficiency, and user control over their data.

Users can export their data using supported protocols such as Object, HDFS, and NFS, which are facilitated through a customer-accessible portal. The portal enables users to create, view, and manage their storage resources independently. Data exports are typically generated in formats such as CSV files, ensuring they are accessible and usable for the customer's needs. For example, in specific scenarios, data may be exported to an AWS bucket, where users can securely access it using their credentials.

To maintain compliance with standards such as GDPR, Vysiion employs secure processes for data handling. The company adheres to principles of data protection by design and default, including procedures for data minimisation and encryption. This ensures that exported data is handled securely and complies with legal and organisational requirements.

Vysiion has implemented robust exit management procedures. Upon contract termination, the company securely removes client data following documented policies, ensuring no residual data is left behind. This process further underscores their commitment to secure data handling throughout the data lifecycle.

By combining user-friendly export mechanisms with stringent data security protocols, Vysiion offers a reliable and compliant framework for data exportation, ensuring customer data remains secure and accessible as needed.

Independence of Resources

Vysiion ensures that users of its IaaS and PaaS offerings are not affected by other users' demands through robust architecture, monitoring, and tailored resource allocation.

We employ a robust infrastructure strategy to prevent service impact from cross-tenant demands across its IaaS and PaaS solutions. Dedicated or electronically segregated resources within our Virtual Data Centre ensure complete separation of compute and storage, mitigating noisy neighbour risks. Logical separation of client data and workloads is maintained through multi-tenant data encryption and resource partitioning.

Operating on VMware ESXi in two UK-based availability zones, Vysiion ensures redundancy and availability SLAs between 99.9% and 99.99%. With vSphere, tenants receive Virtual Data Centres with reserved resources and enforced limits, guaranteeing performance stability during demand peaks.

To ensure users are not affected by other users' demands, Vysiion employs a robust personnel resource strategy. We manage skills centrally to allocate qualified staff to tasks without overcommitment. Our team includes SC and DV-cleared personnel, supported by a skills matrix of certifications like VMware, Cisco, and Microsoft. Resource requirements are modelled at project initiation to ensure accurate allocation of personnel and timelines. Real-time tracking of resource utilisation via project management platforms enables dynamic adjustments to meet demand. We maintain agreements with vetted, security-cleared specialist partners for supplementary expertise during peak periods or niche requirements.

Availability and Resilience

TCaaS Availability

The TCaaS Service availability is defined, for each particular Customer Site, as the ability to make/receive calls to/from the PSTN from the SDP.

	Target Availability
TCaaS	99.99%

In the event an access method other than an uncontended Vysiion private Ethernet over Fibre connectivity service is used to access the TCaaS Platform (e.g. Ethernet over Copper or Broadband or 3rd party Ethernet over Fibre) the SLA will not apply in the event of a connectivity failure or impairment.

Service Credits

	Measure	Service Credit*
Availability	>0.1 Below Target	5%
	>0.5 Below Target	10%

** The service credit is applied as a percentage of the fixed Monthly Charge for the TCaaS for the affected Customer Site only (not including variable call spend).*

Resilience

The service is provided via Geo resilient architecture with full redundancy. The platform Data Centres are Global, UK and EEA and we continually evolve our architecture to ensure geographical service and best-of-breed technology.

Service Reporting of Outages

Email Alerts

Vysiion provides automated email alerts for outages related to teams calling services, ensuring effective communication during incidents. Notifications are sent to the primary customer contact, with the option to agree on additional contacts during the onboarding process. Updates are continuously provided until the issue is resolved.

Customers can also report incidents 24/7 via telephone, email, or the Service Centre portal, powered by ServiceNow.

API integration

For an additional optional charge, an API integration between a customer's ITSM tool and Vysiion's instance of ServiceNow can be provided.

Vysiion's API integration facilitates seamless communication between customer ITSM tools and Vysiion's ServiceNow instance. This integration supports automated ticket creation, change request submissions, and alert synchronisation while preserving the customer's existing workflows. Leveraging an API-driven architecture, Vysiion ensures data sharing, consolidated dashboards, and proactive incident handling without operational disruption. For clients with bespoke requirements, Vysiion collaborates to define and align ITSM processes, including field mapping and system configurations, ensuring tailored solutions.

Dashboards

In addition to a mandatory agent license, there are a number of optional, chargeable dashboard add-ons for the service.

Information Security Policies and Processes

Vysiion implements robust information security policies and processes, aligning with international standards such as ISO/IEC 27001 and the UK Network and Information Systems (NIS) Directive to safeguard customer data and operational integrity. The organisation adopts a 'Secure by Design' approach, ensuring security is embedded into the design and delivery of systems, covering IT and operational technology (OT) environments. This methodology integrates controls for confidentiality, integrity, and availability of information, while also considering compliance with frameworks like NCSC guidelines and IEC-62443.

Vysiion's policies are enforced through a structured framework, including annual reviews and updates of security policies. The company maintains comprehensive Information Security and a Data Protection Policies, which address key aspects such as data breach management, risk assessment, and access controls. For incident management, Vysiion employs ITIL-aligned procedures, logging all incidents and ensuring major breaches are reported to relevant authorities within 72 hours. Post-incident reviews are conducted to identify causes and implement preventive measures.

A dedicated Data Protection Officer (DPO) oversees compliance with data protection laws, supported by a Personnel Security Controller to manage personnel assurance and mitigate insider threats. All employees and contractors are required to cooperate with supervisors on security matters and are trained on corporate policies during induction. Annual online security training and simulated attack tests further ensure staff adherence to security protocols.

The effectiveness of these measures is monitored through real-time network surveillance using industry-standard tools. Vysiion also conducts formal security risk assessments at least annually or following significant changes to highlight and mitigate new risks. Regular board and staff meetings include security as a discussion point, fostering a culture of awareness and accountability.

To ensure compliance across its supply chain, Vysiion employs rigorous supplier management processes, including assessments. Subcontractors are required to meet stringent security requirements, demonstrating their capability through certifications and compliance checks.

Operational Security

Vysiion's security framework ensures protection, compliance, and efficiency in cloud services. A 24/7 in-house Cyber Security Operations Centre (CSOC) ensures real-time monitoring and incident response. This eliminates reliance on third-party IT providers, ensuring full control over security.

Vysiion adheres to ISO 27001, Cyber Essentials Plus, and ISA/IEC 62443 standards to ensure top-tier security. A 'Secure by Design' approach integrates security into all project phases, from planning to maintenance. This aligns with NCSC guidelines and NIS-2 directive for regulatory compliance.

Vysiion uses the Purdue Model and automated monitoring to map data flows and ensure resilience. Tier 3+ sovereign data centres with multilayered security and biometric access host Vysiion's infrastructure. These facilities ensure secure data processing and integration with various cloud platforms.

Technical assurance involves rigorous design reviews to ensure industry and customer compliance. This includes cross-functional reviews, dependency management, and risk mitigation. CREST-approved third-party penetration testing validates infrastructure security.

Vysiion delivers secure, scalable solutions for defence, government, and critical national infrastructure (CNI). Its framework ensures resilient, compliant, and optimised cloud services for modern demands.

Configuration and Change Management Approach

We govern configuration and change through an ITIL-aligned process embedded in our Service Operations and ISMS, ensuring standard methods, procedures, authorisation and auditability for all changes across supported items and suppliers. Every change is logged as a Request for Change, assessed, approved and implemented in a controlled workflow that minimises service disruption and keeps configuration records accurate and current. Our Service Management platform provides real-time tracking, automated notifications and transparent reporting of planned changes, giving stakeholders clear visibility and audit trails. Oversight is maintained by ITIL function specialists and Service Managers operating a 24/7/365 Service Desk, ensuring changes and related incidents are coordinated for rapid recovery and minimal business impact.

We track service components as Configuration Items and assets from introduction through to disposal, maintaining ownership, configuration, and status in our managed records and asset register. Our responsibilities include delivery, installation, configuration, support, re-configuration and disposal of user devices and in-scope items, which ensures full lifecycle control and traceability. The Change Management process requires that any approved modification updates the status of affected Configuration Items, keeping our records aligned with the live environment. Documentation such as low-level designs, network diagrams, configurations and knowledge articles is maintained to support faster resolution and accurate service documentation throughout the lifecycle.

All changes, including supplier-initiated, follow a standardised workflow covering initial logging, impact assessment, risk evaluation and formal authorisation before implementation. We apply consistent methods and procedures across supported items, so every planned or unplanned change is controlled, transparent and auditable. The Service Management platform underpins this with real-time tracking, notifications and reporting, ensuring change windows, approvals and outcomes are visible. When customer-specific processes exist, we integrate with them; otherwise, we use our framework to minimise operational disruption through risk assessment and contingency planning.

We assess every change for potential security impact as part of formal evaluation, covering effects on security posture and compliance requirements before authorisation. Our Cyber Security and Compliance team conducts formal security risk assessments at least annually and after any significant change, ensuring new risks are identified and mitigated. We embed Secure by Design practices and align to ISO 27001, Cyber Essentials Plus, ISA/IEC 62443, NIS-2 (UK) and NCSC's Cyber Assessment Framework to ensure changes do not compromise confidentiality, integrity or availability. Access impacts are reviewed against our least-privilege access management controls to prevent unauthorised exposure when roles, systems or configurations change. Legal and regulatory obligations are considered within our ISO 27001 ISMS and Incident Response Plan, with documented processes to evidence compliance during change and post-implementation review.

Vulnerability Management Approach

Vysiion employs a robust vulnerability management process that integrates threat assessment, timely patch deployment, and reliable threat intelligence sources. This ensures the security and resilience of its services.

Assessing Potential Threats: Vysiion's Cyber Security Operations Centre (CSOC) continuously monitors the environment to detect vulnerabilities, untriggered threats, or attack vectors. This is achieved through a Unified Security Management device, which provides a web-based dashboard displaying results prioritised by risk levels. The CSOC team conducts vulnerability scans using tools like Nessus, which align with recognised standards such as IEC 62443 and NIST. These scans identify misconfigurations, missing patches, and known vulnerabilities, enabling effective risk management.

Deploying Patches: Vysiion follows a stringent patch management policy to apply security updates promptly. This practice ensures compliance with vendor recommendations and covers a comprehensive range of IT systems, including endpoint devices, servers, network equipment, and applications. Regular service tickets are raised automatically to ensure timely review and patch implementation. For operational systems, Vysiion conducts in-place upgrades through automated mechanisms within predefined patching windows, ensuring minimal disruption to services.

Sources of Threat Information: To stay ahead of emerging threats, Vysiion's Cyber Security and Compliance team collaborates with appointed security advisors and accreditation bodies. The company participates in the Cyber Security Information Sharing Partnership (CISP), a joint initiative with the government, which provides real-time updates on cyber threats. Additionally, Vysiion subscribes to industry threat intelligence feeds and uses these insights to proactively address risks. These sources allow the team to adopt new technologies or enhance processes to mitigate potential threats.

Vysiion's integrated approach ensures vulnerabilities are identified, prioritised, and mitigated effectively, safeguarding its services against an evolving threat landscape.

Protective Monitoring Approach

Vysiion employs a robust protective monitoring process to ensure the security and integrity of its systems and data. The process is underpinned by real-time monitoring of internal networks using industry-standard tools. This approach enables the detection and logging of any suspected security breaches, ensuring swift intelligence gathering to identify potential compromises.

When a potential compromise is identified, Vysiion follows documented procedures for incident management. These frameworks provide a structured approach for reporting, escalation, and investigation of incidents, including suspected fraud or misconduct. Incidents are reported immediately to a dedicated incidents email with as much detail as possible to facilitate a thorough investigation.

Response times to incidents are prioritised within Vysiion's ITIL-aligned service delivery framework. The Network Operations Centre (NOC), manned 24/7 by security-cleared staff, ensures incidents are addressed promptly. For major incidents, such as security breaches, notifications to supervisory authorities occur within 72 hours, followed by a Major Incident Review to identify causes and implement preventive measures. This structured and proactive approach ensures that response times are optimised and aligned with stringent service level agreements (SLAs).

Incident Management Approach

Vysiion's incident management processes for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) are robust, ITIL-aligned, and tailored to ensure minimal disruption and optimal service delivery. These processes are supported by advanced tools, clear escalation paths, and proactive incident handling strategies:

Pre-defined Processes for Common Events: We employ pre-defined processes aligned with ITIL standards to manage incidents effectively. The incident management lifecycle is initiated through the ITIL-aligned service management tool, ServiceNow. ServiceNow integrates with advanced monitoring tools, enabling seamless detection, logging, categorisation, and escalation of incidents. Pre-set workflows are configured to handle common events, ensuring swift and appropriate resolution.

How Users Report Incidents: Users can report incidents via multiple channels, including telephone, email, or through a dedicated web portal. For urgent or critical incidents, telephone reporting is encouraged to ensure immediate attention. When an incident is logged, users receive a unique reference number to track progress throughout its lifecycle. Automated status updates are provided in accordance with the SLA and assigned priority, ensuring users remain informed. Additionally, customer access to the web portal offers real-time ticket tracking.

Provision of Incident Reports: Incident reports are generated and shared with customers in accordance with agreed timelines. These reports include detailed records of incident cause, resolution, and preventive measures. For major incidents, a formal review is conducted post-resolution to capture lessons learned and identify service improvements. Reports are coordinated with the Customer Service Delivery Manager (CSDM), ensuring transparency and structured communication throughout the incident lifecycle.

Escalation Procedures: Vysiion operates a structured escalation path to ensure accountability and rapid issue resolution. Escalation levels include Service Desk, Service Desk Manager, Director of Engineering, and Managing Director, with additional oversight provided by the CSDM. Automated alerts notify teams if service levels are at risk, triggering the escalation process as needed.

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.

Identity and Authentication

Vysiion employs stringent measures to restrict access to management interfaces and support channels when providing Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). These measures ensure the security and integrity of customer environments while maintaining operational efficiency.

Access to management interfaces is controlled through robust technical and procedural security controls. Vysiion utilises multi-factor authentication (MFA) across all remotely accessible services, including internal IT systems and third-party SaaS platforms. This ensures that only authorised personnel can access critical systems and data. Additionally, access to key infrastructure components, such as routers and equipment, is regulated via secure protocols like SSH and HTTPS. Management traffic is segregated through out-of-band Virtual Private LAN Service (VPLS), with all access meticulously logged via the ServiceNow portal. These practices comply with ISO27001 and PCI-DSS standards, ensuring comprehensive protection of customer data.

Vysiion enforces access control policies based on the principle of least privilege. Employees are granted access only to the applications, data, and servers necessary for their specific roles and responsibilities. This minimises the risk of unauthorised access and ensures compliance with security best practices. The ITIL-aligned Access Management process further bolsters this approach by providing structured oversight of user access.

To enhance accountability and traceability, all network connections undergo rigorous risk assessments. Vysiion maintains a tightly secured, ring-fenced customer network, which is isolated from external exposure. Connections within this network are limited to secure Site-to-Site (S2S) VPNs, further safeguarding customer environments from external threats.

Vysiion's commitment to security is reflected in its adherence to ISO 27001 standards, Cyber Essentials Plus certification, and compliance with frameworks such as ISA/IEC 62443 and NIS-2 directives. These guidelines ensure security is embedded into the design and operation of infrastructure services.

By combining secure access controls, stringent policies, and adherence to international standards, Vysiion ensures the integrity and security of management interfaces and support channels for IaaS and PaaS solutions.

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**