

G-Cloud 15 Service Definition

Managed IT Service

Lot 3 Cloud Support

Contents

1. About Vorboss	3
1.1. Company overview	3
1.2. Value Proposition	3
1.3. What the Service Provides	4
1.4. Social Value	5
2. G-Cloud Service	6
2.1. Overview	6
2.2. Service Tiers and Service Levels	7
2.3. Service Components	8
2.4. Associated Services	12
2.5. Pricing	13
2.6. Data protection	13
2.7. Using the service	15
2.8. On-Boarding, Off-Boarding, Service Migration and Scope	16
2.9. Implementation Plan	18
2.10. Service Management	19
2.11. Outage and Maintenance Management	20
2.12. Financial Recompense Model	20
2.13. Customer Responsibilities	20
2.14. Technical Requirements and Client-Side Requirements	21
2.15. Outcomes and Deliverables	23
2.16. Development Life Cycle	25
2.17. After-sales Account Management	25
2.18. Termination Process – Needs Work	26
2.19. Our Experience	26
2.20. Contact details	27

1. About Vorboss

1.1. Company overview

Vorboss Limited is a London-based telecoms provider building a dedicated, business-only full-fibre network designed to meet the performance and reliability needs of modern organisations. Vorboss delivers 10 Gbit/s connectivity as standard, with bandwidth scalability up to 100 Gbit/s for customers requiring higher capacity to support cloud adoption, data-intensive workloads, multi-site operations, and business-critical services.

Owned by Fern Trading (managed by Octopus Investments), Vorboss works with both enterprise and SME customers, providing secure, scalable connectivity and supporting services that help organisations modernise and simplify their IT and network estates. Alongside fibre connectivity, Vorboss offers UK-wide delivery of managed IT, cybersecurity, and network services through Vorboss Managed Services and related business units. This enables customers to procure connectivity and operational support through a single supplier, with services that can be tailored from standalone components to fully managed solutions.

Vorboss' approach is focused on business outcomes: high-capacity connectivity, operational resilience, and security-led service delivery aligned to customer requirements.

1.2. Value Proposition

Public sector organisations require reliable, secure and resilient IT services to maintain productivity and continuity of service delivery. Many organisations face increasing demand from users, limited internal IT capacity, inconsistent device and application configurations, and growing cyber risk across users and endpoints. These challenges can lead to reduced service availability, slower response to IT incidents, inefficient onboarding and user support processes, and limited visibility of operational risk.

Vorboss IT Managed Service provides structured operational IT management designed to reduce disruption, improve reliability and provide consistent support outcomes. The service combines responsive IT service desk delivery with optional proactive monitoring, device maintenance and management, and tier-aligned security tooling. This supports buyers in maintaining stable IT operations while enabling IT teams and stakeholders to focus on strategic priorities rather than reactive workload.

The service supports public sector buyers to:

- Improve user experience and workforce productivity through consistent support and faster issue resolution
- Reduce downtime and minimise disruption through proactive monitoring and preventative maintenance (where applicable)
- Improve visibility of IT performance and recurring issues through structured ticketing processes and operational reporting

- Strengthen IT hygiene and cyber resilience through managed endpoint tooling and security controls aligned to service tier
- Support onboarding and organisational change by providing repeatable support processes and scalable service capacity
- Provide predictable and measurable service outcomes through defined service levels and prioritisation aligned to operational needs

By delivering IT support and operational management through a single managed service, Vorboss helps buyers standardise IT processes, improve consistency across users and devices, and strengthen operational resilience in a controlled and cost-effective manner.

1.3. What the Service Provides

Vorboss provides a managed IT service delivered by a UK-based team. The service supports buyers by providing consistent operational processes for end-user support, incident management, and service oversight, helping organisations maintain reliable day-to-day IT operations and reduce disruption to business-critical activity.

The service is designed to support organisations where internal IT capacity is limited or where consistent service levels, repeatable processes, and operational visibility are required. Support is delivered through structured workflows, prioritisation rules, and service reporting, enabling buyers to maintain control of IT operations while ensuring end users receive timely support.

The service includes:

- **IT support for end users via portal/telephone/email**
Support for day-to-day issues raised by users, including guidance, troubleshooting and resolution through defined support routes.
- **Ticket-based incident and request handling**
Incidents and service requests are logged, tracked and managed through a structured ticketing process. This provides visibility of progress, auditability of actions taken, and support performance tracking.
- **Troubleshooting and issue resolution for common workplace IT issues**
Support for common workplace and productivity issues affecting endpoints, user access, applications and connectivity (where within agreed scope), including escalation where required.
- **Defined response and resolution targets based on severity (P1/P2/P3)**
Support delivery is aligned to service level targets based on incident priority, enabling buyers to manage critical incidents with appropriate urgency while maintaining predictable handling for lower-severity issues.
- **Optional onsite support (Tiers: Standard and Advanced)**
Where required, onsite support can be requested to resolve issues that cannot be completed remotely or where a physical presence is operationally necessary.

- **Proactive monitoring and device management (Tiers: Standard and Advanced)**
Where included within tier selection, proactive services support the ongoing health and stability of devices through monitoring, preventative maintenance, patching, and device management controls designed to reduce recurring incidents.
- **Optional security tooling aligned to tier selection**
Security capabilities vary by tier and may include antivirus/endpoint protection, enhanced email security controls, and managed detection and response tooling, supporting improved IT hygiene and cyber resilience.
- **Service performance reporting and operational review (where applicable)**
Operational reporting can be provided to support visibility of service performance, incident volumes and trends, and recurring issues. Review cadence and reporting format can be agreed during onboarding and documented within the Order Form.

Overall, Vorboss IT Managed Service enables buyers to maintain consistent IT operations through a scalable support model, improved operational oversight, and service levels aligned to organisational needs.

1.4. Social Value

As part of delivering this service, Vorboss is committed to delivering meaningful social value outcomes aligned to the Public Services (Social Value) Act 2012. We take a long-term, responsible approach to service delivery that prioritises positive impact for people, communities, and customers – through fair work, inclusive employment practices, skills development, and a supportive workplace culture that enables individuals to thrive.

Vorboss is committed to creating and retaining high-quality jobs that are secure, supportive, and built for long-term progression, with a clear focus on widening access for people who may face barriers to entering the industry, such as those from disadvantaged backgrounds. Through our purpose built, in-house Vorboss Academy, we train technicians from scratch and provide a direct route into a high-growth, skills-shortage sector for individuals who may not have traditional entry pathways. Our approach combines ongoing training and mentoring with funded development budgets and structured secondments, giving colleagues meaningful opportunities to build experience, broaden their skills, and progress into more advanced roles over time.

We are deliberate in removing barriers and improving representation for under-represented groups, including women and ethnic minorities, through inclusive recruitment practices such as gender-neutral job adverts, unconscious bias training, and diverse interview panels. Alongside this, we support retention by investing in the everyday success of our people, ensuring they have the stability, development opportunities, and flexibility needed to thrive – helping us build a resilient workforce and deliver consistently high service standards for customers.

2.G-Cloud Service

2.1. Overview

Vorboss IT Managed Service provides structured IT operational delivery suitable for public sector environments where controlled processes, consistent support performance, and service oversight are required. The service is designed to support the ongoing operation of workplace IT and core user services through a managed service model, providing predictable support outcomes and operational visibility.

The service is delivered through defined service management processes, supported by service tooling and service performance targets. Buyers can select an appropriate service tier (Core, Standard or Advanced) based on operational requirements, support coverage expectations, and desired levels of proactive management and security controls.

Key capabilities include:

- **End-user IT support and ticket-based incident management**
Day-to-day IT issues and service requests are logged and managed through a structured ticket-based workflow. This provides traceability of actions taken, consistent prioritisation and escalation, and a repeatable approach to issue resolution.
- **Defined service levels and response targets**
Incidents are handled according to severity (P1/P2/P3) with response and resolution targets aligned to the selected tier. This supports predictable operational performance and prioritisation of service-impacting issues.
- **Optional proactive monitoring and device management**
Where included, the service provides proactive maintenance and monitoring of managed endpoints to improve device stability, reduce repeat issues, and support better operational performance over time.
- **Optional security tooling aligned to tier selection**
Security capabilities are tier-dependent and may include endpoint protection, enhanced email security controls, and managed detection and response tooling. These services support improved IT hygiene and resilience against common cyber threats.
- **Operational support for applications and licensing environments**
Vorboss provides high-level operational support for common workplace applications and licensing environments, helping to ensure users can access the tools they require and supporting visibility of licensing and entitlement issues.
- **Optional backup and storage support depending on scope and tier**
Where included, Vorboss supports operational requirements relating to storage and backup tooling (e.g., Microsoft 365 backup capabilities via Axcient on applicable tiers), ensuring requests and restoration activity can be tracked through service processes.

2.2. Service Tiers and Service Levels

Service Tier Comparison Table (Core / Standard / Advanced)

Category	Core	Standard	Advanced
Scope Range	Solve issues reported by users via telephone or email (PC and MS Apps only)	Solve issues reported by users via telephone or email + proactive device maintenance, monitoring and management	Solve issues reported by users via telephone or email + proactive device maintenance, monitoring and management
Support Levels	Remote only. Unlimited tickets.	Remote as standard. Onsite on request. Unlimited tickets.	Remote as standard. Onsite on request. Unlimited tickets.
Coverage Hours	8am–6pm	8am–6pm	Proactive hours 8am–6pm + PI reactive 24x7x365
Security Level	None	Webroot AV + Microsoft Defender	Microsoft MDR & XDR
Device Management / Patching / Reporting	None	ConnectWise	ConnectWise Microsoft Intune
Email Security	None	Defender	Defender P2
M365 Backup	None	Axcient	Axcient
Target Response (P1)	60 mins	30 mins	30 mins
Target Response (P2)	4 hours	2 hours	2 hours
Target Response (P3)	8 hours	8 hours	8 hours
Pricing Structure	Per user monthly contract	Per user monthly contract (min. 12 months)	Per user monthly contract (min. 12 months)

Support Medians	Phone/Email	Phone/Email/Portal	Phone/Email/Portal
-----------------	-------------	--------------------	--------------------

Note: Severity definitions, escalation routes and operational reporting can be agreed with the buyer prior to service commencement and confirmed within the Order Form.

2.3. Service Components

2.3.1. IT Service Desk (Incident Management and End User Support)

The IT Service Desk provides day-to-day user support through a structured, ticket-based support model. It is designed to help buyers maintain operational continuity by resolving end-user issues efficiently and consistently, while providing visibility of service performance and incident trends.

Support is delivered through defined communication routes and prioritisation processes. Incidents and service requests are handled in line with agreed service levels and may include troubleshooting, escalation and coordination with third parties where required and agreed.

The IT Service Desk includes:

- Incident logging via Portal/telephone and email**
 Users raise issues through agreed contact channels, with incidents recorded and tracked through the service desk process.
- Ticket creation, categorisation and prioritisation**
 Each issue is categorised and prioritised based on severity (P1/P2/P3) to ensure appropriate response handling and timely resolution.
- Troubleshooting, remote resolution and user guidance**
 Support includes diagnosis, troubleshooting and remediation of common workplace IT issues, including advice and guidance to enable users to return to normal working.
- Escalation aligned to severity**
 Where incidents require additional input, escalation routes are followed in line with priority requirements and service scope. Escalation may include specialist resources or onsite support (where included/requested).
- Progress updates and resolution confirmation**
 Users receive updates throughout the lifecycle of the ticket. Tickets are closed following confirmation that the issue has been resolved, or the request has been completed.
- Support for onboarding and leaver / mover activities (where agreed)**
 Where within scope, support can include operational tasks required to support organisational change such as device onboarding steps and user access guidance.
- Service visibility and management insight (where applicable)**
 Buyers may receive visibility through service reporting, including ticket volumes, response performance, common issue categories and recurring incidents.

2.3.2. Applications and Licensing Support (Operational Management)

Vorboss provides operational support for common workplace applications and licensing environments. This supports IT consistency and reduces the administrative burden on internal teams by helping ensure users have appropriate access to required software and services.

Applications and licensing support is intended to be delivered as part of operational IT management and is aligned to the buyer's defined scope and service tier.

This may include:

- **Microsoft workplace applications (in scope)**
Support for commonly used Microsoft tools and services such as email, productivity applications and collaboration tools, including troubleshooting access and functional issues.
- **Patching**
Critical and Security OS Patching (included Standard/Advanced Tiers). Additional patching is available on request.
- **Teams telephony operational support (where enabled)**
Support for Teams voice services where implemented, such as:
 - user enablement checks
 - telephony access troubleshooting
 - incident handling and escalation support (where required)
- **Licensing oversight and administration support**
Operational support for licensing environments, including:
 - access and entitlement troubleshooting
 - user licensing checks (where applicable)
 - supporting visibility of assigned vs required licences
 - reducing delays caused by licence allocation and access issues
- **Licensing environments may include:**
 - Microsoft
 - Google
 - Adobe
- **Support for server-connected applications (where required and agreed)**
Where buyers operate server-based workloads or applications, Vorboss can provide support aligned to the agreed scope, including troubleshooting and operational coordination where required.
- **Standardisation support (where applicable)**
Where appropriate, Vorboss can support consistent configuration and access practices by

promoting standard tooling and repeatable setup processes aligned to the buyer environment.

- **Storage, Backup and Hardware Support (Tiers Standard and Advanced, optional)**

Depending on the buyer's requirements and selected tier, Vorboss may provide operational support for storage, backup and hardware provisioning processes. These components are designed to improve resilience, ensure continuity, and support consistent endpoint availability.

Support may include:

Storage Services

Operational support for cloud-based storage and document platforms such as:

- SharePoint
- Azure

This may include user access troubleshooting, platform-related support queries, and operational coordination aligned to agreed scope.

- **Backup Tooling and Recovery Support (Tiers: Standard and Advanced, optional)**

Where included, Vorboss supports backup tooling and operational recovery processes, which may include:

- Veeam
- Axcient Cloud 360 (Office 365, G-suite) and X360 Recover (Server Backup) (and other agreed services where applicable)

Backup scope, restore expectations and retention requirements are agreed at onboarding and documented in the Order Form.

- **Hardware Provisioning and Coordination (where applicable)**

Vorboss can provide support for hardware-related operational tasks, including:

- Device provisioning coordination (where applicable)
- Replacement device workflow support
- Onboarding support for new devices (where agreed)
- Sourcing through approved distribution channels such as Westcoast Distribution

This supports buyers by maintaining device availability and reducing delays caused by unsupported or unmanaged hardware processes.

Scope statement:

The specific storage, backup and hardware components included are agreed during onboarding and documented within the Order Form.

2.3.3 Network Management (Operational Management – where applicable)

Depending on the buyer's requirements and selected service tier, Vorboss may provide operational support for core network services and network-connected infrastructure. This component is designed to help maintain reliable connectivity, support secure network operations, and reduce disruption caused by network faults, configuration issues, or device failures.

Network Management is delivered in line with agreed scope and may include operational coordination, troubleshooting, configuration support, and incident handling for in-scope network devices and services.

Support may include:

- **Firewall Management (where in scope)**

Operational support for firewall services, which may include:

- Monitoring and troubleshooting connectivity or security policy-related issues
- Configuration support and rule change requests (subject to approval and agreed governance)
- Incident response coordination for firewall-related outages or service degradation
- Support for logging and audit requirements where applicable

- **Router Management (where in scope)**

Support for routing services and edge connectivity, including:

- Troubleshooting WAN/LAN connectivity issues
- Configuration support aligned to buyer network design
- Incident handling and escalation for routing-related faults
- Coordination with carriers or third-party providers where applicable

- **Switching Management (where in scope)**

Support for internal network switching, including:

- VLAN configuration support (where agreed)
- Port configuration and troubleshooting
- Hardware fault identification and replacement coordination (where applicable)
- Support for network changes aligned to agreed maintenance windows

- **Wireless Access Point Support (where in scope)**

Support for access points and Wi-Fi services, including:

- Troubleshooting wireless connectivity, coverage and performance issues
- Support for configuration changes where agreed
- Escalation support for persistent wireless issues

- Coordination of access point replacement workflows where applicable

Scope statement:

Network Management scope (devices, sites, configuration responsibilities, change approvals and service boundaries) is agreed during onboarding and documented within the Order Form.

2.3.4 Licensing Requirements (Where Applicable)

Some service components require third-party tooling and licensing (e.g., Microsoft, Axcient Backup, ConnectWise). Vorboss can supply and manage these licences as part of transition into the managed service, or operate using buyer-provided licences where agreed. Final requirements are confirmed during onboarding and documented in the Order Form.

2.3.5 Service management and operational oversight

The service includes structured operational governance, including incident logging, prioritisation, escalation routes, and service reporting (where applicable). This supports buyers in maintaining oversight of service performance, recurring issues, and operational risk.

The scope of service delivery, tier selection, and any optional inclusions are confirmed during onboarding and documented in the Order Form.

2.4. Associated Services

2.4.1 Cloud and Digital Transformation

Vorboss provides cloud and digital transformation services as to support structured modernisation and controlled change delivery. This associated service is designed for organisations that need to introduce new cloud capabilities, improve the performance or security of existing environments, or complete planned IT change activity with reduced operational risk.

These activities are delivered as defined pieces of work with agreed scope, sequencing and governance, and can be used to support continuous improvement of the buyer's IT and cloud environment alongside the ongoing IT Managed Service.

This may include:

- **Microsoft 365 optimisation and hardening**
Configuration improvements to strengthen security, improve reliability, and support consistent operational outcomes across user services.
- **Modern workplace solutions**
Enablement and enhancement of cloud-based collaboration and productivity platforms to support hybrid working and consistent user experience.
- **M365 optimisation and security hardening**
Implementation of security-led configuration controls to reduce cyber risk, improve baseline protection, and align settings to buyer requirements.

- **Teams telephony and licensing management**
Support for planned enablement, configuration and rollout of Teams telephony functionality, alongside licence oversight and operational readiness.
- **Cloud and identity management**
Support for cloud identity configuration and management practices, including access control improvements and operational alignment for user access governance.
- **Private / hybrid Azure cloud solutions**
Support for Azure-based cloud infrastructure requirements, including hybrid environments where buyers require integration between on-premise and cloud services.

Pricing will be in accordance with the Vorboss Rate Card.

2.5. Pricing

Pricing is provided separately and is typically offered as a per-user monthly contract, with a minimum contract term of 12 months for Standard and Advanced service tiers.

Please refer to the Vorboss rate card/pricing for detailed pricing information.

2.6. Data protection

2.6.1. Informational Assurance

Vorboss follows structured processes to support secure and reliable service delivery, including controls for information security, operational quality, environmental responsibility, and cyber resilience. These processes are designed to support the secure handling of customer information, protect managed devices and user accounts, and ensure that service delivery activities are carried out in a controlled and auditable manner.

Information assurance practices may include:

- Controlled access to systems and administrative functions, aligned to role-based responsibilities
- Secure operational processes for delivering remote support and managing incidents
- Service governance and documentation to support traceability of support activity
- Risk-aware working practices aligned to security and compliance expectations
- Continuous improvement through review of service performance and recurring issues (where applicable)

Accreditations and Certifications include:

- ISO 9001 – Quality Management Systems, supporting consistent delivery and service improvement
- ISO 14001 – Environmental Management Systems, supporting responsible operational practices
- ISO 22301 – Business Continuity Management System
- ISO 27001 – Information Security Management Systems, supporting structured security controls and governance
- ISO 45001 – Occupational health and Safety Management Systems
- Cyber Essentials Plus – Independently tested cyber security controls to help protect against common cyber threats

2.6.2. Data Back-Up and Restoration (Of the service)

Vorboss maintains backup and restoration procedures to support continuity of service delivery and protect the operational data required to deliver the IT Managed Service. This ensures that, in the event of disruption, Vorboss can continue providing support services and restore access to key delivery systems in a controlled manner.

These procedures may include backup and recovery controls for service delivery components such as service desk systems, operational tooling configurations, service documentation, and reporting data (where applicable). Backup frequency, retention and restoration processes are reviewed and maintained as part of ongoing operational management.

Where the buyer's environment includes backup services within scope (for example Microsoft 365 backup via Axcient on applicable tiers), restoration activities for the buyer may be supported through the service desk process, with requirements confirmed during onboarding and documented within the Order Form.

2.6.3. Business Continuity Plan

Vorboss maintains continuity procedures designed to maintain service delivery in the event of disruption and to minimise the impact of unexpected incidents on operational support. These procedures are intended to ensure that IT Managed Service delivery remains available, prioritised appropriately, and coordinated through clear operational processes.

Business continuity procedures include:

- **Continuity of service desk operations**
Maintaining the ability to receive, log, prioritise and manage incidents and requests through agreed support channels, ensuring users can continue to access support during disruption.
- **Dependencies on support tooling and customer contact routes**
Identification and management of key service dependencies such as service desk tooling,

remote support methods, monitoring platforms (where applicable), and customer communication routes required to deliver support.

- **Prioritisation aligned to severity levels**
Applying severity definitions (P1/P2/P3) to ensure incidents affecting critical business services are handled with the appropriate urgency and escalation.
- **Operational measures to support service availability**
Measures designed to sustain service delivery, including clear escalation routes, defined responsibilities within the support team, and operational coordination to manage disruption and restore service as quickly as possible.
- **Communication and coordination during disruption**
Supporting timely updates to buyer stakeholders (where applicable) and coordination of support activity to ensure issues are tracked through to resolution and outcomes are confirmed.
- **Recovery and stabilisation approach**
Structured handling to restore service, validate performance following recovery, and support early review of any recurring issues or follow-on actions required.

A more detailed plan can be provided to buyer on request.

2.6.4. Privacy by Design

- All Vorboss security products are designed with data segregation in mind.
- SIEM systems are deployed within the customer's tenant
- Monitoring platforms are provisioned for each customer and not shared
- All Vorboss staff are UK based and all Vorboss systems which process security data (SOAR, ITSM etc. are EEA/EU/UK based)

2.7. Using the service

Buyers can order Vorboss IT Managed Service through the G-Cloud 15 framework using the standard Call-off Contract process. Ordering is completed using an Order Form to confirm the scope of service, selected tier, user volumes, and any service-specific requirements.

Ordering steps:

- **Step 1 – Buyer enquiry and requirements confirmation**
The buyer contacts Vorboss to outline requirements, including desired service tier, expected user volumes, and any specific operational or compliance requirements.
- **Step 2 – Scope and service tier agreement**
Vorboss confirms the agreed scope of service delivery, including support boundaries and the selected tier (Core / Standard / Advanced).

- **Step 3 – Completion of the G-Cloud Order Form (Call-off Contract)**
Vorboss supports the buyer in completing the Order Form, which forms the basis of the Call-off Contract and documents agreed service scope, service levels, onboarding requirements, and reporting expectations (where applicable).
- **Step 4 – Onboarding and service commencement**
Following contract award and confirmation of the Order Form, Vorboss completes onboarding activities and begins service delivery on the agreed start date.

Invoicing:

- Charges are applied in line with the pricing structure agreed within the Order Form and relevant rate card/pricing.
- Invoices are issued on an agreed schedule (typically monthly) and reflect the contracted service tier and user volumes.
- Where applicable, invoicing adjustments for changes in user numbers or scope are managed in accordance with the Order Form and agreed contract terms.
- Buyers receive invoices with sufficient reference information to support internal purchase order and approval processes.

Ordering Contact Email: *Supplier@Vorboss.com*

Availability of Trial Service

Trial services may be offered at Vorboss' discretion depending on scope and buyer requirements.

2.8. On-Boarding, Off-Boarding, Service Migration and Scope

Vorboss supports buyers through a structured onboarding and service mobilisation process to ensure the IT Managed Service can be delivered effectively from the start. Offboarding is managed in a controlled way to support a smooth transition at the end of the contract or where services change over time. The onboarding and offboarding approach are designed to minimise disruption, confirm service boundaries, and establish clear operational processes and governance.

2.8.1. Onboarding

Onboarding typically includes:

- **Kick-off meeting and scope confirmation**
Confirming the selected service tier, user volumes, in-scope services, operational priorities, governance contacts, and any service constraints or dependencies.

- **Setup of support routes and ticketing workflow**

Establishing how users contact the service desk (telephone/email), confirming ticket handling processes, and ensuring users understand how to log incidents and requests.

- **Agreement of escalation routes and reporting cadence**

Agreeing who key contacts are, how escalations are handled for priority incidents, and what level of reporting is required (where applicable).

- **User and device onboarding guidance (where applicable)**

Supporting the onboarding of users/devices into agreed processes and tooling, including onboarding guidance for new starters and devices where included within scope.

- **Access and permissions confirmation (where required)**

Confirming any required access approvals, delegated admin permissions, or tooling requirements needed to deliver the service securely and efficiently.

2.8.2. Service Migration (where applicable)

Where the buyer is transitioning from an existing provider or internal process, Vorboss can support a controlled migration approach. This may include confirming existing support processes, validating current in-scope services and tooling, and establishing continuity for user support during transition. Pricing will be in accordance with the Vorboss Rate Card

2.8.3. Offboarding

Offboarding typically includes:

- **Notice of termination in line with contract**

Confirming termination notice in accordance with contractual terms and agreed timelines.

- **Exit planning and timeframe agreement**

Working with the buyer to agree an exit approach and timeline, including any key dependencies or transition requirements.

- **Removal of access following service end date**

Ensuring Vorboss access to buyer systems and service tooling is removed in a controlled and secure manner following contract end (in line with agreed scope).

- **Transition support where required**

Supporting a handover to alternative arrangements where applicable, including knowledge transfer and operational coordination during the agreed exit period.

2.8.4. Training

Training includes service orientation, support routes, and severity understanding to ensure users and stakeholders can engage with the service effectively from day one. This typically covers:

- How to contact the service desk (telephone/email) and what information to provide when raising a request or incident

- Understanding ticket priorities (P1/P2/P3) and how severity impacts response and resolution handling
- Guidance on common user support scenarios, including basic troubleshooting steps and service expectations
- Introduction to escalation routes and key service contacts (where applicable)
- Onboarding guidance for new users and devices (where included within scope)

Additional training can be provided depending on scope and buyer requirements, including tailored sessions for admin users or key stakeholders. Training approach and delivery method can be agreed during onboarding and documented within the Order Form. Pricing will be in accordance with the Vorboss Rate Card

2.9. Implementation Plan

A detailed implementation plan can be provided to the buyer on request, however, a High-Level Plan (indicative) may include the following:

Milestone	Phase	Objective	Typical Activities (High-Level)
1	Service Kick-off & Scope Confirmation	Confirm service scope and mobilisation requirements	Confirm selected tier (Core/Standard/Advanced), user volumes, in-scope services, escalation routes, governance contacts, reporting expectations, and any operational constraints.
2	Access & Tooling Enablement	Establish service access routes and enable delivery tooling	Configure service desk access and contact routes, confirm required admin permissions, enable monitoring/security tooling (where included), and validate secure access methods for support delivery.
3	Asset Discovery & CMDB Baseline <i>(where applicable)</i>	Establish visibility of the IT estate to support delivery	Create an initial inventory of managed devices, establish baseline asset records/CMDB entries, capture key attributes (device owner, type, status), and confirm the approach to ongoing asset updates.

4	User & Device Onboarding	Bring users/devices into support and management workflows	Onboard users into support processes, validate supported endpoints, align device configurations where required, enable endpoint management/patching controls (Standard/Advanced), and confirm onboarding approach for starters/movers/leavers.
5	Service Go-Live	Start operational delivery against service levels	Activate support operations, begin ticket-based incident/request handling, confirm service level tracking, and establish escalation pathways for priority incidents.
6	Stabilisation & Early Life Support	Embed service delivery and identify early improvements	Review early incident trends, confirm recurring issues and quick wins, validate service performance against SLAs, and agree any priority remediation or improvement actions with the buyer.

2.10. Service Management

Vorboss delivers IT Managed Service using structured service management processes aligned to the principles of the ITIL framework. This supports consistent handling of incidents and requests, clear prioritisation and escalation, improved service visibility, and an approach to continual service improvement. ITIL alignment supports buyers by ensuring the service operates through defined workflows and repeatable processes that provide auditability, operational control, and service performance oversight.

In addition, Vorboss provides operational reporting (where applicable) to support service governance and transparency. Reporting helps buyers understand service performance, recurring issues, and areas for improvement over time.

Key ITIL-aligned practices include:

- Incident Management – restoring service operation as quickly as possible
- Service Request Management – handling standard user requests in a controlled and repeatable way
- Problem Management (where applicable) – reducing recurring issues by identifying root causes and preventative actions
- Change Enablement / Change Management (where applicable) – supporting controlled implementation of planned changes

- Knowledge Management – maintaining consistent guidance and resolution approaches
- Service Reporting (where applicable) – providing visibility of ticket volumes, SLA performance, incident trends, and recurring issues to support governance and oversight
- Continual Improvement – using operational reporting and trend analysis to improve service performance and reduce repeat incidents over time

2.11. Outage and Maintenance Management

Vorboss supports service continuity through proactive monitoring (where included), preventative maintenance, issue trend analysis, and planned communications where required.

Unplanned service interruptions are captured through Incident Management, ensuring outages are formally logged, prioritised appropriately (P1/P2/P3), and managed through to resolution. Where applicable, incidents are used to support service visibility by capturing key information such as service impact, time to restore service, and recorded downtime for operational reporting and review.

Planned maintenance activities and service changes are managed in a controlled way (where applicable) to reduce operational risk. This includes selecting appropriate maintenance windows to minimise disruption, communicating planned impact to relevant stakeholders where required, and validating service performance once changes are completed.

Where repeat issues or patterns are identified, Vorboss can use trend analysis to support continual improvement and help reduce recurrence of service disruption over time.

2.12. Financial Recompense Model

Service credits may be available depending on contract terms and documented within the Order Form.

2.13. Customer Responsibilities

To help the service run effectively, the customer plays an important role in keeping information accurate, ensuring requests enter the service through the agreed routes, and maintaining appropriate oversight of access and operational decisions. Clear responsibilities help incidents get resolved faster, reduce delays caused by missing approvals or incomplete information, and support consistent governance across users and devices.

Customers are expected to:

- **Maintain accurate user and device records**
Provide up-to-date information on users, devices, and key contacts, including changes relating to new starters, leavers, role moves, and device replacements.

- **Use the agreed support channels**

Ensure incidents and service requests are raised through the agreed routes (Portal/telephone/email) so they can be logged, prioritised, tracked and reported appropriately.

- **Provide appropriate internal contacts and escalation points**

Nominate suitable operational contacts (and escalation contacts where required) to support service coordination, decision-making and communication during priority incidents.

- **Approve access and permissions where required**

Provide timely approvals for administrative access, account permissions, or security-related changes needed to resolve incidents securely and deliver agreed service activities.

- **Support onboarding and offboarding activities**

Ensure internal processes are in place for onboarding/offboarding, including device allocation updates, access removal requirements, and confirmation of leaver dates.

- **Communicate business-critical services and priorities**

Inform Vorboss of key systems, operational constraints, or critical service periods that may affect prioritisation, planned maintenance windows, or escalation routes.

- **Coordinate third-party supplier relationships where applicable**

Where services rely on third-party suppliers (e.g., external application vendors or connectivity providers), support coordination where required to enable end-to-end incident resolution.

- **Maintain internal governance and decision-making**

Retain ownership of business decisions relating to policy, access permissions, and service scope, including approvals for any changes that may introduce operational or security risk.

- **Support security and compliance requirements**

Where relevant, ensure internal compliance requirements (e.g., mandated policy controls or approval routes) are communicated so service delivery can align with organisational obligations.

- **Engage in service review and continuous improvement (where applicable)**

Participate in agreed operational review cycles to discuss service performance, recurring issues and improvement opportunities, ensuring the service remains aligned to changing needs.

2.14. Technical Requirements and Client-Side Requirements

Vorboss delivers the IT Managed Service primarily through remote support and (where included) monitoring, endpoint management, security tooling and reporting. To enable secure and efficient service delivery, buyers must ensure that devices, connectivity and access arrangements meet baseline requirements. Any additional or organisation-specific requirements are confirmed during onboarding and documented within the Order Form.

Typical technical and client-side requirements include:

Endpoint Devices and Operating Environment

- Supported endpoint devices (PCs), suitable for remote support and management
- Operating systems in a supported state (including regular updates where applicable)
- Devices available for onboarding into monitoring, patching or management tooling (where included in tier)
- Local device access provided by users where required to complete troubleshooting (e.g., rebooting or confirming outcomes)

Connectivity and Remote Support Enablement

- Reliable internet/network connectivity to enable remote troubleshooting and secure remote sessions
- Network routes available for required service tooling connectivity (where applicable)
- Ability to support remote access and remote assistance workflows in line with organisational policy

Applications and Services in Scope

- Microsoft workplace applications and services included within scope (as agreed in the Order Form)
- Access to required productivity platforms (e.g., Microsoft 365 tenant access where agreed and required for support)
- Where Teams telephony support is included, required configuration access and user enablement details

Access, Permissions and Approvals

- Appropriate permissions granted to enable incident resolution and service delivery
- Administrative access or delegated permissions where required to support device management, patching, security configuration or reporting (where included)
- Timely customer approvals for any activities requiring elevated access or change implementation

Security Tooling and Device Management

Where included within the selected tier, requirements may include the ability to deploy and operate:

- Endpoint protection/antivirus tooling
- Email security controls
- Device monitoring and patching tools
- Endpoint management platforms (e.g., Intune where applicable)

Identity and Account Requirements

- User account and identity details provided for onboarding/offboarding and support delivery
- Access to identity management platforms (where required and agreed) for troubleshooting authentication and access issues
- Multi-factor authentication (MFA) and access policy requirements communicated to Vorboss where relevant

Third-Party Dependencies (where applicable)

- Where the buyer uses third-party suppliers (e.g., hosted applications or external IT providers), coordination or access may be required to support end-to-end resolution
- Buyer support to facilitate third-party engagement where contractual ownership sits with the buyer

Information Provided During Onboarding

To support smooth mobilisation, buyers may be required to provide:

- User lists and key contacts
- Device inventory (where applicable)
- Operational priorities and escalation contacts
- Any restrictions or policies that affect remote access, tooling, or support processes

2.15. Outcomes and Deliverables

Vorboss IT Managed Service is designed to provide practical operational outcomes that support continuity, workforce productivity, and consistent IT service delivery. Deliverables focus on maintaining stable day-to-day IT operations, improving service visibility, and reducing disruption through structured processes, tier-aligned capabilities, and repeatable service management.

Deliverables and outcomes typically include:

Operational Service Delivery

- **End-user incident resolution through a managed service desk model**
Incidents and service requests are logged, tracked and managed through structured processes, ensuring consistent delivery and prioritisation.
- **Consistent support experience across users and locations**
Users receive access to a defined support route (telephone/email) and predictable handling based on severity.

- **Priority-based handling for business-impacting incidents**
Support is delivered against agreed service levels (P1/P2/P3), ensuring the right urgency is applied based on operational impact.

Reduced Downtime and Improved Continuity

- **Reduced operational disruption**
Faster incident handling, structured escalation, and proactive services (where included) support continuity and help reduce productivity loss.
- **Improved service stability over time**
Issue trend analysis and preventative activity (where included) help reduce repeat incidents and recurring disruptions.

Device Reliability and IT Hygiene (Tier Dependent)

- **Improved device health and reliability (Standard/Advanced)**
Where included, proactive monitoring, device management and patching help maintain endpoint stability and reduce avoidable issues.
- **More consistent device configuration and supportability**
Standardised support processes help maintain greater consistency across the managed IT estate.

Security and Resilience Improvements (Tier Dependent)

- **Improved security posture aligned to tier selection**
Depending on tier, deliverables may include endpoint protection, enhanced email security and managed security capabilities that support improved cyber resilience.
- **Stronger operational control over common risks**
Structured access handling, monitoring, and proactive controls (where included) help reduce exposure to common cyber threats.

Service Visibility, Reporting and Governance

- **Operational reporting and performance visibility (where applicable)**
Buyers may receive reporting to support oversight of ticket volumes, recurring issues, response performance, and operational trends.
- **Improved auditability and traceability of support activity**
Ticket-based handling supports transparency by capturing actions taken, timelines, and resolution outcomes.

Support for Organisational Change

- **Scalable service delivery through growth or change**
The service supports onboarding/offboarding workflows and adapts to changes in user volumes and operational requirements.

- **Improved consistency during business change**

A managed service approach helps buyers maintain support and stability during growth, restructuring, or technology refresh activity.

2.16. Development Life Cycle

This service is delivered as an operational managed service rather than bespoke software development. Service improvements may be delivered through continuous service improvement practices.

2.17. After-sales Account Management

Following service go-live, Vorboss provides ongoing account management to support operational governance and continual service improvement. This includes structured service reviews and a Customer Service Improvement Plan (CSIP)–aligned approach to monitoring performance, identifying recurring issues, and agreeing improvement actions with the buyer.

Ongoing account management supports:

- **Regular service performance reviews**

Review of service activity, ticket volumes, and service level performance to ensure the service continues to meet operational requirements.

- **Recurring issue and trend analysis (Problem-focused review)**

Identification of recurring incidents and common failure points, helping to reduce repeat disruption through targeted improvements and preventative actions (where applicable).

- **CSIP-style improvement actions**

Agreed improvement actions documented and tracked through to completion, focusing on stabilisation, service quality improvements, and operational efficiency.

- **Change and maintenance review (where applicable)**

Review of planned changes, maintenance activity, and any service impact to ensure changes are delivered in a controlled manner and lessons learned are captured.

- **Scope and tier alignment over time**

Regular validation that scope, service tier, and included tooling remain appropriate as organisational requirements, user volumes, and operational priorities change.

- **Service governance and stakeholder engagement**

Clear buyer points of contact, escalation routes, and governance processes to support communication and timely decision-making during service delivery.

2.18. Termination Process – Needs Work

Termination is managed in line with Contract terms:

- Per-user contract basis
- Minimum Initial Period: 12 months (Standard/Advanced)
- Early termination in accordance with terms of the Contract

2.19. Our Experience



Leading health company revolutionising early disease detection partnering with the NHS, private healthcare providers and life science companies to deliver improved diagnostic services.

Highly regulated sector and continually audited, Vorboss (Optimity) leads their information security management system (ISMS) and is responsible for the scope, planning, execution, remediation of audits and mitigation of risk within the ISO 27001:2022 Standard.

Vorboss (Optimity) has a 24-month contract providing a close technical partnership with the executive management team as well as the software engineering department, laboratory and HQ infrastructure, providing enterprise machine management, device protection and full-service desk & support services.

Currently generating over £11K MRR, with growth anticipated following clinical trials.

“As a rapidly expanding biotech company we identified the need to bring on an IT support partner in a quick turnaround. Vorboss (Optimity) was adaptable and able to provide support services with little notice, filling identified gaps and onboarding at speed. Once onboard Vorboss (Optimity) conducted a detailed analysis of our organisational systems with a highly pragmatic approach and understanding of our requirements as a business.

Over the past couple of years Vorboss (Optimity) has become a trusted IT management partner helping us work towards cyber compliance in a heavily regulated sector. They have embedded themselves into our business well and provide an extremely personable approach with the team; this has enabled them to tackle complex obstacles dealing with legacy systems as well as tailoring their systems to support our unique operational needs.”

Head of People, Cyted



Global design and brand strategy agency with clients including Meta, Google, Amazon & Coca-Cola. Entire technology footprint of five international studio's outsourced to Vorboss (Optimity) to include management of infrastructure, service desk & dedicated support. It also includes the management and execution of Koto's information security & data governance function.

Vorboss (Optimity's) introduction of enterprise machine management and endpoint device protection across a geographically diverse, unregulated estate has allowed the business to expand safely but allows staff the freedom of access required.

Vorboss (Optimity) have a new two-year contract (originally signed in 2022 and re-awarded in January 2024)

Currently generating over £20K MRR.

"We have been working with Vorboss (Optimity) for nearly three years. Over this time, they have truly understood our business and have offered insight into improving our internal processes as well as introducing major technical change and deep technical support. Our brief has been extensive - including the design of our new network infrastructure (2023), creating an information security roadmap & the introduction of endpoint management & protection of all our devices. They have been able to tackle challenges as well as tailoring their systems to support our unique operational needs. Their responsive support team is knowledgeable and flexible and have easily integrated into how we work as an organisation. Vorboss (Optimity) have carefully guided us towards achieving cyber compliance and providing us with ongoing technical peace of mind."

COO & Founder, Koto Studio

2.20. Contact details

For G-Cloud enquiries:

Toby Morgan-Grenville

Head of Public Sector

E: supplier@vorboss.com

T: +44 (0) 73 5037 1723