SERVICE 2
Infrastructure Monitoring & Management Services

Service Definition Document

G-Cloud15 Procurement Submission

testfyra

1. SERVICE OVERVIEW

TestFyra provides comprehensive infrastructure monitoring and management services for networks, servers, applications, and cloud environments. Our service delivers 24/7 visibility into your IT infrastructure health, performance, and availability through industry-leading monitoring platforms and expert operational support.

What We Do: We monitor your IT infrastructure continuously, detect issues before they impact users, and help you optimise performance. We provide real-time dashboards, intelligent alerting, log analysis, and proactive capacity planning.

Who It's For: Government agencies, healthcare providers, educational institutions, telecom operators, financial services, retail organisations, and any public sector body requiring reliable infrastructure monitoring and management.

Key Deliverables:

- 24/7 infrastructure monitoring and alerting
- Real-time dashboards and KPI tracking
- Monthly performance and capacity reports
- Incident management and escalation
- Log intelligence and analysis
- DHCP and IP address management (optional)

2. KEY FEATURES

2.1 Network Monitoring

- Device Monitoring: Routers, switches, firewalls, load balancers, wireless controllers
- Availability Tracking: Uptime monitoring with automatic ping and SNMP polling
- Bandwidth Monitoring: Real-time traffic analysis and capacity planning
- Interface Monitoring: Port status, errors, discards, and utilisation
- Network Mapping: Automatic topology discovery and visualisation
- Threshold Alerting: Customisable alerts for bandwidth, CPU, memory, and errors

2.2 Server Monitoring

- OS Monitoring: Windows, Linux, Unix server health and performance
- Resource Tracking: CPU, memory, disk, network utilisation
- Process Monitoring: Critical service and application process tracking
- Performance Metrics: Response times, throughput, queue lengths
- Windows Event Logs: Security, application, and system event monitoring
- Linux Syslog: Centralised log collection and analysis

2. KEY FEATURES (continued)

2.3 Application Monitoring

- Web Application: HTTP/HTTPS endpoint monitoring with response time tracking
- Database: SQL Server, MySQL, PostgreSQL, Oracle performance monitoring
- Middleware: Tomcat, IIS, Apache, Nginx monitoring
- API Monitoring: RESTful API availability and performance testing
- Synthetic Transactions: Simulated user journeys to detect issues
- Application Dependencies: Dependency mapping and impact analysis

2.4 Cloud Monitoring

- AWS: EC2, RDS, S3, CloudWatch integration
- Azure: Virtual Machines, SQL Database, Storage, Azure Monitor integration
- Google Cloud: Compute Engine, Cloud SQL, Cloud Storage monitoring
- Hybrid Cloud: Unified monitoring across on-premises and cloud
- Cost Monitoring: Cloud spend tracking and optimisation recommendations

2. KEY FEATURES (continued)

2.5 Log Management & Intelligence

- Log Collection: Centralised collection from servers, network devices, applications
- Log Parsing: Automatic extraction of key fields and metrics
- Log Analysis: Pattern detection, anomaly identification, trend analysis
- Search & Filter: Powerful search across millions of log entries
- Correlation: Cross-system event correlation for root cause analysis
- Compliance: Audit-ready log retention and reporting

2.6 DHCP & IP Management (Optional)

- DHCP Server Management: Configuration, monitoring, and failover
- IP Address Management: IP allocation, tracking, and conflict detection
- Subnet Planning: Capacity planning and subnet utilisation reporting
- DNS Integration: DNS record management and synchronisation

3. KEY BENEFITS

Prevent Outages Before They Happen

Proactive monitoring detects issues early, often before users are affected, reducing downtime by 60-80%.

Reduce MTTR by 50%

Intelligent alerting and automated diagnostics help your team resolve incidents faster.

Optimise Infrastructure Costs

Capacity planning and utilisation reporting identify underused resources, typically saving 15-25% on infrastructure spend.

Improve User Experience

Application performance monitoring ensures optimal response times and availability for end users.

testfyra

3. KEY BENEFITS (continued)

Simplify Multi-Vendor Management

Unified monitoring across vendors eliminates tool sprawl and provides single-pane-of-glass visibility.

Meet Compliance Requirements

Comprehensive audit trails, log retention, and reporting support compliance with ISO 27001, Cyber Essentials, and sector-specific regulations.

Free Up Internal Resources

Managed monitoring service reduces burden on internal IT teams, allowing them to focus on strategic projects.

Gain Actionable Insights

Monthly reports with trend analysis and recommendations help you plan infrastructure improvements.

testfyra

4. HOW THE SERVICE WORKS

Phase 1: Discovery & Assessment (1 week)

- Audit existing infrastructure and monitoring tools
- Identify monitoring requirements and priorities
- Define alerting thresholds and escalation procedures
- Document access requirements and firewall rules

Deliverable: Monitoring Requirements Document

Phase 2: Design & Planning (1 week)

- Design monitoring architecture and sensor placement
- Create monitoring groups and device hierarchies
- Define custom dashboards and reports
- Configure alert templates and notification rules

Deliverable: Monitoring Design Document

testfyra

4. HOW THE SERVICE WORKS (continued)

Phase 3: Implementation (2-4 weeks)

- Install and configure monitoring platform
- Deploy agents/sensors to monitored devices
- Configure SNMP, WMI, SSH access
- Set up log collection and parsing
- Create initial dashboards and alerts

Deliverable: Monitoring Platform Operational

Phase 4: Testing & Validation (1 week)

- Verify all devices are monitored correctly
- Test alert generation and notification
- Validate dashboard accuracy
- Conduct failover testing (if applicable)

Deliverable: Test Report and Sign-off

4. HOW THE SERVICE WORKS (continued)

Phase 5: Operational Service (Ongoing)

- 24/7 monitoring and alerting
- Incident response and escalation
- Weekly health checks and optimization
- Monthly reporting and reviews
- Quarterly service review meetings

Deliverable: Monthly Performance Reports

5. SERVICE LEVELS & SUPPORT

Service Availability

- Platform Availability: 99.9% uptime (measured monthly)
- Monitoring Coverage: 24/7/365 continuous monitoring
- Data Collection: Every 1-5 minutes (configurable per device)

Response Times (by Severity)

P1 - System Down Critical (Service Down): Initial Response: 2 Hrs

Escalation: Immediate to customer contacts

P2 –High (Degraded Service): Initial Response: 8 Hrs

Escalation: Within 2 hours if unresolved

Medium (Warning Threshold): Initial Response: 8-16 Hrs

Escalation: Within 4 hours if unresolved

Low (Informational): Initial Response: Next business day

Escalation: As needed

testfyra

5. SERVICE LEVELS & SUPPORT (continued)

Support Channels

- Email: support@testfyra.com
- Ticket Portal: JIRA Service Management
- Alert Notifications: Email

Reporting – As per Customer Requirement

- Real-Time: Live dashboards accessible 24/7
- Daily: Automated summary emails (optional)
- Weekly: Health check reports
- Monthly: Comprehensive performance analysis with trends and recommendations
- Quarterly: Service review meetings with strategic recommendations

Maintenance Windows

- Scheduled Maintenance: Quarterly
- Advance Notice: 7 days minimum
- Emergency Maintenance: As needed with 4-hour notice where possible

testfyra

6. TECHNICAL REQUIREMENTS

Customer Requirements

Network Access:

- SNMP v2c or v3 access to network devices
- WMI access to Windows servers
- SSH access to Linux/Unix servers
- API access to cloud platforms (AWS, Azure, GCP)

Firewall Rules:

- Inbound: HTTPS (443) for web interface access
- Outbound from monitored devices: SNMP trap (162), Syslog (514), HTTPS (443)
- VPN or dedicated connection for on-premises monitoring

Credentials:

- Read-only SNMP community strings or v3 credentials
- Service accounts for Windows (WMI) and Linux (SSH)
- Cloud platform API keys or service principal credentials

Prerequisites:

- Documented device inventory
- Network diagrams (if available)
- List of critical services and applications
- Existing alert thresholds (if any)

6. TECHNICAL REQUIREMENTS (continued)

TestFyra Infrastructure

Monitoring Platform:

- SolarWinds Network Performance Monitor (primary)
- SolarWinds Server & Application Monitor
- SolarWinds Log Analyser (optional add-on)
- Custom log management framework (optional)

Hosting:

- UK-based data centres (London and Manchester)
- ISO 27001 compliant facilities
- Redundant infrastructure with failover
- Encrypted data in transit (TLS 1.3) and at rest (AES-256)

Supported Technologies:

- Network Devices: Cisco, Juniper, HP/Aruba, Dell, Fortinet, Palo Alto
- Operating Systems: Windows Server 2012+, RHEL 7+, Ubuntu 18.04+, CentOS 7+
- Virtualisation: VMware vSphere, Microsoft Hyper-V, KVM
- Databases: SQL Server, MySQL, PostgreSQL, Oracle, MongoDB
- Cloud: AWS, Azure, Google Cloud Platform
- Protocols: SNMP v1/v2c/v3, WMI, SSH, Syslog, NetFlow, API

Data Collection Methods:

- Agentless: SNMP, WMI, SSH, API polling
- Agent-based: Optional for advanced application monitoring
- Flow Data: NetFlow, sFlow, IPFIX for traffic analysis
- Log Collection: Syslog, Windows Event Forwarding, API

7. SECURITY, COMPLIANCE & CONSTRAINTS

Security Measures

- Certifications: Cyber Essentials, ISO 27001 (in progress, expected Q2 2026)
- Data Encryption: TLS , AES-256 at rest
- Access Control: Multi-factor authentication, role-based access (RBAC)
- Credential Management: Encrypted credential storage, automatic rotation
- Audit Logging: Complete audit trail of all configuration changes
- Security Monitoring: Integration with SIEM for security event correlation

Compliance

- GDPR: UK GDPR and Data Protection Act 2018 compliant
- Data Residency: All monitoring data stored in UK data centres
- Audit Support: Audit-ready reports and log retention
- Sector Standards: NHS Data Security and Protection Toolkit, Cyber Essentials

Backup & Disaster Recovery

- Configuration Backup: Daily backup of all monitoring configurations
- Data Backup: Continuous replication to secondary site
- Retention: 30 days online, 13 months archive, 5 years cold storage
- RTO: 4 hours for complete platform recovery
- RPO: 5 minutes (maximum data loss)

7. SECURITY, COMPLIANCE & CONSTRAINTS (continued)

Service Constraints

Dependencies:

- Customer must provide network access (VPN or direct connection)
- Firewall rules must permit monitoring traffic
- Credentials with appropriate privileges required
- Some monitoring requires agent installation (application monitoring)

Limitations:

- Cannot monitor devices without SNMP, WMI, or SSH access
- Encrypted traffic cannot be inspected without SSL certificates
- High-volume log environments may incur additional storage costs
- Physical on-site work subject to location and security clearance

Excluded from Service:

- Infrastructure remediation (fixes are customer's responsibility)
- Change management and implementation
- Capacity upgrades (recommendations only)
- Security incident response (monitoring only)

testfyra

7. SECURITY, COMPLIANCE & CONSTRAINTS (continued)

Service Constraints

Lead Times:

- Standard implementation: 3-4 weeks from contract signature
- Simple deployments: 1-2 weeks
- Complex migrations: 6-8 weeks
- Emergency deployment: 1 week (subject to 15% premium)

Onboarding & Offboarding

Onboarding (3-4 weeks):

- Discovery workshop and requirement gathering
- Network access and credential provisioning
- Platform installation and configuration
- Device discovery and baseline monitoring
- Alert tuning and dashboard creation
- Team training (2-hour session)

Offboarding (30 days):

- Data extraction period for historical reports
- Configuration export and documentation handover
- Credential removal and access revocation
- Platform decommissioning
- Final performance report and recommendations

CONTACT INFORMATION - TESTFYRA LTD

Registered Office:

11 Dormer Place
Royal Leamington Spa
CV32 5AA
United Kingdom

General Enquiries:

Email: contact@testfyra.com
Phone: +44 7814 154655
Website: www.testfyra.com

Sales & Commercial:

Email: customer@testfyra.com,
gurjit.badesha@testfyra.com

Company Details:

Company Registration number – 08586825
VAT number - 165527005

This Service Definition Document should be read in conjunction with TestFyra's Terms & Conditions, SFIA Rate Card, and Pricing Document for complete service details.

Version Control: Version 1.0 - December 2025 - Initial G-Cloud 15 submission

END OF SERVICE DEFINITION