Crown Commercial Service *Supplier*

G-Cloud 15

Vulnerability Managed Service

Atos

Table of contents

Crown Commercial Service *Supplier*

Atos

1. What is the Vulnerability Managed Service?

Atos Vulnerability Management Service (VMS) is a comprehensive, proactive cybersecurity offering that provides continuous identification, assessment, prioritisation, and mitigation of vulnerabilities across an organisation's entire digital estate. Operating as a fully managed service delivered through Atos' global security operations centres, VMS combines advanced scanning technologies, expert security analysis, and systematic remediation processes to protect organisations from potential security threats before they can be exploited.

The service delivers enterprise-wide vulnerability management through a risk-based approach, addressing vulnerabilities across traditional IT infrastructure, cloud environments, web applications, and external attack surfaces. By leveraging both automated scanning capabilities and Atos security expertise, VMS transforms vulnerability data into actionable intelligence, enabling organisations to make informed decisions about their security investments and risk tolerance.

As a managed service, VMS operates 24x7 through security operations centres, providing continuous monitoring, regular assessment cycles, and rapid responses to emerging threats. The service integrates with existing IT service management and governance frameworks to ensure that vulnerabilities are not only identified but also effectively remediated within agreed service levels.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

Atos Vulnerability Managed Service is designed as a modular service platform, enabling organisations to select and implement components that align with their specific security requirements and risk profile. This flexible approach ensures customers invest only in capabilities they need while maintaining the ability to expand coverage as their security programme evolves. The service combines mandatory core components that provide foundational vulnerability management capabilities with optional modules that address specialised requirements such as web application security, cloud native protection, and compliance monitoring. Each component operates either independently or as part of an integrated vulnerability management ecosystem, enabling organisations to start with essential services and expand as demonstrated value and evolving requirements warrant.

Core Service Components

Service Core Production Support (Mandatory)

- 24x7 service desk and incident management
- Service performance monitoring and SLA management
- Regular service reviews and continuous improvement programmes
- Technical escalation and vendor management
- Service integration with the customer's existing ITSM and security tools.

Vulnerability Scanning Service (VSS) - Optional

- Authenticated and unauthenticated network vulnerability scanning
- Operating system and application vulnerability assessment
- Database and middleware security scanning
- Infrastructure device configuration assessment
- Virtual environment and hypervisor scanning
- Scheduled and on-demand scanning capabilities
- Asset discovery and inventory maintenance
- Compliance with customer security policies.

Web Application Scanning Service (WAS) - Optional

- Dynamic application security testing (DAST) based on discovered applications or provided URLs
- API security testing and assessment

- Authentication handling for complex applications
- Business logic vulnerability testing
- OWASP Top 10 vulnerability identification
- Application inventory and change detection.

Cloud Native Application Protection Platform (CNAPP) - Optional

- Cloud security posture management (CSPM) across multi-cloud environments
- Cloud workload protection and vulnerability assessment
- Infrastructure as Code (IaC) security scanning
- Container and Kubernetes security assessment
- Cloud compliance monitoring and reporting
- Cloud asset inventory and configuration management.

Policy Compliance Monitoring Service (PCM) - Optional

- Configuration baseline assessments against security standards
- Compliance monitoring for PCI-DSS, CIS benchmarks, NIST frameworks, and DISA STIGs
- Governance regulations compliance checking
- Reduction of security and compliance risk from misconfigured assets
- Custom policy creation and enforcement
- Automated compliance reporting and evidence collection
- Remediation Enablement Service (RES).

CYS Remediation Enablement Service Core (Mandatory)

- Data gathering and normalisation from multiple vulnerability sources
- Business risk evaluation and impact analysis
- Risk-based prioritisation of remediation activities
- Remediation workflow orchestration and tracking
- Work progress oversight
- Tactical and operational reporting for IT teams
- Strategic reporting for leadership.

Processing Options - Optional

- Manual Processing: Expert-led remediation planning and validation
- Semi-Automated Processing: Tool-assisted remediation workflows
- Integration with customer patch management systems
- Change advisory board (CAB) preparation and support
- Post-remediation validation and verification
- External Attack Surface Management (EASM) - Optional.

Attack Surface Management (ASM) - Mandatory when EASM is selected

- Web-based inventory tool for identifying internet-accessible assets
- Discovery using DNS records, IP addresses, and ASN
- Shadow IT identification for unknown assets
- Collection of over 180 metadata columns per asset
- Integration with the Tenable One Cloud platform for a consolidated view
- Organisation and inventory management capabilities.

Automated Security Testing (AST) - Mandatory when EASM is selected

- Continuous security testing of external-facing assets
- Port and service identification
- Technology stack fingerprinting
- Vulnerability validation and verification
- Exposure assessment of internet-facing infrastructure.

Exploit Intelligence (EI) - Optional

- Real-time threat intelligence integration
- Active exploit monitoring and alerting
- Ransomware campaign tracking
- Zero-day vulnerability intelligence
- Industry-specific threat briefings.

Service Benefits

Improved Security Posture

- Regular identification and addressing of vulnerabilities reduces the attack surface
- Proactive approach mitigates risk of security breaches and data compromises

- Strengthened overall security defences
- Continuous monitoring ensures new vulnerabilities are promptly identified.

Risk Reduction

- Prioritisation based on severity and potential impact
- Focus on the most critical risks first
- More effective resource allocation
- Reduced likelihood of successful attacks.

Compliance Adherence

- Demonstrates compliance with regulatory requirements and industry standards
- Avoids potential fines and penalties for non-compliance
- Automated compliance monitoring and reporting
- Audit-ready documentation.

Cost Savings

- Proactive vulnerability management prevents costly security breaches
- Avoids legal fees, regulatory fines, and reputational damage
- Early vulnerability identification requires less effort and cost than incident response
- Reduced operational overhead through automation.

Increased Operational Efficiency

- Automated scanning and assessment processes streamline vulnerability identification
- Reduced manual effort for security teams
- Focus on strategic initiatives rather than routine tasks
- Improved response time to emerging threats.

Enhanced Customer Trust

- Demonstrates commitment to security through proactive vulnerability management
- Transparent security posture reporting
- Protection of customer data and sensitive information
- Improved business reputation.

Continuous Improvement

- Ongoing monitoring, analysis, and feedback loops
- Learning from past vulnerabilities and security incidents
- Strengthened defences over time
- Adaptation to evolving threat landscape
- Reporting & Analytics.

Executive Reporting

- Risk dashboards with business context
- Compliance status reporting
- Security posture trends
- Mean-time-to-remediate metrics
- Board-level briefings.

Operational Reporting

- Vulnerability discovery reports
- Remediation progress tracking
- Asset inventory reports
- Technical vulnerability details
- SLA performance metrics.

Strategic Analytics

- Vulnerability trending analysis
- Root cause analysis
- Security programme maturity assessment
- Benchmark comparisons.

Crown Commercial Service *Supplier*

Atos

3. What technology does it use?

Atos VMS 3.0 is built on the Tenable vulnerability management platform, leveraging industry-leading scanning technology and threat intelligence to deliver comprehensive vulnerability detection and assessment capabilities. This partnership with Tenable ensures customers receive proven, continuously updated vulnerability detection while Atos adds value through service delivery, expert analysis, and remediation orchestration.

Core Vulnerability Management Platform

Tenable Technology Foundation

- Tenable One Cloud Platform: Consolidated platform for vulnerability data and attack surface management
- Tenable Vulnerability Management (Tenable.io): Cloud-based vulnerability assessment and management
- Tenable Nessus: Industry-leading vulnerability scanner with 130,000+ vulnerability and configuration checks
- Tenable Web App Scanning: Dynamic application security testing capabilities
- Tenable Attack Surface Management: External asset discovery and monitoring for the ASM component.

Tenable Platform Capabilities

- Continuous asset discovery and vulnerability assessment
- Risk-based vulnerability prioritisation with VPR (Vulnerability Priority Rating)
- Real-time threat intelligence from Tenable Research
- Cloud native architecture with global availability
- API-driven integration capabilities
- FedRAMP Moderate authorisation for government sectors.

Scanning Infrastructure

Tenable Nessus Scanners

- Physical and virtual scanner deployment options
- Agent-based scanning for continuous assessment
- Cloud scanners for AWS, Azure, and Google Cloud environments
- Network-based scanning for authenticated and unauthenticated assessments
- Credentialed scanning for deep configuration analysis.

Coverage Capabilities

- Operating systems (Windows, Linux, Unix, macOS)
- Network devices and infrastructure
- Databases and middleware platforms
- Web applications and APIs
- Virtual environments and containers
- Cloud workloads and configurations
- IoT and OT devices.

Integration Capabilities

Tenable.io API Integration

- RESTful API for data export and automation
- Vulnerability data export with chunked processing
- Asset synchronisation capabilities
- Scan scheduling and management
- Custom reporting and dashboard creation.

Service Management Integration

- ServiceNow integration for ticket creation
- ITSM platform connectivity via REST APIs
- Automated workflow triggers
- SLA tracking and reporting
- Change management integration.

Data Management & Analytics

Tenable Platform Features

- Vulnerability database with continuous updates
- CVSS v3.1 and v4 scoring support
- EPSS (Exploit Prediction Scoring System) integration
- Threat intelligence correlation
- Asset criticality scoring
- Attack path visualisation.

Reporting Capabilities

- Executive dashboards
- Compliance reporting (PCI-DSS, CIS, NIST)
- Vulnerability trending
- Remediation tracking
- Custom report generation.

Compliance & Standards

Supported Frameworks

- CIS Benchmarks
- NIST Cybersecurity Framework
- PCI-DSS requirements
- ISO 27001 controls
- DISA STIGs
- Vendor security baselines
- Custom policy templates.

Service Delivery Infrastructure

Atos Service Management Layer

- Service desk and incident management
- SLA monitoring and reporting
- Customer portal for report access
- Service review and improvement processes
- Technical escalation procedures.

Security Operations Centres

- 24x7 monitoring and response
- Global delivery locations
- Follow-the-sun support model
- Expert vulnerability analysts
- Remediation specialists.

Performance Specifications

- Scanning Performance
- Support for enterprise-scale deployments
- Parallel scanning capabilities
- Scheduled and on-demand scanning
- Minimal network impact scanning options
- Agent-based continuous monitoring.

Service Levels

- Platform availability targets
- Vulnerability detection timeframes
- Critical vulnerability notification SLAs
- Report delivery schedules
- False positive rate management.

This technology foundation, centred on the Tenable platform and enhanced by Atos service delivery capabilities, provides organisations with enterprise-grade vulnerability management that scales to meet complex security requirements while maintaining operational efficiency.

Crown Commercial Service *Supplier*

Atos

4. What terms apply?

To the fullest extent permitted under G-Cloud 15 Framework Agreement and the Call-Off Contract, Atos will provide the Services in accordance with the Atos Supplier Terms (which will include, but may not be limited to , the Supplier Acceptable Use Policy, Supplier Data Processing Agreement, Supplier Specific Shared Responsibility Model, Supplier SLAs and Supplier Licence Terms and any applicable Third-Party Terms outlined in this Service Description document and the Order Form) and this Service Description document.

For clarity:

- Atos Supplier Terms may be modified in accordance with the provisions of the Call-Off Contract, and remain effective except where expressly overridden.
- Hyperlinks included in the Atos Supplier Terms and Service Description document remain effective where they point to Atos' or the relevant Third-Party Terms or documents. Should a hyperlink cease to function, Atos will work with the client to update it through the agreed procedure.

Crown Commercial Service *Supplier*

Atos

5. Termination

Termination shall be in accordance with:

- The G-Cloud 15 Framework terms and conditions
- Any terms agreed within the Order Form of the relevant Call-Off Contract
- For this specific service, by default Atos ask for at least thirty (30) days prior written notice of termination without cause.

Atos commits to the continued provision of services for the duration of the Call-Off Contract subject to the terms and conditions of the G-Cloud 15 Framework Agreement, the Call-Off Contract, the Atos Supplier Terms and the applicable Third Party Agreements (as defined in the Atos Supplier Terms and indicated in the Order Form) related thereto.

Crown Commercial Service *Supplier*

Atos

6. How do I order?

Please contact our team at: gcloud@atos.net

- We will prepare a quotation for your review, including any applicable volume discounts.
- Once the quotation is agreed, we will issue the necessary documentation (as required by the G-Cloud Framework) and request a purchase order from you.
- Upon receipt of your purchase order, we will configure the services in line with the agreed requirements. Where applicable, you will also receive access to our self-service portal to begin provisioning services.
- If you are a new customer, you may need to complete additional 'new supplier' forms.
- Invoices will be issued to you and to Crown Commercial Service (CCS), quoting the purchase order number, for the services procured.
- We will also submit the required monthly management information reports to Government Procurement.

7. Glossary

Term	Definition
ACR	Azure Container Registry
AES	Advanced Encryption Standard
API	Application Programming Interface
ARM	Azure Resource Manager
ASM	Attack Surface Management
ASN	Autonomous System Number
AST	Automated Security Testing
AWS	Amazon Web Services
CAB	Change Advisory Board
CASB	Cloud Access Security Broker
CI/CD	Continuous Integration/Continuous Deployment
CIS	Centre for Internet Security
CNAPP	Cloud Native Application Protection Platform
COBIT	Control Objectives for Information and Related Technologies
CSPM	Cloud Security Posture Management
CVSS	Common Vulnerability Scoring System
DAST	Dynamic Application Security Testing
DISA	Defence Information Systems Agency
DMZ	Demilitarised Zone
DNS	Domain Name System
DSPT	Data Security and Protection Toolkit
EASM	External Attack Surface Management
ECR	Elastic Container Registry
EDR	Endpoint Detection and Response
EI	Exploit Intelligence
EPSS	Exploit Prediction Scoring System
ETL	Extract, Transform, Load
FedRAMP	Federal Risk and Authorisation Management Program

Term	Definition
GDPR	General Data Protection Regulation
GRC	Governance, Risk and Compliance
HIPAA	Health Insurance Portability and Accountability Act
IaC	Infrastructure as Code
IAM	Identity and Access Management
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organisation for Standardisation
IT	Information Technology
ITSM	IT Service Management
KPI	Key Performance Indicator
MTTD	Mean Time to Detect
MTTR	Mean Time to Remediate
NCSC	National Cyber Security Centre
NHS	National Health Service
NIST	National Institute of Standards and Technology
OAuth	Open Authorisation
OT	Operational Technology
OWASP	Open Web Application Security Project
PAM	Privilege Access Management
PCI-DSS	Payment Card Industry Data Security Standard
PCM	Policy Compliance Monitoring
RES	Remediation Enablement Service
REST	Representational State Transfer
ROSI	Return on Security Investment
RPA	Robotic Process Automation
SAML	Sarbanes-Oxley Act
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOAR	Security Orchestration, Automation and Response

Term	Definition
SOC	Security Operations Centre
SOX	Sarbanes-Oxley Act
SSO	Single Sign-On
STIGs	Security Technical Implementation Guides
TLS	Transport Layer Security
UK	United Kingdom
VMS	Vulnerability Management Service
VPR	Vulnerability Priority Rating
VSS	Vulnerability Scanning Service
WAS	Web Application Scanning

Crown Commercial Service *Supplier*

Atos

8. Why Atos

Atos has been a trusted partner on every G-Cloud iteration since the framework began, helping public sector organisations modernise with confidence. We combine global expertise with deep UK experience, delivering secure, scalable cloud solutions that meet the highest government standards.

As Europe's leading provider of cloud and cybersecurity services, Atos offers end-to-end capabilities - from migration and hosting to SaaS and consultancy - supported by UK delivery centres and strategic partnerships with hyperscalers.

Our focus on innovation, sustainability, and social value ensures that customers not only achieve operational excellence but also contribute to a greener, fairer future. With Atos, you gain a proven partner committed to driving efficiency, resilience, and transformation across public service.

About Atos

Atos Group is a global leader in digital transformation with c. 67,000 employees and annual revenue of c. €10 billion, operating in 61 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE is listed on Euronext Paris.

The purpose of Atos Group is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Learn more at: atos.net

105043-RR