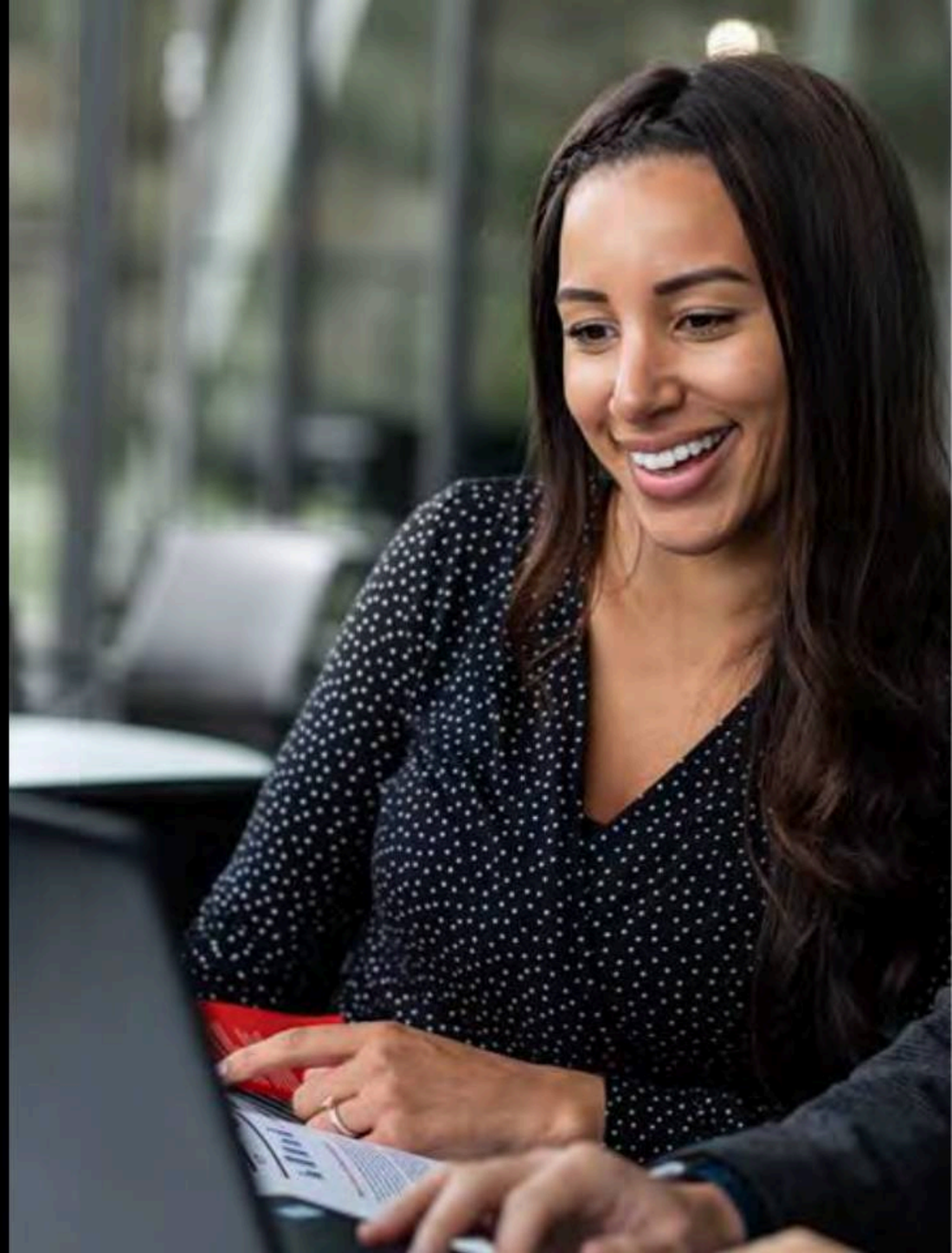
Vulnerability Management Service (VMA)

Service guide



About ROCK
Our Services
Our Approach
Key Features
Key Benefits
Management & Governance
Security & Data Protection
Customer Benefit
Values & Outcomes
Working with Us
Accreditations
How to Buy

About ROCK

ROCK is a technology services group delivering cloud, cybersecurity and managed IT services to public sector, healthcare, education, housing and regulated organisations.

Headquartered in the UK, the ROCK Group supports clients globally across and beyond Europe and North America.

The group is structured for scale and resilience, combining disciplined delivery with deep regulatory understanding. This enables ROCK to operate as a trusted partner in complex, high-assurance environments where reliability and security are critical.

The group operates through two focused service disciplines:

- As a Managed Service Provider (MSP), ROCK runs and optimises cloud platforms, infrastructure and modern workplace environments.
- As a Managed Security Service Provider (MSSP), ROCK delivers continuous cyber defence, risk management and compliance-led security operations.

These services can be consumed independently or combined into a unified operating model.

Clients partner with ROCK for clarity and confidence. From a client standpoint, every partnership is shaped by three principles.

Commitment - Through clear ownership and long-term partnership.
Proof - Through measurable outcomes, service metrics and transparent reporting.
Certainty - Through predictable delivery, resilient design and controlled change.

ROCK supports organisations to modernise securely and operate more effectively. We pair technical depth with practical guidance to support informed decisions and keep technology aligned to business priorities.

The group operates within a mature governance framework aligned to ISO 27001:2022, ISO 9001:2015 and Cyber Essentials Plus.

Engineering and service practices are consistent, repeatable and auditable, enabling scale while managing risk.

Ongoing investment in people, platforms and innovation strengthens capability and keeps services responsive to evolving needs. As a strategic partner, ROCK helps clients improve today while building the foundations for long-term change.

Responsible & Sustainable Delivery

ROCK is committed to delivering Social Value alongside high-quality technology services. Our approach is aligned to the UK Government Social Value Model and focuses on creating good jobs, developing skills, supporting inclusive employment, strengthening supply chains, protecting the environment, and promoting workforce wellbeing.

Social Value is embedded into how we operate as an organisation and how we deliver services, including through fair working practices, skills development and training, responsible supply chain management, environmental sustainability, and community engagement.

For each contract, commitments are tailored to customer needs and local context, and agreed during mobilisation and contract governance.



About ROCK
Our Services
Our Approach
Key Features
Key Benefits
Management & Governance
Security & Data Protection
Customer Benefit
Values & Outcomes
Working with Us
Accreditations
How to Buy

Our Services

ROCK's Vulnerability Management Service (VMA) provides public-sector leaders with a proactive, high-precision model for identifying and mitigating the technical risks that threaten operational continuity.

We move beyond the noise of traditional automated scanning to provide a risk-based exposure management program that safeguards your organisation's digital assets and public reputation.

Rather than providing a generic list of technical flaws, VMA focuses on business-impact prioritisation. We help you understand exactly where your environment is exposed, which vulnerabilities pose a material threat to your specific services, and how to direct your remediation budget for the greatest possible impact.

The Executive Pillars of VMA:

Continuous risk visibility
We provide a live view of your technology estate, ensuring that newly discovered threats, including Zero Day vulnerabilities, are identified before they can be exploited.

Fiscal discipline & prioritisation
We filter out the thousands of low risk alerts to focus your internal or third-party engineering teams on the 5% of vulnerabilities that represent 95% of your actual risk.

Outcome led remediation
VMA isn't just about finding problems; it's about the controlled and proportionate reduction of exposure, ensuring your teams spend their time fixing what matters most.

Integrated assurance
Whether acting as a standalone oversight function or integrated with your wider Managed IT, our service provides the evidence-based reporting required to satisfy the Board and SROs that risks are being actively managed.



"Proactive vulnerability reduction through continuous identification, prioritisation and remediation support."

Ian Elsbury, COO at ROCK

Our Approach

Our approach is based on Cyber Essentials (CE) as the foundational standard for organisational resilience. We replace point in time assessments with a Continuous Exposure Management lifecycle.

By integrating Qualys for deep-tissue vulnerability intelligence with LogicMonitor for full-stack visibility and Cloud-Native automated patching, we ensure your organisation remains always compliant.

Phase 1: Full Stack Estate Discovery (LogicMonitor & Qualys)

Goal: Eliminate blind spots and establish an immutable inventor state.

Unified visibility
We use LogicMonitor's cloud-to-edge monitoring to identify every connected asset across your hybrid estate. This ensures that Shadow IT or forgotten cloud instances are brought under governance.

Deep tissue scanning
Qualys provides the intelligence layer, auditing your estate against the five key Cyber Essentials controls (Firewalls, Secure Configuration, User Access, Malware Protection, and Patch Management).

Customers will benefit from a definitive asset inventory and a live exposure dashboard that highlights deviations from the Cyber Essentials standard.

Phase 2: Risk-Based Prioritisation & Monthly Oversight

Goal: Filter technical noise to focus executive attention on material risks.

Intelligent risk scoring
We move beyond generic scores. By combining Qualys vulnerability data with LogicMontior's performance context, we identify which weaknesses are truly exploitable and threaten critical business services.

Monthly risk velocity reports
We provide a high-level executive summary each month. This translates complex telemetry into a "Risk Velocity" metric, showing the Board exactly how much risk has been neutralised.

Customers will benefit from a monthly prioritised remediation roadmap that directs engineering effort toward the Top 5% of vulnerabilities that represent the highest material risk.

Phase 3: Cloud-Native Remediation & Annual Validation

Goal: Close the vulnerability window through machine speed response.

Automated cloud-native patching
We leverage Cloud-Native tools (e.g., Azure Update Manager, AWS SSM) to automate the deployment of security patches. This ensures critical vulnerabilities are closed within the CE-mandated 14-day window without manual intervention.

Annual independent penetration testing
To validate our continuous controls, we conduct an annual, high-intensity Penetration Test. This "stress tests" your defences using human-led adversary tactics to confirm that your automated systems are effective.

Customers will benefit from a certification ready posture for Cyber Essentials Plus and documented assurance artefacts for your annual report and regulatory bodies.

Our Approach

We break our delivery into three distinct cadences: Continuous Intelligence, Monthly Strategic Oversight, and Annual Independent Validation

Always on: The digital guardrail

The always on layer provides the foundation of your security posture. It operates silently in the background to prevent risk from accumulating.

Continuous Estate Discovery (LogicMonitor)
24/7 identification of assets and cloud instances, to ensure your estate is always up to date.

Persistent Vulnerability Scanning (Qualys)
Real-time detection of newly disclosed threats and zero day exploits as they emerge globally.

Automated Remediation (Cloud-Native)
Machine-speed deployment of security patches via Azure/AWS, ensuring critical holes are closed within the Cyber Essentials Plus 14-day window.

Proactive Alerting
Immediate notification to your technical teams for any critical" or high severity vulnerabilities that bypass automated controls.

Monthly: The Strategic Pulse

Each month, we translate technical activity into Board-level accountability. This is where we demonstrate the ROI of your security spend.

Monthly executive risk velocity report
A non-technical summary showing how much risk has been drained from the organisation versus new emerging threats.

Prioritised remediation roadmap
A strategic to do list for your engineering teams, ensuring they are focused on the 5% of risks that represent 95% of your actual business threat.

Governance & risk acceptance meeting
A formal session to review deferred risks, ensuring that any decision to not patch is documented and signed off by the appropriate SRO.

Annually: The Independent Stress-Test

The annual cadence provides the final proof of protection for your stakeholders, regulators, and insurers.

Independent penetration test
A high-intensity, human-led stress test designed to find weaknesses that automated tools might miss.

Cyber Essentials Plus recertification
A formal audit of your estate to maintain your government-mandated security standing.

Annual resilience statement
A comprehensive executive document summarising the year's performance, technical debt reduction, and strategic recommendations for the next fiscal period.

Key Features

The ROCK Vulnerability Management service provides a suite of executive grade capabilities designed to ensure your organisation is continuously compliant and resilient.

Unified Estate Visibility & Asset Truth

LogicMonitor full stack discovery
Continuous identification of every asset, from cloud workloads to on-premise infrastructure, ensuring that Shadow IT is eliminated and the entire estate is under governance.

Dynamic cloud-native inventory
Real-time synchronisation with Azure and AWS environments to automatically identify and secure newly spun-up resources as they appear.

Cyber Essentials (CE) asset baselining
Classification of all assets against the scope requirements for Cyber Essentials Plus, ensuring no gaps exist in your primary defensive perimeter.

Intelligence & Prioritisation

Qualys Deep-Tissue Scanning
Industry-leading vulnerability detection that identifies technical flaws, misconfigurations, and out-of-date software with surgical precision.

Risk based contextualisation
We move beyond generic severity scores. We evaluate vulnerabilities based on their exploitability and the criticality of the service they support, focusing effort on what matters most.

Monthly executive risk velocity reports
A board-ready summary translating millions of technical data points into a single metric showing the speed and volume of risk reduction.

Automated Remediation & Validation

Cloud-native patch automation
Direct integration with Azure Update Manager and AWS Systems Manager to automatically deploy security patches within the CE-mandated 14-day window.

Remediation tracking & decision logs
A permanent, auditable record of all vulnerabilities identified, the remediation actions taken, and the technical decisions made for audit-readiness.

Annual independent penetration testing
A high-intensity, human-led stress test of your defences, providing the ultimate validation of your security controls for SROs and external regulators.

Key Benefits

Our service ensures that vulnerability management is no longer a hidden technical overhead, but a transparent management control that delivers measurable business value.

Financial Efficiency & Budgetary Control

Optimised Resource Allocation
Stop wasting engineering time. By using Qualys intelligence to identify the Top 5% of critical risks, we ensure your team's effort, and your budget, is focused only on threats that could cause a material service outage.

Avoided cost of breach
The average cost of a UK data breach is measured in millions. Proactive remediation is a fraction of the cost of emergency incident response, legal fees, and regulatory fines.

Maximised infrastructure ROI
By using Cloud-Native patching and LogicMonitor visibility, you get more out of your existing cloud investments without the need for expensive, third-party legacy security suites.

Reputational Integrity & Public Trust

Safeguarding the mission
Vulnerabilities lead to downtime. Our continuous approach ensures that your public-facing services remain stable and available, protecting the organisation's reputation for reliability.

Executive confidence
Move from hoping you are secure to knowing you are resilient. Monthly reporting provides the Board with documented proof that the attack surface is shrinking, not growing.

Crisis prevention
Most major breaches exploit known vulnerabilities that went unpatched. We close these open doors, ensuring your organisation doesn't become the next headline.

Operational Agility & Compliance

Frictionless compliance
We turn Cyber Essentials Plus from a stressful annual fire drill into a continuous state of readiness. You are always prepared for an audit, with the evidence already gathered.

Increased delivery velocity
Secure-by-design guardrails and automated patching mean your developers and IT teams can deploy new services faster, knowing the foundation is automatically maintained.

Unified vendor oversight
Gain a single source of truth for your entire estate. Whether your servers are in Azure, AWS, or on-premise, you have one unified view of your risk and compliance status.

Management & Governance

Our governance model is designed to provide you with a Continuous Assurance Loop. We ensure that vulnerability management is not a background task, but a transparent and governed management discipline.

The Strategic Governance Framework

We provide a structured interaction model that ensures your security posture is always aligned with your risk appetite and operational goals:

The strategic security liaison
ROCK provides a dedicated lead who acts as the bridge between technical remediation and executive oversight, ensuring that findings are contextualised for your business.

Monthly risk velocity reviews
A formal, non-technical briefing for the Board or SROs. We review the risk velocity the rate at which vulnerabilities are being closed versus new ones emerging, providing a clear metric for the ROI of your security spend.

Exception & risk acceptance governance
Not every vulnerability can (or should) be patched immediately. We provide a formal process for risk acceptance, ensuring that any decision to defer remediation is documented, justified, and approved by the appropriate authority.

Managed Remediation Workflow

To ensure that identification leads to action, we govern the remediation lifecycle:

SLA driven patching
We monitor remediation against the Cyber Essentials Plus 14-day mandate. Using Cloud-Native automation and LogicMonitor tracking, we provide real-time alerts if a patch cycle is at risk of missing its deadline.

Remediation validation
Every fix is independently validated. Once a patch is deployed, we re-run the Qualys scan to provide "Proof of Resolution," closing the loop and updating your compliance status.

Supplier coordination
We act as the oversight layer if you have third-party infrastructure providers. We hold your vendors accountable for patching their environments, ensuring they meet your security standards.

Board-Ready Reporting & Artefacts

We maintain a Single Source of Truth (SSOT) for your security compliance, producing tangible artefacts for audit and leadership:

The monthly executive insight pack
A high-level summary of the estate's health, focusing on critical exposure, compliance trends, and strategic recommendations.

The traceable decision log
A permanent, auditable record of all vulnerability findings and the specific actions taken (or deferred), providing absolute protection during external audits.

Annual assurance statement
A formal document summarising the year's security performance, supported by the results of the Annual Penetration Test, ready for inclusion in your annual report.

Security & Data Protection

We treat your vulnerability telemetry with the same rigour we apply to your most sensitive financial records. Our focus is on ensuring that the data used to protect you is itself protected by world-class controls.

ISO-Aligned Security Governance

The service operates within ROCK's ISO 27001:2022 certified framework. The outcome is a globally recognised level of security that ensures your risk data is handled with absolute confidentiality and precision.

We do not extract or store your customer production data. Our focus is exclusively on the security metadata (vulnerability logs, asset inventories) required for oversight. Your "Crown Jewels" remain in your environment.

Access Control & Personnel Trust

Access to your vulnerability reports is governed by Microsoft Entra ID with mandatory Multi-Factor Authentication (MFA). Only vetted experts assigned to your account can access your data, preventing internal or external leakage of your risk profile.

All ROCK staff undergo rigorous background screening aligned to BS7858:2019. For high-sensitivity public sector environments, we provide personnel with Security Check (SC) or Enhanced DBS clearance.

Data Sovereignty & Disposal

All data handling complies with UK GDPR and Cyber Essentials Plus. We ensure that your strategic security insights are stored and processed within protected UK jurisdictions.

At contract conclusion, all vulnerability data and decision logs are either transferred to your permanent custody or permanently deleted in line with ISO-aligned sanitisation practices

Data Ingestion & Sovereignty

We use Qualys and LogicMonitor to ingest only technical telemetry (e.g., version numbers, configuration settings, and patch levels).

Alanalytical data is processed and stored within UK-based jurisdictions, ensuring full alignment with UK GDPR and the Data Protection Act 2018. Your organisational risk data never leaves protected borders.

The "Single Source of Truth" (SSoT)

We maintain a tamper-proof record of every vulnerability identified and every remediation action taken. This serves as your primary evidence for ISO 27001 and Cyber Essentials Plus audits.

Through continuous discovery, we maintain a live inventory. If a new server is spun up in your cloud environment, it is automatically identified and brought under the same data protection guardrails.

Data Resilience & Destruction

Your security configuration data is protected by immutable, air-gapped backups. Even in a catastrophic breach, your security posture history is recoverable and protected.

At contract end, we follow a formal Data Sanitisation Process. All strategic reports and risk logs are either returned to your permanent custody or permanently destroyed in line with ISO standards, leaving no "knowledge footprint" behind.



Values & Outcomes

The outcome of our security posture is absolute strategic confidentiality. We ensure that your most sensitive organisational data, your vulnerabilities and risk logs, are handled with the same rigour you expect for your financial records.

Strategic & Reputational Value

Board level certainty
We replace cyber anxiety with clear, non-technical Risk Velocity Reports. You lead with the confidence that comes from a 360-degree view of your exposure.

Brand protection
By proactively closing the open doors that hackers exploit, we prevent the reputational fallout and public service disruption associated with a major breach.

Financial & Commercial Value

Optimised capital allocation
We eliminate wasteful security spend. The outcome is a budget focused exclusively on the Top 5% of risks that represent 95% of your actual business threat.

Avoided cost of crisis
Proactive vulnerability management is a fraction of the cost of emergency incident response. We protect your bottom line from the millions of pounds in legal fees and fines typical of post-breach recovery.

Operational & Compliance Value

Frictionless Innovation
Our Secure-by-Design guardrails and Cloud-Native automated patching allow your teams to deploy new services faster without being slowed down by security bottlenecks.

Continuous Compliance
We turn Cyber Essentials Plus into a background outcome. You remain in a permanent state of audit-readiness, eliminating the stress and resource-drain of annual compliance fire drills.

About ROCK
Our Services
Our Approach
Key Features
Key Benefits
Management & Governance
Security & Data Protection
Customer Benefit
Values & Outcomes
Working with Us
→ Accreditations
How to Buy

Accreditations & Certifications

ROCK maintains a proven, independently assessed way of working that underpins every service, helping us provide the best IT solutions to our clients. Our certifications and partnerships show that we take security, governance and quality seriously, strengthening our credibility through best-practice services, recognised standards, and ongoing accreditation.

Security Clearances

BS7858:2019 Screening
All staff undergo background screening aligned to BS7858:2019 for roles with access to client systems or sensitive information.

Security Check
Staff can hold UK Government Security Check clearance where required by the service scope, buyer requirements or contractual obligations.

Enhanced DBS Checks
Enhanced DBS checks are performed for staff supporting regulated or sensitive environments where required by client contracts or service scope.

Strategic Partnerships

ROCK works with a range of leading cloud and technology providers to deliver secure, resilient and well-governed services.

Microsoft Partner
Cloud, identity, security and productivity services across Azure, Microsoft 365, Microsoft Entra ID and Microsoft Defender.

AWS Partner
Infrastructure and platform services including compute, storage, networking and security.

Cisco and Meraki
Cloud-managed networking, SD-WAN and secure connectivity solutions.

Cloud Security & SASE
Secure access, firewalling, SD-WAN and ZTNA capabilities, including cloud security.

Backup & Recovery | N-Able & Cove
Cloud-based backup, replication and disaster recovery solutions supporting cloud, hybrid and endpoint environments.

Endpoint & Device Management
Endpoint security, configuration, monitoring and lifecycle management tooling across user devices and servers.

SonicWall
Network security, firewalling, secure remote access and SD-WAN capabilities for on-premise and cloud-connected environments.

Certifications & Compliance

ISO 27001:2022
Certified information security management system demonstrating effective controls for data protection, access management and operational security.

ISO 9001:2015
Certified quality management system supporting consistent service delivery, continuous improvement and effective governance.

Cyber Essentials Plus
Independently verified assurance of strong baseline cybersecurity controls across all operational systems.

ICO registration
Fully registered with the Information Commissioner's Office for data processing compliance.

How To Buy

This service can be procured quickly and compliantly through the Crown Commercial Service (CCS) G-Cloud 15 Framework under the Cloud Support lot.

This provides a streamlined route for public-sector organisations to access high-quality managed support without needing to run a full tender.

What Buyers Can Expect

→ Fast mobilisation, with service commencement scheduled quickly after award.

→ No contract negotiation, as all terms follow the standard G-Cloud framework.

→ Transparent pricing, published and fixed in accordance with the G-Cloud catalogue.

→ Clear onboarding processes, including asset discovery, documentation intake and communication setup.

Purchasing Steps

1. Search for ROCK on the Digital Marketplace under: Managed IT Services - Cloud Support

2. Review the Service Definition, pricing document and terms.

3. Shortlist ROCK based on your technical, operational and commercial criteria.

4. Evaluate shortlisted suppliers following CCS guidance.

5. Award a Call-Off Contract directly to ROCK through G-Cloud 15.

6. Agree service scope and onboarding timelines with our mobilisation team.

Support with Procurement

ROCK can support buyers with:

- Responding to clarification questions
- Helping shape scope within the boundaries of G-Cloud
- Providing guidance on service levels, onboarding and shared responsibilities
- Supporting internal approvals or business case preparation

We remain fully compliant with CCS rules - no pre-award customisation of terms.

HM Government
G-Cloud
Supplier

ROCK

Your cybersecurity partner to reduce risk, strengthen resilience and build trust.

rock.co.uk

V1.0 | 2026