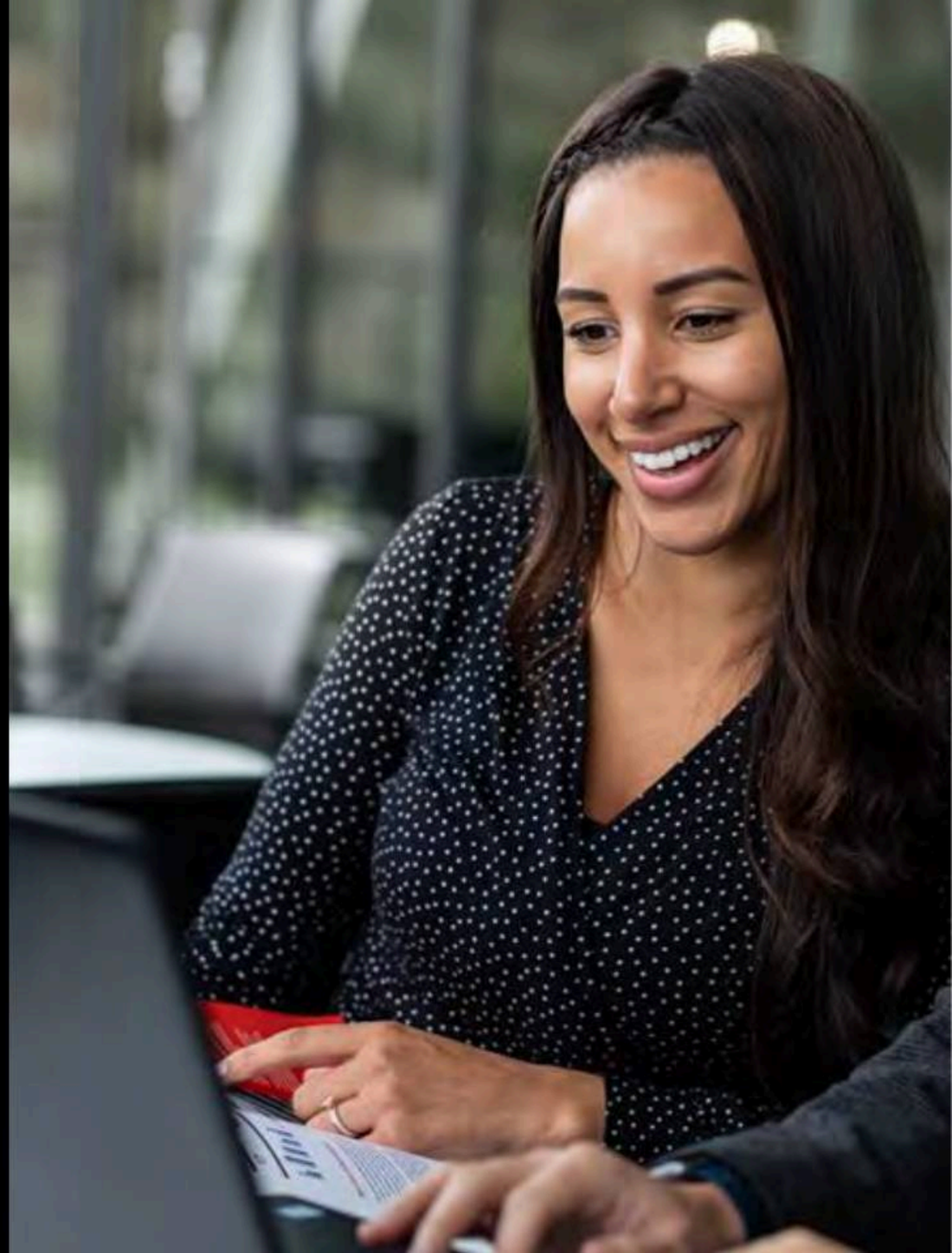
Incident Response

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 Incident Response service supports public-sector organisations in preparing for, responding to and recovering from cybersecurity incidents.

The service is designed to help organisations contain threats quickly, minimise operational impact and restore services safely while maintaining clear communication and governance throughout an incident.

The service can be used to support live incidents, provide structured response capability where in-house resources are limited, or enhance existing security arrangements. It is suitable for a range of incident scenarios, including malware outbreaks, ransomware events, unauthorised access, data breaches and suspected compromise.

Our approach focuses on calm, methodical response and evidence-based decision-making, ensuring incidents are handled proportionately and in line with organisational and regulatory expectations.

Our Approach

Our incident response approach prioritises speed, control and clarity. We begin by establishing the nature and scope of the incident, confirming affected systems, data and users. This allows us to contain risk quickly and prevent further impact while preserving evidence where required.

Response activities follow structured, well-documented processes aligned to recognised best practice. We work closely with client stakeholders to agree actions, communicate status and manage escalation.

Throughout the incident, we provide clear guidance on containment, eradication and recovery steps.

Following resolution, we support post-incident review activities to identify root causes, lessons learned and recommended improvements. This helps organisations strengthen their security posture and reduce the likelihood of future incidents.



"Rapid, structured response that contains threats quickly and restores operational stability with confidence."

Ian Elsbury, COO at ROCK

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

Key Benefits

Our Incident Response service delivers critical value during high-pressure situations by providing structure, expertise and reassurance.

Faster incident containment
Faster containment of security incidents, reducing operational and data impact.

Reduced service disruption
Reduced disruption to services and users through coordinated response actions.

Improved incident confidence
Improved confidence during incidents, with clear guidance and communication.

Lower escalation & recurrence risk
Reduced risk of escalation or repeat compromise through thorough investigation.

Compliance-ready reporting
Support for compliance obligations, including incident documentation and reporting.

Stronger cross-team coordination
Improved coordination across technical, operational and leadership teams.

On-demand specialist expertise
Access to specialist expertise without the need to retain full-time resources.

Clear root cause understanding
Clear understanding of root causes and contributing factors.

Actionable post-incident improvements
Actionable recommendations to strengthen defences post-incident.

Greater organisational resilience
Greater organisational resilience in the face of future incidents.

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

Key Features

Our Incident Response service provides a structured and dependable response capability across the full incident lifecycle. Each feature is designed to reduce impact, restore services safely and support informed decision-making.

Rapid Triage & Assessment
Rapid triage and assessment of suspected or confirmed security incidents.

Immediate Containment
Containment actions to limit spread, access or further compromise.

Root Cause Investigation
Investigation and analysis to understand root cause and impact.

Threat Eradication & Remediation
Guidance on eradication of threats and remediation of affected systems.

Safe Service Restoration
Support for service restoration and return to normal operations.

Evidence Preservation & Documentation
Evidence preservation and documentation to support internal or regulatory review.

Cross-Functional Coordination
Coordination with internal IT, security, legal and communications teams.

Third-Party Escalation Management
Vendor coordination and escalation where third-party platforms are involved.

Timeline, Logs & Action Tracking
Clear incident timelines, decision logs and action tracking.

Post-Incident Review & Improvements
Optional post-incident review and improvement recommendations.

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

Management & Governance

Incident Response services are delivered through a clearly defined engagement framework that ensures accountability, control and transparency during incidents.

Engagement & Response Framework

ROCK provides a named incident lead responsible for coordinating response activity, communication and decision-making. Roles, responsibilities and escalation paths are confirmed at the outset of the engagement or incident.

Incident Coordination & Communication

We work closely with nominated client contacts to provide regular updates, agree actions and manage escalation. Communication is clear, timely and appropriate to the severity of the incident.

Decision Logging & Audit Trail

Key actions, decisions and findings are documented throughout the incident to support accountability, review and reporting requirements.

Post-Incident Review

Following resolution, we support structured post-incident reviews covering:

- Incident timeline and impact
- Root cause analysis
- Effectiveness of controls and response actions
- Recommended improvements and next steps

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

Security & Data Protection

Security and confidentiality are fundamental to incident response activities. ROCK applies strong controls to protect information accessed during an incident.

Security Framework & Best Practice Alignment

Incident response activities are aligned to recognised standards and best practice, including ISO-aligned incident management principles.

Data Handling & Privacy

ROCK accesses only the information required to investigate and respond to the incident. No data is retained beyond what is necessary to deliver the service.

All handling complies with UK GDPR and Cyber Essentials Plus requirements

Identity & Access Controls

Access to systems and information is granted on a least-privilege basis, logged and removed promptly when no longer required.

Secure Storage & Transmission

Any artefacts, evidence or documentation produced during the incident are stored securely and transmitted using encrypted channels.

Data Retention & Secure Disposal

Incident-related data is retained only for the duration required to support response and reporting, then securely deleted in line with ISO-aligned sanitisation practices.



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

Values & Outcomes

Our Incident Response service delivers value by reducing the impact of security incidents and strengthening organisational readiness.

Operational Value

Faster restoration of services following security incidents.

Clear coordination during high-pressure situations.

Reduced internal strain on IT and security teams.

Financial Value

Avoided costs associated with prolonged outages or unmanaged incidents.

Reduced likelihood of secondary incidents through effective containment.

Predictable engagement costs with defined scope and activities.

Security & Compliance Value

Improved alignment with regulatory and reporting obligations.

Stronger evidence base for audit and assurance activities.

Reduced risk of repeat incidents through post-incident learning.

Strategic & Organisational Value

Greater leadership confidence in incident handling capability.

Improved organisational resilience and preparedness.

A clearer roadmap for strengthening security controls and response processes.

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.

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

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