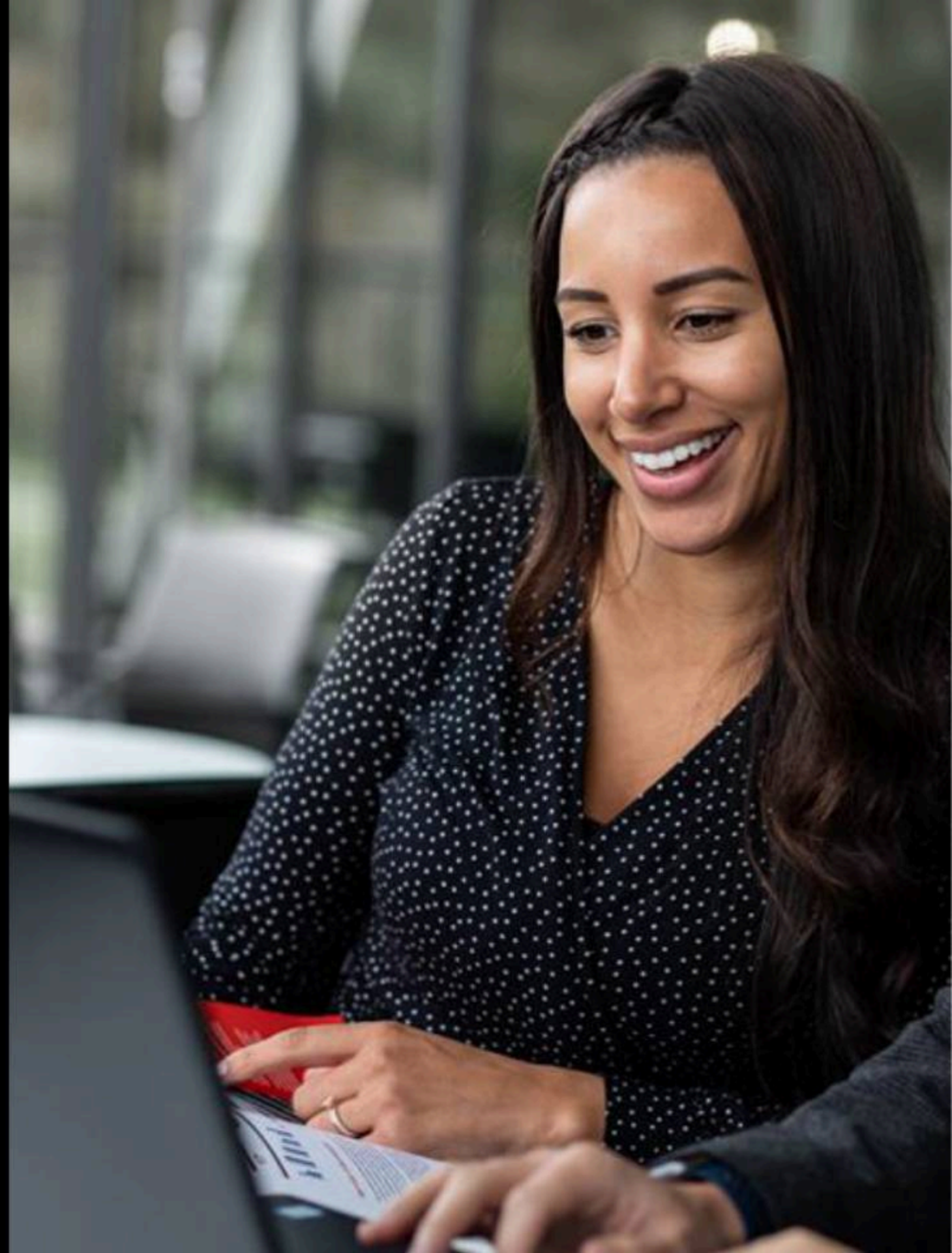
Virtual Chief Information Security Officer (vCISO)

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 vCISO service provides your organisation with senior-level cybersecurity leadership and board-ready expertise without the significant cost or long-term commitment associated with an internal full-time executive appointment. This allows you to scale your security leadership in direct alignment with your strategic needs and budget constraints.

Safeguarding Public Value & Reputation

The vCISO acts as an independent, objective advisor to the CEO, Board, and Senior Responsible Owners (SROs). By establishing clear accountability for technology decisions, we reduce delivery risk and provide the necessary assurance that your technology investments, especially during cloud adoption or digital transformation, are secure and resilient.

Turning Risk into Business Insight

We specialise in translating complex technical and architectural risks into clear, insights for the executive team.

This enables you to make documented, evidence-based decisions on investment and risk acceptance, ensuring that security strategy is always a core enabler of your organisational objectives.

Optimised Value for Money

The service directly supports your financial obligations by:

- **Improving Prioritisation -** Ensuring technology investment is focused on issues that materially affect service delivery and public value.
- **Reducing Rework -** Providing architectural direction and standards that prevent costly "bolt-on" security fixes or duplicated efforts.
- **Supplier Assurance -** Increasing oversight over supplier performance and multi-vendor dependency risks to ensure contractual outcomes are met.

Compliance & Resilience Certainty

Operating within ROCK's ISO 27001:2022 and Cyber Essentials Plus certified framework, the vCISO ensures your organisation is always prepared for audit and regulatory scrutiny.

We strengthen your readiness for statutory obligations, providing confidence when engaging with regulators and internal assurance functions.



"Strategic security leadership that strengthens governance, compliance and decision-making without full-time overhead."

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

Our Approach

Our approach replaces technical ambiguity with Board-level certainty. We do not operate in a vacuum of generic security checklists; instead, we align security leadership with your specific organisational objectives to ensure that protection never comes at the expense of progress.

Risk-Based Discovery & Baseline Asset Alignment

We begin by establishing a definitive baseline of your current security posture and regulatory obligations. By mapping your technology estate against your strategic priorities, we identify the "Crown Jewels" of your organisation.

This ensures our leadership activity is focused exclusively on areas that materially affect service delivery, public value, and reputation.

Executive Transparency & Decision-Ready Insight

We bridge the gap between the server room and the Boardroom. We translate "technical debt" and complex vulnerabilities into plain-language business impact.

You receive the evidence-based insight required to make informed decisions on risk acceptance and capital allocation, ensuring security spend is always traceable to a business outcome.

Collaborative Oversight & Delivery Velocity

The vCISO acts as a "unifier" across your internal teams and third-party supplier ecosystem. We remove the friction often caused by siloed security functions, reducing duplication of effort and streamlining governance.

We ensure that security standards act as safe guardrails for innovation, accelerating your delivery velocity rather than acting as a bottleneck to digital transformation.

Framework Maturity

We apply global standards, such as the MITRE ATT&CK® framework and ISO 27001, to objectively measure your defensive maturity. This moves your security narrative from feeling safe to being resilient.

Organisations will benefit from a measurable, year-on-year improvement in your resilience that is fully defensible to regulators, auditors, and stakeholders.

Key Features

The ROCK vCISO service provides a suite of executive-grade capabilities designed to give organisations a board-level, documented single source of truth for their security posture.

Strategic Leadership & Board-Level Assurance

MITRE ATT&CK® Defensive Heat Map
A visual, evidence-based assessment of your defensive maturity against real-world threat actor tactics.

Cyber Investment Portfolio & ROI Analysis
Strategic oversight of your security budget, ensuring every pound spent is mapped to a documented risk reduction.

Executive Security Briefings
Monthly, non-technical "Decision Packs" for the Board, translating complex cyber telemetry into operational and financial impact.

Risk & Exposure Management

Material Risk Register
A prioritised, business-aligned register of technical and operational risks, ensuring leadership focus remains on high-impact areas.

Third-Party & Supply Chain Governance
Security oversight of the vendor ecosystem to prevent upstream vulnerabilities disrupting service delivery.

Shadow IT & Asset Discovery
Continuous identification of unmanaged technology across the estate to eliminate blind spots and unmanaged technical debt.

Compliance & Resilience Operations

Always Ready Audit Documentation
A central repository of security policies, standards, and decision logs, maintained for instant submission to regulators.

Incident Response & Crisis Playbooks
Development and testing of crisis management protocols, ensuring the Board knows how to respond during high-pressure incidents.

Identity & Access Guardrails
Strategic oversight of user privileges and "Zero Trust" architectures to protect the organisation's primary defensive perimeter.

Feature	CEO Value Add	Primary Deliverable
MITRE Mapping	Objective proof of protection	Defensive Heat Map
Strategy Roadmap	Aligns tech to business goals	3-year security strategy
Risk Register	Prioritises budget on high impact	Business aligned risk log
Incident Playbooks	Protects reputation during crisis	Executive response manual
VFM Oversight	Eliminates wasteful security spend	Security ROI report

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 vCISO service delivers a resilience dividend, ensuring that every pound invested in security contributes to the stability, speed, and reputation of your organisation.

Strategic Risk & Reputation

Board-Level Certainty
We transform technical noise into a clear, prioritised risk map, allowing you to lead with confidence rather than reacting to headlines.

Crisis Resilience
By establishing executive-level crisis playbooks, we protect the organisation's reputation and ensure the leadership team can act decisively under pressure.

Financial & Value for Money

Capital Efficiency
We eliminate wasteful or duplicated security spend by aligning every investment to a documented, material business risk.

Cost Avoidance
By embedding Secure-by-Design principles early in your digital transformation, we prevent the 5x–10x costs associated with retrofitting security to broken systems.

Operational Velocity

Frictionless Innovation
We provide the safe guardrails that allow your teams to deploy new cloud and digital services faster, without being stalled by security bottlenecks.

Vendor Accountability
We bring senior-level oversight to your supply chain, ensuring that third-party vendors meet your standards and do not introduce "upstream" liabilities.

Governance & Compliance

Sustained Audit Readiness
We maintain a state of continuous compliance, ensuring your organisation is always prepared for ISO 27001, UK GDPR, and Cyber Essentials Plus without the usual audit disruption.

Defensible Decision-Making
We provide a clear, documented trail of all technology and risk decisions, protecting the Board and SROs during internal or external scrutiny.

Management & Governance

Our governance model is designed to move beyond traditional IT support to provide a Strategic Security Office. We ensure that every interaction is purposeful, every risk is tracked, and every decision is defensible.

The vCISO Engagement Model

We operate as an integrated part of your leadership team. Our engagement is defined by:

Strategic Appointment;A dedicated, senior security leader is assigned to your organisation, ensuring continuity of knowledge and long-term alignment with your mission.

Defined Accountability
We establish clear terms of reference at the outset, defining where the vCISO provides oversight, challenge, and decision support.

Monthly Strategic Reviews (The "Insight Cycle")

The vCISO leads a structured executive level governance monthly session. This is not a technical meeting; it is a risk management session covering:

MITRE ATT&CK® Maturity
A review of the defensive heat map to show where protection has improved and where gaps remain.

Risk Register Velocity
A status update on material risks, what has been remediated, what is emerging, and what requires Board-level risk acceptance.

Investment Performance
A review of security spend against the strategic roadmap to ensure maximum value for money.

Technical & Supplier Assurance

To ensure the Board has confidence in the entire supply chain, we provide:

Multi-Vendor Coordination
We lead the security dialogue between your internal teams and third-party suppliers (e.g., MSPs, Cloud Providers), breaking down silos and ensuring unified standards.

Change & Architectural Board Representation
The vCISO provides Secure-by-Design oversight for all major technology changes, preventing the introduction of unmanaged technical debt.

Documentation & Audit Trail

For a CEO, the most important outcome of governance is the Audit Trail. We maintain:

Traceable Decision Logs
A permanent record of all technology and security decisions made, including the evidence used and the risks accepted.

Compliance Evidence Vault
A continuous repository of documentation required for ISO 27001, Cyber Essentials Plus, and UK GDPR, ensuring you are always prepared for external scrutiny.

Security & Data Protection

We treat your strategic security data with the same rigour we apply to your production environments.

Our goal is to ensure that the insights we generate for you are never used against you.

ISO-Certified Governance

The ROCK vCISO service operates within our ISO 27001:2022 certified Information Security Management System (ISMS).

This ensures that every piece of advice, every risk log, and every strategic roadmap is handled according to international best practices for information security, quality (ISO 9001), and data privacy. 22 certified Information Security Management System, ensuring consistent and auditable control of information.



Data Sovereignty & Confidentiality

Metadata-Only Processing
We do not store or process your customer production data. Our focus is exclusively on operational metadata (e.g., system logs, risk registers, and architecture diagrams) required to provide strategic oversight.

UK-Based Operations
All vCISO activity is governed by UK GDPR and Cyber Essentials Plus standards, ensuring that your strategic data never leaves protected jurisdictions unless explicitly agreed.

Secure Vault for Governance Artefacts

Strategic documents (Board reports, MITRE Heat Maps, and Incident Playbooks) are stored in a highly secure, encrypted environment.

Identity-First Access
Access is controlled via Microsoft Entra ID with mandatory Multi-Factor Authentication (MFA).

Least-Privilege Principle
Only the specific vCISO and designated support analysts assigned to your account have access to your artefacts. All access is logged and auditable.

Personnel Integrity & Vetting

We recognise that a vCISO is a position of high trust.

All ROCK personnel undergo rigorous background screening aligned to BS7858:2019.

Government Clearance
For public-sector contracts involving higher sensitivity, we provide staff with Security Check (SC) or Enhanced DBS clearance as required.

Secure Data Disposal

At the conclusion of a contract, ROCK follows strict ISO-aligned sanitisation practices. We ensure all strategic metadata, risk logs, and board reports are either securely transferred to your permanent custody or permanently deleted, leaving no residual "knowledge footprint" outside your organisation.

Values & Outcomes

Our vCISO service delivers evidenced value across four critical dimensions of your organisation. We ensure that every security action translates into a documented business benefit.

Strategic & Reputational Value

Executive Certainty
Transform cyber anxiety into a state of controlled risk. You gain a clear, evidence-based understanding of your security posture, allowing the Board to lead with confidence.

Reputation Safeguarding
By proactively managing exposure and establishing crisis playbooks, we protect the public's trust and the integrity of your brand against the fallout of a breach.

Defensible Governance
We provide a permanent decision log of all security choices, protecting the Board and SROs during internal audits or external regulatory scrutiny.

Financial Value

Capital Allocation Efficiency
Stop throwing money at the problem. We ensure your security budget is targeted exclusively at the risks with the highest material impact on your organisation.

Avoided Cost of Rework
By embedding security into your digital transformation early Secure-by-Design, we prevent the massive costs associated with retrofitting security to failed or vulnerable systems.

Scalable Leadership ROI
Access elite, C-suite level expertise on a fractional basis, providing a high-performance leadership model without the executive recruitment overhead.

Operational & Delivery Value

Accelerated Delivery Velocity
Our safe guardrails allow your digital and cloud teams to innovate and deploy faster, knowing they are operating within pre-approved security standards.

Supplier Performance Assurance
We bring senior-level discipline to your multi-vendor ecosystem, ensuring that third-party providers meet their security obligations and deliver value for money.

Reduced Internal Friction
We resolve the silos between IT, Security, and Business units, streamlining decision-making and removing security as a bottleneck to change.

Compliance & Regulatory Value

Continuous Audit Readiness
We eliminate the compliance crunch. Your organisation remains in a constant state of readiness for ISO 27001, UK GDPR, and Cyber Essentials Plus.

Objective Maturity Metrics
Using the MITRE ATT&CK® framework, we provide a measurable, year-on-year improvement in your defensive capabilities that is fully auditable

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