G-Cloud 15 Service Definition Document

Virtual Chief Information Security Officer

Executive Summary

Virtual CISO (vCISO) is a strategic leadership service designed to provide Government departments and regulated organisations with high-assurance cybersecurity governance without the overhead of a full-time executive.

We understand that experienced security leadership is scarce and expensive. Our service bridges that gap by providing a seasoned, veteran-led security authority to sit alongside your Board. We translate complex technical risks into clear business impacts, ensuring that security investment is proportionate, risk-based, and aligned with your broader organisational goals.

This service is designed for organisations that require Strategic Governance and Executive Oversight of their security posture, moving from reactive to proactive resilience.

About Inductive Solutions

We are a specialist consultancy delivering Cyber Security, Red Teaming, Cloud FinOps, and Predictive Intelligence. Founded by a veteran, we bring a disciplined approach to complex government challenges.

Our team is built on three core pillars:

1. **Strategic Command:** We apply proven leadership principles to bring order to complex programmes.
2. **Cybersecurity:** We integrate security into the foundation of every service, not as an afterthought.
3. **Data Science & Insight:** We model outcomes using data and facts, providing certainty in decision making.

Social Value & Corporate Responsibility

We are committed to delivering value beyond the contract:

- **Veteran founded:** We bring the ethos of service and discipline to our engagements.
- **Disability Confident:** We are committed to recruiting diverse talent to ensure we have varied perspectives required to solve complex challenges.
- **Armed Forces Covenant Pledge:** We are in the process of submitting our Armed Forces Covenant Pledge to formalise our support to the Armed Forces community.
- **Women in STEM:** We actively promote gender diversity to close the skills gap in technical roles.
- **Net Zero:** We are on track to achieve Net Zero by 2030 through sustainable business architecture and remote-first working practices.

Service Overview

Our vCISO service provides specialised, on-demand cybersecurity leadership. We align security with business strategy, assess and mature your security posture, manage risk, and lead incident preparedness. Delivered on a flexible, fractional basis, this service ensures you have access to senior-level governance, risk management, and compliance expertise exactly when you need it.

Features and Benefits

Service Features

- **Strategic Leadership:** Development of a Cyber Security Strategy directly aligned to business objectives.
- **Board Engagement:** Translation of technical risks into clear business impact for Senior Leadership Teams.
- **Governance & Policy:** Creation and oversight of security policies, standards, and frameworks (e.g., NIST, ISO 27001).
- **Risk Management:** Identification, prioritisation, and tracking of cyber risks, including Supply Chain risks.
- **Incident Readiness:** Leadership during cyber incidents, including tabletop exercises and post-incident reviews.
- **Compliance Oversight:** Support for regulatory obligations (GDPR, NIS2, DORA) and standards (Cyber Essentials).
- **Vendor Management:** Independent evaluation and oversight of third-party security tools and suppliers.
- **Culture Building:** Leading security awareness initiatives to embed a "secure-by-design" culture.

Service Benefits

- **Cost-Effective Expertise:** Access to senior security leadership without the cost of a full-time executive.
- **Informed Decision Making:** improved Board-level visibility of risk, enabling data-driven investment decisions.
- **Risk Reduction:** Proactive identification of gaps in strategy and controls before they are exploited.
- **Vendor Agnostic:** Independent advice not tied to specific software or hardware vendors.
- **Scalable Support:** Flexible engagement model that scales up or down based on organisational needs.
- **Regulatory Assurance:** Stronger governance and accountability to satisfy auditors and regulators.
- **Crisis Resilience:** Experienced leadership to guide the organisation through cyber attacks and recovery.
- **Access to Specialists:** The vCISO is backed by our wider team of GRC and Technical experts.

Our Methodology

We approach the vCISO engagement with a structured lifecycle designed to deliver immediate control and long-term maturity.

Phase 1: Assessment & Baseline:

We begin by establishing a factual understanding of your current posture.

- **Maturity Assessment:** We review your existing governance, people, processes, and technology against a recognised framework (e.g., NIST CSF or Cyber Assessment Framework).
- **Risk Review:** We audit your current Risk Register and interview key stakeholders to understand the business context.
- **Outcome:** A clear state report and a prioritised list of immediate risks that need attention.

Phase 2: Strategy & Roadmap:

We move from analysis to planning.

- **Strategy Definition:** We define good practice for your specific organisation, aligning security goals with business outcomes.
- **Roadmap Creation:** We build a phased implementation plan (Short, Medium, Long term) to bridge the gap between your current state and your target maturity.
- **Budgeting:** We assist in building the business case for necessary security investments.

Phase 3: Governance & Operational Oversight (BAU):

We transition into the ongoing leadership role.

- **Steering:** The vCISO attends regular Board/Risk Committee meetings to report on progress and Key Risk Indicators (KRIs).
- **Oversight:** We oversee the delivery of the roadmap, managing internal teams or external vendors to ensure controls are implemented effectively.
- **Response:** We remain on standby to lead the response to any security incidents or emerging threats.

Onboarding and Offboarding

Pre-boarding Process

To ensure compliance from the start of the engagement we follow a standard pre-boarding protocol in preparation for project delivery.

1. **Compliance & Contracting:** Exchange of Contracts, NDAs, and Statements of Work via secure digital signing to prevent administrative delays.
2. **Security Vetting:** Pre-submission of all consultant details to the Client Security Controller to ensure site and network access upon start of project.
3. **Technical Access:** We provide a prerequisite list of technical access requirements to allow the client to issue IT permissions.

Onboarding Process

Our Onboarding process is designed to ensure our team is operational and delivers value from Week 1, without administrative delays:

1. **Success Criteria & Scope:** A formal workshop to introduce the team, define specific outcomes, Key Performance Indicators (KPIs), and boundaries of the project.
2. **Communication Schedule:** We establish a clear routine for updates, agreeing on the exact format and timing of reports to ensure transparency.
3. **Stakeholder Mapping:** We identify key decision-makers and subject matter experts required for interviews and data gathering.
4. **Evidence Gathering:** We move immediately into discovery and access logs, billing data, or legacy documentation to establish a factual baseline.
5. **Early Value Delivery:** We aim to deliver an initial findings report within the first few weeks (if applicable to the project scope).

Offboarding & Knowledge Transfer

We plan for offboarding from the start of the engagement. Our goal is to leave the client capable of managing the service independently, ensuring sustainable long-term value.

1. **Knowledge Transfer:** We conduct structured handover sessions with permanent staff to explain strategies, operational processes, or maintenance requirements. We focus on upskilling your internal teams to ensure operational independence.
2. **Documentation & Deliverables:** We provide a full handover of all contractually agreed outputs.
3. **Intellectual Property:** While the Client owns the specific deliverables created for them and specified in the contract, Inductive Solutions retains ownership of its methodologies, models and all other Intellectual Property. We do not transfer our proprietary internal tools or code libraries unless explicitly agreed to in the contract prior to the start of the engagement.
4. **Secure Data Deletion & Asset Return:** Upon project closure, we execute a secure data destruction process. Client data is permanently deleted from our systems in compliance with GDPR and government security standards, with a confirmation certificate provided if required. Any assets belonging to the client are dutifully returned.
5. **Closure Report:** We submit a final engagement report summarising the outcomes achieved, lessons learned, and recommended next steps.

Service Constraints & Requirements

- **Access to Leadership:** Successful delivery requires direct access to the Board/Senior Leadership Team to ensure strategic alignment.
- **Stakeholder Availability:** Availability of internal process owners and IT staff is required for accurate risk assessment.
- **Authority:** The vCISO must be empowered to make recommendations and influence security decisions; they cannot be effective if treated solely as an administrator.
- **Scope Dependent:** The level of operational delivery work vs. strategic oversight is defined in the Call-Off Contract.

Service Levels & Support

- **Direct Access:** Clients have direct contact with their assigned vCISO via email and phone, subject to the agreed scope of engagement.
- **Account Management:** In addition to the vCISO, an Account Manager is available for commercial or contractual escalations.

Standard Support Hours

Our standard support hours are 9:00 - 17:00 GMT/BST, Monday to Friday (excluding UK Public Holidays).
Support is available via:

- **Email:** For general enquiries, reporting, and non-urgent issues.
- **Phone:** For urgent matters and immediate escalation.

Account Management

Every engagement is assigned a dedicated Programme Delivery Manager to ensure quality and alignment with strategic goals. Clients also have a direct escalation route to the Company Directors if required.

Security & Business Continuity

Security Vetting & Personnel

- **Clearance:** All consultants hold a minimum of BPSS (Baseline Personnel Security Standard) clearance. We can submit staff for SC (Security Check) and DV (Developed Vetting) clearances for sensitive engagements upon request, if sponsorship is provided by the Client.
- **Training:** All staff undergo regular security awareness training and data handling instruction.

Data Security and Encryption

- **Data Residency:** Client data is processed and stored within the United Kingdom and the European Union (EU), in full compliance with UK GDPR and the Data Protection Act 2018.
- **Data Sovereignty:** Strict Data Sovereignty (guaranteed processing and storage solely within the UK) is available upon request, subject to a minimum contract size.
- **Encryption:** We enforce strict encryption policy. All data is encrypted in transit and at rest to ensure confidentiality and integrity.
- **Secure Communication:** Standard email communication is secured via TLS. Enhanced End-to-End Encryption is available upon request, subject to a minimum contract size.
- **Accreditation:** We are Cyber Essentials certified, demonstrating our commitment to fundamental cybersecurity controls.

Business Continuity & Resilience

- **Cloud Native Model:** We operate a secure, cloud-native business model. We do not rely on physical on-premise servers or single-site infrastructure. This ensures that our services are resilient to physical site failures.
- **Remote Working:** Our systems and security architecture support secure remote working. In the event of a physical office disruption, our team can continue to deliver services remotely without operational downtime.
- **Backup & Recovery:** All critical business data is backed up securely in the cloud with redundancy to ensure data availability and rapid recovery.

Pricing

Pricing is directly linked to the Project Scope and complexity of the requirement.

- We work with the Client to define the specific deliverables and timeline.
- We estimate the resource effort required to deliver that scope.
- We apply the corresponding daily rates from our SFIA Rate Card to calculate the total engagement cost.

All daily rates are listed in our separate SFIA Rate Card (Skills Framework for the Information Age).Our daily rates are fully inclusive of all consultant overheads, equipment, software tools (except client systems), and insurance. We do not charge administrative fees.

Discounts

To deliver maximum value to the public sector, we offer the following discounts:

- **Educational Discount:** We offer a standard discount to schools, colleges, and universities (institutions with .ac.uk domains).
- **Volume Discounts:** Volume discounts are available for long-term engagements or large team deployments. These are applied on a sliding scale based on the total number of days purchased.