

Virtual Chief Information Security Officer (vCISO)

Service Definition

G-Cloud 15

Lot 3: Cloud Support

Contact Details

Email: tenders@reliancecyber.com

Contact Number: +44 (0) 845 519 2946

Contents

1 What is a CISO? 3

 1.1 Why would you need a CISO? 3

 1.2 What is our vCISO service? 3

 1.3 Benefits 4

 1.4 Outcomes 5

2 Why Reliance Cyber? 6

 2.1 Core Capabilities 6

1 What is a CISO?

A Chief Information Security Officer's (CISO) primary goal is to manage cyber and information security risk while enabling a business to meet its business objectives. They achieve this by aligning security initiatives with an organisation's programmes and business objectives, ensuring information assets and technologies are suitably protected. The CISO's responsibilities include developing, implementing and enabling security policies to protect critical data. Most importantly, it is a CISO's responsibility to effectively communicate with the board and senior leadership and interpret the increasing complexities of regulation and compliance for them. CISOs will do this whilst managing and guiding teams responsible for the organisation's defence. These teams often traverse the first, second and third lines of defence.

The size and scope of the role will vary according to the organisation's size, type, and complexity. A CISO at a smaller organisation may be more 'hands-on' for day-to-day work, whereas a larger business would have a team aligned to support the role.

1.1 Why would you need a CISO?

CISOs are typically hard to find and highly sought after, especially for larger organisations. Whether a CISO or a named Cyber Security or information security specialist, organisations of all sizes need someone responsible for information security. Where a named CISO is not aligned with your business, the role is likely implicit, such as an IT manager who has taken responsibility for enforcing security protocols across the organisation. They may be managing risk, without the board being aware of those activities or residual risks.

In today's threat environment, every business needs a cyber security leader. It may not be appropriate to employ a full-time CISO or there may be benefit to having an independent security advisor working in the office of the CISO/CIO. One option that companies explore is to employ a Virtual CISO: an established cyber leader working with either your internal team or with their own team of independent security professionals, supporting the business to address cybersecurity challenges, build and maintain systems, address compliance, and meet security milestones.

1.2 What is our vCISO service?

Managed by a principal consultant as your key contact, our Virtual CISO (vCISO) service combines a range of our internal subject matter experts (SMEs) and senior team members who have experience delivering interim and permanent CISO roles across a range of organisations. This team of experts will use their knowledge to support you in a way that is tailored to your organisation's needs.

The vCISO will help you achieve your security programme and transformation goals. Our vCISO support can be tailored to your needs. This could typically take the form of:

- Defining or improving security strategy across the organisation.
- Supporting the implementation of ongoing or new compliance requirements that must be adhered to by the organisation, such as GDPR, Data Protection and PCI DSS.
- Communicating the importance of security-enforcing functions, security processes and requirements to a board-level audience.
- Supporting the implementation of change across your organisation through improved security posture and security management.

The key aim of our vCISO service is to provide input that can help to shape, evolve and improve your overall security posture through whichever means you require. This is a capped time-and-materials engagement based on day rates specified in our Price Model. We will provide an agreed number of days for your organisation to support your growing security needs, aligned with your timelines. This could take the form of quarterly check-ins, a number of days of support each month or longer-form engagements over a number of weeks.

1.3 Benefits

- Sought-after expertise from an experienced CISO delivered through an efficient delivery model.
- Additional support from a team of subject matter experts with years of experience in their chosen fields.
- Multi-disciplinary and cross-industry knowledge. Our CISO and SMEs have built their expertise by working across industries and understand what works best for different organisations.
- Scalable and flexible working on a daily, weekly or monthly basis, built around your needs as you need them.
- An impartial perspective on your approach to cybersecurity with support based on experience and best practice.
- Our vCISO will work with you to understand not only the change you are looking to make, but the impact and challenges that your organisation faces to help further long-term goals.
- Reduced risk through immediate, impactful support from a centralised resource. This creates visibility, awareness and accountability quickly.
- Demonstrable, increased security return-on-investment (ROI) by supporting the review of security portfolios, supplier relationships and negotiation from a position of internal market knowledge.

1.4 Outcomes

- **Improved Security Strategy** – Our vCISO will help to develop and refine your cybersecurity strategy, aligning it with growing or developing business and compliance objectives.
- **Risk Management** – Through organisation-wide risk analysis, we mitigate the likelihood and impact of security breaches, safeguarding assets and reputation.
- **Policy Governance** – Whether it's developing, tailoring, updating or enforcing policies, our vCISO guides you through all stages of policy management, ensuring alignment with industry best practices and regulatory requirements.
- **Compliance Adherence** – Our vCISO will apply their expertise to ensure you comply with all relevant compliance requirements, such as Data Protection, GDPR, etc.
- **Supplier and Contract Oversight** – Evaluation of third-party vendors against delivery performance and security practices, ensuring they meet your expectations and contribute to your organisation's overall security posture.
- **Transparent Executive Leadership** – Our vCISO provides clear, concise, and open communication at all organisational levels, empowering executives with the insights needed for informed decision-making.
- **Cost Saving** – By supporting budgeting, forecasting and cost optimisation initiatives, we help to streamline security expenditures, improving long-term budgetary requirements and resource allocation.

2 Why Reliance Cyber?

Reliance Cyber is a Managed Security Services Partner (MSSP), dedicated to fortifying our clients through cyber security. With a rich legacy spanning 20 years, Reliance Cyber has emerged as a trusted and innovative MSSP, continually reinvesting to ensure our clients receive the best security support on the market. This has enabled us to recruit the best SC specialists and develop market-leading capabilities focused solely on cyber security.

Operating 24x7x365, we prioritise collaboration, transparency and long-term trust-based relationships with clients to navigate the ever-evolving landscape of cyber threats.

2.1 Core Capabilities

Reliance Cyber's core services are structured around three strategic pillars, reflecting our holistic approach to cyber threat management across managed, proactive and reactive services.

- **Managed Services** – We deliver enhanced security operations through continuous monitoring, proactive threat detection, and rapid remediation. Operating 24x7 on our clients' behalf, our managed services include Managed Detection and Response (MDR), Managed Endpoint Detection and Response (EDR), Managed Secure Access Service Edge (SASE), Phishing Monitoring and Vulnerability Management.
- **Proactive Consulting Services** – We support clients in identifying and addressing vulnerabilities before threat actors can exploit them. Our proactive security offerings include Cyber Threat Intelligence, Crisis Simulations, Compromise Assessments and a range of bespoke solutions tailored to meet each client's unique risk landscape.
- **Reactive Consulting Services** – When incidents occur, we provide expert incident response and recovery support. Our services are delivered using methodologies certified by CREST and aligned with guidance from the National Cyber Security Centre (NCSC). Leveraging deep digital forensics expertise, we help clients contain, investigate, and recover from cyber incidents swiftly and effectively, minimising impact and enabling lessons learned to strengthen future defences.



