vCISO

Service Definition Document

January 2026

Document Control

Document Type	Confidential - Customer Facing		
Company	Maple Networks		
Address	The Print Rooms 164/180 Union Street London SE1 0LH		
Primary Contact	Graham Tetley	**Role**	CTO/Lead Consultant
Phone Number	020 3858 0048	**Email address**	gt@maple-networks.com

Revision History

Issue Date	Author	Version	Revision Description
12/01/2026	Rory Leanord	0.1	Initial Draft
29/01/2026	Graham Tetley	1.0	QA and Release

Table of Contents

Contents

Services Overview

Maple Networks are next generation Digital and IT service provider in the UK with skills in various areas across the digital landscape. Maple Networks have developed a range of services to support customers in their digital, data and business transformations.

This Document provides overview service definition information for the Maple Networks vCISO (Virtual Chief Information Security Officer) service.

Maple's vCISO (Virtual Chief Information Security Officer) service provides organisations with senior-level cybersecurity leadership on a flexible, outsourced basis. Instead of hiring a full-time CISO, companies gain access to an experienced security expert who guides strategy, risk management, compliance, and incident readiness.

Service Description

Incident Response

Maple's vCISO service provides organisations with executive-level cybersecurity leadership on a flexible, outsourced basis. It delivers strategic direction, governance, risk management, compliance oversight, and incident readiness without the cost or commitment of a full-time CISO. The service is designed to strengthen an organisation's security posture, support regulatory obligations, and embed a culture of security across the business.

The vCISO who is a senior member of the Maple Security team acts as a trusted advisor to senior leadership, translating technical risks into business-aligned decisions and ensuring that cybersecurity becomes an integrated part of organisational strategy.

Service Overview

Maple's vCISO service operates as an extension of the organisation's leadership team, providing ongoing strategic and operational security expertise. It covers the full lifecycle of cybersecurity management, including assessment, planning, implementation guidance, and continuous improvement.

Key focus areas include but are not limited to:

- **Cybersecurity Strategy & Roadmap** Development of a tailored security strategy aligned with business objectives.
- **Governance, Risk & Compliance** Establishment and maintenance of policies, risk frameworks, and regulatory alignment.
- **Security Architecture & Controls** Review and enhancement of technical and procedural controls.
- **Incident Preparedness & Response** Planning, exercising, and leadership during security incidents.
- **Third-Party & Supply Chain Security** Assessment and oversight of vendor security risks.
- **Security Culture & Awareness** Programmes to improve staff awareness and reduce human-related risks.

The service is delivered remotely or on-site as required, with flexible engagement models to suit organisational size, maturity, and budget.

Service Package

Onboarding & Initial Assessment	• Discovery workshops with leadership and technical teams • Review of existing policies, controls, and risk posture • Baseline maturity assessment and gap analysis
Strategic Planning	• Development of a multi-year cybersecurity roadmap • Prioritised action plan aligned with business goals • Executive-level reporting and board presentations
Governance & Compliance Management	• Creation or refinement of security policies and standards • Support for frameworks such as ISO 27001, NIST CSF, Cyber Essentials, GDPR, PCI DSS • Risk register development and ongoing management
Operational Security Oversight	• Review of security operations, monitoring, and incident processes • Guidance on technology selection and control implementation • Oversight of vulnerability management and remediation activities
Incident Response Leadership	• Development of incident response plans and playbooks • Facilitation of tabletop exercises • Executive coordination during real incidents
Continuous Advisory & Support	• Regular check-ins, steering meetings, and progress reviews • Ad-hoc advisory for new projects, cloud adoption, or digital transformation • Ongoing risk and compliance reporting

Service Features

	Description
Strategic Leadership	• Executive-level cybersecurity guidance • Board-ready reporting and risk communication • Alignment of security initiatives with business priorities
Policy & Governance Frameworks	• Comprehensive policy suite development • Governance structures and accountability models • Risk management processes and documentation
Compliance & Regulatory Support	• Gap assessments against relevant standards • Preparation for certifications and audits • Data protection and privacy guidance
Security Architecture & Technical Oversight	• Architecture reviews across cloud, network, identity, and data • Recommendations for control improvements • Oversight of technical security initiatives
Incident Management & Readiness	• Incident response planning and testing • Crisis leadership and coordination • Post-incident reviews and improvement plans
Third-Party Risk Management	• Supplier assessments and due-diligence processes • Contractual security requirements • Ongoing monitoring of vendor risk
Culture & Awareness	• Security awareness programmes • Phishing simulation oversight • Executive coaching on cyber responsibilities
Flexible Delivery Model	• Part-time, fractional, or retainer-based engagement • Remote or hybrid delivery • Scalable support as the organisation evolves