e2e assure

Virtual CISO (vCISO) Service

Service Definition Document

vCISO Service

Service Definition Document – G-Cloud 15

Contents

SERVICE INTRODUCTION

A Chief Information Security Officer (CISO) is the beating heart of your cybersecurity strategy. Having one helps drive towards a safer organisation and reassures customers, stakeholders and regulators.

Your CISO will, be your trusted advisor on cyber risk mitigation strategies, help you create and improve security governance and work with your leadership team to align cybersecurity with business goals.

For organisations that do not require a full-time, in-house executive, our Virtual CISO (vCISO) service provides high-level insight and acumen on an “as and when” basis.

SERVICE OVERVIEW

The e2e-assure vCISO service empowers organisations to define and execute comprehensive information security strategies, lead business change, and drive improvement in controls and risk reduction. Our team of experienced CISOs offers a credible, trusted service by working closely with your leadership and internal teams.

SCOPE OF ACTIVITIES

The engagement encompasses a holistic approach to security, moving beyond technical operations to address the Target Operating Model (TOM) and Human Firewall:

DISCOVERY, CONTEXT & TARGET OPERATING MODEL (TOM)

- Stakeholder Interviews: Conduct Interviews with security, IT, and risk owners to understand business properties and risk appetite.
- TOM Review: Evaluate the existing security operating model, including internal vs. outsourced capabilities and key security tools.
- Regulatory Alignment: Capture relevant regulatory, customer, or contractual drivers that influence security expectations.
- Governance Architecture: Assess how security decisions are made, integrated into business processes, and reported to the board.

MATURITY ASSESSMENT ACROSS CORE PILLARS

- Visibility & Data: Assess visibility of telemetry and security-relevant data from key assets and environments.
- Detection & Defence: Evaluate detection capability, including use of threat models and alignment to common attack techniques.
- Incident Response: Review response processes, playbooks, and escalation paths for common incident types.
- Technical Operations: Consider skills, roles, and responsibilities that underpin SOC decision-making and operation.

PEOPLE,CULTURE & AWARENESS

- Security Culture Assessment: Evaluate the prevailing attitude towards security across different departments and levels of seniority.
- Awareness Programmes: Review the effectiveness of existing security training, phishing simulations, and employee engagement initiatives.
- Roles & Responsibilities: Clarify security duties for non-security staff to ensure accountability is distributed throughout the organisation.
- Behavioural Change: Identify opportunities to move from simple "compliance-based" training to a culture of proactive security awareness.

GAP ANALYSIS & RISK MAPPING

- Maturity Scaling: Compare current maturity against a defined multi-level scale across each pillar.
- Critical Blind Spots: Identify material gaps and overlaps with potential impact on threat detection and business continuity.
- Business Impact: Relate findings to business-critical services and assets to support risk-based decision-making.

ROADMAP & RECOMMENDATIONS DEVELOPMENT

- Short-term Wins: Define practical improvements that can be implemented with minimal additional investment.
- Medium-term Structural Change: Outline enhancements such as process refinement, role clarity, or cultural shifts.

- Long-term Strategy: Highlight objectives to move towards a proactive, measurable, and culturally-embedded security capability.

SCOPE OF DELIVERABLES

The following tangible outputs will be provided as part of the engagement sign-off:

EXECUTIVE SUMMARY & MATURITY SNAPSHOT

- A concise summary of overall maturity, key strengths, and priority areas for improvement for senior stakeholders.

DETAILED ASSESSMENT REPORT

- A structured narrative describing current-state observations across people, process, and technology, with prioritised recommendations based on effort and impact.

IMPROVEMENT ROADMAP & ACTION PLAN

- A time-banded roadmap (near-term, mid-term, longer-term) showing the sequencing of recommended initiatives and suggested milestones.
- Follow-on Support Options: Options for periodic reassessment or complementary services, such as managed awareness training to ensure progress is tracked.

SERVICE OUTCOMES

- Business-Focused View: Provides a clear view of security maturity that can be communicated to boards, auditors, and insurers.
- Risk Reduction: Identifies critical gaps in both technology and culture before they contribute to avoidable incidents.
- Balanced Investment: Supports better-aligned investment in people, process, and technology by linking recommendations to business risk.
- Strategic Confidence: Strengthens confidence in the organisation's resilience by providing a clear roadmap to a realistic target state.