e2e assure

SOC Maturity Assessment

Service Definition Document

SOC Maturity Assessment

Service Definition Document – G-Cloud 15

Contents

SERVICE INTRODUCTION

Security operations centres (SOCs) are under pressure from evolving threats, tool sprawl, and increasing regulatory expectations, making it difficult for organisations to understand whether their current capabilities are truly effective. Without a clear and objective view of SOC maturity, security leaders risk blind spots, inefficient spending, and reduced confidence from stakeholders and auditors. This service provides an independent, structured assessment that clarifies current state, highlights gaps, and defines a pragmatic path to improvement.

SERVICE OVERVIEW

The e2e-assure SOC Maturity Assessment is a structured engagement designed to evaluate how effectively an organisation detects, responds to, and manages cyber threats across people, processes, technology, and data. Using a clearly defined multi-level maturity scale and a small set of core assessment pillars, the service gives security leaders an accessible "You Are Here" view and a realistic target state aligned to business risk. The outcome is an actionable improvement roadmap, not a theoretical score, enabling prioritised investment and measurable progress over time.

SCOPE OF ACTIVITIES

The assessment will include the following actions and areas of assessment:

DISCOVERY & CONTEXT GATHERING

- Conduct stakeholder interviews with security, IT, and risk owners to understand business priorities and risk appetite.
- Review existing SOC operating model, key security tools, and current monitoring coverage at a high level.
- Capture relevant regulatory, customer, or contractual drivers that influence SOC expectations.

MATURITY ASSESSMENT ACROSS CORE PILLARS

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

GAP ANALYSIS & RISK MAPPING

- Compare current maturity against a defined multi-level SOC maturity scale across each pillar.
- Identify material gaps, overlaps, and blind spots with potential impact on threat detection and response.
- Relate key findings to business-critical services and assets to support risk-based decision-making.

ROADMAP & RECOMMENDATIONS DEVELOPMENT

- Define practical short-term improvements that can be implemented with existing or minimal additional investment.
- Outline medium-term structural enhancements such as process refinement, role clarity, or technology optimisation.
- Highlight longer-term strategic objectives to move towards a more proactive and measurable security operations capability.

SCOPE OF DELIVERABLES

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

EXECUTIVE SUMMARY & MATURITY SNAPSHOT

- Concise summary of overall SOC maturity, key strengths, and priority areas for improvement for senior stakeholders.
- High-level visual representation of maturity across the core assessment pillars and overall target state.

DETAILED ASSESSMENT REPORT

- Structured narrative describing current-state observations, supporting evidence, and identified gaps across each pillar.
- Prioritised recommendations with indicative effort and relative impact to support planning and budget decisions.
- High-level guidance on optimising use of existing security tooling and data sources.

IMPROVEMENT ROADMAP & ACTION PLAN

- A time-banded roadmap (e.g. near-term, mid-term, longer-term) showing sequencing of recommended initiatives.
- Suggested milestones and simple outcome measures that allow progress to be tracked over time.
- Options for follow-on support, such as periodic reassessment or complementary services, if required by the client.

SERVICE OUTCOMES

- Provides a clear, business-focused view of SOC maturity that can be communicated to boards, auditors, and insurers.
- Identifies the most important security operations gaps before they contribute to avoidable incidents or inefficient spend.
- Supports better-aligned investment in people, process, and technology by linking recommendations to business risk.
- Strengthens confidence in security operations by providing a clear roadmap that defines a realistic target state and outlines a practical path to achieve it.