Security Operations Centre (SOC) Readiness Assessment

Minimise onboarding risks and ensure a Managed SOC delivers value from day one

Organisations face increasing regulatory and board-level scrutiny of their cyber security posture, particularly their ability to detect, respond and recover from security incidents. As cyber threats intensify and compliance requirements become more complex, many organisations turn to a Managed Security Services Provider (MSSP) to provide 24x7 detection and response capability as part of a Managed SOC. For most organisations, maintaining this level of capability internally is neither feasible nor sustainable.

However, moving to an outsourced Managed SOC model without adequate organisational readiness creates its own risks. Like any transformational initiative, your organisation needs readiness across people, process and technology to realise the full value of a Managed SOC partnership.

What is the Lumen SOC Readiness Assessment?

Lumen's SOC Readiness Assessment is a focused two-week engagement that evaluates an organisation's readiness to onboard a Managed SOC service.

Our experienced Security Consultants review your organisation's existing capabilities in terms of personnel resources, documented processes and underlying technologies with the goal of strengthening operational readiness, reducing transition risk and ensuring your organisation is positioned to realise the full value of a Managed SOC investment. To underpin this engagement, our consultants will make use of relevant cyber security frameworks (ASD E8, ASD ISM, APRA 234, ISO 27001).

Scope of the Service

The assessment evaluates the core pillars of people, process and technology.

People

We assess leadership oversight, escalation expectations and coordination across IT, security, risk and compliance to confirm that governance and capability are sufficient for SOC operations.

Process

We evaluate the maturity of detection, triage and incident response processes, including playbooks, regulatory notifications and integration with ITSM workflows. We also identify how well current processes align to SOC operating requirements and the uplift needed for effective MSSP integration.

Technology

We look at security tooling coverage, log availability, telemetry quality and SIEM readiness. We also identify any monitoring gaps to determine how well the technical environment supports SOC integration, including options for organisations without an existing SIEM.

Who is the SOC Readiness Assessment designed for?

- **Organisations evaluating whether to build, buy or co-manage a SOC**
  For organisations that have uplifted policies and controls and who may have appointed a security lead, but have not yet implemented a SIEM or 24×7 monitoring, and require an assessment of their operational readiness before deciding whether to build, buy or co-manage a SOC.
- **Organisations seeking a risk-based understanding of operational maturity before or during MSSP engagement**
  For organisations that require an evidence-based view of their detection and response capability to inform decisions about the scope of a Managed SOC, or to determine the uplift required to integrate effectively with an MSSP.
- **Organisations already working with an MSSP but are struggling to derive the expected value from the service**
  For organisations that have already embarked on an MSSP SOC Service only to realise that the service is not performing as expected, it can be beneficial to independently validate the maturity of the client capabilities and determine if there are any client-side contributing factors impacting the performance of the SOC service. Often addressing these factors can provide a quick win to improve the performance of the service for the remainder of the contract term and avoid the cost and disruption associated with early termination.

LUMEN

How a SOC Readiness Assessment Works – Process and Timeline

Our SOC Readiness Assessment follows a structured, two-week timeline designed to give you clarity and confidence.

Week 1 – Discovery & Current State

- Kick-off & scope confirmation
- Stakeholder interviews and workshops (security, IT, risk, compliance)
- Review of governance artefacts, incident workflows and logging architecture

Week 2 – Analysis & Recommendations

- Maturity assessment aligned to ASD ISM, Essential 8, CPS 234, ISO/IEC 27001
- Gap, dependency, and SOC onboarding risk identification
- Validation workshop and roadmap finalisation

At the end of the assessment, we will provide a draft report for your review and feedback. Once refined, we issue the finalised report, which can be shared confidently with executives, boards, auditors or external partners.

All assessments are delivered by Senior SOC Consultants.

Key Deliverables

Every assessment includes an Executive Summary and a business case component, ready for board, audit and risk committee review. The deliverables include:

SOC Readiness Assessment Report

The assessment report includes:

- Executive summary tailored for leadership and boards, highlighting key findings and priorities
- Security operations maturity overview
- Alignment against relevant Australian and International standards
- SIEM and telemetry assessment, including log coverage and data quality
- Identified risks and onboarding considerations for Managed SOC integration

SOC Transition Roadmap

A phased roadmap designed to guide a smooth transition to a Managed SOC, covering:

- Pre-SOC onboarding requirements and foundational uplift actions
- Short-term remediation activities addressing critical gaps
- Medium-term capability uplift aligned to Essential Eight and ISM expectations
- MSSP integration considerations, including roles, responsibilities, workflows and escalation paths
- Milestones and sequencing to support structured SOC enablement and value realisation

Benefits to Your Organisation

- Reduce MSSP onboarding risk by proactively identifying gaps
- Support board level assurance and risk discussions
- Align with relevant ASD and APRA expectations and remediation steps
- Make informed decisions through evidence-base vd readiness insights
- Establish a defensible RACI as part of MSSP onboarding

Why Lumen?

Lumen brings deep expertise in security operations, incident response and enterprise-scale monitoring, supported by proven methodologies aligned to international cyber security and risk standards. We provide independent, evidence-based advice focused on clarity, risk reduction and operational uplift to help leaders strengthen governance, improve readiness for Managed SOC engagements and build confidence with executives, boards and regulators.

Contact us to Schedule a Free Scoping Call

Book a scoping call with Lumen's security specialists to confirm your objectives. This first step gives you immediate clarity on scope and expected outcomes.

lumen.com | apac.mail@lumen.com

LUMEN