Lumen Cybersecurity Resilience Assessment

Benchmarking your current security posture to moot security improvement programs

Lumen's Cybersecurity Resilience Assessment benchmarks and sets the current baseline upon which improvement measures can be implemented, managed, monitored and performance measured. Our highly skilled and trained professionals can help you understand security risk and draw mitigation plans that aligns to your risk tolerance and appetite levels.

Aligning security objectives to business objectives

Incorporating a review of your business environment, our assessment will provide you with an overview of the organisation's security posture that is aligned to your business objective. This will enable an understanding of the organisation's business context, including primary processes, data types, location, IT service arrangements, suppliers, and legal and regulatory requirements, and how security measures applied in the organisation to enable it to meet its business objectives.

Establish security benchmark

Through our review, the organisation will gain visibility of its "crown jewels", and the measures implemented to protect them, including the understanding of whether the security measures are managed in-house or outsourced to third-parties. This sets the benchmark or baseline for improvement efforts.

Build Better

Following our assessment, we will help you strategise a security improvement plan that will facilitate the organisation to take a top-down, risk-based approach to optimise your security investments and protect the organisation's "crown jewels".

Typical compliance assessments

- ISO 27001
- NIST
- PCI DSS
- Privacy laws
- Regulatory requirements

  e.g. MAS TRM, Australia state-base CSF, ASD, ISM, Essential 8, APRA CPS234, etc.

LUMEN TECHNOLOGIES

Features and Specs

Gain oversight

- Driven by business objectives, to obtain oversight of information/cybersecurity posture of the organisation that impacts on its ability to meet its business strategies.

Manage threats and risk

- Know where to invest resources to protect the organisation's crown jewels.

Ensure compliance

- Support in the assessment and implementation of the organisation's legal, regulatory and contractual obligations.

Our Cybersecurity Resilience Assessment methodology

Step 1: Understand the business and core business function(s), business security context, covering governance, risk and compliance.

Step 2: Review business processes and security measures implemented through discussions, documentary evidence review and observation of action in practice.

Step 3: Determine maturity level based on COBIT's capability levels for processes. The COBIT framework provides guidance on the capability level of controls implemented to protect the organisation's "crown jewels" viewed from a maturity of 0 (no controls implemented) to 5 (controls are optimised).

Step 4: Draft a report that will provide all levels of the organisation from Senior Management to operational teams with the current view of the security posture and recommendations of a security improvement roadmap.

Step 5: Provide the organisation with a walkthrough of the review and next steps.

Why Lumen?

Partner with Lumen to build an effective managed security program that helps reduce your risk exposure and ease resource constraints. With our combination of in-house solutions, skilled people, and extensive networking, cloud, and managed services experience, we can be your single provider to augment and optimise your security team.

877-453-8353 | lumen.com | info@lumen.com

LUMEN TECHNOLOGIES