Cybesecurity Strategy

KAON SecurITy

t. NZ +64 9 570 2233 | t. VIC +61 3 9913 3248 | t. QLD +61 7 3194 3664 | t. NSW +61 2 9098 8206

www.kaonsecurity.co.nz | e. sales@kaonsecurity.co.nz | www.kaonsecurity.com.au | e. sales@kaonsecurity.com.au

Introduction

According to ISACA's annual State of Cybersecurity Survey report 2024, 55% of respondents indicated that their organisation is experiencing more cyber-attacks than a year ago, this calls for a more concerted and broad-based approach to protecting critical information assets.

Cybersecurity threats are dynamic and insidious, organisations therefore need to be agile in evaluating and modifying their cybersecurity priorities based on a sound risk management approach that factors in the latest intelligence and real-world incidents, and is informed by enterprise-wide lessons learned.

Understanding the capability of cybersecurity within an enterprise means comprehensively analysing the operational efficiency and effectiveness of actions taken; resiliency of the people, processes, or technology in use; maturity of practices; gap analyses; total cost of ownership and more, and doing it across the axis of risk.

While developing the cybersecurity strategy, organisations must consider standards, best practices and business goals.

A well-developed viable cybersecurity strategy, based on sound risk management practices, is critical to the defence of an organisation's assets. The strategy and associated implementation plan identifies the steps necessary to ensure that resources are allocated across the organisation as effectively as possible. It is a crucial roadmap that translates these priorities into actions in order to protect the organisation's most valuable assets.

Kaon Security assists organisations to build the foundation to a resilient and cyber-minded culture that is aimed at reducing risk. We work with organisations to develop a cybersecurity strategy that is realistic, achievable and tailored to suit their unique operational realities.

Why Create A Cybersecurity Strategy?

A cybersecurity strategy:

- Provides a proactive approach to risk
- Helps senior management prioritise investments to protect valuable information assets
- Provides visibility of the Information Technology environment
- Builds resilience in IT operations
- Reduces information security risk
- Promotes continuous improvement

Organisations Have Unique Requirements

Cybersecurity has few, if any, one-size-fits-all solutions. Each organisation is unique, as are its needs and goals. Although risks impact every enterprise, the ways in which they are affected are different, as is in the way in which they develop and deliver their cybersecurity strategy.

Cybersecurity Scorecard

The scorecard is used to create a dataset for illustrating a cybersecurity improvement programme (CIP) progress over time, by tracking the maturity of the current state of controls and the effect of future improvements and actions over time.

This illustrates and supports an organisation's cybersecurity roadmap and allows them to target specific areas for improvement based on their individual risk appetite and available resources (budget, people) within an agreed timeframe.

Cyber Security Strategy

Cybersecurity strategy typically builds on the scorecard analysis of current and future (desired) state of security, specific to the organisation.

The cybersecurity strategy covers the following areas:

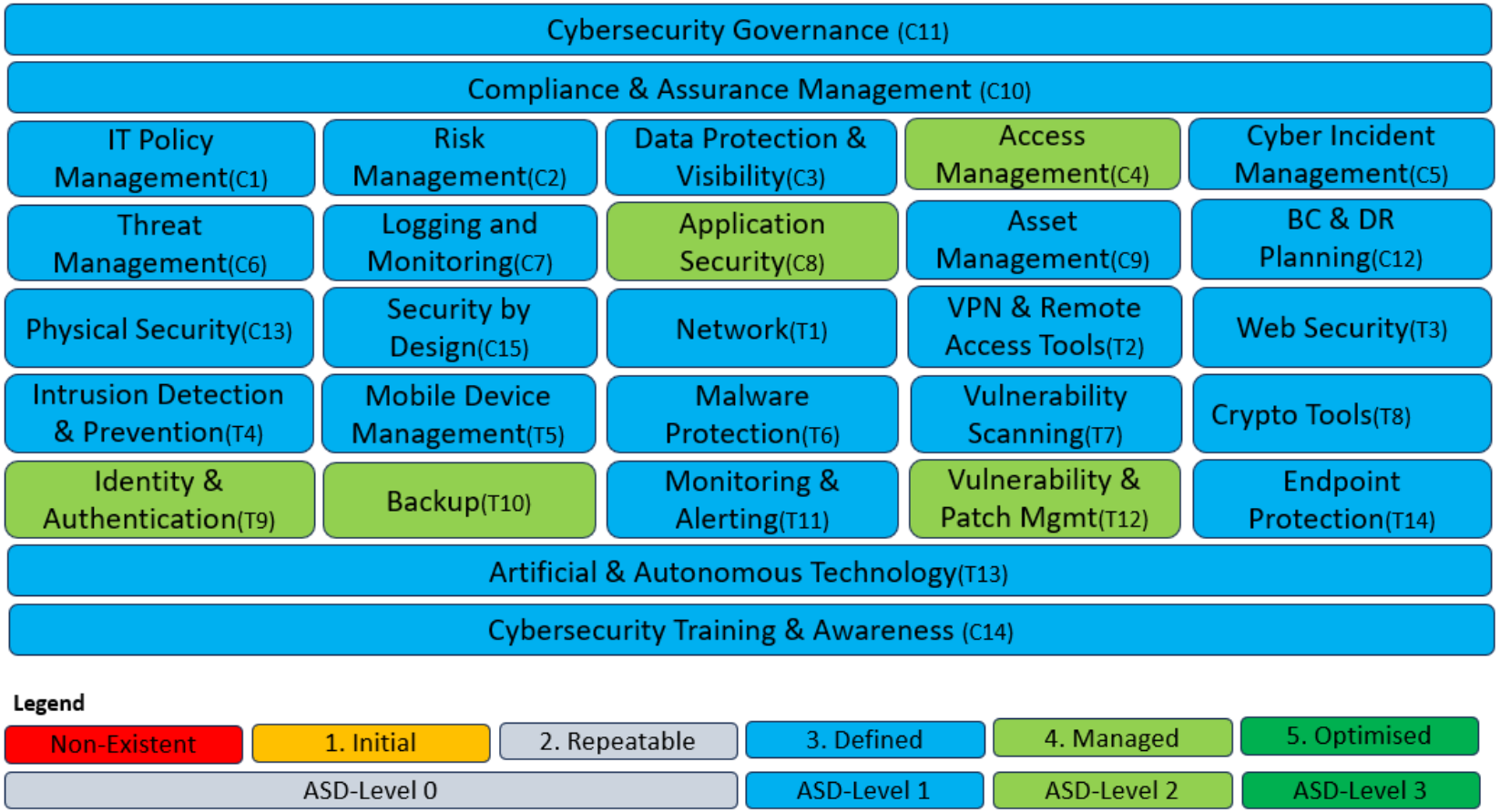
- Strategic goals, mission & vision
- Scope definition - aligned to a cybersecurity framework e.g. (ISO, NIST CSF, PDSP)
- Guiding principles
- Objectives as aligned to the goals
- Identify stakeholders
- Communication plan
- Cybersecurity needs and objectives
- Implementation strategy – identifying required initiatives
- Detailed cybersecurity implementation plan and roadmap

Additional components

- Risk register updates to capture identified gaps in current state
- Assisting to draft scope statements for initiatives

Cybersecurity Scorecard

The diagram below illustrates the essential elements of a robust cybersecurity program.



The scorecard measures 15 cybersecurity categories and 14 technical categories to provide an accurate summary of an organisation's deployed controls.

This example above illustrates a target state for an organisation with a target minimum of DEFINED, with ASD Essential-8 controls at MANAGED.

KAON SecurITy