SERVICE OVERVIEW

# Cybersecurity Maturity Assessment

Our Cybersecurity Maturity Assessment evaluates your organisations current security program looking beyond technical competency, in relation to its ability to protect, detect and respond to security threats.

Secarma have developed a simplified version of the NCSC Cyber Assessment Framework, tailoring the assessment to focus on responsive solutions, organisations can implement to become more robust.

## WHO IS IT FOR?

At Secarma we believe that all businesses, regardless of size should be given the opportunity to develop a thorough understanding of the risks they face and be given direction by a trusted advisor to improve their own cybersecurity maturity.

This assessment is for any organisation that wants to assess and improve their current security program to ensure they are prepared to deal with todays most advanced threats.

## HOW CAN WE HELP?

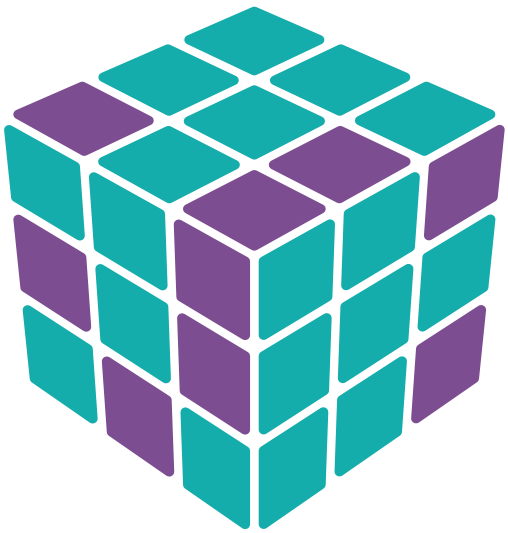
Many organisations have the intention to improve their cybersecurity, but simply don't know where to start or worry they may miss an area of concern. Secarma's CSMA mission is to simplify implementations that align cybersecurity practices with your organisational objectives and policies.

We will perform a gap analysis and risk assessment on your current security posture through an initial orientation meeting, a documentation review and interview workshops. This will give your organisation a deeper understanding, not only in the areas of security strategy you are successfully, but to what degree of maturity has been achieved and how to improve it.

## WHAT WE TEST

The Cybersecurity Maturity Assessment will evaluate an organisation's preparedness and grade their maturity in the following areas:

- **Risk Management:** Security policies ranging from organisational roles, security training, assessing risks and communicating security goals.
- **Security Protections:** Documenting and grading an organisation's technical enforcement of security policy.
- **Incident Detection:** Monitoring the essential services for security concerns which may impact the security of the systems and the effectiveness of security measures.
- **Minimising Impact:** An organisations ability to address incidents that are detected in terms of planning, testing, and backing up vital information.



0800 231 5977 secarma.com enquiries@secarma.com

SERVICE OVERVIEW

# Cybersecurity Maturity Assessment

In each maturity area we look at the following points:

### 1. RISK MANAGEMENT

a. Security Policy
b. Security Culture
c. Security Training
d. Supply Chain
e. Asset Management
f. Risk Management
g. Board-led Security
h. Security Roles

### 2. SECURITY PROTECTION

a. User Accounts
b. Access Control
c. Secure Configuration
d. Vuln Management
e. Penetration Testing
f. Network Segmentation
g. Data Management

### 3. INCIDENT DETECTION

a. Monitoring Coverage
b. Alert Generation
c. Abnormality Detection
d. Staff Capability
e. Threat Intelligence
f. Threat Hunting

### 4. MINIMISING IMPACT

a. Response Planning
b. Response Testing
c. Root Cause Analysis
d. Backups
e. Recovery Capability

## RESULTS

Post assessment the organisation will receive a report of findings, which offers a real world insight into areas of security in which the organisation may improve.