



## Cybersecurity Improvement Program

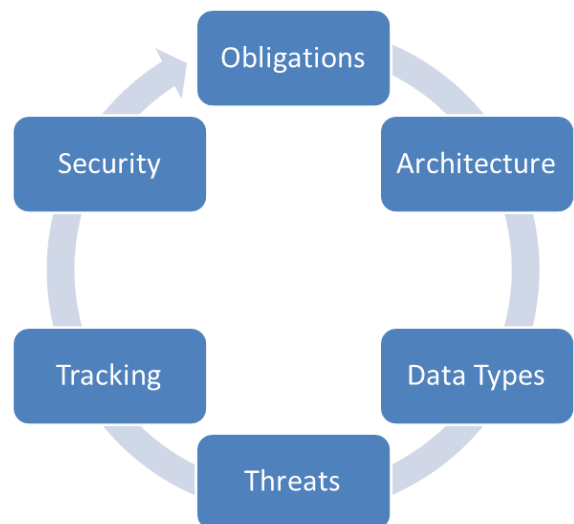
Our Cybersecurity Improvement Program (CIP) enables businesses to use technology to pursue new opportunities in a safe manner, and helps to protect the data assets that are key to an organisation interacting with customers, gaining insights, and operating their business.

Ultimately all the money invested in security is designed to protect data, which needs to be assessed for levels of value, sensitivity and criticality. Visibility of data is hard to maintain - location, access and distribution. Our comprehensive Cybersecurity Improvement Program is tailored to your organisation to deliver measurable and effective improvement to your organisation's cyber security posture. Using a modern data driven risk-based approach we enable you to know your data, risks, threats and the appropriate controls.

Often organisations have an aspiration to improve their security posture; however, due to resource constraints and existing workloads those aspirations fail to materialise. Finding the right mix of skills and expertise to deliver security improvement is challenging given that experience in diverse disciplines such as governance, architecture, network security and application security is a requirement.

The Cybersecurity Improvement Program is a 3 year collaborative exercise designed to take an organisation through a series of key initiatives so that it reaches an optimised state of security maturity.

For the duration of the program our Consultants are engaged each month with our clients to guide them through the program.



It is through close and long term partnerships that we ultimately achieve the best results, which enable executive management and other stakeholders to have confidence that they are addressing cyber risks in a measured and effective manner.

## Key Benefits Of The Program:

- Improved cyber security posture and maturity
- Access to experts well versed in communicating with business people on business risk, cyber security and other key topics
- Eliminate the challenge of sourcing the right mix of cyber security skills and experience required to deliver a program in-house
- High value structured security program designed to be delivered more cost effectively than running it in-house.
- Your agreed cyber security strategy is executed using a pragmatic and measured approach
- Existing investments in security controls can be streamlined and applied more effectively

## Program Overview – Key Elements

### On Site CIP Scoping Workshop

This first step of the program is exploratory and designed to review the current status and scope of cyber security within the organisation. We discuss the CIP process, agree high level objectives and determine the next steps.

Following this workshop Kaon Security will provide a report that contains:

- A high level executive summary
- Commentary on the current status and scope of cyber security within the organisation
- A high level program draft

### On Site CIP Tuning Workshop

A tuning workshop is held to review the output of the initial scoping workshop and assess any stakeholder feedback. With this completed we then agree on the final version of the program, priorities, roles and responsibilities, timelines and next steps.



## Deliverables

Following this workshop Kaon Security will provide a Cybersecurity Improvement Program plan document that contains:

- A high level executive summary
- Program scope
- Priorities
- Program customisation
- Roles and responsibilities
- Timelines

## Sample Program Outline

An example of the types of activities that may be incorporated within your CIP plan and program:

- Review
- Baseline
- Security architecture
- Risk assessment
- Scope and strategy
- Security advisory
- Security controls
- Security posture tracking
- Regular review

### Program Kick Off Meeting

- Introduce key contacts
- Confirm ongoing reporting arrangements
- Identify any constraints
- Commence program of work

### Ongoing Program Management

- Fortnightly - online cadence meeting
- Quarterly - on site review meeting to measure progress against the Cybersecurity Improvement Program

