MOBIUS
CONSULTING
Actualising change

CYBER SECURITY

MATURITY ASSESSMENT AND IMPROVEMENT SERVICES

Organisations need to ensure that they have identified their cyber-related risks and have implemented the appropriate controls required for the protection of their digital information assets from external threats. This includes ensuring that that they are adequately prepared to detect and respond to a cyber attack when it happens.

Our team of experts provide a cyber security assessment service that helps you to improve the overall maturity of your organisation's cyber security capability.

We start off by assessing the cyber security controls in your environment against good practices and standards. The assessment is followed by a gap analysis and the development of a remediation roadmap. This includes designing high level plans to enhance your organisations cyber security control maturity.

The end result? Improved cyber security maturity and a subsequent reduction in cyber security-related risks for your organisation.

WHY MOBIUS

The Mobius Consulting approach to assessing an organisations cyber security maturity is aligned to the NIST Cybersecurity Framework (CSF). Our assessment service enables organisations, regardless of size, or degree of technological sophistication, to understand the gaps which exist within its current cyber security capability.

We help you to ensure that key cyber security control deficiencies have been identified, and that practical and appropriate solutions can be implemented to improve the overall cyber security maturity of your organisation.

BENEFITS

Benchmark against leading practice framework

A holistic approach to cyber security across governance, people, process and technology

Improve overall cyber security maturity

Develop customised roadmaps and high level plans

Define cyber security roles and responsibilities

Understand current cyber security control gaps

PHASE 1: PLANNING

- Identify stakeholders and understand the business
- Understand critical business processes and supporting systems
- Gather all cyber security related documentation required
- Understand the existing cyber security process, functions and controls

PHASE 2: CURRENT STATE ASSESSMENT

- Review policies, procedures and other artefacts
- Assess each process and control area against the NIST CSF
- Assess the existing cyber security capabilities
- Review existing cyber security resourcing model and roles and responsibilities

PHASE 3: FUTURE STATE ARTICULATION

- Determine the to-be state based on organisational requirements and in consultation with key stakeholders
- Perform a gap analysis based on the current and desired state of maturity for the organisation
- Determine the actions and recommendations to reach the desired state of maturity

PHASE 4: REPORT AND ROADMAP

- Correlate the findings and develop a detailed report outlining the outcome of the assessment and improvement recommendations
- Determine the initiatives required to address the maturity gaps identified
- Develop the high-level roadmap to achieve the future state and improve maturity
- Develop the resourcing model and detail the roles and responsibilities for cyber security

PHASE 5: REMEDIATION

- Implement the initiatives identified to achieve the desired state of maturity
- Manage and monitor the improvement roadmap

MOBIUS
CONSULTING
Actualising change

CONTACT US NOW

Mauritius Office: +230 5297 0903 | Email: info@mobiusconsulting.mu | Website: mobiusconsulting.mu