MOBIUS INFORMATION SECURITY GAP ASSESSMENT AND ROADMAP

The Mobius Consulting Information Security gap assessment enables an organisation to evaluate the current state of their Information Security against an internationally recognised framework and enables the articulation of a desired future state and Information Security strategy.

Organisations undertaking an Information Security gap assessment can expect the outcomes to include a greater understanding and awareness of their current Information Security maturity, risks, and issues as well as insight into practical steps that can be followed to improve the maturity in line with the strategy of the organisation and address the risks and issues identified. The gap assessment aids in identifying the governance, people, processes and technologies required for realising an organisation's Information Security strategy and developing an Information Security programme capable of successfully executing this strategy.

Mobius Consulting utilises the International Organisation for Standardization's ISO27000 standard as the framework and guideline for our current state assessments and also utilise elements of COBIT 5 (Control Objectives for Information and related Technology) and ITIL (IT Infrastructure Library) where necessary. This approach allows an organisation to evaluate their current state maturity level and determine their desired maturity level against leading best practices. Alignment with internationally recognised frameworks also facilitates compliance with legislation such as POPI and provides comfort for auditors and risk management functions.

OUR INFORMATION SECURITY GAP ASSESSMENT AND ROADMAP SPANS THE FOLLOWING ASPECTS OF INFORMATION SECURITY:

- Information Security policy
- Organising information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- Systems acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity
- Compliance

For more information, contact Mobius Consulting on +27 21 20 111 20 or +27 10 590 6111
email info@mobiusconsulting.co.za or visit our website www.mobiusconsulting.co.za

The approach we follow during our information security gap assessments and roadmap development is illustrated and explained in the diagram and table below:

Discovery

- To provide context to our engagement, aid project efficiency and effectiveness, as well as to ensure accurate recommendations, which take into account all relevant factors, Mobius Consulting starts the engagement by performing an initial discovery of the organisation's information security environment and context.

Current state assessment

- During this phase we gather information relating to the current state of Information Security by means of interviews, workshops, and surveys; review of policies, procedures, and other artefacts; as well as review of internal and external audit reports and previous Information Security reviews and reports that may exist.
- Each control area is rated against the ISO standards based on the design and level of maturity of the controls in place.
- We utilise a proprietary assessment tool to capture the results of the gap assessment and score the specific controls detailed in ISO27000.
- The rating of each ISO control is averaged into a total control strength for each domain.

Desired future state articulation

- During this phase we engage with the key stakeholders to determine the desired future state information security maturity that is appropriate to the organisation and industry.
- This step facilitates discussion amongst the stakeholders and enables buy-in and agreement on the future state of information security that is appropriate to the organisation.

Roadmap development

- As preparation for this stage we correlate the findings and improvement areas noted across the various aspects of our current state assessment.
- The governance, process, people, and technology gaps between the current state and desired future state are grouped into logical projects and tasks.
- These projects and tasks are plotted onto a remediation roadmap which identifies the relative priority, dependencies, and indicative duration of each project / tasks

Remediation activities

- As a follow-on to the gap assessment Mobius Consulting can assist with resources and expertise that may be required for the implementation of the remediation roadmap.
- Examples of remediation activities that we could assist with include the formalisation of the Information Security governance framework and reference model, documentation of policies and standards, definition of processes and procedures, provision of Information Security personnel, etc.