MOBIUS
CONSULTING
Actualising change

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 a number of internationally recognised frameworks. The result is a holistic understanding of your current maturity in relation to Information Security, as well as a view of key Information Security gaps within the environment, from a Governance, People, Process and Technology perspective.

We conduct Information Security assessments in alignment with a number of international best practice frameworks, including:

- The ISO 27000 series
- NIST
- SWIFT Customer Security Controls Framework (CSCF)
- ITIL
- COBIT 5 & 2019
- A hybrid of frameworks, based on the context of Information Security within the organisation

By comparing your actual Information Security practices against industry leading best practices, companies can determine key Information Security gaps, and furthermore identify where vulnerabilities and risks are imminent.

But, more than that, an Information Security gap assessment provides a clear path forward for improving your Information Security posture.

THE BENEFITS OF AN INFORMATION SECURITY GAP ASSESSMENT

Understand the current state of your organisation's Information Security practices, across Governance, People, Process and Technology aspects.

Articulate the desired future state for Information Security, to ensure alignment with the Information Security Strategy as well as a broad range of Information and Cyber Security best practices, laws and regulations.

Identify initiatives required to improve Information Security and achieve the desired state for Information Security.

THE MOBIUS APPROACH TO
INFORMATION SECURITY GAP ASSESSMENTS

PLANNING AND DISCOVERY
To provide context to our engagement, aid project efficiency and effectiveness, as well as to ensure accurate recommendations, Mobius Consulting starts the engagement by performing an initial planning and discovery of the Information Security environment and context.

CURRENT STATE ASSESSMENT
We ascertain the current state of security practices within the environment, across governance, people, process and technology aspects. This is performed against a best practice standard for Information Security (or combination of), with a view to identify areas of improvement and remediation recommendations.

DESIRED FUTURE STATE ARTICULATION
During this phase we engage with the key stakeholders to determine the desired future state of Information Security maturity that is appropriate to the organisation, in alignment with their Information Security strategy and relevant best practices as well as laws and regulations.

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, people, process and technology gaps between the current state and desired future state are grouped into logical projects and tasks and are plotted onto a practical roadmap.

IMPLEMENTATION AND REMEDIATION
Using the remediation roadmap, we assist with driving implementation and hand-over of prioritised activities.

PHINITY PLATFORM INTEGRATION – CONDUCTING THE ASSESSMENT, CONTROL TRACKING, MONITORING AND REPORTING

MOBIUS
CONSULTING
Actualising change

CONTACT US NOW

Cape Town: +27 21 201 1120 | Johannesburg: +27 10 590 6111 | Email: info@mobiusconsulting.co.za | Website: mobiusconsulting.co.za