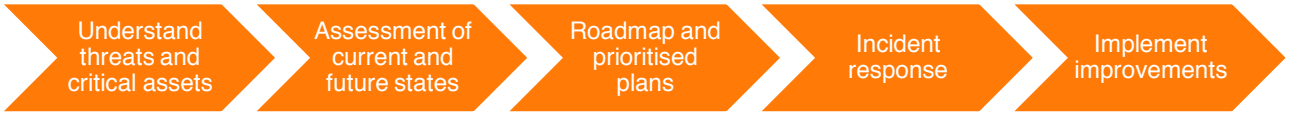
MOBIUS CYBERSECURITY APPROACH

The information security threat landscape has changed dramatically in recent times. Cyber related incidents are on the increase with ransomware, denial of service attacks (DoS) and highly organised cybercrime impacting organisations across the globe. Organisations are implementing new monitoring and response processes and adjusting their existing Information Security practices, controls and capabilities to cater for this new wave of threats. Whilst Cybersecurity is part of the organisations overall Information Security management, focus on Cybersecurity is required to ensure that cyber related risks are identified and mitigated so that the organisation is adequately prepared to detect, respond to, and recover from a Cybersecurity incident.

Mobius's approach to Cybersecurity ensures that investments and processes are sustainable and effectively mitigate risks. We:

- Assist organisations to understand the threats and identify critical assets and systems.
- Assess the existing capabilities required to continually identify, protect, detect, respond and recover from a cybersecurity incident.
- Develop a roadmap articulating the plans required to achieve a target future state required to mitigate cyber related risks. The roadmap includes remediation plans to address the gaps between the current and future states, and will typically include improvements to the existing Information Security practices, controls and technologies.

Our holistic and sustainable approach includes implementing governance required to support the changes, as well as processes that address the immediate requirement to effectively respond to an incident.



Details of each of the phases are on the next page.

For more information, contact Mobius Consulting on +27 21 201 1120 (CPT) or +27 10 590 6111 (JHB)
email info@mobiusconsulting.co.za or visit our website www.mobiusconsulting.co.za

Phase	Service	Description and deliverables
Understand threats and critical assets	Executive briefing	Our customised and industry specific briefings ensure that Executives gain an understanding of cybersecurity, industry specific risks and their role to initiate and support Cybersecurity.
	Critical asset ID and threat profiling	Mobius assists with the identification of critical assets and systems and the potential cyber-related threats that are applicable to the organisation.
Assessment of existing and future states	Cybersecurity assessment	The Mobius Cybersecurity assessment follows the NIST Cybersecurity Framework to provide organisations with a view of how prepared they are to effectively identify, detect, protect, respond and recover from cybersecurity incidents. It includes the articulation of the current and desired states of cybersecurity capabilities, as well as remediation requirements spanning people, process and technologies.
	Assessment of critical assets and systems	In order to identify critical asset and system related vulnerabilities Mobius provides the following services: • Attack path mapping - an analysis of how a real-life attacker could gain access to the organisation's critical assets and systems. • Infrastructure and system vulnerability assessments - testing the network infrastructure and critical systems for vulnerabilities. • Penetration testing - testing if vulnerabilities are exploitable.
Roadmap and prioritised plans	Cybersecurity roadmap planning	Mobius develop roadmaps required to remediate gaps and improve Cybersecurity. This details the overall remediation plans with timelines and all interdependent projects required.
Incident response	Response process development and testing	Mobius develop and implement incident response processes that integrate with existing organisational functions such as Crisis Management, BCM, Legal, HR and Public Relations. Mobius conduct Cybersecurity incident response simulations and Red Teaming exercises to test the effectiveness of controls, the incident response process, and awareness of individual's roles and responsibilities.
Implement improvements	Governance & process improvements	Mobius assists organisations with defining roles and responsibilities, training, changes to existing governance artefacts (policies and standards), changes to risk management processes, and updating the existing Information Security Management System (ISMS).
	Implement sustainable solutions	Mobius follows a holistic approach to solution implementations that includes governance, people, process and technology to ensure that the solution is sustainable and supports the objectives of reducing cybersecurity risks.