MOBIUS APPROACH TO INFORMATION RISK MANAGEMENT

Organisation's focus on information protection has intensified over the last few years. Key drivers include King 3, increased reputational, operational and financial risk relating to data breaches and legislative requirements including the Protection of Personal Information Act. With ever-increasing legislative and regulatory pressures to ensure information protection, this burden is set to continue increasing.

An essential starting point to effective information protection is an organisation-wide understanding of the risk profile of organisational information assets and a correlation to information systems in use. This understanding sets the platform for the selection, prioritisation and implementation of adequate treatment plans to adequately protect information assets. The Mobius Consulting approach to Information Risk Management (IRM) provides a holistic approach to:

- Identify information assets and attributes
- Perform information impact assessments and categorisation
- Perform information risk assessments
- Assess and select adequate and appropriate treatment plans
- Implement treatment plans
- Audit and monitor the effective sustainable implementation of treatment plans

The Mobius Consulting Information Risk Management (IRM) methodology includes a cycle of four key phases. Within the Information risk assessment phase, the key activities are expanded and are depicted in the diagram below.

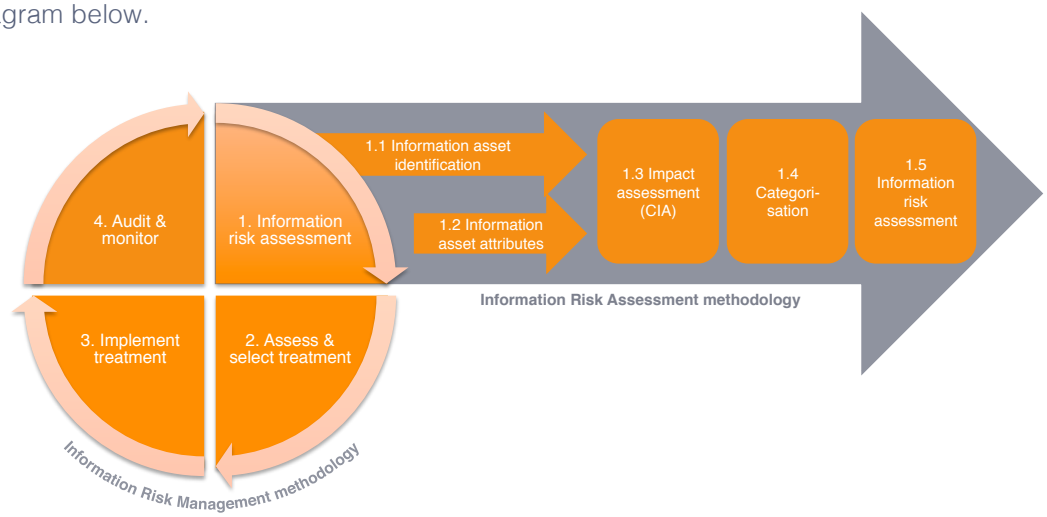

Figure 1: The Mobius Consulting Information Risk Management (IRM) methodology

The primary purpose of the Mobius Risk Assessment methodology is to establish the platform for effective and adequate protection of information assets. We recognise the value that this information has within the broader organisation and recommend and facilitate the sharing of Information Risk Assessment information at the conclusion of the Information Risk Assessment with other relevant organisational units responsible for:

- Business impact analysis (BIA)
- Capital planning and investment control
- Enterprise architecture (EA)
- System design
- Business contingency and disaster recovery planning

A MORE DETAILED BREAKDOWN OF THE ACTIVITIES WITHIN THE FOUR KEY PHASES OF THE MOBIUS IRM METHODOLOGY IS DESCRIBED BELOW:

1. Information Risk Assesment

- 1.1 Information asset identification: gain a high level of understanding of the business through discussion, existing documentation and investigation.
- 1.2 Gather information asset attributes: facilitated discussion to determine detailed assets attributes
- 1.3 Perform impact assesment: investigate the impact of information asset loss or compromise within the organisational context
- 1.4 Categorise information assets: determine the type of information associated with each asset (personal, internal, confidential or public)
- 1.5 Information Risk Assessment: evaluate the overall risk presented by each identified asset.

2. Assess & select treatment

- Assess current controls and implement appropriate additional controls in response to the risks highlighted in in the Information Risk Assessment.

3. Implement treatment

- Implement and enforce the controls selected during the "2. Assess & select treatment" phase.

4. Audit and monitor

- Periodically monitor and perform audits on the implementation and operating effectiveness of the treatment plans implemented in phase 3.