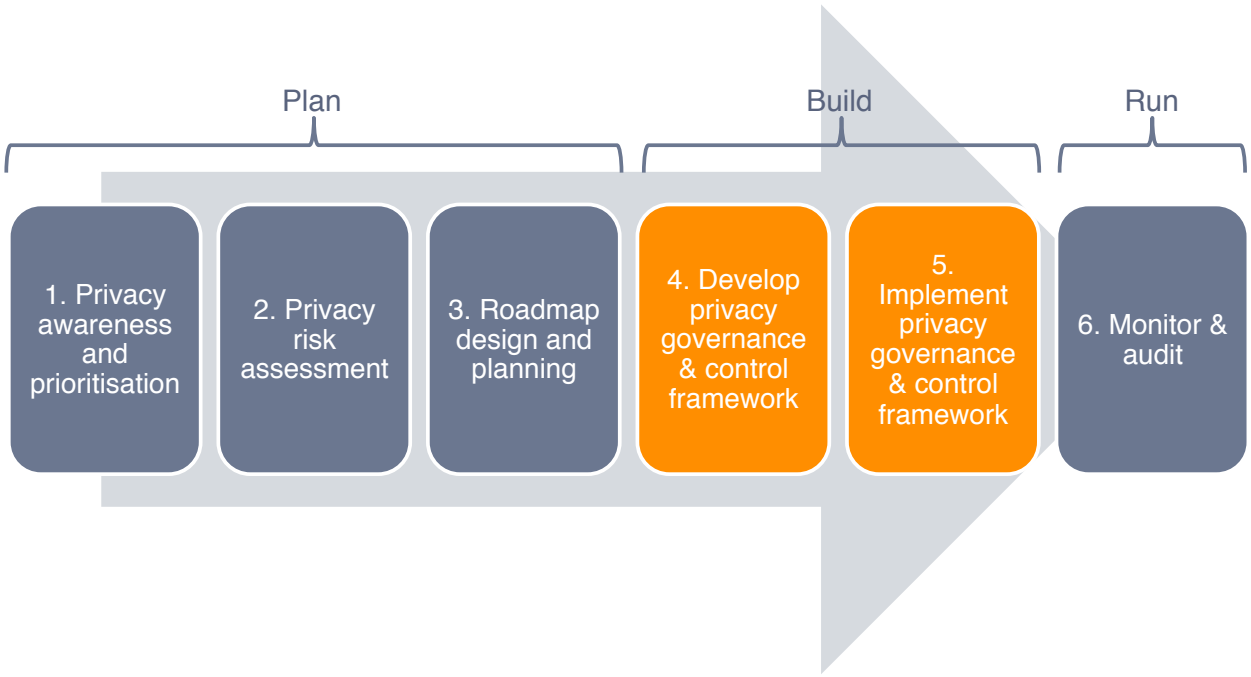
MOBIUS INFORMATION PRIVACY – REMEDIATION

In light of the enactment of the Protection of Personal Information Act (POPI), organisations are taking a pro-active approach in assessing and aligning their information processing practices with the Act's requirements. As part of an organisation's road to compliance we can assist our clients in defining the remediation actions they need to consider to align their information processing practices with POPI.

As depicted in the Mobius Consulting Information Privacy methodology below, the development and implementation of a Privacy governance and control framework are core components in our approach to preparing for POPI. *(NOTE: our team is able to provide insight and assistance in both the development and implementation phases of remediation):*



SUMMARY OF THE SCOPE OF OUR INVOLVEMENT IN REMEDIATION PLANNING AND IMPLEMENTATION

This summary is high-level and not an exhaustive list of remediation activities that Mobius Consulting has identified as categories, which most remediation activities fall into. We are in a position to assess and provide additional assistance or involvement required to assist our clients become compliant with POPI and related legislative requirements.

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

Category	Phase: Planning	Phase: Implementation
Training and awareness	(a) Identify training requirements that consider the organisation, third parties and stakeholders. (b) Develop a formal POPI training strategy and plan that considers the organisation, third parties and stakeholders.	(a) Create relevant content as per the defined POPI training plan (excluding development of software) (b) Deliver training modules as per the defined POPI training plan and/ or provide oversight during delivery of POPI training modules (to assist business ownership of POPI training (c) Create assessment material relevant to the defined POPI plan.
Business processes	(a) Identify business processes that require review and updating to align with fair and lawful processing requirements (business process analysis, interviews etc.) (b) Develop a privacy governance framework (considering policies, the need for relevant committees or structures to support POPI, communication and alignment with business) (c) Identify the requirements to align application forms, contracts, web forms and other points of personal information collection with fair and legal processing requirements	(a) Engage with business owners and stakeholders to identify solutions for aligning business processes with fair and lawful processing requirements (advise and provide assistance) (b) Implement the privacy governance framework. (as part of the privacy team) (c) Advise and assist to implement leading practice and reasonable steps to align application forms, contracts, web forms and other points of personal information collection with fair and legal processing requirements (note that third parties are managed separately from clients and employees)
Policies	(a) Identify the need for the creation of relevant policies to govern privacy and security practices within the organisation. (b) Identify existing privacy, security and other relevant organisational policies that require review and updating to align with privacy requirements.	(a) Develop required privacy and security policies to govern privacy and security practices within the organisation. (b) Review and update existing privacy, security and other relevant organisation policies that require review and updating to align with privacy requirements.
Third party management	(a) Assist with understanding the current third party management practices within the organisation. (b) Identify third party relationships that must be considered as part of the organisation's POPI compliance strategy. (c) Develop a comprehensive third party management framework.	(a) Advise and assist with implementing required actions to update third party management practices (legal expertise available through our outsourced partners) (b) See above. (c) Perform third party management actions as per the comprehensive third party management framework.
Information security	(a) Understand and identify security, system development and change requirements to enable information security.	(a) Understand and identify security, system development and change requirements through: • security assessments (ISO 27000) • vulnerability assessments • data discovery assessments

NOTE: implementation of the controls, policies and procedures listed in this document does not guarantee compliance with local or international privacy legislation. Organisations should align privacy related security controls with their information risk assessment, strategic objectives and the regulatory requirements applicable to their country, industry or organisation.