

## PRIVACY MANAGEMENT PROGRAM - AT A GLANCE

### A. BUILDING BLOCKS

<b>Organizational Commitment</b>	<b>a) Buy-in from the top</b>	Senior management support is key to a successful privacy management program and essential for a privacy respectful culture.
	<b>b) Privacy Officer</b>	<ul style="list-style-type: none"> <li>• Role exists and is fundamental to business decision-making process.</li> <li>• Role and responsibilities for monitoring compliance are clearly identified and communicated throughout the organization.</li> <li>• Responsible for the development and implementation of the program controls and their ongoing assessment and revision.</li> </ul>
	<b>c) Privacy Office</b>	<ul style="list-style-type: none"> <li>• Role is defined and resources are identified and adequate.</li> <li>• Organizational structure supports the ability of staff to monitor compliance and foster a culture of privacy within the organization.</li> <li>• Ensures privacy protection is built into every major function involving the use of personal information.</li> </ul>
	<b>d) Reporting</b>	Reporting mechanisms need to be established, and they need to be reflected in the organization's program controls.

<b>Program Controls</b>	<b>a) Personal Information Inventory</b>	The organization is able to identify: <ul style="list-style-type: none"> <li>• the personal information in its custody or control,</li> <li>• its authority for the collection, use and disclosure of the personal information, and the sensitivity of the personal information.</li> </ul>
	<b>b) Policies</b>	<ul style="list-style-type: none"> <li>i. Collection, use and disclosure of personal information, which include requirements for consent and notification</li> <li>ii. Access to and correction of personal information</li> <li>iii. Retention and disposal of personal information</li> <li>iv. Responsible use of information and information technology, including administrative, physical and technological security controls and role-based access</li> <li>v. Challenging compliance</li> </ul>
	<ul style="list-style-type: none"> <li><b>c) Risk Assessment Tools</b></li> <li><b>d) Training and education requirements</b></li> <li><b>e) Breach and incident management response protocols</b></li> <li><b>f) Service Provider management</b></li> <li><b>g) External communication</b></li> </ul>	

## B. ONGOING ASSESSMENT AND REVISION

<b>Oversight and Review Plan</b>	<b>a) Develop an oversight and review plan</b>	Privacy Officer should develop an oversight and review plan on an annual basis that sets out how s/he will monitor and assess the effectiveness of the organization's program controls.
<b>Assess and Revise Program Controls As Necessary</b>	<ul style="list-style-type: none"> <li><b>a) Update personal information inventory</b></li> <li><b>b) Revise policies</b></li> <li><b>c) Treat risk assessment tools as evergreen</b></li> <li><b>d) Modify training and education</b></li> <li><b>e) Adapt breach and incident response protocols</b></li> <li><b>f) Fine-tune service provider management</b></li> <li><b>g) Improve external communication</b></li> </ul>	