## PRIVACY MANAGEMENT PROGRAM - AT A GLANCE

### A. BUILDING BLOCKS

<table>
<thead>
<tr>
<th>Organizational Commitment</th>
<th>a) Buy-in from the top</th>
<th>b) Privacy Officer</th>
<th>c) Privacy Office</th>
<th>d) Reporting</th>
</tr>
</thead>
</table>
|                           | Senior management support is key to a successful privacy management program and essential for a privacy respectful culture. | • Role exists and is fundamental to business decision-making process.  
• Role and responsibilities for monitoring compliance are clearly identified and communicated throughout the organization.  
• Responsible for the development and implementation of the program controls and their ongoing assessment and revision. | • Role is defined and resources are identified and adequate.  
• Organizational structure supports the ability of staff to monitor compliance and foster a culture of privacy within the organization.  
• Ensures privacy protection is built into every major function involving the use of personal information. | Reporting mechanisms need to be established, and they need to be reflected in the organization’s program controls. |
### Program Controls

| a) Personal Information Inventory | The organization is able to identify:  
|                                  | • the personal information in its custody or control,  
|                                  | • its authority for the collection, use and disclosure of the personal information, and  
|                                  | • the sensitivity of the personal information. |
| b) Policies | i. Collection, use and disclosure of personal information, which include requirements for consent and notification  
|                                  | ii. Access to and correction of personal information  
|                                  | iii. Retention and disposal of personal information  
|                                  | iv. Responsible use of information and information technology, including administrative, physical and technological security controls and role-based access  
|                                  | v. Challenging compliance |

c) Risk Assessment Tools  
d) Training and education requirements  
e) Breach and incident management response protocols  
f) Service Provider management  
g) External communication

### B. ONGOING ASSESSMENT AND REVISION

| Oversight and Review Plan | a) Develop an oversight and review plan | 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. |

| Assess and Revise Program Controls As Necessary | a) Update personal information inventory  
b) Revise policies  
c) Treat risk assessment tools as evergreen  
d) Modify training and education  
e) Adapt breach and incident response protocols  
f) Fine-tune service provider management  
g) Improve external communication |