**Guide to preparation for completion of the POPIA & PAIA Compliance Framework Assessment Tools**

**Description of POPI Act toolkit compliance assessments scope of work**

**Introduction**

The overall objectives of the POPI Act (POPIA) & PAIA compliance assessments are to meet the requirements of POPIA &PAIA

* Help to identify risks of non-compliance with the POPI Act, including security assessments as also stipulated in Condition 7
* To help to ensure good policies, procedures and practices are available to protect personal information (Section 109(3)g)
* To minimise any negative impacts on the organisation should any instance of non-compliance occur
* Decide which assessments are to be completed: review the assessment titles and descriptions to help you in your choice.
* Decide who will complete each assessment: review who in your organisation or outside your organisation has the appropriate authority, area of responsibility, knowledge, skills and experience to best equip them as individuals or in a team of individuals to complete the selected assessments.
* Decide when the assessments will be completed (note most assessments take an hour two to complete if you have all the necessary supporting materials readily available)

**Assessment types**

The assessments are of two basic types:

* An assurance level assessment. This type explores multiple aspects of the focus area being assessed through the various questions and criteria included in the assessments
  + To achieve a High or Reasonable Assurance rating, there should be evidence provided of that level of achievement; the lower levels of assurance are Limited and Very Limited assurance
  + Some assessments are more easily addressed via a binary response which is available
  + In some assessments it is also possible to assign a priority level for each assessed item
* An inventory assessment. This type requires the identification of specific items, such as digital devices, policies, contracts.

**Summary**

Once the overall assessment exercise has been completed, an integrated risk report in two parts is produced for approval of the proposed remediation plan items. The table below provides an overview of the assessments. These will be used on a selective base according to the needs and preferences of the customer and the objectives of the assessment project.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Common or basic POPIA & PAIA compliance assessment tools for completion*** | | | | | | |
| **Tool name** | **Assessment Purpose** | **Usually completed by** | **Completion Action required** | **Assessment Output** | **Implications of not completing this assessment** | **Suggested preparation**  **Prior to completing the assessment** |
| POPIA Cloud Services Assessment Tool | Identify risks associated with the use of Cloud Services Providers; may be used to select suppliers; may be used with multiple suppliers | Information Technology management team with input from suppliers | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; 22 assessment items | Risk that Cloud Services and their providers will not comply with security safeguards as required in POPIA | Identify all Cloud Services and documented proof of approved certification schemes they support. If nil, complete the assessment per service provider. |
| POPIA Data Protection Assurance Assessment Tool | Covers policy for data protection, management responsibility and related topics | Enterprise Information Officer or Compliance Officer or Legal team | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph for 15 questions | Failure to adequately identify risks associated with policy management and implementation | Obtain copies of any existing policies, processes and procedures which refer to personal information (PI) protection. |
| POPIA Digital Devices Assessment Tool | Helps to identify all the digital devices which may be used to store personal information (PI); | Information Technology management team with input from suppliers | Implement appropriate remedial action in line with Info security and related policies | Has up to 24 data points per device identified presented in a table format | Failure to adequately identify risks associated with the use of digital devices | Prepare an inventory of all digital devices both owned by the organisation and provided by staff for use of organisation’s business (Bring Your Own Device) |
| POPIA Direct Marketing Assessment Tool | Assesses risks associated with DM consent, postal and electronic marketing | Marketing Officer with input from external suppliers | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; 15 assessment questions | Failure to adequately identify risks associated with Direct Marketing | Obtain copies of existing direct marketing policies, processes and procedures |
| POPIA Existing Contract & Policy Review Tool | Identifies all existing contracts and policies which may need amendment, replacement or updating | Procurement Officer  Business Unit heads  Corporate Services  Legal team | Identify all affected customer, supplier, employee and other contracts; create new contracts where required.  Identify all affected policies; create new policies where required. | Detailed inventory with assurance scale rating per item identified; reviews multiple parameters per contract or policy | Failure to adequately identify risks associated with Contracts & Policies | Obtain copies of existing contracts and policies which may have personal information related content |
| POPIA Governance Assessment Tool | Assesses accountability (Condition 1) across the organisation for ongoing compliance; may also be used as a project management tool | Enterprise Information Officer or Compliance Officer or Legal team with input from various internal stakeholders | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; 30 parameters assessed | Failure to adequately identify risks associated with Governance | Obtain copies of existing governance policies, processes and procedures relating to PI protection |
| POPIA Information Security Assessment Tool | Covers all the essential elements of cyber security | Information Technology management team with input from suppliers | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; 67 assessment questions;  Note: customer may opt to use the NSIT Cyber Security Framework Assessment as an alternative at no additional cost (98 assessment items) | Failure to adequately identify risks associated with Information Security (Cyber Security) | Obtain copies of existing policies, processes and procedures relation to PI cyber security |
| POPIA Information Sharing & Data Subject Access Assessment Tool | Assesses information sharing risks; also assesses readiness for data subject access requests | Enterprise Information Officer or Compliance Officer or Legal team with input from various internal stakeholders | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; 32 assessment items | Failure to adequately identify risks associated with Information Sharing & Data Subject Access | Obtain copies of existing policies, processes and procedures relating to Information Sharing & Data Subject Access |
| POPIA NIST Incident Response Readiness Assessment Tool | Identifies readiness of incident management capability | Information Technology management team with input from suppliers | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; 20 assessment items  Note: customer may opt to use the CREST incident response tool at no extra cost; 15 assessment items | Failure to adequately identify risks associated with Security Compromise / data breach response non-compliance | Obtain copies of existing policies, processes and procedures relating to Incident Response Readiness and data breach or loss or compromise management |
| POPIA Operator Selection Matrix Tool | Identifies Operators as required in Condition 7 to ensure appropriate contracts and oversight can be implemented | Procurement Officer with input from suppliers | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; creates an Operator inventory with up to 10 selection criteria per Operator | Failure to adequately identify risks associated with Operator appointment | Obtain copies of existing policies, processes and procedures relating to appointment rules for Operators |
| POPIA Personal Information Diagnostic Tool | Inventory tool which documents multiple dimensions of personal information | Data owners with input from internal stakeholders | Supply field and record level profile on all PI processed | Completed inventory down to field level of personal information processed; includes multiple compliance checks for POPIA conditions; has over 100 data points per record | Failure to adequately identify risks associated with identification of Personal Information processed by the organisation | Obtain copies of existing policies, processes and procedures relating to processing of PI. Includes mapping of PI; data owner responsibilities etc |
| POPIA Physical security risk management Tool | Identifies and assesses the physical risks of loss of personal information | Enterprise Risk Officer with input from internal stakeholders | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | A completed risk register; risks identified, sized, responses documented; documents 11 parameters per risk; includes an issue register | Failure to adequately identify risks associated with Physical security risks of loss of personal information | Obtain copies of existing policies, processes and procedures relating to Physical security risk management |
| POPIA Records Management Assessment Tool | Assesses organisation factors, policy, training, outsourcing, information standards and related topics | Enterprise Information Officer or Compliance Officer or Legal team with input from various internal stakeholders | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; 59 assessment items | Failure to adequately identify risks associated with cords Management policies and procedures | Obtain copies of existing policies, processes and procedures relating to Records Management |
| POPIA Responsible Party Assessment Tool | Assess performance of duties of the Responsible Party | Enterprise Information Officer or Compliance Officer or Legal team | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; 124 assessment items; | Failure to adequately identify risks associated with meeting the accountability for duties of the Responsible Party | Obtain copies of existing policies, processes and procedures relating to processing of PI |
| POPIA Social media Assessment Tool | Assesses social media platforms and related risks | Marketing Officer with input from external suppliers | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; 15 assessment items; provides inventory of social media profiles | Failure to adequately identify risks associated with use of Social media | Obtain copies of existing policies, processes and procedures relating to Social media management |
| POPIA Training needs assessment Tool | Assess staff general awareness and specialist training needs | Human Resources or Training executive | Identify training needs and how to address them | Eight parameters for multiple training needs to be identified | Failure to adequately identify risks associated with staff awareness training | Obtain copies of existing policies, processes and procedures relating to PI protection training |
| POPIA Web Site Assessment Tool | Assesses risks derived from the use of internal and external web sites | Marketing Officer with input from external suppliers | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; 47 assessment items | Failure to adequately identify risks associated with use of a public facing web site | Obtain copies of existing policies, processes and procedures relating to management of the corporate public web site(s) |
| PAIA Assessment | Identify readiness to comply with PAIA | Information Officer | Compare PAIA Manual to model template; identify suitability of support processes for Access Requests | List of remedial actions | Sanctions as defined in PAIA | Obtain copy of latest PAIA Manual (if any) and supporting access request process documents. |
| ***Optional or Advanced assessments*** | | | | | | |
| **Tool name** | **Assessment Purpose** | **Usually completed by** | **Completion Action required** | **Assessment Output** | **Implications of not completing this assessment** | **Suggested preparation**  **Prior to completing the assessment** |
| Business Continuity ISO-22301-Self-Assessment-checklist | Identify risks associated with availability of information and information systems; physical delivery environment; policies for business continuity | Enterprise Risk Officer with input from internal stakeholders | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Summary of 88 assessment questions with Yes/No count per sub-set of questions | Failure to adequately identify risks associated with Business Continuity availability of personal information | Obtain copies of existing policies, processes and procedures relating to Business Continuity |
| POPIA CAT 37 Questions Compliance Assessment Tool | Assess overall alignment with the POPI Act. Reviews all the relevant sections of the POPIA for Responsible Party and Operator | Enterprise Information Officer or Compliance Officer or Legal team | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting report with assurance level question count and graph; covers 37 key provisions of the POPIA | Failure to adequately identify risks associated with formal legal compliance mapped to specific sections of POPIA | Obtain copies of existing policies, processes and procedures relating to legal compliance with POPIA &PAIA |
| POPIA Conditions Assessment Tool | Ensure compliance with POPIA 8 conditions | Enterprise Information Officer or Compliance Officer or Legal team | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Evidence of POPIA conditions met for each business process involving PI | Failure to adequately identify risks associated with meeting the 8 conditions of the POPIA | Obtain copies of existing policies, processes and procedures relating to POPIA conditions |
| POPIA Consent Compliance Assessment Tool | Ensure compliance with POPIA consent management requirements | Enterprise Information Officer or Compliance Officer or Legal team with input from relevant stakeholders | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Evidence of POPIA conditions met for each business process involving consent as the basis for lawful processing | Failure to adequately identify risks associated with consent compliance management | Obtain copies of existing policies, processes and procedures relating to data subject consent management |
| POPIA CSA CAIQ Assessment Tool | Ensure compliance with POPIA Operator and security safeguards requirements | Information Technology management team with input from suppliers | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Evidence of over 200 assessed items for Cloud Services providers in lieu of certifications of POPIA compliance | Failure to adequately identify risks associated with the CSA approach to Cloud Services security. NOTE this is an alternative to the Cloud Services Assessment Tool for those preferring use of the CSA methodology | Obtain copies of existing policies, processes and procedures relating to Cloud Service provider assurance |
| POPIA Digital Devices User Survey Template | Ensure compliance with POPIA security safeguards requirements risk identification | Information Technology management team with input from staff | Staff should complete this survey when deployed to assist in disclosure of BYOD devices | Provides a profile of BYOD devices based on which security safeguards can be implemented in line with risk appetite | Failure to adequately identify risks associated with BYOD devices | Obtain copies of existing policies, processes and procedures relating to BYOD device management |
| POPIA Internal data process flow assessment Tool | To support a better understanding of the processing of PI internally in the organisation | Business process owners and PI custodians | Complete the mapping of PI flows or provide existing documentation of such | Provides a matrix of internal PI flows per business process allowing improved risk management | Failure to adequately identify risks associated with internal flow of personal information | Obtain copies of existing policies, processes and procedures relating to PI process flows |
| POPIA NIST Cyber Security Assessment Tool | Ensure compliance with POPIA security safeguards requirements risk identification | Information Technology management team with input from suppliers | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Self-documenting assessment of 98 questions.  Provides an alternative to the Information Security Assessment Tool | Failure to adequately identify risks associated with Cyber Security. Note: this is an alternative to the Information Security Assessment Tool which is based on the UK Government Cyber Essentials framework | Obtain copies of existing policies, processes and procedures relating to Cyber Security assessments |
| POPIA Operator Assessment Tool | Ensure compliance with POPIA Operator management requirements | Operator representatives | Operators should complete this assessment to demonstrate they can provide POPIA-compliant services | Self-documenting assessment of 48 compliance duties of Operators to demonstrate their compliance.  Can be used to support Operator selection, appointment and monitoring | Failure to adequately identify risks associated with Operator appointments | Obtain copies of existing policies, processes and procedures relating to Operator compliance assessments |
| POPIA Privacy Notice Assessment Tool | Ensure compliance with POPIA transparency management requirements | Marketing Officer | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Uses 12 assessment parameters for a privacy notice | Failure to adequately identify risks associated with compliant privacy notices | Obtain copies of existing policies, processes and procedures relating to privacy notices |
| POPIA Processing Lawfulness Assessment Tool | Ensure compliance with POPIA lawfulness management requirements | Enterprise Information Officer or Compliance Officer or Legal team | Complete the assessment and ensure actions taken to change the assurance level in line with risk appetite | Documents eight criteria with supporting comments to support lawful processing as per POPIA sections 9 to 11 | Failure to adequately identify risks associated with meeting the POPIA requirements for lawful processing | Obtain copies of existing policies, processes and procedures relating to Processing Lawfulness Assessment |

**For further information on this document please contact your project consultant.**

**Correct as at 21 October 2019**