



YOUR STARTING POINT

Know where you stand.

Example Company (Pty) Ltd

Prepared for Example Owner | 18/10/2026

38%

SELF-ASSESSMENT SCORE

30 responses need review. 10 marked Not sure.

Your answers indicate areas to review before relying on your current controls. Start with Purpose Specification, Further Processing, Security Safeguards. The score reflects reported controls, not verified evidence.

A report to use, not a certificate.

Use this report to brief management, assign actions and prepare for a discussion with a qualified legal adviser. It covers 40 self-reported controls across eight POPIA areas. It does not establish legal compliance, constitute legal advice or replace a context-specific legal assessment.

Inside: your section scores, a prioritised action list, a practical 30/60/90-day starting plan and all 40 question-level findings.

Not assessed in depth: special personal information, children's information, cross-border transfers, direct marketing, prior authorisation and industry-specific rules. Ask your adviser which additional requirements apply.

Reference: assessment1 | Questionnaire: 2026-10-18



01 / EXECUTIVE BRIEF

The picture by section.

Accountability 50%



Processing Limitation 40%



Purpose Specification 30%



Further Processing 30%



Information Quality 50%



Openness 40%



Security Safeguards 30%



Data Subject Participation 30%



How scoring works: Yes = 1, Partially = 0.5, No or Not sure = 0. Each section contains five questions. The overall score is the average of the eight section percentages.

Below 50%: priority review. 50% to 74%: needs attention. 75% or above: stronger reported controls. These are product thresholds, not statutory compliance grades. A serious individual gap can matter even when the overall score is high.



02 / NEXT ACTIONS

Start with what matters.

01**Security Safeguards | Not in place**

Review technical and organisational safeguards against your actual risks and assign owners for improvements.

02**Security Safeguards | Not sure**

Document and test an incident response process covering detection, containment, assessment and notification.

03**Accountability | Partially in place**

Check the Information Officer's registration record and retain evidence from the Information Regulator.

04**Security Safeguards | Partially in place**

Review written operator arrangements for security obligations, responsibilities and incident reporting.

A practical first 90 days

Days 1-30: validate the gaps with evidence, name an accountable owner and address urgent safeguards or active incidents. Days 31-60: agree policies, notices, operator terms and request procedures. Days 61-90: train the team, test the changes and schedule a review. Your adviser should tailor scope and timing.



03 / DETAILED FINDINGS / 01

Accountability

Section score: 50%. Review the answers and supporting evidence with your team.

Q1 / In place

Has your organisation identified its Information Officer and documented their responsibilities?

Next step: Maintain evidence that this control is in place and check that it operates effectively.

Q2 / Partially in place

Has your Information Officer completed the mandatory registration with the Information Regulator?

Next step: Check the Information Officer's registration record and retain evidence from the Information Regulator.

Q3 / Not in place

Does your organisation have a documented POPIA compliance framework or policy?

Next step: Create a practical compliance framework with a named owner, review dates and a management approval record.

Q4 / Not sure

Are staff who handle personal information trained on POPIA obligations?

Next step: Deliver role-specific staff training and keep attendance, materials and refresher dates.

Q5 / In place

Does your organisation maintain a record of all personal information processing activities?

Next step: Maintain evidence that this control is in place and check that it operates effectively.



03 / DETAILED FINDINGS / 02

Processing Limitation

Section score: 40%. Review the answers and supporting evidence with your team.

Q6 / Partially in place

Does your organisation only collect personal information that is adequate, relevant and not excessive for its stated purpose?

Next step: Review each collection field and remove information that is unnecessary for the documented purpose.

Q7 / Not in place

Where you rely on consent, do you obtain and record informed, specific and voluntary consent before processing?

Next step: Where consent is the lawful basis, record how informed, specific consent is obtained and evidenced.

Q8 / Not sure

Do you have documented lawful grounds for each category of personal information you process?

Next step: Record the applicable section 11 lawful ground for each processing activity and ask legal counsel to review it.

Q9 / In place

Do you collect personal information directly from the data subject wherever possible?

Next step: Maintain evidence that this control is in place and check that it operates effectively.

Q10 / Partially in place

Do you have a process to handle withdrawal of consent by data subjects?

Next step: Provide a clear withdrawal route and define how consent-based processing stops after withdrawal.



03 / DETAILED FINDINGS / 03

Purpose Specification

Section score: 30%. Review the answers and supporting evidence with your team.

Q11 / Not in place

Is the purpose for collecting personal information clearly defined before collection begins?

Next step: Write down a specific purpose before collecting information and assign an owner to approve changes.

Q12 / Not sure

Are data subjects informed of the purpose for which their information is collected?

Next step: Review the collection notice so people understand the purpose and relevant disclosures at collection.

Q13 / In place

Do you retain personal information only for as long as necessary to fulfil the stated purpose?

Next step: Maintain evidence that this control is in place and check that it operates effectively.

Q14 / Partially in place

Do you have a documented data retention and disposal policy?

Next step: Adopt a retention schedule showing record types, periods, owners and approved disposal methods.

Q15 / Not in place

Are records securely destroyed or de-identified once the retention period expires?

Next step: Test secure deletion or de-identification and keep an auditable disposal record.



03 / DETAILED FINDINGS / 04

Further Processing

Section score: 30%. Review the answers and supporting evidence with your team.

Q16 / Not sure

Do you assess whether any secondary use of personal information is compatible with the original collection purpose?

Next step: Use a documented compatibility check before personal information is reused for another purpose.

Q17 / In place

Do you assess compatibility and the applicable legal conditions before using personal information for another purpose?

Next step: Maintain evidence that this control is in place and check that it operates effectively.

Q18 / Partially in place

Do you have controls to prevent personal information from being used for undisclosed purposes internally?

Next step: Restrict access by role and review whether internal use matches the disclosed purpose.

Q19 / Not in place

Do you have agreements with third parties that restrict how they may use personal information you share with them?

Next step: Review recipient and operator terms to limit use, onward sharing and unauthorised processing.

Q20 / Not sure

Do you conduct due diligence on third parties before sharing personal information with them?

Next step: Check third parties' safeguards, contracts and intended use before sharing personal information.



03 / DETAILED FINDINGS / 05

Information Quality

Section score: 50%. Review the answers and supporting evidence with your team.

Q21 / In place

Do you have processes to ensure that personal information is accurate, complete and up to date?

Next step: Maintain evidence that this control is in place and check that it operates effectively.

Q22 / Partially in place

Do you provide data subjects with a mechanism to update their personal information?

Next step: Make the correction route easy to find and explain how identity and requested changes are verified.

Q23 / Not in place

Do you validate personal information at the point of collection?

Next step: Add proportionate validation at collection and monitor recurring data quality issues.

Q24 / Not sure

Do you have a process to correct or delete inaccurate personal information upon request?

Next step: Document the correction or deletion request workflow, including verification, exceptions and response records.

Q25 / In place

Are quality control checks performed regularly on personal information you hold?

Next step: Maintain evidence that this control is in place and check that it operates effectively.



03 / DETAILED FINDINGS / 06

Openness

Section score: 40%. Review the answers and supporting evidence with your team.

Q26 / Partially in place

Do you have a publicly accessible Privacy Notice that complies with POPIA requirements?

Next step: Review your privacy notice against the collection and notification requirements applicable to your activities.

Q27 / Not in place

Does your Privacy Notice clearly describe the categories of personal information you collect?

Next step: Compare the notice with your processing register so it accurately describes the information you collect.

Q28 / Not sure

Do you notify data subjects of any changes to your Privacy Notice?

Next step: Define when processing changes require updated notices or further notification and record the decision.

Q29 / In place

Do you have a PAIA Manual published as required by the Promotion of Access to Information Act?

Next step: Maintain evidence that this control is in place and check that it operates effectively.

Q30 / Partially in place

Is your contact information for privacy queries clearly displayed and accessible?

Next step: Publish a working privacy contact route and test that requests reach the right accountable person.



03 / DETAILED FINDINGS / 07

Security Safeguards

Section score: 30%. Review the answers and supporting evidence with your team.

Q31 / Not in place

Do you have documented technical and organisational security measures to protect personal information?

Next step: Review technical and organisational safeguards against your actual risks and assign owners for improvements.

Q32 / Not sure

Do you have a documented data breach response plan?

Next step: Document and test an incident response process covering detection, containment, assessment and notification.

Q33 / In place

Do you report data breaches to the Information Regulator and affected data subjects within the required timeframe?

Next step: Maintain evidence that this control is in place and check that it operates effectively.

Q34 / Partially in place

Do you have signed data processing agreements with all operators who process personal information on your behalf?

Next step: Review written operator arrangements for security obligations, responsibilities and incident reporting.

Q35 / Not in place

Do you conduct regular security risk assessments on systems that hold personal information?

Next step: Schedule risk reviews for systems holding personal information and track each agreed treatment.



03 / DETAILED FINDINGS / 08

Data Subject Participation

Section score: 30%. Review the answers and supporting evidence with your team.

Q36 / Not sure

Do you have a documented process to respond to data subject access requests within the prescribed timeframe?

Next step: Create an access request procedure covering identity checks, records searches, applicable deadlines and exceptions.

Q37 / In place

Do you have a process to handle requests for correction or deletion of personal information?

Next step: Maintain evidence that this control is in place and check that it operates effectively.

Q38 / Partially in place

Do you have a complaints process for data subjects who believe their POPIA rights have been violated?

Next step: Create an accessible complaints route, assign an owner and retain the response and escalation record.

Q39 / Not in place

Do you have a mechanism to allow data subjects to object to processing of their personal information?

Next step: Provide a practical objection mechanism and assess objections against the applicable processing ground.

Q40 / Not sure

Can data subjects easily request that their personal information be deleted once it is no longer needed?

Next step: Make deletion requests easy to submit and define how lawful retention and other exceptions are assessed.



04 / LEGAL DISCUSSION

Turn findings into a plan.

Bring this report and evidence of your current controls to your selected legal partner. Ask them to validate the gaps, identify the requirements specific to your organisation and agree a prioritised remediation scope.

Which findings require urgent action?

Which additional POPIA or PAIA requirements apply to our activities?

What evidence should we retain for each control?

Who owns the legal, operational, HR and technical work?

What are the agreed deliverables, fees and review dates?

Your referral does not create a professional engagement. Availability, scope and fees are agreed directly with the legal partner.

Official reference sources: Information Regulator, POPIA resources: <https://infoeregulator.org.za/popia/> and PAIA resources: <https://infoeregulator.org.za/paia/>. This questionnaire is a starting point and does not cover every legal obligation.