GUIDE TO ISRS 4400 ENGAGEMENTS ON THE PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013 ("POPIA")

For Business Accountants in Practice (SA)

saiba
SOUTHERN AFRICAN INSTITUTE
FOR BUSINESS ACCOUNTANTS

For further information on this guide, please email technical@saiba.org.za. Registered SAIBA members in good standing may download this publication from the SAIBA website: http://www.saiba.org.za.

The mission of The Southern African Institute for Business Accountants NPC (SAIBA) is to serve the public interest, strengthen the accountancy profession in Southern Africa and contribute to the development of a strong regional economy by establishing and promoting adherence to high-quality professional standards, furthering co-operation on such standards and speaking out on public interest issues where the profession's expertise is most relevant. This will enable SAIBA to deliver trusted advisors to Southern African small business and support staff to big business.

Table of Contents

1. INTRODUCTION

Sections 2 to 38, 55 to 109, 111 and section 114(1), (2) and (3) of the Protection of Personal Information Act, 4 of 2013 (“POPIA”) commenced on 1 July 2020.

These sections form the core provisions of POPIA and pertain to, amongst others, the processing of personal information, the processing of special personal information, the Information Officer, direct marketing by means of unsolicited communications, flow of information outside of South Africa and enforcement of POPIA.

All forms of processing of personal information must, in terms of section 114(1) of POPIA, conform with POPIA by 1 July 2021. However, it stands to reason that, in preparation for the aforesaid deadline, Members should attempt to comply with the provisions of POPIA as soon as possible.

This Guide to Engagements on the Protection of Personal Information Act, 4 of 2013 (“POPIA”) for Business Accountants in Practice (“this Guide”) was commissioned by SAIBA to provide guidance to members on performing services to clients in relation to clients’ readiness for POPIA.

Only those SAIBA members that have been awarded the designation Business Accountants in Practice (SA) / BAP(SA) may perform a ISRS4400 engagement for clients. Where the Guide refers to “member” the meaning is that of a BAP(SA) designated member.

This guide merely provides members with useful templates in relation to the responsible engagement. You hereby absolve SAIBA and its employees, officers, directors, contractors and agents (“the Indemnified Parties”) from all liability and indemnify them from any claim for damages, penalties or loss of whatever nature (including but not limited to consequential damages or special damages) arising from your use of this Guide and/or the templates contained herein.

Nicolaas van Wyk

CEO

September 2020

2. OVERVIEW OF ISRS 4400: AGREED UPON PROCEDURES

2.1. The International Standard on Related Services 4400[1] (ISRS4400 or ISRS) deals with: (a) the member's responsibilities when engaged to perform an agreed-upon procedures (AUP) Engagement; and (b) the form and content of the agreed-upon procedures report.

2.2. This ISRS applies to the performance of agreed upon procedures engagements on financial or non-financial subject matters.

2.3. ISRS is issued by the International Audit and Assurance Standard Boards (IAASB) and is prescribed by SAIBA whenever a member performs an AUP engagement.

2.4. The revised ISRS 4400 is effective 1 January 2022, however SAIBA encourages early adoption. This Guide is based on the revised ISRS4400.

2.5. According to the ISRS4400, in an agreed-upon procedures engagement the member performs the procedures that have been agreed upon by the member and the engaging party where the engaging party has acknowledged that the procedures performed appropriate for the purpose of the engagement. The member communicates the agreed-upon procedures performed and the related findings in the agreed-upon procedures report. The engaging party and other intended users consider for themselves the agreed upon procedures and findings reported by the member and draw their own conclusions from the work performed by the member.

2.6. ISRS4400 details the following concepts and requirements of an AUP engagement:

- Definitions;
- Conduct of an Agreed-Upon Procedures Engagement,
- Relevant Ethical Requirements;
- Professional Judgment;
- Engagement Level Quality Control;
- Engagement Acceptance and Continuance;
- Agreeing the Terms of the Engagement;
- Performing the Agreed-Upon Procedures;
- Using the Work of a Practitioner's Expert;
- The Agreed-Upon Procedures Report;

---

[1] https://www.iaasb.org/publications/international-standard-related-services-isrs-4400-revised

- Undertaking an Agreed-Upon Procedures Engagement Together with Another Engagement;
- Documentation that should be kept.

2.7. The practitioner shall have an understanding of the entire text of this ISRS including its application and other explanatory material, to understand its objectives and to apply its requirements properly.

2.8. ISRS4400 includes illustrative engagement letters for an agreed-upon procedures engagement, and illustrations of agreed-upon procedures reports.

2.9. The value of an agreed-upon procedures engagement performed in accordance with this ISRS results from: (a) The practitioner's compliance with professional standards including relevant ethical requirements; and (b) Clear communication of the procedures performed and the related findings.

2.10. An agreed-upon procedures engagement is not an audit, review or other assurance engagement.

2.11. An agreed-upon procedures engagement does not involve obtaining evidence for the purpose of the practitioner expressing an opinion or an assurance conclusion in any form.

3. AGREEING THE ENGAGEMENT

3.1. All engagements between members and their clients should be performed in terms of applicable statutory requirements, common law principles relating to care, skill and diligence and SAIBA’s code of conduct and ethics.

3.2. The member should not accept the engagement unless the member understand the purpose of the engagement, and the terms of the engagement have been agreed with the client, including:

3.2.1. the scope of the engagement and the services to be provided by the member;

3.2.2. the duties and responsibilities of the client, including the duty to provide the member with all information that the member reasonably requires to perform the engagement, and which is true and correct in all respects; and

3.2.3. the fees payable to the members for the engagement.

3.3. The procedures should be appropriate, the members should have access to necessary information, and any findings should be able to be described clearly.

3.4. The agreed terms of engagement should be recorded in a letter of engagement or other suitable written agreement prior to the commencement of any work, and

include reference to: the subject matter; purpose, responsible party; engaging party; ethical requirements; independence statement; nature of engagement; appropriateness of procedures; addressee; nature, timing and extent of procedures; form and content of the report.

3.5. **Appendix 1** includes a template engagement letter.

3.6. Before using the template, the member should ensure that the document is amended to reflect their requirements, the requirements of the client and to include any other additional services that the member will provide.

4. CONDUCTING THE ENGAGEMENT

4.1. The member should communicate with management or those charged with governance of the client during the course of the engagement on all matters which, in the member's professional judgment, are relevant to the engagement.

4.2. The member should obtain an understanding of the following matters sufficient to enable the member to assess the client's preparedness for POPIA:

4.2.1. the nature of the clients business;

4.2.2. the client's internal and external policies pertaining to the processing of personal information;

4.2.3. the identity and the role of the client's information officer and deputy information officers;

4.2.4. the manner in which the client collects and retains personal information and whether the client has any procedures in place governing the internal processing of personal information;

4.2.5. the client's retention procedures;

4.2.6. the security safeguards employed by the client;

4.2.7. whether any personal information is being transferred by the client; and

4.2.8. all systems and software in place.

4.3. In addition, in accordance with good practice, the member should obtain written representations from the management on the relevant matters.

4.4. **Appendix 2** provides, to this end, a template representation letter. The template can be sent direct to the client (with the appropriate amendments).

4.5. This template is drafted to cater for compliance with all of the sections of POPIA. Not all of the sections will apply to each and every client and care should be taken to ensure that the inapplicable sections are deleted.

4.6. If, in the course of the engagement, the member becomes aware that the records, documents, representations or other information provided by management are incomplete, inaccurate or otherwise unsatisfactory, the member shall bring that to the attention of management and request the additional or corrected information.

4.7. If the member is unable to complete the engagement because management has failed to provide the requested representations, documents or other information, the member shall withdraw from the engagement and inform management of the reasons for withdrawing in writing.

5. CONCLUDING THE ENGAGEMENT: THE FACTUAL FINDINGS REPORT

5.1. Following the member's enquiries and observations, and upon receipt of all of the required information (which is carefully documented), the member will issue his report on the factual findings.

5.2. Documentation should include: (a) the written terms of engagement and, if applicable, the agreement of the engaging party as to modifications to the procedures; (b) the nature, timing and extent of the agreed-upon procedures performed; and (c) the findings resulting from the agreed-upon procedures performed.

1.1. The findings report shall be in writing and shall not express an opinion on the client's compliance with POPIA but shall identify the areas of weakness and propose steps to rectify them.

1.2. **Appendix 3** provides a template that can be utilised by the member for the report. The template must be adapted by the member to ensure that the appropriate findings are included and the inapplicable sections are deleted.

6. APPENDIX 1: ILLUSTRATIVE ENGAGEMENT LETTER

[TO BE PLACED ON MEMBER'S LETTERHEAD]

MANAGEMENT / THE BOARD OF DIRECTORS
[NAME OF CUSTOMER]
[ADDRESS]

OUR REF.: [INSERT]
[DATE]

Dear Sirs,

PROTECTION OF PERSONAL INFORMATION ACT, 3 OF 2013, READINESS ASSESSMENT: ENGAGEMENT LETTER

We would be pleased to accept your instruction.

This letter sets out the terms and conditions upon which we will provide the services set out hereunder and the limitations of such services.

You have requested that we perform an agreed-upon procedures engagement as a readiness assessment to the **PROTECTION OF PERSONAL INFORMATION ACT, 3 OF 2013 (POPIA)**. This letter is to confirm our understanding of the terms and objectives of our engagement and the nature and limitations of the services that we will provide.

Our engagement will be conducted in accordance with the International Standard on Related Services (ISRS) 4400 (Revised), Agreed Upon Procedures Engagements. In performing the agreed-upon procedures engagement, we will comply with International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which does not require us to be independent.

An agreed-upon procedures engagement performed under ISRS 4400 (Revised) involves our performing the procedures agreed with you, and communicating the findings in the agreed-upon procedures report. Findings are the factual results of the agreed-upon procedures performed. You and if relevant other parties acknowledge that the procedures are appropriate for the purpose of the engagement. We make no representation regarding the appropriateness of the procedures. This agreed-upon procedures engagement will be conducted on the basis that [**Responsible Party**] is responsible for the subject matter on which the agreed-upon procedures are performed. Further, this agreed-upon procedures engagement is not an assurance engagement. Accordingly, we do not express an opinion or an assurance conclusion.

The procedures that we will perform are solely for the purpose of assisting you in determining your readiness to implement relevant POPIA requirements. Accordingly, our report will be addressed to you and our report may not be suitable for another purpose.

1. **OBJECTIVE AND SCOPE OF ENGAGEMENT**

1.1. Sections 2 to 38, 55 to 109, 111 and section 114(1), (2) and (3) of the Protection of Personal Information Act, 4 of 2013 ("POPIA") would commence on 1 July 2020.

1.2. All forms of processing of personal information must, in terms of section 114(1) of POPIA, conform with POPIA by 1 July 2021.

1.3. The purpose of our engagement is to assess the entity's readiness for POPIA and report on our factual findings.

1.4. In order to do so, you acknowledge and agree that:

1.4.1. When conducting our engagement, we will adopt such procedures and conduct such enquiries in relation to the entity as we agreed with you and consider necessary in the circumstances, which will include obtaining and relying on representations obtained by you in relation to POPIA.

1.4.2. Our engagement does not contemplate obtaining an understanding of the entity's internal control, assessing fraud risk, tests of accounting records observation, confirmation, or the examination of source documents and other procedures ordinarily performed in an audit and therefore we do not provide any assurances relating to the entity's compliance with POPIA or whether the representations made to us in this regard provide a true and fair view.

1.4.3. Accordingly, our engagement cannot be relied upon to disclose errors, fraud, or illegal acts that may exist. However, we will naturally inform you if such acts come to our attention during the course of our engagement.

1.4.4. As part of our engagement, we will issue our report, which will describe the agreed-upon procedures and the findings of the procedures performed [insert appropriate reference to the expected form and content of the agreed-upon procedures report.

1.4.5. By signing the attached copy of this letter, indicates your acknowledgement of, and agreement with, the arrangements for our engagement, including the specific procedures which we have agreed will be performed and that they are appropriate for the purpose of the engagement'

1.5. This engagement letter authorises us to perform the engagement described in paragraph 1.3 above. Any other services that you may request from us will be subject to separate engagement letters.

2. MANAGEMENT RESPONSIBILITIES

2.1. You are responsible for:

2.1.1. making all management decisions and performing all management functions;

2.1.2. designating an individual who possesses suitable skill, knowledge, and/or experience, preferably within senior management, to oversee the engagement;

2.1.3. evaluating the adequacy and results of the services performed;

2.1.4. accepting responsibility for the results of the services;

2.1.5. establishing and maintaining internal controls, including monitoring ongoing compliance with POPIA;

2.1.6. providing us with access to all information of which you are aware that is relevant to the engagement, such as records, documentation and other matters, additional information that we may request from you for the purpose of the engagement, and

2.1.7. providing us with unrestricted access to persons within the entity from whom we determine it necessary to obtain information.

2.2. As part of engagement procedures, we may require certain written representations from management about the entity's compliance with POPIA and matters related thereto. Our engagement is dependent on the information submitted by you and we are entitled to assume that all such information is true, accurate and complete in all respects. We will not be liable, and you indemnify us against any claim, by you or any third party for damages, penalties or loss of whatever nature (including but not limited to consequential damages or special damages) arising from any information provided to you by us or a failure by you to disclose any relevant information to us.

2.3. If, for any reason, we are unable to obtain such representations and/or access any information identified in paragraphs 2.1 and 2.2 above, we will not be in a position to issue a factual findings report.

2.4. We will use all reasonable efforts to complete the engagement within the agreed-upon time frames. However, we will not be liable for failures or delays in performance that arise from causes beyond our control, including the untimely performance of the responsibilities set out in this paragraph 2.

3. FEES

3.1. Our fee for these services will be based on the number of hours required by the staff assigned to complete the engagement.

3.2. In accordance with our recent discussion, we believe that the engagement fee will not exceed Rxxxx. However, if we encounter unexpected circumstances that require us to devote more staff hours to the engagement than estimated, we will discuss the matter with you.

3.3. We will charge you for all disbursements and out-of-pocket expenses incurred in the performance of our engagement, such as travelling, subsistence and goods and services purchased for and/or on your behalf.

4. INVOICING AND PAYMENT

4.1. We will present our invoices for fees and expenses/disbursements will be presented as agreed or on completion of the engagement. Invoices are payable on receipt.

4.2. We reserve the right to charge interest on overdue amounts at 2% per month.

5. ACCESS AND REPORTS TO REGULATORY AUTHORITIES

5.1. We may be required to submit information related to your entity to relevant statutory authorities that are empowered by law or regulation to request this information. In some instances, we are not allowed to inform you should we receive such a request.

5.2. By accepting this engagement letter, you authorise us to share the information disclosed to us during the engagement with these authorities. We may also be required to provide access to our working papers or your client documentation to our professional membership body.

6. **ACCESS TO DOCUMENTS**

6.1. Any document produced, altered or originated by us during our engagement remains our property and will not be shared with any party.

6.2. Upon payment, in full, of monies owed to us, your documents shall be released to you

7. **DISPUTE RESOLUTION**

Any dispute that may arise between our firm or any staff member and you will be subject to our Dispute Resolution Policy. Any matter must be referred to our firm to be resolved. If any matter remains unresolved, we may refer the matter to our professional body to mediate the issue.

8. **LIMITATION OF LIABILITY**

8.1. You hereby agree to indemnify, defend, and hold harmless our firm and its partners, agents, or employees, from and against any and all losses, costs (including legal fees), damages, expenses, claims, demands, or liabilities arising out of or in consequence of this engagement save for liability arising from our wilful misconduct or gross negligence.

8.2. Our liability in terms of this engagement is limited, in accordance with all applicable law, to the fees charged by us for the engagement.

8.3. We look forward to a continued relationship with your company, and we are available to discuss the contents of this letter or other professional services you may desire. If the foregoing is in accordance with your understanding, please sign the copy of this letter in the space provided and return it to us.

9. **TERMINATION**

9.1. You are entitled to terminate our mandate at any time by written notice to us but without prejudice to all our accrued rights and obligations, whether actual, prospective or contingent.

9.2. We reserve the right to terminate our mandate should a conflict of interest arise, should payment which is due to us not be made, or should we be unable to obtain full and proper instructions, information and/or representations timeously.

9.3. Upon termination of our engagement, and you will pay our charges and disbursements incurred prior to the date of termination. Upon payment, in full, of monies owed to us, your documents and/or other information shall be released to you.

Yours faithfully,

_____

[INSERT NAME OF SIGNATORY]
[DESIGNATION] i.e. BAP(SA)
[SAIBA MEMBERSHIP NUMBER]

7. APPENDIX 2: ILLUSTRATIVE REPRESENTATION LETTER

[TO BE PLACED ON CLIENT'S LETTERHEAD]

To: [NAME OF ACCOUNTANT]
[SAIBA DESIGNATION AND MEMBERSHIP NUMBER]
[NAME OF MEMBER'S FIRM]
[ADDRESS OF FIRM

[DATE]

Dear Sirs,

ENGAGEMENT ON POPIA COMPLIANCE CHECKLIST

This representation letter is provided in connection with your engagement to declare the compliance status of [**NAME OF CLIENT]** ("the Company") with the Protection of Personal Information Act, 3 of 2013 ("POPIA"), by way of the completion of the compliance checklist.

I confirm that I have performed such internal assessment as I considered necessary to enable me to assess the Company's compliance with the applicable sections of POPIA.

I also confirm to the best of my knowledge and belief the following representations made to you in relation to the Company, the board of directors of the Company ("the Board"), the Company's information officer, policies and procedures during the performance of your engagement for the purposes of compiling your report on factual findings. Where I know such representation to be incorrect or not-applicable, I have disclosed this to you by ticking the relevant column below.

		Question	Yes	No	NA
1.	Accountability: Information Officer and Employees	Do you have a POPIA compliance framework?			
2.		Does your Information Officer have the requisite capacity, knowledge and ability to discharge the duties required of the Information Officer in terms of POPIA and the Regulations?			
3.		If not, have you appointed deputy Information Officer(s) to assist the Information Officer?			
4.		Has the Information Regulator been notified of the appointment of the Information Officer?			
5.		If the Information Officer has other responsibilities, have they been assessed to avoid conflicts of interest?			
6.		Has the Information Officer developed and completed a personal information impact assessment to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information?			
7.		Has the Information Officer developed, monitor, maintain and made available a manual as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2 of 2000?			

8.		Has the Information Officer developed internal measures together with adequate systems to process requests for information or access thereto?			
9.		Does the Information Officer conduct regular internal awareness sessions regarding the provisions of POPIA and the Regulations?			
10.	Processing Principles: Collection and Retention of Personal Information	Is personal information collected for specified, explicitly defined and lawful purpose, and not further processed in a manner incompatible with those purposes?			
11.		Is personal information relevant, limited and minimised to what is necessary in relation to the purposes for which they are processed?			
12.		Are there documented principles to justify retention of personal information periods?			
13.		Have Data Subjects consented to the retention of personal information?			
14.		Is personal information kept only for as long as is necessary for the purposes for which it is processed?			
15.		Do you have a process for the destruction or declassification of personal information?			
16.		Are there security systems in place, whether electronic or not, to ensure that all retained personal information is appropriately secured, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage?			
17.	Systems and Software	Has there been implemented processes to ensure privacy by design and default is embedded into projects, to include measures that ensure data minimisation, pseudonymisation, encryption and the processing of only personal information necessary for specified purposes?			
18.		Are systems and services frequently audited and tested to ensure ongoing confidentiality, integrity, availability and resilience?			
19.		Are records of processing activities maintained in writing and available to the Information Regulator on request?			
20.	Processing of Personal Information	Where a data subject exercises their right of access, do you have the appropriate policies and procedures in place to:			
		(a) confirm, free of charge, whether or not you hold personal information about that data subject;			
		(b) within a reasonable time, at a prescribed fee (if any), in a reasonable manner and format and in a form that is generally understandable, provide the data subject with the record or description of the personal information about that data subject held by you, including the identities of all third parties (or categories of third parties) who have, or have had, access to the information?			
21.		Are processes maintained for rectifying inaccurate personal information and having incomplete personal information completed?			
22.		Where a data subject requests the erasure of personal information, is every reasonable step to erase all data, links and copies without undue delay?			
23.		Where data subjects object to having their data processed for direct marketing, is the data no longer processed and removed?			
24.		Is it ensured that data subjects have the right not to be subject to legal or similarly affecting decisions based on automated processing?			

25.		Are you able to demonstrate that data subjects have consented to the processing of their data?			
26.		Are consent requests clearly distinguishable from other matters, in an intelligible and accessible form, and written in clear and plain language?			
27.		Are data subjects asked to positively opt-in?			
28.		Do data subjects have the right to withdraw consent at any time?			
29.		If yes, to 29: Is withdrawing consent as easy and giving consent?			
30.		Where processing data of subjects below the age of 16 years, is consent given and authorised by the holder of parental responsibility?			
31.		If yes to 31, are reasonable efforts made to verify this consent?			
32.		Are privacy notices and policies clearly provided to data subjects with processor and Information Officer contact details, purposes of processing, legal bases for processing, recipients of personal information, international transfers, data retention periods and data subject rights?			
33.		Where personal information is not obtained directly from data subjects, are categories of personal information provided and the originating sources and whether those are publicly accessible?			
34.		Are privacy notices and policies provided to data subjects at the time of collection from data subjects or within one month when not obtained from data subjects?			
35.		Are all communications with data subjects provided in writing using clear, concise and transparent language?			
36.	Security Compromises	Are breach incident and notification policies and procedures kept?			
37.		Are security measures implemented and appropriate for data risks?			
38.		Is there a data breach response plan for employees?			
39.		Are investigations conducted and corrective action implemented for all personal information breaches?			
40.		Are employees aware that the Information Regulator must be notified without undue delay after becoming aware of a data breach?			
41.		Is a data breach register maintained which includes: • including facts related to the breach; and • the effects and remedial actions taken?			
42.		Do you communicate breaches to affected data subjects without undue delay and in clear and plain language?			
43.	Transfer of Personal	When transferring or disclosing personal information, is the data encrypted?			
44.		When transferring or disclosing personal information, is the data sent only what is necessary and relevant?			
45.		Are secure data transfer methods for all communications utilised?			

Yours faithfully,_____

[NAME OF SIGNATORY]

8. APPENDIX 3: ILLUSTRATIVE REPORT

[TO BE PLACED ON MEMBER'S LETTERHEAD]

MANAGEMENT / THE BOARD OF DIRECTORS
[NAME OF CUSTOMER]
[ADDRESS]

OUR REF.: [INSERT]
[DATE]

Dear Sirs,

[CLIENT NAME]: FACTUAL FINDINGS REPORT IN RELATION TO THE PERSONAL INFORMATION ACT, 3 OF 2013 ("POPIA")

Introduction

We have performed the procedures agreed with the directors of [Client name] ("the Company") to evaluate the Company's readiness for POPIA.

Our engagement was undertaken in accordance with the terms of engagement agreed with the Company which includes that engagement was performed in accordance with International Standard on Related Services 4400 (Revised): Agreed-Upon Procedures.

An agreed-upon procedures engagement involves: (a) performing the procedures that have been agreed between the parties and reporting the findings; (b) findings are the factual results of the agreed-upon procedures performed; and (c) the directors of [Client name] ("the Company") acknowledge that the agreed upon procedures are appropriate for the purpose of the engagement, and that the directors are responsible for the subject matter on which the agreed-upon procedures are performed.

The engagement was performed solely to assist the Company in evaluating whether or not, it needs to undertake further steps or implement additional procedures to ensure compliance with POPIA (the subject matter).

In performing the engagement we have complied with the International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants. There are no independence requirements with which we are required to comply. We apply the International Standard on Quality Management (ISQM) 1 as a firm when performing agreed-upon procedure engagements.

Procedures and Findings

The procedures performed by us and our corresponding findings are as follows:

Procedures	**Findings**

1.	Obtain and review POPIA Compliance Framework, obtain representations from management.	Per discussion with The Company [does / does not] have a POPIA compliance framework. Regulation 4 of the POPIA Regulations require the Information Officer to ensure that a compliance framework is developed, implemented, monitored and maintained. ***Recommended Corrective Action:*** ***[None / The drawing up and adoption of a POPIA compliance framework.]***
2.	Request and review correspondence addressed to the Information Regulator notifying the Information Regulator of the appointment of the Information Officer, obtain representations from management.	The Information Regulator [has / has not] been notified of the appointment of the Information Officer. ***Recommended Corrective Action:*** ***[None / The drafting of a letter to the Information Regulator containing the details of the Information Officer.]***
3.	Interview Information Officer and review terms of reference, obtain representations from management.	The Information Officer [has / has not] been assigned clearly defined responsibilities in terms of POPIA. ***Recommended Corrective Action:*** ***[None / The drafting of a POPIA compliance framework setting out the terms of reference for the Information Officer / If the Information Officer does not have the requisite capacity, knowledge and ability, appointment of a deputy Information Officer to assist with compliance.]***
4.	Review personal impact assessment conducted by the Information Officer, obtain representations from management.	The Information Officer [has / has not] conducted a personal impact assessment. ***Recommended Corrective Action:*** ***[None / The drafting of a POPIA compliance framework containing a checklist for the assessment.]***
5.	Request and review available the manual prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2 of 200, obtain representations from management.	The Company [does / does not] have such a manual. ***Recommended Corrective Action:*** ***[None / The drafting and adoption of the manual.]***
6.	Request and review internal procedures regulating access to personal information, obtain representations from management.	The Company [does / does not] have adequate internal measures and systems to process requests for information or access thereto. ***Recommended Corrective Action:*** ***[None / The drafting and adoption of a POPIA manual setting out the procedure to be followed for requesting access to personal information.]***
7.	Interview Information Officer, obtain representations from management.	The Information Officer [does / does not] provide regular internal training to employees on the provisions of POPIA and the Regulations. ***Recommended Corrective Action:*** ***[None / Training sessions, and refresher sessions, be scheduled at least once a year for employees.]***
8.	Review internal systems / software and interview Information Officer and appropriate employees regarding the collection of personal information, obtain representations from management.	The Company [collects personal information for a specified, explicitly defined and lawful purpose / indiscriminately collects personal information for no identifiable purpose]

		Recommended Corrective Action: ***[None / A review of and adjustment to the Company's systems to ensure that personal information is only collected to the extent required to provide a service to the Company's customers.]***
9.	Review internal systems / software and interview Information Officer and appropriate employees regarding the processing of personal information, obtain representations from management.	The processing of personal information by the Company [is / is not] limited and minimised to what is necessary in relation to the purpose of such processing. ***Recommended Corrective Action:*** ***[None / A review of and adjustment to the Company's systems to ensure that only relevant personal information is processed to the extent required to provide a service to the Company's customers.]***
10.	Review the Company's data retention policies and settings for its information management system, obtain representations from management.	The Company [has / does not have] a personal information retention policy with conditions for the destruction of the records containing personal information. ***Recommended Corrective Action:*** ***[None / The creation of a written information retention policy and implementing such policy through the Company's information management system.]***
11.	Review the Company's system of collecting personal information and inspect electronic customer records, obtain representations from management.	As a part of the Company's sign-up or customer initiation process, the Company [requests / does not request] electronic consent from the data subjects to the retention of their personal information. ***Recommended Corrective Action:*** ***[None / Amend the Company's customer onboarding system to request electronic consent from customers to the retention of their personal information.]***
12.	Review and test the security systems employed by the Company to secure personal information, obtain representations from management.	The Company [does / does not] utilise an ISO27001 certified information security management system to secure all personal information under its control. ***Recommended Corrective Action:*** ***[None / Transfer or uploading of all personal information to an ISO27001 compliant cloud storage provider such as AWS and the regular review of the access conditions applicable to such storage.]***
13.	Request sample records of processing activities, obtain representations from management.	The Company [does / does not] maintain written records of processing activities. ***Recommended Corrective Action:*** ***[None / Creation of an automatic electronic log of all processing activities in a format that can be provided to the Information Regulator on request.]***
14.	Review the Company's policies and procedures pertaining to communications with data subjects, obtain representations from management.	The Company [has / does not have] a procedure governing the manner and form in which data subjects can obtain records or descriptions of the personal information held by the Company and the identities / categories of third parties who have had access to such information, request the deletion of their personal

		information and object to the processing of their information for direct marketing. The procedure [is / is not] publicly available to data subjects. ***Recommended Corrective Action:*** ***[None / Publication of a privacy policy setting out the aforegoing.]***
15.	Review the Company's template / sample communications with data subjects, obtain representations from management.	The Company [communicates / does not communicate] with data subjects in writing using clear, concise and transparent language. ***Recommended Corrective Action:*** ***[None / Draft template communications or amend the templates using clear, concise and transparent language.]***
16.	Obtain representations from management on the transfer of personal information.	When transferring or disclosing personal information, the Company [encrypts / does not encrypt] the information and [does / does not] use secure data transfer methods. ***Recommended Corrective Action:*** ***[None / The POPIA compliance framework should include the adoption of data encryption technology and procurement of secure transfer methods.]***

Conclusion

The above procedures do not constitute an assurance engagement conducted in accordance with International Standards on Auditing, International Standards on Review Engagements or International Standards on Assurance Engagements.

We do not express any assurance as to whether the Company is compliant with POPIA. Had we performed additional procedures or had we performed an audit or review, or other assurance engagement, other matters might have come to our attention that would have been reported to you.

This report is solely for the purpose set out in the first paragraph of this report and is restricted to those parties that have agreed to the procedures being performed.

[INSERT NAME OF SIGNATORY]

[DESIGNATION] i.e. BAP(SA)

[SAIBA MEMBERSHIP NUMBER]