IST-Africa 2023 Conference Proceedings
Miriam Cunningham and Paul Cunningham (Eds)
IST-Africa Institute and IIMC, 2023
ISBN: 978-1-905824-71-7

Towards a Privacy Compliance Assessment Toolkit

Terrence MOABALOBELO, Sipho NGOBENI, Bokang MOLEMA, Phumeza PANTSI, Moses DLAMINI, Norman NELUFULE
Council for Scientific and Industrial Research, P.O. Box 395, Pretoria, 0001, South Africa
[1]Tel: +27 12 841 4394, Email: tmoabalobelo@csir.co.za, sngobeni@csir.co.za, bmolema@csir.co.za, ppantsi@csir.co.za, tdlamini1@csir.co.za, nnelufule@csir.co.za

Abstract: The South African Protection of Personal Information Act (POPIA) No.4 of 2013 makes it illegal to collect, use, process or store personal information unless it is done in accordance with the prescribed legal and regulatory clauses enshrined in the Act. Organisations should take stock of the personal information they collect and who they share it with before they can put controls in place to safeguard it. Failure to comply with POPIA may potentially expose the responsible party and its associated third parties to steep legal penalties including possibly imprisonment of up to 10 years or R10 million fine which is imposed by the Information Regulator of South Africa. This paper presents the results of a system called Protection of Personal Information Act Compliance Assessment Toolkit (PCAT). The PCAT's objective is to assist organisations to assess their current state of compliance to POPIA. The PCAT followed an experimental research and development process, where three existing similar technologies in the market were analysed and compared to the PCAT. The results show that it simplifies the POPIA compliance requirements compared to the other three existing technologies.

Keywords: Privacy, POPI Act, Assessor, Assessee, Approver, Assessment

1. Introduction

The Protection of Personal Information Act (POPIA) No.4 of 2013 is modelled based on the European General Data Protection Regulation (GDPR) and affects all organisations that handle personal information [1, 2, 3, 4]. The United Nations Conference on Trade and Development (UNCTD) has found that adoption levels for the development of appropriate data protection and privacy legislation are as follows; 61% of African countries have developed such legislation; 11% have drafted the legislation, and 19% have no legislation and the remaining 9% has no public data regarding the legislation [5].

POPIA regulates the processing of personal information by both public and private bodies in the Republic of South Africa [6,7,8]. This act is now a legal compliance obligation, and the one-year grace period has passed from the 1st of July 2021. As the enforceable deadline draws closer, organisations are increasingly discovering the serious legal implications and challenges of achieving, demonstrating, and maintaining mandatory compliance with POPIA are not as straight forward as they would have preferred, and panic is slowly creeping in. POPIA compliance is seen as exorbitant, intimidating, and complex; leaving many organisations unsure of how to tackle it.

POPIA makes it illegal to collect, use, process or store personal information unless it is done in accordance with the prescribed legal and regulatory clauses enshrined therein. It is important for organisations to take stock of the personal information they collect and share, and then put in place the adequate safeguards to protect it. The legal consequences of non-compliance to this act will likely come from information security and privacy control deficiencies that relate to the processing and storage of personal information and

organisations not doing their due diligence in safeguarding personal information. It may also come because of gaps in policies and procedures that govern the handling of personal information. Failure to comply with certain provisions of POPIA may potentially expose the responsible party and its associated third parties to steep legal penalties including possibly imprisonment of up to 10 years or R10 million from the Information Regulator.

Organisations have been given enough time to prepare and put their ducks in order when it comes to POPIA compliance, but many are now scrambling to tick the boxes and become compliant over-night. They have since realised the seriousness of non-compliance and the financial penalties thereof. Unfortunately, compliance to POPIA cannot be an over-night exercise. Organisations must invest time and money to be compliant.

It is no secret that preparedness for POPIA compliance has become a top priority for most organisations, and more so as we approach the enforcement deadline. Therefore, the main purpose of this paper is to present the results of a technology demonstrator called POPIA Compliance Assessment Tool. The main essence of this toolkit is to assist organisations to assess their current state of compliance to the POPIA.

2. Objectives

The objective of this study is to develop a system that can be used to assess the current state of compliance to the POPIA. In order the achieve this objective, the following sub-objectives were followed:

- Analysis of the existing POPIA compliance assessment systems to gain understanding of they work.
- Design and implement the proposed POPIA compliance assessment toolkit.
- Develop criteria to measure performance of the PCAT against the existing system.
- Assess the PCAT through comparing it with the identified existing systems.

3. Methodology

The methodology followed in this research is Experimental Development [6]. This is systematic work, drawing on the knowledge gained from research and practical experience and producing additional knowledge, which is directed to producing new products or processes or to improving existing products and processes. It this paper, we study three POPIA compliance assessment systems, and try to develop an improved system, called PCAT. We then formulated performance criteria and used them to measure the performance of the proposed system against the three proposed systems. These criteria include compliance analysis and reporting, provision of compliance maturity level over time, user management, prioritised implementation road map, provision of key performance indicators for the categories where the organisation is compliant to POPIA.

The results shows that the experimental development process yielded an improved system that performs or provides improved capability for organisation to self-assess their current state of compliance to the POPI Act. This, in itself a contribution to the Cybersecurity Privacy body of knowledge.

4. Technology Description

The proposed system is cloud-based, developed for organisations that collect, use, process or store Personal Identifiable Information (PII). The system architecture was designed to ensure decoupling of front and back-end data to ensure scalability and flexibility.

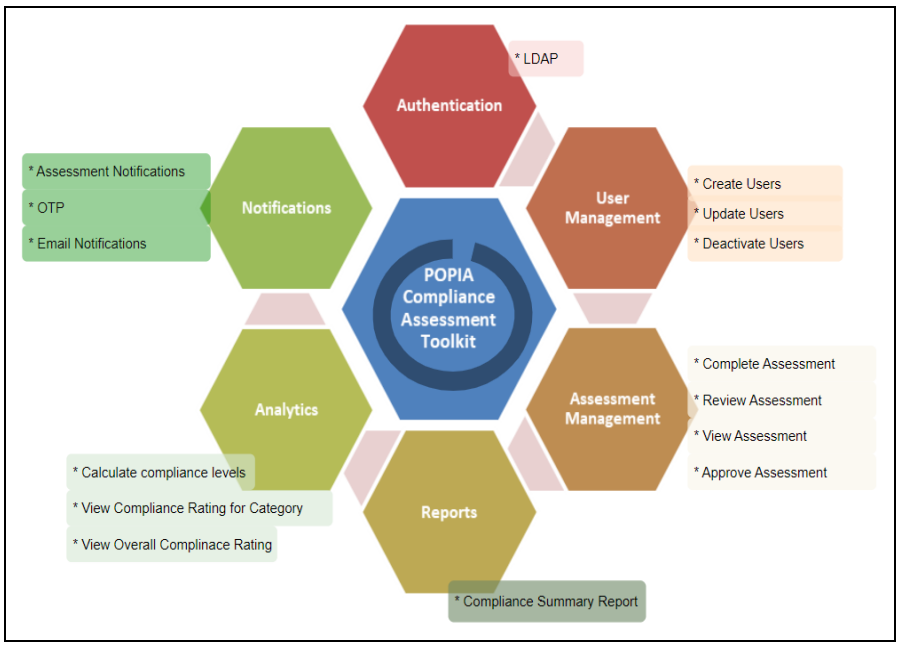

Figure 1. System Overview

The PCAT system consist of eight capabilities which are described below:

- **Authentication** – the system requires users or the assessed organisation to submit their details to initiate the compliance assessment process. These details are then used to register the organisation, and representatives who will be taking the assessment.
- **User and Assessment Management** – the system uses role-based access control, which include:
  - **System Administrator** – adds organisation/s to be assessed in the system.
  - **Assessor** – initiates the assessment evaluation process and sends the organisation's representative (Assessee) a link for completing a self-assessment.
  - **Assessee** – completes the assessment on behalf of the assessed organisation.
  - **Approver** – reviews and approves assessments.
- **Reporting** – an executive summary report is generated for all approved assessments. The assessor will send this final report to Assessee upon approval.
- **Analytics** – provides a results visualisation of the organisation's compliance posture.
- **Notifications** – provides assessment email notifications.

To support these capabilities, the backend stores data in two forms, that is, a relational database using PostgreSQL and a File server to store the uploaded documentary evidence.

5. Developments

An assessment is created for an organisation as depicted in Figure 2. An organisation can choose to have one or more business units (BU) to undergo compliance assessments.

Once an assessment(s) is created, the (PCAT) will automatically send the representative(s) a link for the assessment. In an event where multiple BUs are being assessed the system sends a notification with a unique link for each BU. To access the PCAT the Assessee will be authenticated with a unique One-Time-Pin (OTP).

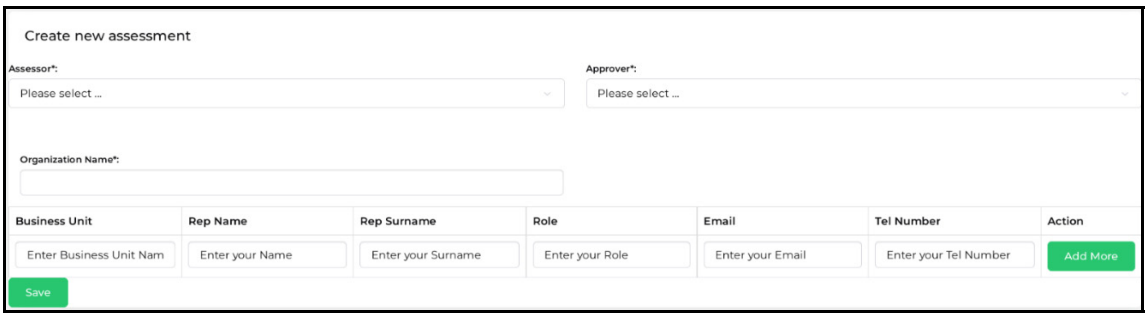

Figure 2. Creating an Assessment for an Organisation

Upon authentication the Assessee will be presented with a set of questions grouped into categories that align to the conditions defined in POPIA. In responding to each question, the Assessee will be able to provide comment and file-based evidence to support the compliance criteria selected (either Yes, No, or N/A) as indicated in Figure 3.

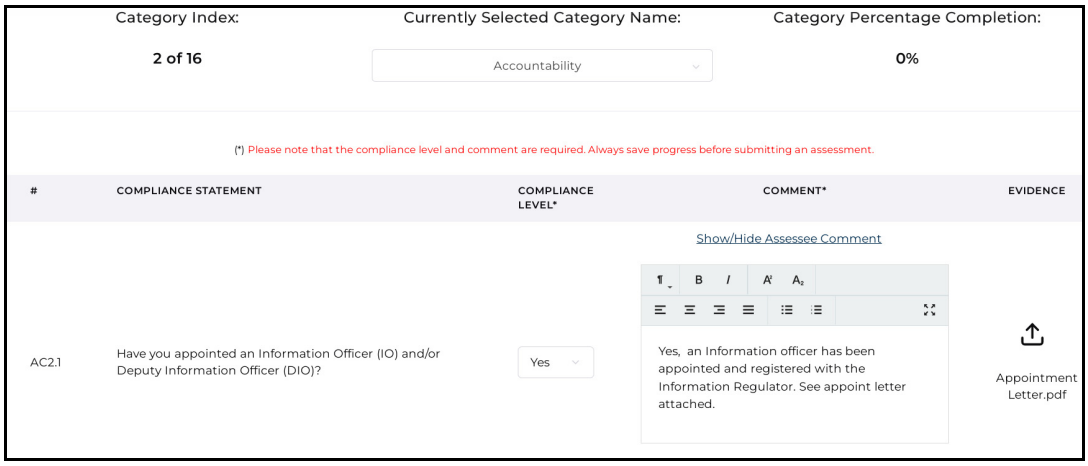

Figure 3. Assessment Presented in a Questionnaire Format

On completion of the assessment the Assessee will receive notification that their assessment has been submitted for review. To assure quality of evidence and assessment results, the PCAT will route the completed assessment to an Assessor who will review and comment on the assessment. Once satisfied, the assessor will then submit the assessment to the Approver for finalization and approval (refer to Figure 4). Upon approval of the assessment the system will generate results of the assessment as depicted in Figure 5.

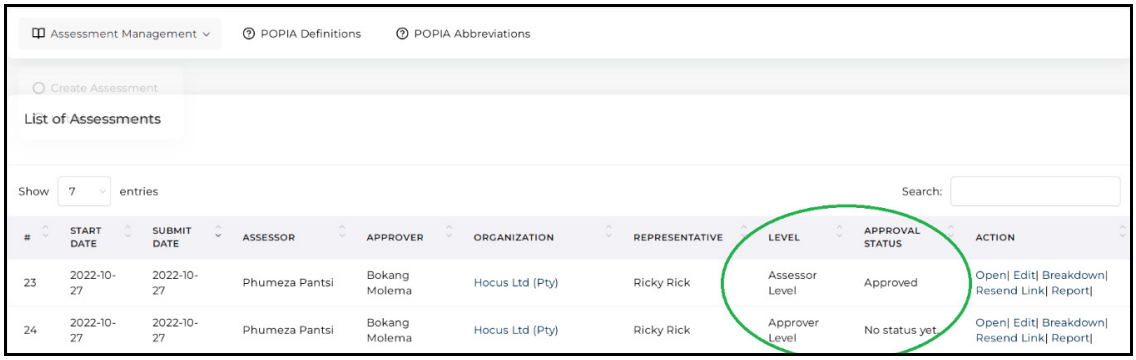

Figure 4. 2-Stage Quality Assurance

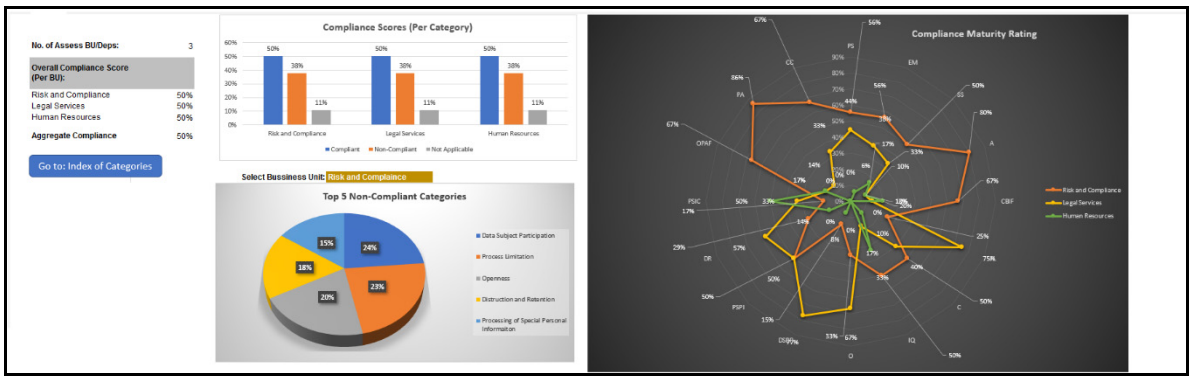

Figure 5. Results Visualisation Dashboards

6. Results

6.1 Performance Analysis

Table 1 presents the results of the performance analysis of the PCAT when compared with similar systems, that is, Easy POPI Compliance Toolkit, LexisNexis POPIA, and Simple POPI. Below is a high-level description of the prescripts in Table 1.

- **Measured Criteria** – are measured against the existing systems.
- **Measured performance** – this is the optimal performance expected to be achieved by the proposed system and measured against the three existing systems.
- **PCAT** – this is the proposed POPIA Compliance Assessment Toolkit described in Section 3 and Section 4 above.
- **Easy POPI Compliance Toolkit** – this is a complete set of documents, assembled and ready to use with an aim to guide an organisation through their POPIA compliance audit journey.
- **LexisNexis POPIA** – This is a proprietary tool for POPIA compliance assessment built to ensure an organisation can understand key issues including implementation of POPIA through use of checklists and templates that continue to evolve.

Table 1. Performance Analysis of the Proposed System

Measured Criteria	Measured Performance	PCAT	Competitors		
			Easy POPI	LexisNexis	Simple POPI
Compliance analysis and reporting.	Generating analytics based on the compliance score and highlight POPIA Compliance Categories that need attention.	Generate analytics based on the compliance score and highlight POPIA Compliance Categories that need attention.	Provides high level analytics based on categories only.	Does not provide analytics.	Does not provide analytics.
Provide compliance maturity level over time.	The technology provides for organisations to mature their compliance over time and plot related maturity levels based on	PCAT provide regulatory compliance maturity rating based on the levels: a. Non-existent (Level 0) b. Initial (Level 1) c. Defined (Level	No regulatory compliance maturity rating.	No regulatory compliance maturity rating.	No regulatory compliance maturity rating.

			Competitors		
	historical assessments.	2) d. Standardized (Level 3) e. Measured & Managed (Level 4 Optimized (Level 5)			
User Management.	Role-based access.	PCAT provides for role-based access control, that is, System Administrator, Assessee, Assessor, and Approver	Some elements of access management provided.	Status unknown.	No role-based access management.
Prioritise implementation road map.	Provide key focus areas for improvement.	PCAT provides prioritised areas of improvement based on top non-compliant assessment categories.	Not implemented.	Not implemented.	Not implemented.
Provide key performance indicators for the categories where the organisation is compliant to POPIA.	Provide key focus areas where the organisation is compliant to POPI Act.	PCAT provides a prioritized key performance indicators for the categories where the organisation is compliant to POPIA.	Not implemented.	Not implemented.	Not implemented.

Table 2 presents a summary of the performance results in Figure 1 and a detailed discussion of the results is presented in Section 5.2. The legend "✓" depicts that the measured performance criteria is met and "✕" depicts that the measured performance is Not met, while "(✕)" depicts that the status is not known.

Table 2. Summary of Performance Analysis

Measured Criteria	Measured Performance	PCAT	Competitors		
			Easy POPI	Lexis Nexis	Simple POPI
Compliance analysis and reporting.	Generating analytics based on the compliance score and highlight POPIA Compliance Categories that need attention.	✓	✓	✕	✕
Provide compliance maturity level over time.	The technology provides for organisations to mature their compliance over time and plot related maturity levels based on historical assessments.	✓	✕	✕	✕
User Management.	Role-based access.	✓	✓	(✕)	✕
Prioritise implementation road map.	Provide key focus areas for improvement.	✓	✕	✕	✕
Provide key performance indicators for the categories where the organisation is compliant to POPIA.	Provide key focus areas where the organisation is compliant to POPI Act.	✓	✕	✕	✕

6.2 Discussion

This section is dedicated to the discussion of the performance analysis results presented in Section 5.1. It is noted from Table 1 that the PCAT is the most optimal solution compared to the three systems regarding:

Compliance analysis and reporting – this criterion measures the ability of the system to generate compliance scores and highlight areas of improvement to ensure improved compliance posture. It can be noted that the PCAT provides analytics based on the compliance score and highlights arears that need attention. Additionally, the tool provides for automatic generation of two types of executive summary reports, one for each assessed BU, and one that consolidates the results for a case where multiple BUs are assessed. The Easy POPI does provide high level analytics based on categories only, while the LexisNexis and Simple POPI does not provide analysis and reporting features.

Provision of compliance maturity level over time – this criterion measures the ability of the systems to allow for organisations to mature their compliance over time and plot related maturity levels based on historical assessments. In this instance, the PCAT also outperforms its competitors as it provides a capability to determine compliance maturity ratings based on the following levels: Non-existent (Level 0), Initial (Level 1), Defined (Level 2), Standardized (Level 3), Measured & Managed (Level 4 Optimized (Level 5). All the other three systems do not provide regulatory compliance maturity ratings.

User Management – this criterion measures the ability of the system to ensure role-based access control. It can be noted from Table 1 and Table 2 that the PCAT provides a capability for role-based access control. The Easi POPI does provide some elements of access management. The status of LexisNexis is not known, this could be due to vendor lock-in software, while Simple POPI does not provide for access management.

Prioritised implementation road map – this criterion measures the capability of the system to provide for an implementation roadmap after completing the systems, that is, key focus areas for improvement. The PCAT has proven to provide this capability by making provision for prioritised areas of improvement based on top non-compliant assessment categories. All the other three compared systems do not make provision for this capability.

Provide key performance indicators for the categories where the organisation is compliant to POPIA – this criterion is the fundamental feature for such systems. Its aim is to provide key focus areas where the organisation is compliant to POPIA after completing the assessment. PCAT provides a prioritised key performance indicators for the categories where the organisation is compliant to POPIA, while the other three systems does not provide for this capability.

7. Business Benefits

The PCAT provides the following benefits:

- The most salient benefit is to assist organisations to assess their current state of compliance to POPIA.
- The PCAT allows organisation to assess itself as whole or certain Bus. This suggest that a user can create an assessment only for Human Resources department.
- The PCAT forms a basis from which other Cybersecurity governance and compliance tools can be birthed from, e.g., compliance toolkit for ISO/IEC 27001 family of standards, privacy impact assessments, etc.
- The users of the PCAT are organisations in both the private and the public sector. In addition, this tool could be used by organisations responsible for conducting audits for regulatory compliance, e.g., The Auditor-General of South Africa (AGSA).
- To bring the PCAT to the market, the toolkit should first be tested in the realistic environment, then conduct a market feasibility to understand market needs, market

segments including size, growth rate, and competitive environment, market saturation, possible licensing approaches.

- The system has been successfully piloted in three operational environments, i.e., in a Municipality, Medical division and Human Resource department. Part of the feedback obtained from the pilots show that the different entities were able to identify the current state of compliance, or lack thereof. Additionally, other benefits included: improved risk management, assistance with the audit process, and improved data management with regards to sensitive data.

8. Conclusion

The outcome from the development if the PCAT showed that it was possible for an organisation to self-assess its compliance against POPIA and by so doing they are then able to develop a road map for full compliance based on the results provided by the tool.

Furthermore, the toolkit will be improved to have a compliance assessment completion workflow that will include other role players within the assessed organisations to assist in the completion of the assessment. The other role players may include Privacy Information Officer, Chief Information Security Officer, etc.

References

[1] M. Goddard, "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact" International Journal of Market Research, Vol. 59, No. 6, pp. 703-710, 2018.

[2] B. C. Stahl and D. Wright, "Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation," in IEEE Security & Privacy, Vol. 16, No. 3, pp. 26-33, 2018.

[3] E. Politou, E. Alepis and C. Patsakis, "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions", Journal of Cybersecurity, Vol. 4, No. 1, pp. 1-202018

[4] D. Wright, "Making privacy impact assessment more effective", The Information Society, Vol. 29, Issue 5, pp. 307-315, 2013.

[5] United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide [Online]. Available: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide [Last Access: 03 March 2023]

[6] N.S. Netshakhuma, "Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA)", Global Knowledge, Memory and Communication, Vol. 69 No. 1/2, pp. 58-74, 2020.

[7] A. Rachel et al, "POPIA Code of Conduct for Research", South African Journal of Science, Vol. 117, No. 5-6, pp. 1-12, 2021.

[8] C. Staunton, R. Adams, M. Botes, J. de Vries, M. Labuschaigne, G. Loots, S. Mahomed, N.N. Loideain, A. Olckers, M.S. Pepper, A. Pope and M. Ramsay, "Enabling the use of health data for research: Developing a POPIA code of conduct for research in South Africa", South African Journal of Bioethics and Law, Vol. 14, No. 1, 2021.

[9] C. Patsakis, J. van Rest, M. Choras M, "Privacy-preserving biometric authentication and matching via lattice-based encryption", International Workshop on Data Privacy Management, pp. 169-82, 2015.

[10] F. Schaub, R. Balebako, A.L. Durity, "A design space for effective privacy notices", Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), pp. 1-17, 2015.

[11] Frascati Manual 2015, "Guidelines for Collecting and Reporting Data on Research and Experimental Development", The Measurement of Scientific, Technological and Innovation Activities, OECD Publishing, 20 October 2022, [Online]. Available: http://dxdoi.org/10.1787/9789264239012-en