Mapping 'Security Safeguard' Requirements in a Data Privacy legislation to an International Privacy Framework: A Compliance Methodology

I.Govender
Department of Mathematical Sciences/Computer Science
Stellenbosch University
ieg@sun.ac.za

***Abstract*—It is commonplace for organisations to collect personal information to be processed and stored on their systems. Until recently, there was no comprehensive legislation that addressed the 'processing' of personal information by organisations in South Africa. The Protection of Personal Information Bill ("POPI") was signed into law in November 2013 and is expected to come into effect, later this year (2015). POPI is informed by international data privacy legislation. The implications are that it will be incumbent for organisations to revisit how they 'handle' peoples' personal information. This can be a daunting task as evidenced by countries that still find it a challenge to comply with data privacy laws that have been enacted there, a while ago. This article proposes a methodology to comply with POPI. The Generally Accepted Privacy Principles (GAPP) is an American/Canadian framework containing international privacy requirements with best practices. Both, POPI and GAPP address a common purpose: 'How personal information is collected, used, retained, disclosed, and disposed.' GAPP is reputed as a solid benchmark for good privacy practice, comprising of ten overarching privacy principles which yields a set of criteria for effective management of privacy risks and compliance. Much of the provisions in POPI is addressed in GAPP. A key condition (Security Safeguards) in POPI stipulates what aspects of personal information must be adequately secured, with limited insight on how to go about this process. Accordingly, this article proposes a methodology to fill this gap. All of the provisions under 'Security Safeguards' in POPI is mapped onto GAPP, thereby contextualising GAPP to facilitate compliance with South Africa's data privacy legislation and to the same end, complying with international privacy laws. This framework could also be implemented as a checklist/auditing document, guiding the organisation in its implementation of data privacy and POPI compliance.**

Keywords-Information Security, Data Privacy, Personal Information, GAPP, POPI, framework, methodology, mapping

I. INTRODUCTION

The writing was already on the wall in the mid-1980s, when Mason [1] stated that a major concern of the information age would be information privacy. His prediction turned out to be accurate since privacy has been of serious concern over the years [2]. Information privacy issues address consumer privacy, collection and use of personal information, workplace privacy and online social media privacy [3]. Information privacy is studied in various disciplines, inclusive of information systems, marketing, law, management and psychology. A privacy survey [4] reflected that 85 percent of companies had some sort of privacy breach while 63 percent experienced multiple breaches. The majority of the companies spent their time addressing privacy breaches as opposed to proactively attempting to prevent them [4].

A. International Data Privacy Legislation

International debates have addressed data privacy and the efficacy of direct regulation through government laws; self-regulation by firms without the penalties of law but the sanctions of community stakeholders; and co-regulation involving a legislation that places enforcement in the hands of non-governmental partners [5]. Xu et al. [6] pointed out 'scepticism about the effectiveness of industry self-regulation in protecting consumer privacy has resulted in privacy advocates and consumers clamouring for strong and effective legislation to curtail rampant abuses of information by firms.' Senden [7] and [8] argued that co-regulation and self-regulation are ''soft laws,'' which do not have the same level of impact as government laws.

One of the first international initiatives to address privacy concerns was the guidelines adopted in 1980 by the Organisation for Economic Cooperation and Development (OECD). Many countries since then, including, the European nations, Canada, Australia etc. have followed suite and adopted privacy laws. Australia's Privacy Act of 1988 establishes information privacy principles that apply to the activities of most federal government agencies. Since January 1, 2004, Canadians' personal information is protected by the "Personal Information Protection and Electronic Documents Act" (PIPEDA); a law that lays ground rules for the collection, use, and disclosure of personal information. New Zealand's 1993 Privacy Act is based on the 1980 OECD guidelines. The European Union's Data Protection Directive, also informed by the OECD, applies to the 28 European member states. Data privacy in the USA varied according to industry sectors; such as the Health sector has the 'Health Insurance Portability and Accountability Act' (HIPAA). HIPPA legislation protects the privacy and confidentiality of patients' medical information; including security and privacy provisions.

A. Protection of personal information: South Africa

The Constitution of the Republic of South Africa (Section 14), enshrines the right to privacy in the Bill of Rights; explicitly stipulating that "everyone has the right to privacy." Personal information is protected through the right to privacy. South Africa's privacy legislation, referred to as POPI (Protection of personal information), was signed into law in November 2013. The POPI act states that "the purpose of this act is to give effect to the constitutional right to privacy, by safeguarding personal information when processed by a

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

responsible party" [9]. Almost all organizations in the private sector and the public sector in South Africa will be required to comply with stringent requirements regarding why, and how they collect, use, disclose and store personal information belonging to both natural and juristic persons [9]. Specific sections of POPI commenced on 11 April 2014. These sections enable the establishment of the information regulator together with the power for regulations to be made under the Act. The commencement date for the obligations under the Act has not yet been announced and the appointment of the regulator is expected in 2015. Organisations will have 12 months from the commencement date to become compliant. Privacy compliance is an entity's accordance with established personal information protection guidelines, specifications or legislation. The POPI legislation is based on the European Union (EU) Data Protection Directive (Directive 95/46/EC), which attempts to ensure that Personal Information (PI) is processed in a way that accords with internationally accepted data protection principles. The EU directive has undergone stringent changes to data privacy and is soon to be enacted as the new 'General Data Protection Regulation'.

The essence of the POPI legislation is that security infraction dealing with personal data can have significant consequences for an entity. The Act establishes a new set of rules governing the handling of data about people and entities. Central to POPI is that it is obligatory for organisations to comply with the eight conditions stipulated in the legislation. This new piece of legislation brings South Africa in line with international best practice that enforce commitment to good corporate and data governance. It empowers citizens by strictly enforcing the way in which individuals' PI is processed. POPI provides individuals with a legally backed right to privacy of their PI and enacts persons to take legal action if their right to privacy is not respected [9]. POPI impacts on nearly every area of business processes, and will require, among other things, amending legal documents, reviewing subcontracting practices and cross-border data flows [10]. It outlines stringent cross-border data transfer requirements as PI may not be relocated to countries with inadequate information protection frameworks.

This research project is based on the problem statement that organisations are bound to find compliance with POPI a challenging experience, as encountered globally with data privacy legislations. A survey [10] to gauge the level of POPI-readiness of organisations, found that many companies are generally unprepared, and underestimate the gravity and complexity involved with getting compliant. Most organisations do not fully comprehend the operational implementation challenges they will face when embarking on this journey. This survey found that over half of the respondent organisations don't have information security or privacy policies, processes and procedures in place [10].

B. The Generally Accepted Privacy Principle (GAPP) Framework

Even though the introduction of regulations and guidelines seems to have increased firms' awareness and ability to react to recent privacy issues, key questions still remain unanswered: Why do data privacy issues still persist, with organisations grappling to comply with data privacy legislation? [3].This led to the research question for this study: How can organisations comply with security safeguards, as stipulated in a privacy legislation, namely POPI?

Notwithstanding the various regulations and guidelines accessible to organisations to formulate privacy strategies, management still seek actionable plans that are suitable for their own situations and the technical solutions that are available in the marketplace or can be built in-house [3]. Due to the complex and at times conflicting government regulations, the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA/CICA) developed and announced a set of Generally Accepted Privacy Principles (GAPP) [11]. The Generally Accepted Privacy Principles (GAPP) is an internationally recognized privacy framework developed in collaboration with the two aforementioned organisations. Kauffman et al. [3] assert that GAPP delineates best practices that reflect the key principles embraced in all major international privacy legislation, inclusive of 'Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the Australian Privacy Act of 1988 and the European Union data protection framework. The GAPP framework is an amalgamation of international privacy regularity requirements with best practices [12] which also incorporates international security standards such as the ISO/IEC 27001.

Schroeder and Cohen [10] argue that the overarching objective for the application of GAPP is that personal information is collected, used, retained, disclosed, and disposed of in accordance with the entity's privacy notice and with criteria set forth in GAPP. GAPP brings together international privacy regulatory requirements and best practices in one framework based on ten privacy principles. These principles are considered a solid benchmark for good privacy practice [13]. Each privacy principle comprises of objective measurable criteria that form the basis for effective management of privacy risk and compliance in an organization. The security criteria require an organisation to address the security of personal information within its privacy policies, and to ensure that the policies are communicated through a privacy notice. Organisations should take the process of establishing and maintaining an effective IS security policy process seriously, considering that the security and privacy agenda is ranked among the top issues for IT executives [14], together with legislation making demands on organisations to govern security policies [15]. Smith [16] asserts that specific sectors of Industry could develop sets of "generally accepted privacy principles (GAPP)" for their own sector e.g. the Banking Sector. The GAPP should address the specific information privacy issues specific to that sector of the industry. The Information Regulator's office could advise and inform in this regard, and the specific industry sector could provide industry specific knowledge. Smith [16] uses the banking sector to elaborate that GAPP for example, would include guidelines for internal access to customer account and financial information, statements regarding appropriate and inappropriate use of customer information for marketing purposes, and guidelines for external purchases of personal information about customers (if the law permits). Input from the various relevant industry-

specific stakeholders could be solicited. When industry-specific GAPP are established, the Information Commissioner, legislators, consumers, and competitors can use GAPP to assess corporate behaviour [16].

GAPP can be used by organizations for the following: [17]

• Designing, implementing, and communicating privacy policy
• Establishing and managing privacy programs
• Monitoring and auditing privacy programs
• Measuring performance and benchmarking

II. Research Approach

Kauffman [3] assert that prior research that studies information privacy, identifies three distinct theoretical perspectives:

- The societal and public policy perspective: Examines the definition of privacy, standards and regulations regarding privacy, and political developments and social pressures in information privacy.
- The business practice perspective: Investigates how organisations comply with information privacy norms, practices, and laws.
- The individual privacy and consumer behaviour perspective: Explores factors regarding individuals' decisions about sharing personal information with organisations.

This study is situated in the second perspective (The business practice perspective). The POPI Act stipulates that the purpose of this act is, "to regulate, in harmony with international standards, the processing of personal information by public and private bodies" [9]. The act informs that the Information Regulator's role is "to conduct research and to report to Parliament from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the personal information of a data subject" [9]. These legislative stipulations informed this research project to incorporate or map POPI with GAPP in an attempt to facilitate the protection of personal data in accordance with international standards and comply with privacy legislation, namely POPI.

According to Smith [16], the GAPP guidelines provide a quasi-legislative flavour. This research study proposes a methodology by mapping the POPI legislation with an internationally recognised privacy framework: GAPP. In line with the landscape of this conference (Information Security Conference for South Africa), this research study attempts to map South Africa's data privacy legislation (POPI) with GAPP. Although POPI outlines eight conditions to protect personal information, the scope of this research does not permit the mapping of all eight conditions in POPI with GAPP. Condition seven ('Security Safeguards') of POPI [9] states that the organisation must ensure the integrity and confidentiality of personal information by taking the appropriate technical and condition in POPI and also of pertinence to this conference. However, this condition (Security Safeguards) in POPI is not supplemented with comprehensive guidance on how to address 'Security Safeguards'. Consequently, this study attempts to fill this gap, relating to 'Security Safeguards'. Moreover, 'Security Safeguards' is not examined in a vacuum. If any of the other conditions are related to or applicable to 'Security Safeguards', they are also examined in the context of 'Security Safeguards.' Hence, this research project maps 'Security Safeguards' together with related provisions in POPI with the data privacy principles found in GAPP. Furthermore, those provisions under 'Security Safeguards' of POPI that are not covered comprehensively by the GAPP guidelines, are identified and addressed.

Schroeder and Cohen [12] outlined a five step process for the deployment of GAPP. This study proposes a methodology, incorporating GAPP, as a possibility for organisations to comply with the 'Security Safeguards' requirement of POPI in the context of this five step process. The scope of this study does not facilitate an in-depth examination of the five step process, but only those steps pertinent to 'Security Safeguards'. To this end, the mapping process is sequenced as depicted in Fig. 1. The mapping of POPI to GAPP starts with 'Data Inventory and Privacy Nexus' (Fig. 1), as recommended by Schroeder and Cohen [12]. Although 'Security Safeguards', as articulated in POPI does not mention this concept of 'Data Inventory and Privacy Nexus', it is nevertheless integrated into the mapping process, as an originator to 'Security Safeguards'. The remaining sections in Fig. 1 (Risk Assessment, Third Party and Notification) emanate from condition seven of POPI; the focus of this study.

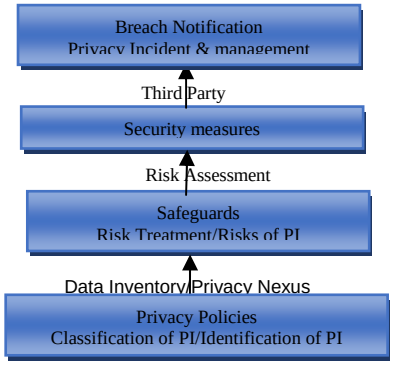

Fig. 1. Sequence for Mapping POPI with GAPP

A. *Step One: Data Inventory and Privacy Nexus*

"Privacy Nexus" refers to the privacy regulations that an organisation is subject to. Although this step is not the focus of this study, it is of relevance, since organisations are bound to ask the question, 'Where do we start?', once POPI is in motion. Moreover, 'Security Safeguards' would be a challenge without addressing this step: 'Data Inventory and Privacy Nexus'.

The first step in managing privacy risks is to understand what personal information (hard copy & electronic copy) the business processes has in its custody. Subsequently, to deliberate over the legal requirements that applies to the personal information. Privacy regulations are both jurisdictional (related to the state or country of an individual's residence) and regulatory (related to certain industries) [10]. The first principle in GAPP is a governance concept referred to as 'Management' that recommends "responsibility and accountability be assigned to a person or team for developing, documenting, implementing, enforcing, monitoring, and

updating the entity's privacy policies" [17]. The responsible person/team, together with management should start with establishing standards used to classify the sensitivity of personal information and to determine the level of protection required. All types of personal information and the related processes, systems, and third parties that are involved in the handling of such information should be identified [17]. Prosch [11] asserts that a company cannot protect data that it does not know it has, therefore this stage calls for a complete inventory of all PI; from the cradle to the grave. The transfer of data to and from third parties; including the collection and processing of data by third parties must be accounted for. This is of relevance to section 19(2)(a) of POPI which calls for identifying the risks to personal information (PI), which is further discussed later. In order to comply with this provision (Risk identification of PI), the PI needs to be first identified and categorised.

In the context of the GAPP framework, the privacy nexus is critical to fulfil criterion 1.2.2 *("Consistency of Privacy Policies and Procedures with Laws and Regulations*") [17]. This criterion elaborates that privacy policies should be reviewed and updated when laws and regulations undergo changes. Smith [16] asserts that a proactive policy process is the backbone of the privacy approach for organisations processing personal information. He advances that to begin such a process, an audit of existing practices will be of relevance. Furthermore, criterion 1.2.11 (Changes in regulatory and business requirements) stipulates that changes in the legal & regulatory requirements is identified and addressed [17]. This criterion is of relevance in light of the imminent enforcement of POPI. Criterion (1.2.2) is linked to several other criteria throughout GAPP that focusses on the pertinent laws and regulations [17]. The GAPP framework, comprising of the ten privacy principles with the relevant criteria can be used to inform the design, implementation and communication of privacy policies [17].

The GAPP criterion 1.2.3 (Personal Information Identification and Classification) stipulates a classification process which identifies and classifies information into one or more of the following categories: Business confidential, Personal information (sensitive and other personal information eg. Special PI), Business general and Public [17]. This is of benefit due to variations in legislative provisions concerning different classes of PI. Identifying the data associated with personal information facilities identifying the processes that involve personal data, and for the owner of those processes [12]

When mapping POPI onto GAPP, there are two types of PI that GAPP does not provide a comprehensive elucidation as compared to POPI, therefore GAPP falls short in providing specific detailed safeguard criteria in these two categories. The first is special personal information, as outlined in sections 26 to 33 of POPI. The second aspect is processing personal information of children (Sections thirty four and thirty five). POPI (Section fifty seven) further elaborates on the processing of these two categories of PI. Therefore, since these two categories of PI is not expanded on under the GAPP principles, it is suggested that the comprehensive provisions in POPI be used relating to 'Security Safeguards' for these two categories of PI. POPI is explicit that in an event of breach of data privacy, fines that are imposed will consider "the nature of the personal information involved" [9] and "any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protect personal information" [9].

Schroeder and Cohen [12] recommend that organisations use a flowchart depicting the flow of PI, including inputs, processing, storage points, outputs, personnel and/or third parties that are involved in various aspects of the flow, as well as persons who have access to PI. The data flow documentation can identify any points in the data flow that represent significant risks and whether mitigating controls exist for those risks. The flow chart should identify the information system components (networks, applications, databases, end-user computing etc.) used in receipt, processing, storage, access and reporting of PI [12]. All documentation from step one are integral for step two (Risk Assessment).

This study now examines its core focus, Security Safeguards (Condition seven of POPI), which is aligned to Principle eight of GAPP ('Security and Privacy'). Table 1 outlines the mapping of POPI onto GAPP with the grey shaded rows containing POPI legislation for 'Security Safeguards' and the unshaded white rows containing GAPP measures. The rest of this section deals with the mapping process, constantly referencing to Table 1 which contains the relevant interrelated content from POPI and GAPP. 'Security Safeguards' begins with Section 19(1) in POPI i.e. 'Security measures on integrity and confidentiality of PI' (Table 1). GAPP recommends an 'Information Security Program' (Table 1) to address the various areas (a-l) in relation to 'Security Safeguards'. These 12 areas identified by GAPP are referenced from ISO/IEC 27002:2005.

B. Step Two: Risk Assessment

Section 19(2) of POPI [9] is explicit on a risk-based approach towards 'Security Safeguards' (Table 1). This correlates with GAPP that asserts once information is identified and categorized, a risk assessment study should be conducted. This study attempts to map the related sub-sections (19(2)(a) to 19(2)(d)) of POPI (Table 1), with GAPP, to address the risk based approach. The documentation compiled in step one (data inventory and privacy nexus) is used to fulfil the GAPP criteria 'Risk Assessment' (Table 1) which falls under GAPP's first principle (Management Criteria) [12]. GAPP asserts that the risk assessment process is used to establish a risk baseline, identify new or changed risks to personal information and to develop and update responses to such risks [17]. This criterion enables the organisation to understand the inherent risks associated with PI; especially, considering that this criterion states that failure to comply with regularity requirement, is a risk. Consequently, the current data privacy legislation such as POPI could inform the risk assessment process which in turn guides privacy policy development as part of the risk treatment. The information flow and understanding of the role of IT and third parties facilitates identifying inherent operational risks associated with the protection of PI, and whether appropriate mitigating controls exist. Considering information security as a critical component of privacy risk management, the risk assessment should include assessment of specific information

security related risks [12]. The two categories of PI mentioned earlier (Special PI and Childrens'PI) for which the criteria in GAPP does not do justice, should be addressed. POPI explicitly outlines the conditions for processing these two categories of PI, hence, one option could be to extract criteria from POPI itself.

Section 19(2)(b) of POPI calls for safeguards against the identified risks which is mapped to GAPP as follows: Proceeding from risk assessment, GAPP provides a comprehensive outline of the administrative, technical, and physical safeguards in accordance with the risk assessment. Table 1 (3. Procedures and Controls) lists these safeguards which GAPP discusses in great length. Section 19(2)(c) of POPI refers to verifying the effective implementation of safeguards and section 19(2)(d) calls for updating of safeguards which is aligned to (3f) and (4) of GAPP (Table 1).

Step three of Schroeder and Cohen's [12] five step process for the deployment of GAPP entails assessing compliance against GAPP criteria, but this research further delves into its key focus area: Security Safeguards. Section (20) of POPI (Table 1) addresses "Information processed by operator or person acting under authority" which relates to third parties. This is mapped to principle seven of GAPP (Disclosure to Third Parties) The GAPP principle eight (Security for Privacy) mentions the identification of "third parties that are involved in the handling of PI", but does not give a detailed account regarding security in the context of third party. However, principle seven of GAPP (Disclosure to Third Parties), covers third party security in its entirety. The responsible party signs agreements with third parties to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms [17].

'Disclosure to Third Parties' of GAPP, starts off by stating "The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual" [17]. The GAPP guideline further elucidates the conditions (5 and 6 of Table 1) under which the third party 'handles' PI, inclusive of recommendations to evaluate the security level of third parties. These matters relating to the third party are aligned with sections 20(a) and 20(b) of POPI (Table 1).

It is incumbent on the responsible party to ensure the security of PI since according to POPI the responsible party is ultimately account able for the personal information of the data subjects even if the privacy breach was caused by the third party. The new 'General Data Protection Regulation' in the European Union proposes imposing direct statutory obligations on third parties to maintain appropriate documentation for data privacy. The GAPP guideline proceeds to provide insight on measures to be taken in case of misuse of personal information by a third party (Number 8 of Table 1).

The last section (22) under condition seven of POPI ('Security Safeguards') addresses 'Notification of security compromises'. This is aligned to the first principle of GAPP ('Privacy Incident and Breach Management') and the last principle of GAPP (Monitoring and Enforcement). Although POPI focuses on explicit procedures to inform the data subject of breach in security of personal information, the guideline goes beyond notification; dealing with managing the privacy breach (9 and 10 of Table 1). Steps Three, Four and Five of Schroeder and Cohen's [12] five step process does not fall within the scope of this study and is therefore not examined in detail. Nevertheless, a brief summary is provided.

C. Step Three: Assess compliance against GAPP criteria

The organisation reviews its existing privacy management policies, procedures and control functions relative to the specific criteria defined in the GAPP framework [12]. Schroeder and Cohen [12] recommend leveraging the criteria included in GAPP, including Privacy Awareness and Training (Criterion 1.2.10), Risk Assessment (Criterion 1.2.4), and Information Security Program (Criterion 8.2.1) to guide a systematic study of policies and procedures governing employers' expectations, monitoring techniques and practices of firms, and employee training processes [17].

D. Step Four: Establish GAPP-based controls

Management remediates control gaps identified in the GAPP compliance assessment [12]. The organization should update the GAPP assessment report periodically together with policies and procedures so that they provide a true reflection of existing controls [12].

E. Step Five: Monitor GAPP controls.

The tenth GAPP principle ("Monitoring and Enforcement") provides criteria associated with monitoring and a range of compliance considerations. The literature on data security underlines management's commitment to policy enforcement; reiterating that policy must be enforced to be effective and without enforcement, policies might as well not exist [20]. In addition, executives should foster a climate where employees can openly raise concerns regarding information privacy [6].

III. DISCUSSION

In light of the pending enactment of the data privacy legislation POPI, in South Africa, entities are anxious on how to comply with this legislation. This study makes a contribution to management and security practitioners by advancing a methodology: How to map POPI with GAPP. The purpose of this study is to advance a possible methodology for the public and private sector to implement security measures to safeguard peoples' personal information in accordance with the POPI legislation; especially condition seven ('Security Safeguards'). A case is argued for implementing 'The Generally Accepted Privacy Principles' (GAPP) framework to comply with the 'Protection of personal information' (POPI) data privacy legislation. The study highlights Schroeder and Cohen's [12] five step process to implement GAPP, thereby informing on the processes/procedures that precede 'Security Safeguards', starting with data inventory. All of the provisions under condition seven of POPI ('Security Safeguards') was then mapped onto the GAPP principles. Provisions in POPI that were not mentioned under condition seven but closely related to 'Security Safeguards' were also examined. A mapping process then followed using the key GAPP criteria to comply

with POPI. There are instances where the GAPP criteria were found wanting, especially with respect to sensitive and children's personal information. In these cases, POPI stipulated more detailed provisions on data security. POPI could be the source of criteria to secure this category of personal information.

IV. CONCLUSION

The literature surveyed highlights GAPP as an internationally recognized privacy framework that embraces all of the major privacy legislation, including the European Union data protection framework. Considering South Africa's new data protection legislation (POPI) has been largely informed by the European Union directive, GAPP could be viewed as an opportunity to facilitate compliance with POPI. Moreover, POPI recommends applying international standards to protect personal information. In this respect, the GAPP integration could advantage entities conducting cross-border transactions, especially concerning personal information. Just as this research project mapped condition seven ('Security Safeguards') and related provisions in POPI with GAPP, a similar process could be pursued to map the other remaining conditions of POPI with GAPP to develop a more comprehensive methodology/tool that could guide information security and comply with data privacy legislation.

References

[1] R. O. Mason, "Four Ethical Issues of the Information Age," MIS Quarterly, Vol. (10:1), pp. 5-12, 1986

[2] F. Bélanger and R. E. Crossler, "Privacy in the digital age: A Review of Information Pivacy Research in Information Systems," MIS Quarterly, Vol (12:1), pp. 1017-1041, 2011

[3] R. J. Kauffman, Y. J. Lee, M. Prosch and P. J. Steinbart, "A Survey of Consumer Information Privacy from the Accounting Information Systems Perspective, Journal of Information Systems, Vol (25:2), pp. 47–79, 2011.

[4] R. Mears and L. Ponemon, "Deloitte:Privacy & Data Protection Survey," 2007. Accessible:

https://www.deloitte.com/assets/DcomShared%20Assets/Documents/us_risk_s&P_2007%20Privacy10Dec2007final.pdf 1 June 2014

[5] J. K. Winn, "Electronic Commerce Law: Direct Regulation, Co-Regulation and Self-Regulation," Facultés Universitaires Notre-Dame de la Paix, Research Centre on IT and Law, An Information Society for ALL: A Legal Challenge Conference, Jan. 21, 2010 (Namur, Belguim)

[6] H. Xu, T. Dinev, J. Smith, & P. Hart. "Information privacy concerns: linking individual perceptions with institutional privacy assurances," Journal of the Association for Information Systems. 2011

[7] L. Senden. Soft Law in European Community Law. Portland, OR: Hart Publishing. 2004

[8] L. Senden, "Soft law, self-regulation and co-regulation in European law: Where do they meet?" Electronic Journal of Comparative Law 9(1). Available at: http://www.ejcl.org 2005

[9] Minister of Justice and Constitutional Development, "The protection of personal information bill," 2013.

[10] D. Kafouris and D. Chivers, "Getting with the POPI programme. 2014

Available: http://www.itweb.co.za/index.php?option=com_content&view=article&id=69449

[11] M. Prosch, "Protecting personal information using Generally Accepted Accounting Principles and continuous control monitoring," International Journal of Disclosure and Governance, Vol. (5:2), pp 153–166, 2008.

[12] D. Schroeder and N.A. Cohen, "GAPP Targets,"Journal of Accountancy, 2011

[13] K. Askelson, "Reasonable Security Practices: The AICPA/CICA Privacy Framework," The CPA Journal, pp. 10-12, 2005

[14] J. Luftman, and R. Kempaiah, "Key Issues for IT Executives," MIS Quarterly Executive, Vol. 7(2). 2008

[15] L. Volonino, G. Gessner and G. Kermis, "Sarbanes-Oxley link to IT Corporate Compliance," AMCIS, 2004

[16] H. J. Smith, "Privacy policies and Practices: Inside the Organisational Maze," Communications of the ACM, Vol. (36:12), pp 105-122, 1993

[17] American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA/CICA). Generally Accepted Privacy Principles (GAPP). Practitioner Version. 2009

[18] G. Eschelbeck, Sophos Security Threat Report 2014. Sophos, Dec. 2013. [Online]. Available: http://blogs.sophos.com/2013/12/10/ sophos-security-threat-report-2014/

[19] K. J. Knapp, R.F. Morris, T.E. Marshall and T.A. Byrd, " Information security policy: An organizational-level process model," Computers & Security Vol. (28) pp 493– 508. 2009

[20] J. Leach. "Improving user security behaviour," Computers & Security Vol. (22:8) pp 685–92. 2003.

TABLE 1. MAPPING OF POPI LEGISLATION (CONDITION 7: DATA SECURITY) WITH GAPP.
SOURCE: POPI [9] AND GAPP [17]

POPI: Condition 7 (Security Safeguards)	**NB. Grey background refers to POPI provisions; white background refers to GAPP principles/criteria**
Security measures on integrity and confidentiality of personal information **Section 19 (1)** A responsible party must secure the integrity and confidentiality of personal information by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information; and unlawful access to or processing of personal information.	
***1.Information Security Program*:** A security program should be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas, insofar as they relate to the security of personal information (ISO/IEC27002:2005): a. Risk assessment and treatment b. Security policy	c. Organization of information security d. Asset management e. Human resources security f. Physical and environmental security g. Communications and operations management h. Access control i. Information systems acquisition, development, and maintenance j. Information security incident management k. Business continuity management l. Compliance
Section 19 (2)(a) The responsible party must take reasonable measures to identify all reasonably foreseeable internal and external risks to personal information, **(b)** establish and maintain appropriate safeguards against the risks identified, **(c)** regularly verify that the safeguards are effectively implemented and **(d)** ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards. NB. Also see Section 108 (g) for how the Regulator imposes fines: "any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protect personal information"	
2. Risk Assessment A process is in place to periodically identify the risks to the entity's personal information. Such risks may be external (such as loss of information by vendors or failure to comply with regulatory requirements) or internal (such as e-mailing unprotected sensitive information). When new or changed risks are identified, the privacy risk assessment and the response strategies are updated. Ideally, the privacy risk assessment should be integrated with the security risk assessment and be a part of the entity's overall enterprise risk management program. The board or a committee of the board should provide oversight and review of the privacy risk assessment. **3. Procedures and Controls** a. Logical Access Controls: Logical access to personal information is restricted by procedures that address various matters as expanded under principle 8 of GAPP. b. Physical Access Controls: Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information). c. Environmental Safeguards: Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.	d. Transmitted Personal Information: Personal information is protected when transmitted by mail or other physical means. Personal information transmitted over the Internet, over public and other non-secure networks, and wireless networks is protected by deploying industry standard encryption technology for transferring and receiving personal information. e. Personal Information on Portable Media: Personal information stored on portable media or devices is protected from unauthorized access. f. Testing Security Safeguards: Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually. **4. Audits**: Periodically undertake independent audits of security controls using either internal or external auditors. Conduct the following: a. test card access systems and other physical security devices at least annually. b. document and test disaster recovery and contingency plans at least annually to ensure their viability. c. periodically undertake threat and vulnerability testing, including security penetration and Web vulnerability and resilience. d. make appropriate modifications to security policies and procedures on a periodic basis, taking into consideration the results of tests performed and new and changing threats and vulnerabilities. e. periodically report the results of security testing to management
Information processed by operator or person acting under authority **Section 20** Anyone processing personal information on behalf of a responsible party (operator/third party), must: (a) process such information only with the knowledge or authorisation of the responsible party, (b) treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties. A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.	
5. Systems and procedures are in place to: a. prevent the disclosure of personal information to third parties unless an individual has given implicit or explicit consent for the disclosure. b. document nature & extent of personal information disclosed to third parties. c. refers any requests for access or complaints about the personal information transferred by the entity to a designated privacy executive, e.g. Privacy Officer. d. specifies how and when third parties are to dispose of or return any personal information provided by the entity. e. test whether disclosure to third parties is in compliance with entity's privacy policies and procedures, or as specifically required by law or regulation. f. document any third-party disclosures for legal reasons.	g. refers any requests for access or complaints about the personal information transferred by the entity to a designated privacy executive, such as a corporate privacy officer. h. specifies how and when third parties are to dispose of or return any personal information provided by the entity. **6. The responsible party has agreements with the third party that:** a. limits the third party's use of personal information to purposes necessary to fulfill the contract. b. communicates the individual's preferences to the third party. **7. The entity evaluates compliance with such contract using one or more of the following approaches to obtain an increasing level of assurance depending on its risk assessment:** a. The third party responds to a questionnaire about their practices. b. The third party self-certifies that its practices meet the entity's requirements based on internal audit reports or other procedures. c. The entity performs an onsite evaluation of the third party. d. The entity receives an audit or similar report provided by an independent auditor.
Section 21. The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person	

8. Misuse of Personal Information by a Third Party: *The entity:* a. reviews complaints to identify indications of any misuse of personal information by third parties b. responds to any knowledge of a third party using or disclosing personal information in variance with the entity's privacy policies and procedures or contractual arrangements.	c. mitigates, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the entity's privacy policies and procedures (for example, notify individuals affected, attempt to recover information disclosed to others, void affected numbers and reissue new numbers). d. takes remedial action in the event that a third party misuses personal information (for example, contractual clauses address the ramification of misuse of personal information).
Section 22. Notification of security compromises	
9. Breach Notification The entity has a privacy breach notification policy, supported by a. a process for identifying the notification and related requirements of other applicable jurisdictions relating to the data subjects affected by the breach, b. a process for assessing the need for stakeholders breach notification, if required by law, regulation, or policy, and c. a process for delivering the notice in a timely manner. The corporate privacy officer or other designated individual is authorized to address privacy related complaints, disputes, and other problems. Systems and procedures are in place that allow for: a. procedures to be followed in communicating and resolving complaints about the entity. b. action that will be taken with respect to the disputed information until the complaint is satisfactorily resolved. c. remedies to be available in case of a breach of personal information and how to communicate this information to an individual. d. recourse and a formal escalation process to be in place to review and approve any recourse offered to individuals.	**10. Privacy Incident and Breach Management** A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following: a. Procedures for the identification, management, and resolution of privacy incidents and breaches b. Defined responsibilities c. A process to identify incident severity and determine required actions and escalation procedures d. A process for complying with breach laws and regulations e. An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties, or discipline as appropriate f. A process for periodic review (at least on an annual basis) of actual incidents to identify necessary program updates based on the following: (i) Incident patterns and root cause (ii) Changes in the internal control environment or external requirements (regulation or legislation) g. Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed.