Towards Building a Privacy Programme: A Personal Journey

By Russell Raizenberg, CGEIT, CRISC

COBIT Focus | 12 October 2015

During November 2013, South Africa enacted legislation that seeks to regulate the processing of personal information. It is known as the Protection of Personal Information Act of 2013 (POPIA). Given its infancy and the number of entities seeking compliance, it is understandable that existing resources are limited, constrained and, very likely, expensive. Once fully promulgated, entities processing personal information will have 12 months to demonstrate compliance. What follows is a glimpse into a personal journey towards building a privacy programme and how COBIT® 5 has assisted in structuring the approach, consolidating research, thinking beyond IT, and providing detailed guidance in most areas of enablement and implementation.

COBIT 5, based on 5 key principles, is a comprehensive framework which helps enterprises, regardless of size or operation, create value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. These principles are:

- Meeting Stakeholder Needs
- Covering the Enterprise End-to-end
- Applying a Single Integrated Framework
- Enabling a Holistic Approach through the following set of Enablers:
  - Principles, Policies and Frameworks
  - Processes
  - Organisational Structures
  - Culture, Ethics and Behaviour
  - Information
  - Services, Infrastructure and Applications
  - People, Skills and Competencies
- Separating Governance From Management

Meeting Stakeholder Needs

Besides information being ever more pervasive, an enterprise's need to create and maintain value is made that much more challenging with the rapid evolution of disruptive technology. The rate and pace of change bring about new risk and sometimes diminish existing capabilities to contain and manage the risk.
This is further impacted by the inherently sensitive nature of personal information and the additional requirements for protection it attracts. The case for responding to legislation should not only be driven by the need to achieve compliance. Risk mitigation, subsequent controls enhancement, audit assurance and opportunities for continuous improvement will certainly be value-driven consequences of an effective and ongoing privacy programme.

---

Regardless of the operation, it is vital that all privacy-impacted processes and all stakeholders, internal and external, local or global, be identified and the stakeholders’ respective responsibilities be communicated, understood and enforced.

---

Covering the Enterprise End-to-end

Privacy issues affect the entire organisation. In today's world it is difficult to imagine any entity, regardless of size, doing business in isolation. For example, there is the possibility that a doctor's practice could communicate the personal information of its 2, and only, administrative staff to a bank when it comes to month-end salary payments and that same doctor's practice could be using, storing and sharing the personal information of hundreds of patients. A medium-sized company could be collecting the biometric information of its employees to support attendance records or perhaps closed-circuit television (CCTV) images of its visitors as part of its security procedures. A supermarket chain could be sharing the personal information of its customers amongst various departments or possibly disclosing personal information to support some litigation or police investigation. A multinational organisation could task the processing of personal information to a division in a different country or, perhaps, to a third-party processor in another country.

Regardless of the operation, it is vital that all privacy-impacted processes and all stakeholders, internal and external, local or global, be identified and the stakeholders’ respective responsibilities be communicated, understood and enforced.

Applying a Single Integrated Framework

Many governments and regional authorities around the world have introduced some form of privacy legislation and, through various institutions, issued standards, frameworks and certifications that assist with the development and implementation of privacy programmes. These include, for example, the US National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO) and various information commissioners’ offices across Europe and Australasia as well as the International Association of Privacy Professionals (IAPP). Some may have a regional or national bias but, by and large, there is a high degree of overlap.

ISACA® has produced, amongst others things, webinars, white papers, articles and training focusing on privacy. As a single, integrated framework, the maturity, depth and applicability of COBIT® 5, even as it stands now, has proven very useful in consolidating my research and approach towards finalising a privacy programme—no doubt, in my opinion, preparing the way for a dedicated professional guide to data privacy.

Enabling a Holistic Approach

Like any goal on its balanced scorecard (BSC), the enterprise's goal to achieve and maintain compliance with external laws and regulations, coupled with the related IT goals, must be translated to enabler goals. It is important to remember that these enablers should not only support IT-related goals, but should cut across the entire
organisation. So, for example, while ‘Managed IT-related business risk’ may be a secondary IT-related goal, it is important to view the risk of non-compliance across the entire organisation.

**Principles, Policies and Frameworks**

In any South African enterprise’s pursuit of its principle to operate within the bounds of legislative and regulatory demands, it must also look to the principles established in POPIA. South Africa’s newly introduced privacy legislation is based on the 8 core privacy protection principles found in legislation within jurisdictions such as the European Union (EU) and the Organisation for Economic Co-operation and Development (OECD). Clearly, it is imperative that the organisation’s executive must define and uphold a data privacy policy that covers all the requirements of the legislation. This is crucial to the organisation’s identification of all stakeholders as well as its understanding of the intent and direction towards the successful deployment and ongoing management and maintenance of its privacy programme.

Supporting the policy should be a code of conduct, standards, practices, procedures, rules and other policies that cover elements such as information classification, labelling, handling and protection, and clear guidelines as to the acceptable use of digital assets. Agreements between the company and any third-party operators or processors must clearly define roles and responsibilities, rights to audit or assess, and consequences for non-compliance. Binding corporate rules are essential to communicating the data privacy policy’s intent and direction across divisions of a South African-based multinational.

A CCTV policy is essential where CCTV is in use. Existing policies, such as monitoring policies in human resources (HR), must be optimised. Depending on operations, data sharing or disclosure policies must be considered. Referencing such frameworks as those mentioned earlier is essential.

The related requirements of other associated South African legislation must also be considered. These include legislation covering areas such as consumer protection, public access to information, credit regulation, interception of communications, electronic communications and transactions, and any codes of conduct as may be defined by industries such as health or finance.

**Processes**

Bear in mind that the enterprise must be covered end to end. While the goals cascade typically culminates in IT-related processes, applying it beyond IT should trigger ideas or opportunities for its application in business-related processes.

By way of example, consider the enterprise goal of compliance mapping to the IT-related goal of compliance, which, in turn, maps to primary COBIT 5 processes such as APO12 Manage Risk and APO13 Manage Security. It is quite possible that, while IT is responsible for controlling the physical access to data centres, services such as building access control or CCTV monitoring are not necessarily managed or controlled by IT, but rather by the business security division. In this scenario, business security and HR would be the primary stakeholders responsible for ensuring compliance with privacy legislation.

**Organisational Structures**

POPIA defines an information officer as being the head of any organisation. He or she is ultimately accountable for the organisation’s compliance. Of course, deputy information officers may be appointed. When developing a Responsible, Accountable, Consulted, Informed (RACI) chart, top-down, bottom-up, internal-external and local-global are the dimensions to be considered.

External stakeholders include the regulator and all data subjects, suppliers and outsourced partners. Internally, information owners (or producers) such as a sales manager or an HR director are specifically responsible for the appropriate access to and classification, integrity and handling of information of their respective data subjects, i.e., customers and employees, respectively. IT is specifically responsible for information custodianship.

These responsibilities cut across the information life cycle from collection and usage to storage and eventual
demise. Employees who might be tasked with using personal information also have a duty of care. The heads of legal, internal control and business security must ensure that the management of privacy risk and assurance is embedded in the enterprise risk management process. Staff must understand the procedures to follow in order to facilitate a subject's data access request or in the event of a privacy breach.

**Culture, Ethics and Behaviour**

As robust as technical controls may be, human behaviour is regularly identified as the weak link causing a security (and, potentially, privacy) breach. A sensitive discussion in an airport lounge, unverified meeting attendees, a lost or stolen unencrypted laptop or flash drive, a soft hack via switchboard, unshredded confidential waste and an uncleaned whiteboard are examples of potential breach scenarios triggered by human behaviour. The executive and senior management must set the tone at the top and lead by example. Everyone is responsible—from the executive through to the person tasked with cleaning a whiteboard after meetings.

Privacy rights and expected behaviours should be embedded in a code of conduct. It is important to stay focused and have the creativity and stamina to maintain training and awareness. One way to do that, for example, is to have an annual privacy housekeeping week. It is also a good practice to recognise good behaviour. A privacy programme is ongoing and not a one-time-only event.

In today's world, people easily, sometimes recklessly, and other times unknowingly give up their rights to privacy. There are big wins in getting employees to appreciate their rights as enshrined in POPIA. It should stand to reason that they would then appreciate how to handle the personal information of others when going about their normal course of business. ‘Know your rights, know your responsibilities!’ could be a good maxim.

**Information**

Information can be structured or unstructured, formalised or informalised, digital or physical, and, as we know, pervasive throughout the enterprise. Many would concur that information is the organisation's most important asset. Stakeholders deriving value from the processing of information can be both internal and external. The conditions, or principles, in POPIA cut to the heart of the proper processing of not only personal information, but also special personal information as well as the personal information of children. These conditions include:

- Processing with limitations and for a specific purpose
- Ensuring information quality and openness with data subjects
- Maintaining confidentiality
- Maintaining availability and integrity
- Facilitating data subjects’ access to their information

A breach of these conditions could lead to litigation with severe financial and reputational implications. It is useful to bear in mind the multiple stages of processing, from collection through demise.

There are a multitude of frameworks, standards and guides provided by the likes of NIST, SANS Critical Security Controls, ISO and ISACA that cover topics such as cyber and information security, privacy risk management, privacy impact analysis, and privacy by design. For example, NIST's *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* provides specific focus to personal information, especially identification, impact levels, safeguards and breach response.

The COBIT 5 professional guides *COBIT® 5 for Information Security* and *COBIT® 5 for Risk*, though similar and complementary to other guides, regularly provide much more detailed guidance, especially around enablement and implementation. *COBIT® 5 for Information Security* addresses all 7 enablers and is particularly useful in triggering ideas for identifying and responding to privacy-related matters.

The COBIT 5 enabler guide *COBIT® 5: Enabling Information* also proves similar, complementary and more detailed guidance. However, in my opinion, the enabler guide, through addressing various governance and management issues, provides a more contemporary view and approach by including topics such as big data, predictive analytics and privacy. It may also prove worthwhile reading the ISACA white paper *Privacy and Big Data*. A useful insight
gained from a recent ISACA webinar is that there can be no privacy without security and that security alone cannot assure privacy.

Though, traditionally, it can be said that IT is the custodian of the greater portion of an organisation's information, the issues of disintermediation, as well as cloud computing, bring about a fresh set of risk factors for security and privacy management. With cloud computing, the development and acceptance of standards, specifications and guidelines appear to be in their relevant infancy. Affected organisations would be wise to pay special attention to these areas when it comes to processing of personal information.

**Services, Infrastructure and Applications**

Of particular concern should be the extent to which privacy-related issues and requirements are identified, embedded and managed within services, infrastructure and applications. In application development, for example, has privacy by design been considered and adopted? To what extent are outsourced service providers privacy-compliant? Are service level agreements (SLAs) optimised to reflect any privacy-related requirements? Do architecture principles embody privacy requirements? If not, could this, for example, be a reason for the pain experienced by HR in using in-house technology or systems?

**People, Skills and Competencies**

The successful development, implementation and ongoing management of a privacy programme is dependent on people, skills and competencies throughout the information life cycle. These will most likely be identified in a properly planned privacy programme. Resource development and utilisation can be optimised by aligning with HR and HR processes, promoting the appropriate accreditations and participating in global privacy and information security forums.

**Separating Governance From Management**

Given the infancy of the legislation and its partial overlap with existing legislation (see earlier examples), there is the risk that some, especially senior, stakeholders may discount the importance, urgency or essence of privacy requirements. This could be due to their knowledge of existing legislation and their assumption that POPIA is, basically, covered by existing legislation. How does the executive level effectively evaluate, direct and monitor if it starts off with this assumption? POPIA states that accountability lies with the head of the organisation. It is often too easy for the chief executive officer (CEO) to delegate responsibility without realising the implications of unclear directions to and expectations of management.

Management must ensure that it has a clear understanding of the data privacy policy requirements and must be empowered to justify, deploy and manage the resources necessary to deliver the privacy programme. As the executive will depend on reliable data for risk management and breach response, management must ensure the efficient deployment and maintenance of the privacy programme.

**Where to Next?**

At the time of writing, POPIA has been partially promulgated, which means that the Regulator's office will soon be established. Certain issues requiring clarity should then be addressed so that privacy programmes can be formalised. This is not to say that the journey to compliance should only start then. Most organisations should already have implemented, for example, an information security management system or a CCTV policy or application access controls. The challenge will come in identifying the specific privacy requirements and how they should be incorporated into existing business activity.

**Russell Raizenberg, CGEIT, CRISC**

Is an independent consultant who develops privacy and risk management solutions for clients. Previously, he was employed with BP Southern Africa in various roles which included accountant, IT manager, IT risk and compliance
manager, and project manager in South Africa and at various African affiliates of BP.