JUTA
POPIA PORTAL

ISSUE 1 • ARE YOU MATURE ENOUGH FOR POPIA? • MAY 2020

1. OVERVIEW

We explain what information governance is and why it is so important to do an information governance maturity assessment before starting a POPIA project.

2. ARE YOU MATURE ENOUGH FOR **POPIA?**

Many of our projects begin with a similar story from new clients, 'We made our first attempt to become POPIA compliant in 2015, but nothing changed. We asked ABC to help us in 2017 and we wrote 1000 policies and sent the whole company on training, but we are no more compliant today than we were in 2015. What are we doing wrong?'

So, we ask ourselves, 'Why do so many POPIA projects fail?' and 'What can we do at the beginning of projects to head trouble off at the pass?'.

After a lot of trial and error, this is our answer:

- do an information governance maturity assessment,
- pay attention to the results, and
- pick the right project for your organisation (hint, it might have nothing to do with POPIA).

2.1. WHY ARE WE TALKING ABOUT INFORMATION GOVERNANCE?

With all the hype around POPIA and data protection, organisations are forgetting that personal information is not the only class of information that is essential for doing business. For many organisations, personal information won't even be the most valuable information they use. Measured in rands and cents, their intellectual property may be more valuable.

Here are some other forms of information:

- all intellectual property (trademarks, designs, inventions, trade secrets, know-how, content or publications the organisation created, technical documents)
- information on the organisation's website
- financial information
- contracts and information about contract negotiations
- strategies and plans
- policies and procedures
- internal memoranda, minutes of meetings and agendas
- emails
- research and statistics
- personal information of customers and prospective customers (leads), employees and employment candidates, suppliers and service providers.

According to IG Initiative information governance is 'the activities and technologies that organisations employ to maximise the value of their information while minimising associated risks and costs.'

This definition by Gartner IT Glossary is a bit more complicated, but it gives you an idea of the full scope of the discipline: '…the specification of decision rights and an accountability framework to ensure appropriate behaviour in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.'

Information governance is often referred to as a 'super-discipline'. It includes records management, information security, risk management, compliance management, legal and e-discovery issues, IT governance, data governance, privacy, corporate governance

2.2. WHAT IS AN INFORMATION GOVERNANCE MATURITY ASSESSMENT?

Information governance maturity assessments help organisations to spot areas that are in need of improvement. We also use it to assess whether an organisation is ready for a POPIA project.

2.3. WHO SHOULD COMPLETE IT?

Resist relying only on your perspective, because information governance is multi-disciplinary. Ask stakeholders across the organisation to complete the information governance maturity assessment. Get perspectives from IT, legal, compliance and risk management, human resources, sales, operations, executive management, information security and records management.

The more the merrier!

2.4. WHAT DO THE RESULTS MEAN?

INFORMATION GOVERNANCE PRINCIPLE	WHAT DOES IT MEAN IF YOU SCORED BELOW 3?
Accountability Information governance is a priority for the organisation, and senior managers are responsible for it (and they know it!). Clear roles and responsibilities concerning information governance have been assigned throughout the organisation. Policies, standards and procedures have been put in place to ensure that the level of information governance can be audited.	How an organisation ranks on the accountability principle, indicates whether information governance is a priority. Becoming POPIA compliant without looking at how all information is governed is not only difficult, it's also dangerous. It is entirely possible that the organisation is faced with more significant risks to other categories of information (e.g., your intellectual property). The organisation should consider starting an information governance project instead of a POPIA project. Compliance with the POPIA can be one phase of the information governance project.
Standardisation There is an agreed way of working at the organisation. Business processes and activities are well-defined and documented in an open and verifiable way. The documentation must be available to employees and third parties who play a role in the processes and activities.	When you evaluate POPIA compliance, you are evaluating policies and procedures. If there are none, or they are poorly implemented, you have nothing to evaluate. So, if your organisation does not have a documented way of working, POPIA compliance will not be possible. The organisation should consider starting a corporate governance project instead of a POPIA project.

INFORMATION GOVERNANCE PRINCIPLE	WHAT DOES IT MEAN IF YOU SCORED BELOW 3?
Confidentiality Confidential and personal information must be protected from unauthorised destruction, modification or access.	Confidentiality is one leg of the CIA triad, which is used in information security management. It is also a requirement of the POPIA. If an organisation does not proactively protect the confidentiality of its information, it should consider starting an information security management project, before it embarks on a POPIA project.
Integrity The right processes are in place to guarantee that information is comprehensible, clear, consistent and reliable.	Integrity is one leg of the CIA triad, which is used in information security management. It is also a requirement of the POPIA (in respect of personal information). If an organisation does not have processes to ensure the integrity of its information, it should consider starting an information security management project, before it starts a POPIA project.
Availability Policies and business continuity plans are in place to ensure that information, and the infrastructure the organisation needs to manage and use that information, is available to the appropriate people at the appropriate time.	Availability is one leg of the CIA triad, which is used in information security management. It is also a POPIA requirement (in respect of personal information). An organisation's business continuity plans must include plans to ensure the availability of information and information infrastructure. If the business does not do business continuity planning, or if information assets are not included in its business continuity planning, the organisation should consider a business continuity management project, before it starts a POPIA project.

INFORMATION GOVERNANCE PRINCIPLE	WHAT DOES IT MEAN IF YOU SCORED BELOW 3?
Compliance The organisation has structures, policies and processes in place to ensure that the organisation complies with all legislation, supervisory requirements created by Regulators, codes of conduct and other rules, codes of conduct or standards that apply to the organisation. There is a continuous process through which compliance risks are identified, analysed (rated according to their impact and likelihood), addressed and monitored. This forms part of the organisation's enterprise risk management process.	Almost all types of information are regulated in some way or another. The introduction of the POPIA creates significant regulatory compliance risk. If an organisation does not have a reasonably mature compliance management function, POPIA compliance is impossible. Also, if the organisation is not currently managing regulatory risk, there are likely areas of non-compliance with other legislation that exposes the organisation to bigger risks than the POPIA. The organisation should consider doing a compliance management project before it starts a POPIA project. If the organisation does not manage any form of risk, it should consider undertaking an enterprise risk management project.
Records management The organisation manages records (information maintained as evidence of actions or decisions). The organisation only retains information for as long as it is required by legal, regulatory, fiscal, operational and historical requirements.	The organisation should consider doing a records management project before it starts a POPIA project.
Change management and empowerment The organisation pro-actively manages change by assessing the impact of events and strategies on its policies, processes, infrastructure and people. The organisation's employees are empowered through training and skills development to work responsibly with information and to protect it.	The POPIA is not an IT problem; it is a people problem. The majority of information risks are either caused or exacerbated by human error. If the organisation does not have a strong culture of change management and empowering people through training and skills development, POPIA compliance will be tough to achieve and maintain. The organisation should consider strengthening its change management function before starting a POPIA project.

2.5. NEXT!

If it turns out that you are ready for POPIA, our first step is always to draft a POPIA Compliance Framework and to check whether you have the right policies.

If you are not ready, take a deep breath. Doing POPIA just for the sake of doing it, is not a good idea. Firstly, because you probably have bigger things to worry about. Secondly, you will end up frustrating the hell out of your organisation and wasting precious time, resources and money on false starts. Record the results of your information governance maturity assessment and create a strategy to address the deficiencies. By all means, include POPIA in that picture, but make sure that it is in the right place.

juta