A guide to implementing the POPIA

UNIVERSITIES SOUTH AFRICA

Table of contents

An overview

We have created this guide for Information Officers to help you create and implement a successful POPIA Programme at your University.

Key concepts

The Information Officer's responsibilities

Before we get started, let's look at what the POPIA says about your duties as an Information Officer. The POPIA says that the Information Officer must:

- develop, implement, monitor and maintain a POPIA Compliance Framework;
- ensure that personal information impact assessments are performed;
- develop, monitor, maintain and distribute a PAIA manual;
- develop procedures and a system to process requests for access to personal information; and
- conduct internal awareness training.

Consider the verbs...

Develop	The Information Officer must ensure that the framework is created. This is done through obtaining executive sponsorship, doing stakeholder consultation, defining roles and responsibilities and policy development.
Implement	This is done by implementing the policies created during the development phase
Monitor and maintain	This is done through compliance monitoring and audit and by responding to the findings made.

Why do we call it a POPIA Programme, and not a Project?

A POPIA Programme is a set of activities that the Information Officer must undertake within a certain period (e.g. annually). Typically, you must review specific policies and procedures, complete personal information assessments and monitor POPIA compliance. It should become a permanent fixture at the University[1].

By contrast, A POPIA Project has a defined beginning and end, with a defined scope, resources and deliverables. The aim of a POPIA Project is often to establish a POPIA Programme.

What is a POPIA compliance framework?

It is referred to in item 4(1)(a) of the POPIA Regulations.

It is not necessarily a document. Rather, it is comprised of all of the strategies, initiatives, policies, procedures, standards and guidelines that work together to achieve POPIA compliance. However, it is a good idea to create a document that ties all of this together to make it easier to audit POPIA compliance and to demonstrate compliance to the Information Regulator.

What are Personal Information Impact Assessments

The assessments are referred to in item 4(1)(b) of the POPIA Regulations. The assessment may be comprised of a procedure, questionnaires, templates and other tools.

[1] This definition is borrowed and adapted from The Generally Accepted Compliance Practice framework ('GACP') definition of 'compliance programme'.

An overview of a POPIA Compliance Framework

One of your responsibilities as an information officer is to 'ensure that…a compliance framework is developed, implemented, monitored and maintained.'[2] Compliance officers will not be strangers to this obligations as it bears an uncanny resemblance to the definition of a 'compliance framework' in the Generally Accepted Compliance Framework issued by the Compliance Institute South Africa. With some minor adjustments, a POPIA compliance framework could be defined as 'all of the interrelated and/or interacting components within a university that:

- Set out the university's approach to the management of [POPIA] risk. The framework addresses aspects such as compliance strategy, objectives, governance, policy, roles and responsibilities, compliance risk appetite, process and techniques and reporting.
- Establish and maintain (or contribute to, support, facilitate or enabling establishing and maintaining) [POPIA] related objectives and the activities, policies, procedures, processes and practices to achieve those objectives; and
- Direct, guide, contribute to, facilitate, enable or support [POPIA] related practices and activities.'[3]

For universities who already have a compliance framework, POPIA and personal information risk, as a category of 'compliance risk' would form part of that larger framework.

[2] Item 4(1)(a) of the POPIA Regulations.
[3] This definition is borrowed and adapted from the definition of 'compliance framework' in the GACP.

Change management

IN THE CODE: PART C SECTION 1; PART D SECTIONS 1 & 2

Change management is built around a set of practices based on an understanding of how people respond to change, to effectively prepare, equip, and support people through change. Like project management, change management requires a plan. While project management focuses on costs and deliverables, a change management plan focuses on the changes in mindsets, skills and knowledge that will be required to achieve POPIA compliance.

Protection of personal information is a people problem.

1. To become POPIA compliant, the University will have to change the way it operates. If people do not adopt these changes, POPIA compliance will remain elusive.
2. Human error is one of the leading causes of data breaches.[4] This means that training should be a large component of your POPIA Project.
3. Some employees will have new roles that will require new skills.

The success of your POPIA Programme depends on how well you manage people and how well you manage change. The worst outcome of a POPIA project is that nothing changes.

[4]https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

DO THIS...

Create a change management plan. A change management plan focuses on the changes that you need to make to become POPIA compliant. These changes can include changes in mindsets, skills and knowledge. Answer these questions in your change management plan:

- **Why** should the University become POPIA compliant? The key is to understand that different groups of people within the University are motivated by different things. Make sure you include all motivations.
- **What** needs to change to achieve POPIA compliance?
- **Who** needs to be involved in the POPIA project? This is also referred to as stakeholder engagement.
- **How** and when do things need to change? A communication and training plan is essential to achieving POPIA compliance.

Resources

The IAPP (International Association of Privacy Professionals) has a great GDPR Compliance Framework template example and guideline that can easily be adapted for POPIA purposes.

The UK's information regulator – the ICO – has recently released a guide and tool to help organisations create their own 'accountability framework' for privacy risk management. The guide and tool were created for GDPR purposes – but can easily be adapted for the POPIA as the core principles are the same.

The Centre for Information Policy Leadership published a fantastic report in 2020 called 'What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework'. This report provides guidance on all the essential elements for a POPIA compliance framework, and uses case studies from many international organisations including several universities about what has and has not worked for their data privacy compliance programmes.

This is a great example of a regular compliance framework by an Australian university which can easily be adapted to incorporate the elements of a POPIA compliance framework.

Executive sponsorship

IN THE CODE: PART A

The POPIA affects most processes in a university, so having the support of its leadership is vital in establishing a sustainable, and well-funded, POPIA Programme.

DO THIS...

Make a list of the executive sponsorship you have or will need for your POPIA framework. If you don't have support from the top, think about how you are going to get it.

Use some of these arguments to convince executives that POPIA Programmes are worth investing in:

- Data breaches can be very costly. According to IBM and the Ponemon Institute, the average cost of data breaches in 2020 stood at $3.9 million. These costs are allocated to regulatory fines, civil liability, disruptions in operations, business continuity risk, unexpected financial expenditure and the loss of goodwill.
- POPIA Programmes can save you money. POPIA Programmes can mitigate losses from data breaches, enable agility and innovation, achieve operational efficiency from data controls, make the University more attractive to investors and build loyalty and trust with stakeholders.
- By embedding privacy in the structures of the University, you can attract stakeholders who feel very strongly about privacy (also called 'privacy actives').
- Other universities are investing in privacy. It is pivotal that the University keeps up with this change in the amount of attention that privacy is getting at universities to stay competitive.

Resources

The 'carrot approach'

Benefits of data privacy programmes for organisations – CISCO has a great report on this.

The Centre for Information Policy Leadership also published a fantastic report in 2020 called 'What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework'. This report gives great guidance on getting executive buy-in for privacy programmes, and why this so important.

The growing stakeholder and consumer base known as the 'privacy actives'. PWC has released a survey which outlines how privacy is becoming more and more important to consumers, and why organisations can benefit from taking the privacy of their customers seriously.

The 'stick approach'

IBM's annual 'Cost of a data breach' report outlines exactly how expensive data breaches are – and how taking preventative measures can save organisations a lot of money if a data breach occurs.

A university example

Here, a UK university Vice-Chancellor discusses why universities need to take data breaches and cybersecurity threats very seriously.

This article explains that half the universities in the UK have suffered data breaches in the past 12 months.

Stakeholder consultation

POPIA compliance, and by extension, a POPIA Programme is a massive exercise in teamwork and coordination, so stakeholder consultation is essential. Failing to manage important stakeholders can undermine a POPIA Programme.

DO THIS...

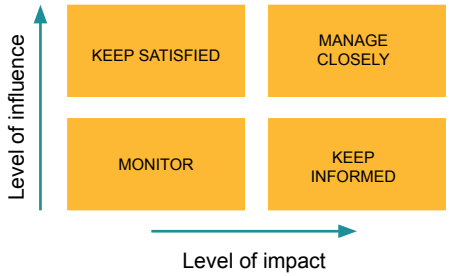
Create a stakeholder engagement plan. Identify the following stakeholders:

- Those who **govern** the change: Who are the decision-makers? Who approves new policies? Who are the leaders?
- Those who must give **input**: Who will help to develop new policies and procedures? Who understands the impacts of new policies and procedures?
- Those who are **affected** by the change: Who will need to change how they work?
- Those whose **support** you need: Who in the university already has some of the skills required to implement a POPIA Programme?

Once you've identified the stakeholders, assess the impact of the POPIA Programme on each stakeholder. You can determine how you should engage a stakeholder by assessing the level of influence of the stakeholder and the degree to which the POPIA Programme will affect them.

In your stakeholder engagement plan, include the following information for each stakeholder:

- What kind of impact well the POPIA have on them?
- Do they already fulfil some of the functions required by the POPIA?
- Can they assist in the POPIA project?
- How can the POPIA project or a POPIA programme assist them?



* Influence means the capacity of the stakeholder to affect the behaviour, development or culture of the university and its employees.

** Impact means the level of change to which the stakeholder will be affected by POPIA.

Resources

Here is a short blog about the important stakeholders and their roles for privacy programmes in general by SAP.

The IAPP has also written a series of articles on stakeholder engagement for privacy programmes called 'the three As of successful privacy programmes'.

'Stakeholders are anyone in [a university] who will kill a good idea out of spite or political ill will'.

- Unsuck-it.com

Stakeholder consultation

One way to identify stakeholders is to make a chart of the different functional areas within a university. Here is a typical one:

Define roles and responsibilities

IN THE CODE: PART D SECTION 1, PART C SECTION 13, PART C SECTION 16.9.1, PART C SECTION 19, PART C SECTION 21, PART D SECTION 2

In risk and compliance management, it is considered best practice to follow the three lines of defence model. To properly comply with the POPIA and manage the POPIA risk, all three lines need to function optimally.

What is the role of the three lines in POPIA compliance?

01	**Management** The university owns and manages the risk (not you)	It is their responsibility to manage the personal information that is processed in their area. They own the risks that could impact the processing of personal information. They must decide whether to do something about the risk or not.
02	**Compliance** Monitor, challenge, advise, and report (this is you)	Information officers and their deputies, information security officers, and other people with 'information' in their title perform a compliance and risk management function. They must interpret the POPIA, develop policies, standards, procedures and guidelines, advise the University and monitor and report on compliance with the POPIA.
03	**Independent assurance** Marks everybody's homework (not you)	They mark the other two lines' homework. Internal and external audits are used to uncover POPIA compliance issues and to avoid surprises.

DO THIS...

Ensure that the responsibilities created by the POPIA programme are included in the organisation's performance management system so that you continuously improve the performance of individuals in their roles within the POPIA Programme.

Performance management should consist of these steps:

- Align individual and team goals with the strategic objectives of the POPIA Programme. Document these goals, e.g., in key performance indicators.
- Develop plans to achieve these goals.
- Review and assess the progress of individuals and teams.
- Incorporate training to develop individuals' POPIA Programme knowledge, skills and abilities.

Resources

The Institute of Internal Auditors has a paper which explains the 'three lines of defence model'.

The Centre for Information Policy Leadership also published a fantastic report in 2020 called 'What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework'. This report gives a great overview of how to pick your 'privacy team', how reporting lines for managing privacy-related risks can work and how to integrate privacy within risk management.

UK's Durham University has a nice example of how to set out your roles and responsibilities in data privacy compliance. This example was done in reference in the GDPR, but can easily be adapted for the POPIA.

More about training

IN THE CODE: PART C SECTION 13, PART C SECTION 16.9.1, PART C SECTION 19, PART C SECTION 21, PART D SECTION 2

As Information Officer you must ensure that 'internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.'[5]

The POPIA doesn't specify who you must train. You can determine who you should train by

- applying the change management principles we have already discussed,
- considering the different groups of stakeholders you identified during the stakeholder consultation process, and
- considering the outcome of the policy impact assessment that we will discuss a little later.

CONSIDER THIS

- ☐ How will you ensure that new employees or employees who move to new positions are trained (i.e. induction training or 'onboarding').
- ☐ When will employees need refresher training?
- ☐ How will you prove that training took place, should the Regulator ask?
- ☐ What kind of infrastructure limitations are you dealing with? E.g. will participants have easy access to computers for online training or will the training have to take place face-to-face?

DO THIS...

Develop a training plan that includes how you will train employees. Work closely with your learning and development specialists in Human Resources; compliance training should not be treated differently to any other form of training.

To ensure that your training hits the mark, think about the characteristics of the audience and the level of knowledge or skill they require.

The characteristics of the audience

- How sophisticated is the audience?
- How busy are they (i.e. how much time do they have for training)?
- When is a good time for the training to take place?
- How are they usually trained, and has that worked well in the past?
- Does a replacement need to be arranged to do their job while they receive training?

The level of knowledge or skill they require:

- Do they just need to be informed of something?
- Do they need to acquire a new skill?
- Should they be tested at the end of the training to ensure that they have developed the new skill?

Resources

The UK's information regulator – the ICO – has recently released a guide and tool to assist organisations with creating their own 'accountability framework' for privacy risk management. The guide and tool were created for GDPR purposes – but again can easily be adapted for POPIA purposes as the core principles remain the same. There is a specific section on data privacy training and awareness which you can find here.

The IAPP also has a wealth of resources on data privacy training and awareness. You can start with this resource here, but have a look at the website for other resources as well.

Here, you can find Durham's University's (in the UK) Data Privacy Training Policy as an example. Durham University also created a Data Protection Awareness Sheet for staff and students that is a great resource example to adapt for POPIA purposes.

[5] Item 4(1)(e) of the POPIA Regulations.

Policy development

IN THE CODE: PART C SECTION 3.3.2, PART C SECTION 3.4.2, PART C SECTION 3.5.2, PART C SECTION 15, PART C SECTION 17, PART C SECTION 18, PART C SECTION 20, PART C SECTION 21, PART C SECTION 22.

The POPIA does not require that a university must have policies that ensure the protection of personal information. Generally speaking, you will meet the compliance obligations that the POPIA imposes by implementing 'compliance controls'. These controls are 'generally incorporated in an organisation's policies, procedures, processes, people, practice and structures, systems and technology.'[6] Policies also play an essential role in the broader discipline of information governance.

DO THIS...

The policies you need in place to manage POPIA risk will differ from university to university. Generally speaking, you need these three policies to achieve full POPIA compliance:

- Information security management
- Privacy
- Records management

They are distinct from one another because they apply to different classes of information. While the Privacy Policy only applies to personal information, the Information Security Management Policy and Records Management Policy applies to all types of information. Often, organisations will make the Information Officer or a specific Deputy Information Officer, the policy owner, but not always. This is another reason to keep them separate.

Important: A 'privacy policy' is not the same as a privacy notice. A privacy notice is a notification to a data subject and are used to comply with section 18.

Resources

For your **Data Privacy Policy** (remember this is different to the privacy notice on your website!), the IAPP has template examples that you can adapt for POPIA purposes.

The Edinburgh University has a good policy (based on the GDPR – but can easily be adapted for POPIA purposes).

There is a specific section in the ICO's accountability framework on data subject access requests.

Here is the IAPP's data subject access request template.

Here are some good university examples of data subject access request portals and procedures:

- Edinburgh University
- Reading University
- Manchester University

Dealing with data subject access requests

As the Information Officer, you must ensure that 'internal measures are developed together with adequate systems to process requests for information and access thereto.'[7] This duty refers to requests for access to information which is one of the data subject's rights in terms of section 23 of the POPIA. It may also refer to your duties in terms of the Promotion of Access to Information Act (PAIA). Be sure to reconcile your existing PAIA processes with your new POPIA processes.

[6] See the definition of 'compliance control' in the GACP.
[7] Item 4(1)*(d)* of the POPIA Regulations.

INFORMATION SECURITY MANAGEMENT POLICY

This policy applies to all types of information, not just personal information.

It describes how the University secures personal information against
- breaches of confidentiality;
- failures of integrity; and
- interruptions to the availability of information.

TOPICS IT SHOULD ADDRESS	CORRESPONDING SECTIONS IN THE POPIA	CORRESPONDING SECTIONS IN THE CODE
Information classification	Sections 5, 14, 17, 18, 19, 22, 23, 26 – 35	Part B Section 1, Part C Section 4, Part C Section 10
Access control	Sections 11, 26 -35, 69 read with Item 6 and Form 4 of the POPIA 2018 Regulations	Part C Section 3, Part C Section 4, Part C Section 5, Part C Section 16.2, Part C Section 20
Third-party management	Sections 10, 11, 13, 19, 20, 21, 22, 23(2), 72	Part C Section 1, Part C, Part C Section 13.2 Section 16, Part C Section 17.3
Information quality	Sections 5, 10, 12, 14, 16, 23(2), 24, 71, Item 3 read with Form 2	Part C Section 12, Part C Section 15, Part C Section 16.5, Part C Section 18.1
Availability and business continuity	Section 19,20, 22	Part C Section 13
Compliance with binding rules (e.g. all relevant privacy regulations, corporate governance standards, internal policies and contractual obligations)		
Responsible, empowered users	Item 4(e) of the POPIA 2018 Regulations	Part D Section 1, Part C Section 13.1, Part C Section 16.9.1,Part C Section 19, Part C Section 21, Part D Section 2
Clear roles and responsibilities in the implementation of the policy	Section 19, 20, 21	Part C, Section 13
Information security assessments	Section 19	Part C, Section 13

Resources

For your **Information Security Management Policy**, the best source is the ISO 27001 standard.

This is an example of Birmingham University's ISM Policy. Here is JISC's policy, that is based on ISO27001. Finally, check out Novation Consulting's blogs about how to formulate an incident response plan and who should be on your incident response team that can help you.

PRIVACY POLICY

This policy ensures that the organisation proactively complies with all relevant privacy regulations and respects the right to privacy of your data subjects. It only applies to personal information.

TOPICS IT SHOULD ADDRESS	CORRESPONDING SECTIONS IN THE POPIA	CORRESPONDING SECTIONS IN THE CODE
Information classification	Sections 5, 14, 17, 18, 19, 22, 23, 26 – 35	Part B Section 1, Part C Section 4, Part C Section 10
Documenting personal information processing activities	Sections 17, 18, 22, 23, 24	Part C Section 2, Part C Section 11
Purpose specification	Sections 10, 13, 14, 15, 17, 18, 69 read with Form 4 of the POPIA 2018 Regulations	Part C Section 2, Part C Section 6, Part C Section 9, Part C Section 14, Part C Section 19, Part C Section 20
Legal basis for processing activities.	Sections 11, 26 -35, 69 read with Item 6 and Form 4 of the POPIA 2018 Regulations	Part C Section 3, Part C Section 4, Part C Section 5, Part C Section 16.2, Part C Section 20
Minimality	Sections 10 and 14	Part C Section 7, Part C Section 14, Part C Section 16.3, Part C Section 19
Lawful sources	Sections 12, 16, 18	Part C Section 8, Part C Section 12.5, Part C Section 9
Transparency	Sections 5, 13, 14, 15, 17, 18, 23	Part C Section 9, Part C Section 11, Part C Section 16.4, Part C Section 17, Part C Section 18, Section 19
Information quality	Sections 5, 10, 12, 14, 16, 23(2), 24, 71, Item 3 read with Form 2	Part C Section 12, Part C Section 15, Part C Section 16.5, Part C Section 18.1
Limit sharing with third parties	Sections 10, 11, 13, 19, 20, 21, 22, 23(2), 72	Part C Section 1, Part C Section 16, Part C Section 17.3
Personal information impact assessments	Item 4(b) of the POPIA 2018 Regulations	Part D Section 1, Part D Section 3
Records retention periods	Section 14	Part C Section 15
Data subjects' rights	Sections 5, 18, 22, 23, 24, 25, 69 read with Form 4, of the POPIA 2018 Regulations, Item 2 read with Form 1, Item 3 read with Form 2, Item 4(c)and (d), Item 7 read with Part I of Form 5 and Part II of Form 5 of the POPIA 2018 Regulations	Part C Section 3.3.2, Part C Section 3.4.2, Part C Section 3.5.2, Part C Section 15, Part C Section 17, Part C Section 18, Part C Section 20, Part C Section 21, Part C Section 22
Responsible, empowered users	Item 4(e) of the POPIA 2018 Regulations	Part D Section 1, Part C Section 13.1, Part C Section 16.9.1,Part C Section 19, Part C Section 21, Part D Section 2
Information security (a cross reference to the ISM Policy)	Sections 14, 19, 20, 21, 22	Part C Section 13, Part C Section 14, Part C Section 15, Part C Section 16.6
Incident management and response (may be same process as ISM Policy)	Sections 19, 21, 22	Part C Section 13

RECORDS MANAGEMENT POLICY

This policy ensures that the organisation's recordkeeping:

- is transparent, consistent, and accountable;
- meets legal, regulatory, fiscal, operational, and historical requirements;
- supports the efficient conduct of its business; and
- ensures the preservation of archives documenting its history and development.

It applies to all types of information, not just personal information.

TOPICS IT SHOULD ADDRESS	CORRESPONDING SECTIONS IN THE POPIA	CORRESPONDING SECTIONS IN THE CODE
Comply with all legal and operational recordkeeping requirements and create a records retention schedule	Section 14(1)(a) and (b)	Part C Section 14
Secure destruction	Section 14(4) and (5)	Part C Section 14
Information security (a cross reference to the ISM Policy)	Sections 14, 19, 20, 21, 22	Part C Section 13, Part C Section 14, Part C Section 15, Part C Section 16.6
Effective version control	Section 14(6),(7),(8), Sections 5, 10, 12, 14, 16, 23(2), 24, 71, Item 3 read with Form 2	Part C Section 15, Part C Section 12, Part C Section 15, Part C Section 16.5, Part C Section 18.1
Minimise duplication by identifying and controlling master records	Section 10 and Section 14	Part C Section 7, Part C Section 14, Part C Section 16.3, Part C Section 19
Manage and preserve knowledge and intellectual property		
Incident management and response (may be same process as ISM Policy)	Sections 19, 21, 22	Part C Section 13
Responsible, empowered users	Item 4(e) of the POPIA 2018 Regulations	Part D Section 1, Part C Section 13.1, Part C Section 16.9.1,Part C Section 19, Part C Section 21, Part D Section 2
Clear roles and responsibilities in the implementaiton of the policy	Sections 19, 20, 21	Part C, Section 13
Records management assessments	Item 4(b) of the POPIA 2018. Regulations	Part D Section 1, Part D Section 3

Resources

Tthe ICO has a great Records Management Policy resource and JISC has a great guide for Records Management at universities.

Implement policy

There is no point in having a policy that nobody follows, owns, updates, or tests compliance against.[7] You have successfully implemented a policy once you measure compliance with the policy (usually through an internal or external audit) and routinely address non-compliance.

DO THIS...

While you are drafting the policy, create a policy implementation plan that includes:

The implementation team usually consists of the policy owner (usually the Information or Deputy Information Officers) and representatives of senior management. They will involve other people when particular skill sets are required.

Policies rarely exist in isolation. They are often referenced in **other policies and supporting documents**. When the University adopts a new policy, the policy implementation team should assess whether other policies must be amended. Policies will have to be amended if they govern specific personal information processing activities or if there is an opportunity to insert POPIA controls in processes governed by other policies (e.g. HR and procurement policies).

A new Privacy Policy will have an **impact on any business process** that involves personal information. You can assess the impact of the policy on these processes by doing personal information impact assessments (PIIAs) to identify instances where the process does not comply with the policy and to manage the POPIA risk that is caused by that non-compliance. The implementation plan must also include a plan for how you will assess changes to processes or the introduction of new processes to ensure that these changes do not introduce new POPIA risks.

Be on the lookout for any i**nfrastructure or equipment requirements**.

Finally, it is vital to assess the impact of the new policy on **people**. Who will have to do something different or differently tomorrow? Do they have the knowledge and skills to make these changes? If they do not, what kind of training or skills development will they require?

[8] http://prism-clarity.com/2016/07/makes-good-policy-5-watchwords/

Implement policy

HOW POLICIES INTERACT - AN EXAMPLE

One of the policy statements of the Records Management Policy is that personal information must be destroyed securely. How will the university do this? The university will need special software for digital information and shredders for paper records. If the Information Security Management Policy provides that access to personal information must be restricted to employees who 'need to know', is it still appropriate for the university to have an open-plan office? If sending personal information by email is not permitted, how must employees share personal information? If the University does not give employees the infrastructure, equipment, hardware, software and other tools to comply with new policies, they will continue to work the way they used to.

KEY CONCEPTS

A policy is a collection of high-level policy statements, but it does not answer the questions 'what is required?' and 'how do we do it?' Usually, policies have to be supported by supporting documents such as:

PROCEDURES: The processes that are required to implement a policy, and that describes who does what, when they do it and under what criteria (i.e. conduct a personal information impact assessment).

STANDARDS: A set of mandatory rules or specifications that gives effect to the principles in the policy (i.e. technical standards for the configuration of systems).

GUIDELINES: General statements, recommendations or instructions to achieve a policy's objectives. They are not mandatory and can change more frequently than procedures and standards.

PROCESS: A process is a collection of related tasks aimed at a specific outcome (e.g. onboarding a new customer or employee).

[8] http://prism-clarity.com/2016/07/makes-good-policy-5-watchwords/

Resources

The Centre for Information Policy Leadership also published a fantastic report in 2020 called 'What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework'. This report gives a great overview and tips on how to implement privacy-related policies and procedures within an organisation.

The UK's information regulator – the ICO – has recently released a guide and tool to assist organisations with creating their own 'accountability framework' for privacy risk management. The guide and tool were created for GDPR purposes – but again can easily be adapted for POPIA purposes as the core principles remain the same. There is a specific resource dedicated to implementing privacy-related policies and procedures within an organisation.

Berkeley University has a change-management toolkit which is worth a look to assist you with implementing your new policies and procedures. Yale University has created this Change Management Process Guide.

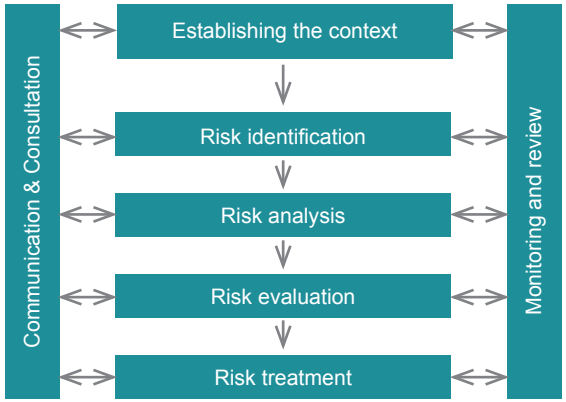
Personal information impact assessments

IN THE CODE: PART D SECTION 3

Assessing, analysing and evaluating risk is an integral part of compliance, and your role as Information Officer. Taking a risk-based approach to POPIA will help you focus on the most relevant threats. In short, and adapted slightly for the context, '[o]ne of the main [POPIA] risks is to think that they don't exist. The other is to try and treat all potential risks. Fix the basics, protect first what matters to your business and be ready to react to pertinent threats.'[9]

Personal information impact assessments (PIIAs) help ensure that your processing activities comply with the POPIA. They help ensure that you have adequate measures and standards in place to comply with lawful processing.

This image is often used to depict the risk management porcess:[10]



Here is a brief explanation of what each of these phrases means:[11]

Communication and consultation: Effective risk management relies on effective communication and consultation. Stakeholders will make decisions based on how they perceive certain risks and ineffective or incomplete communication can undermine these decisions. Also, informed stakeholders can help identify risks.

ALPHABET SOUP: PIAS, PIIAS, AND DPIAS

Although the POPIA doesn't mention PIIAs, the EU GDPR refers to data protection impact assessments (DPIAs) to assess compliance with existing laws. There is also the broader privacy impact assessment (PIA) that is a crucial component of privacy by design. PIAs are not just about complying with regulations, but they help you:

- Identify and evaluate the impact of a project, initiative, or system on the privacy of all stakeholders; and
- Search for ways to avoid or mitigate this impact.

PIIAs are closer to DPIAs than they are to PIAs.

Article 35(1) of the EU GDPR provides that the assessment must include:

- A description of the envisaged processing operations and the purposes of the processing (this includes the 'nature, scope, context and purposes of the processing')[12]
- An assessment of the necessity and proportionality of the processing
- An assessment of the risks to the rights and freedoms of data subjects (this includes the 'origin, nature, particularity and severity of that risk')[13]
- The measures envisaged to address the risks and demonstrate compliance

Be careful not to equate DPIAs with PIIAs. DPIAs are not always required, only 'where a type of processing in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons'.[14] It goes on to list specific types of automated processing and decision-making, large scale processing of special categories of data or data relating to criminal convictions and offences and systematic monitoring of publicly accessible areas as specific activities that require a DPIA. POPIA does not contain similar qualifications – personal information impact assessments are always needed.

[9] Stephane Nappo, Global Chief Information Security Officer, 2018 Global CISO of the year
[10] See *The IRMSA Guide to Risk Management*, page 9.
[11] See *The IRMSA Guide to Risk Management*, from page 34.
[12] Recital 90.
[13] Recital 84.
[14] Article. 35(1) of the EU GDPR.

Personal information impact assessments

Establishing the context: Before you can identify risk, you need to understand the context in which the university operates. Ask yourself 'what are the internal and external circumstances or conditions that could keep the university from achieving its goals?'. Think about the conditions in higher education and the country, but also the context of the specific university.

Risk identification: The university will identify risks and lost opportunities. It does so by taking various approaches (quantitative, qualitative, or semi-quantitative) and using several different tools (risk registers, competitor analysis, market trend research, SWOT analysis, internal questionnaires, sales performance reports).

Risk analysis: Once the university has identified its risks, it should try to understand the risk by

- analysing the cause and source of the risk, and
- gathering the information it needs to evaluate a risk.

The university will assess existing controls, analyse the consequences of a risk, analyse the likelihood and estimate the probability, do probability monitoring, obtain expert opinions, complete risk registers, and account for uncertainties.

Risk evaluation: It must then measure each risk against pre-determined criteria to determine how significant it is to the university. The university assigns a rating to the risk. This rating likely or probable the risk is, the impact or severity, and an assessment of existing controls. At this stage, it may accept some risks immediately 'as is' or take immediate steps to avoid the risk.

Risk treatment: Next, the university decides what to do about the risks it has identified. Generally, it must choose to accept or tolerate the risk, avoid the risk, remove the source of the risk, change the likelihood of the risk, change the consequences, transfer the risk or exploit the opportunity. During this step, the university should develop and implement a risk response plan.

Monitoring and review: Finally, monitoring and review is a continuous process that helps to ensure that risk management works. The university must plan, examine and evaluate information, record the results and communicate them, and improve the process.

This methodology does not only apply to risks but also lost opportunities. These may be opportunities to:

- Create a new process, product or service
- Improve existing processes, products or services
- Improve the reputation of, and trust in, the organisation, or
- Build or strengthen relationships with new and existing stakeholders

When should you conduct a PIIA?

The POPIA doesn't say when you should perform a PIIA. Perhaps this is the first time you are implementing a policy aimed at protecting personal information. You can use PIIAs to bring some of the University's processes in line with the new policy or policies. Perhaps you have already implemented some policies, but they may be based on other data protection legislation or standards, and there may be gaps. Use the PIIAs to identify those gaps.

You can also use a PIIA to measure the impact of a change in the way the University processes information. It will help you ensure that these changes do not introduce new privacy risks.

Here are some changes that could trigger a PIIA:

- Processing personal information for a new purpose
- Launching new products or services
- Expanding into other countries
- Introducing new systems, software or hardware for processing
- Sharing personal information with third parties
- Using a new service provider or supplier
- Changes to privacy regulations

Resources

The CIO has a good guideline, but the Privacy Impact Assessment toolkit created by UCISA is fantastic. Just remember, POPIA always requires personal information assessments. The GDPR only requires them in certain cases.

Edinburgh University has a very thorough resource page on privacy impact assessments.

Bristol University has a useful screening questionnaire template to determine if you need to conduct a privacy impact assessment and a full privacy impact assessment template.

8 STEPS
TO A PIIA

The following eight-step approach is an amalgamation of several guidelines, risk management best practice, and some practical experience:[15]

1

Do you need to do a personal information impact assessment? If a process, project, initiative, contract or activity involves personal information, you should do a PIIA.

Do this:
Train employees in key positions to recognise personal information so they can trigger a PIIA. For instance, asking whether personal information is involved should be a standard part of your project management life cycle and your procurement process.

2

Do an inherent risk-rating: Determine the level of PIIA required
Is the process, project, initiative, contract or activity inherently high risk? Rating the inherent risk will help you allocate your resources to the significant privacy risks.

Do this:
Create a short questionnaire designed to identify processes or activities that have inherently high privacy risks.

Consider:
- The volume of personal information
- Whether there is any special personal information involved
- Whether it is 'further processing'
- Whether it involves profiling or automated decision-making
- Whether the processing is invisible (i.e. the data subject is not aware of the processing) Whether it involves any form of processing that requires prior authorisation (e.g. the further processing of unique identifiers to link information or processing information for credit reporting)
- The value of the personal information (e.g. what would it cost to replace the personal information if it was lost)
- How disruptive it would be if the processing activity were interrupted or if the personal information was no longer available (i.e. how important is this particular processing activity to the organisation)
- How valuable personal information would be to a bad actor

The inherent risk-rating would determine the level of PIIA required, and who can sign off on the assessment.

3

Describe the processing activity
Remember that you are assessing a processing activity to determine whether it complies with POPIA, so you must understand the activity very well.

Do this:
Use data flow mapping to track the data life cycle and document how personal information is collected, used, transferred, archived or destroyed.[15]

4

Identify privacy risks
The methodology you can use to identify privacy risks ranges from questionnaires to face-to-face interactions.

Do this:
Assess the processing activity against the policy statements in the Information Security Management Policy, the Privacy Policy and the Records Management Policy.

The purpose of this process is to provide a list of all possible POPIA risks, regardless of whether there are existing controls that address them. It is appropriate to include both risks to the data subject and the organisation.

8 STEPS
TO A PIIA

5

Identify and evaluate privacy solutions

The aim is to identify solutions that eliminate the risk or reduces it to a level that is acceptable to the university.

Do this:

Record the solutions in a risk response plan. Here are some examples of solutions:

- Accept the risk without further action. Some risks may be unlikely or low-impact.
- Put a contract in place that provides assurance or transfers the liability
- Develop a privacy notice that improves transparency
- Introduce a new policy or amend an existing one
- Introduce a procedure to manage the risk
- Disable certain features of a product or service
- Train people to be aware of the risk and to avoid it
- Implement technical measures like enforcing strong encryption or preventing certain actions
- Abandon the processing activity

These solutions may not eliminate POPIA risk. You should identify and rate the residual risks to ensure that the university is comfortable with the level of residual risk.

6

Sign off and record the outcomes

Depending on how a university has defined roles and responsibilities, senior management would have to decide how to treat the POPIA risks and which solutions to implement. Provided that senior management is the first line of defence.

The Information Officer is in the second line of defence, which means that your primary role is to advise, monitor and report. In other words, it is the Information Officer's role to ensure that there is a PIIA procedure in place. Still, it is senior management's responsibility to follow the procedure and to respond to the POPIA risks that are identified.

While you may play a supporting role as the Information Officer, that is not to say that you do not have a say in the solutions that are proposed and accepted. This is part of your advisory and monitoring role.

Do this:

Ensure that there is a permanent record of who signed off the solutions and when this took place.

7

Integrate the outcomes into a project plan

Integrate your risk response plan into a project plan. This will ensure that there is a clear plan, an implementation timeline and that actions are assigned to a responsible person.

8

Agree on a monitoring plan

The Information Officer, the relevant member of senior management, and internal audit should agree on a monitoring plan to assess that the agreed solutions have been implemented and to ensure that the risk does not recur and that new risks are managed in future.

Compliance monitoring and continuous improvement

IN THE CODE: PART D SECTIONS 1 & 2

As Information Officer it is your job to ensure that the performance and effectiveness of the POPIA Compliance Framework is evaluated and its shortcomings addressed. An independent team must do the monitoring – don't mark your own homework.

DO THIS...

Determine the following:

- What needs to be monitored and measured (usually processes and controls)?
- Which methods will you use for monitoring and measurement?
- When will you monitor and measure?
- Who will do it (often internal or external auditors)?
- When will the results be analysed and evaluated?
  Who will analyse and evaluate the results?

Document this process and any outcome or decision meticulously.

Resources

The Centre for Information Policy Leadership also published a fantastic report in 2020 called 'What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework'. This report gives a great overview and tips on how to monitor and sustain compliance with your privacy framework, policies and procedures. You can find it here.

The UK's information regulator – the ICO – has recently released a guide and tool to help organisations creat their own 'accountability framework' for privacy risk management. The guide and tool were created for GDPR purposes – but again can easily be adapted for the POPIA as the core principles remain the same. There is a specific resource to compliance monitoring and how the third line of defence works in relation to managing privacy-related risks. You can find this here.

The IAPP has a series of articles about monitoring compliance with privacy programmes. You can find them here.