Case Study

Assessing PoPI related Risks for Operators and 3rd Parties

THE CHALLENGE

With the stipulation that a CEO or Managing Director of an enterprise is deemed to be the responsible Information Officer - as per the PoPI Act - risk of non-compliance is a Board level issue. Following on from earlier work on a Capability Model and a Gap Analysis, the client needed to understand how and where personal information was being used in each of his 15 departments, and the risks involved. Of particular concern were unstructured data processes and PI processed by operators and 3rd Party service providers.

THE INDUSTRY

Financial Services

INVESTMENT

$
$$
$$$

WE USED

Visual Process Mapping Change and Project Management

Day 1

Pétanque Consultancy
Clearly Better

Month 6

THE OUTCOME

The risk assessment was done on 3 levels: a) departmental b) process, and c) Operator/ 3rd Parties. The project provided a full understanding of the risks in a manner that is quick and easy to understand, due to the visuals. As such, it served as a baseline from where further compliance related projects could flow. It created a heightened awareness of PI related risks, identified gaps and as a bonus, ensured improvements of processes from an operational point of view.

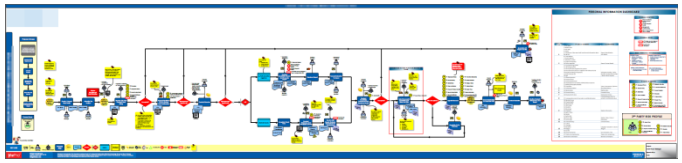
The client said…

● I needed this (map). Apart from the risks assessment, this has helped me to ensure continuity and for my team to take ownership. ● We needed to align ourselves better by standardizing with the rest of the company ● I have a greater awareness of PI used in my department now.

This was the briefing…

"Since PoPI is principle based, we need to identify the risks in each department, particularly the touchpoints where personal information (PI) is handed over for processing to operators and 3rd party service providers. As we are viewed by the Act as the responsible party to ensure that PI is not misused, abused or lost, we need to be clear on PI processing by operators since we remain legally liable if they lose, misuse or abuse our client or employee PI. We need to outline what controls are required to safeguard ourselves and be compliant."

The Result

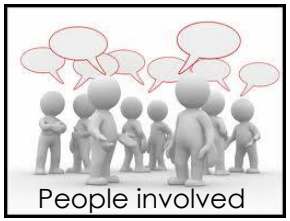


The Result

One of the 15 departmental process and risks assessment maps

What we did…

End-to-end visual mapping of high risk business processes were done, while educating owners on the definition of PI. These maps included Risk Registers by highlighting a) where PI was being processed, b) whether it was done as a responsible party or as an operator, c) unstructured data practices, and d) Operators/ Third Party providers, categorized by privacy processing risk. Controls were identified and Action Lists for improvements developed.



15 Departmental Management Teams
Process owners

TRANSFORMATION ACHIEVED

● Big Picture understanding of processes and where everyone fits in. ● Awareness and recognition of risks. ● Identification of what was missing and what had to change to be compliant. ● Central view of operators and Third Party providers. ● Risk driven budget priorities ● Behavourial changes of all involved (it isn't just an IT issue) ●

2 Visual Process Architects