[company name]

**Consider Phase POPI Risk Appetite Report Template**

Report author:

Report date:

Reviewers list:

Approval list:

Document version control:

Table of Contents

[1 Objective 1](#_Toc468540958)

[2 Definitions 1](#_Toc468540959)

[3 Alignment to strategic objectives 2](#_Toc468540960)

[4 Alignment to COSO ERM Framework 2](#_Toc468540961)

[5 Alignment to risk categories 3](#_Toc468540962)

[6 Impact Rating scale 4](#_Toc468540963)

[7 Likelihood Rating scale 4](#_Toc468540964)

[8 Controls effectiveness scale 4](#_Toc468540965)

[9 Overall risk scoring matrix 5](#_Toc468540966)

[10 Overall risk category 5](#_Toc468540967)

[11 Summary of risks identified 6](#_Toc468540968)

[12 Next steps 7](#_Toc468540969)

# Objective

This report supports the integration and review of the POPI Act compliance assessments which have been undertaken. It presents a draft risk appetite profile for the approval of the relevant authorities.

# Definitions

* Definition of Risk Appetite: *The amount/type of risk the organisation/group will accept.*
* Definition of Risk Tolerance: *The specific maximum risk the organisation/group will tolerate for each specific risk.*

# Alignment to strategic objectives

Table 1 Strategic objectives

|  |  |  |
| --- | --- | --- |
| **Strategic objectives**  (generic objectives to be adapted to specific organisation objectives) | **How might POPI Act compliance impact on this objective?** | **Comments** |
| Pursue revenue growth | POPI is both an opportunity (new products and services) and threat (competitor first mover advantage) | How to pursue revenue growth is out of scope for the current POPI project |
| Improve operating margin | POPI is both an opportunity (new products and services) and a threat (fines or other costs of non-compliance) | Opportunity: out of scope  Threat: a range of 16 assessments have been used to identify risks of non-compliance. |
| Evaluate and improve processes | POPI gives an opportunity to improve operational processes to reduce cost and risk | By implementing the recommended actions to close the gaps identified, improved processes will have a positive impact |
| Improve stakeholder management | POPI is both an opportunity (proactive positive impact on stakeholders) and a threat (negative stakeholder view where non-compliance happens) | The POPI project communications plan currently addresses internal stakeholders only. The scope of this plan needs to be expanded to include external stakeholders |

# Alignment to COSO ERM Framework



[see [www.coso.org](http://www.coso.org) for more information on the COSO ERM update which is under development]

Table 2 COSO ERM Framework

|  |  |  |
| --- | --- | --- |
| **COSO framework** | **How might POPI Act compliance impact on this framework parameter?** | **Comments** |
| Strategy | POPI should be part of a Privacy Impact Assessment (PIA) for any new strategic initiative | The use of the PIA approach needs to be incorporated into the strategic process |
| Operations | There are numerous operational implications for POPI compliance, including:  Policy changes  Contract changes  IT environment changes  Staff training  Direct marketing  Records management procedures | 17 assessments have been used to identify risks of non-compliance. The evaluation of possible risk responses must be justified for each of the potential remedial actions, based on the approach advocated in the POPI Act of “reasonable and appropriate, organisational and technical” measures |
| Reporting | POPI needs to become part of the reporting cycle for enterprise risk | There are a number of reporting tools available which must be tailored to meet stakeholder needs |
| Compliance | POPI needs to be integrated with the overall [company name] approach to the legislative compliance universe | The POPI project forms an input to the [insert appropriate authority] |

# Alignment to risk categories

Table 3 Risk categories

|  |  |  |
| --- | --- | --- |
| **Risk categories**  (to be adapted to specific organisation objectives) | **How might POPI Act compliance impact on this risk category?** | **Comment** |
| Strategy | Nil. The loss of sensitive / business critical information is for non-POPI related information.  Reputation risk is managed in Market and Customer Relations risk categories | POPI Act compliance does not provide a material strategic risk |
| Market | Non-compliance could damage the [company name] brand and reputation | One of the main motivations for POPI Act compliance is protecting the [company name] brand and reputation |
| Contracting | Failure to implement appropriate contracts carries the risk of non-compliance, impacts on supplier integrity | A detailed gap analysis for contracting risk forms part of the POPI project |
| Operational | There is the risk that operational errors will result in non-compliance | International experience |
| Customer Relations | Non-compliance could damage the [company name] brand and reputation | One of the main motivations for POPI Act compliance is protecting the [company name] brand and reputation |
| Legal and Compliance | Non-compliance is a real risk | 17 assessments have been used to identify risks of non-compliance. The evaluation of possible risk responses must be justified for each of the potential remedial actions, based on the approach advocated in the POPI Act of “reasonable and appropriate, organisational and technical” measures |
| Liquidity | Nil | POPI Act compliance does not provide a material liquidity risk |
| Finance | Non-compliance carries the risk of financial penalties being imposed by the Information Regulator; civil damages actions, including Class Action Suits by concerned Data Subjects | 17 assessments have been used to identify risks of non-compliance. The evaluation of possible risk responses must be justified for each of the potential remedial actions, based on the approach advocated in the POPI Act of “reasonable and appropriate, organisational and technical” measures |

# Impact Rating scale

[suggested for a large enterprise, adapt values to meet organisation needs]

* 5 Significant R50 million Description: Large scale action, material breach of legislation with very significant financial or reputational losses
* 4 Major R25 million Description: Regulatory breach with material consequences which cannot be readily rectified
* 3 Moderate R12 million Description: Regulatory breach with material consequences which can be readily rectified
* 2 Minor R5 million Description: Regulatory breach with minimal consequences which can be readily rectified
* 1 Insignificant R2 million Description: Regulatory breach with minimal consequences and readily rectified

# Likelihood Rating scale

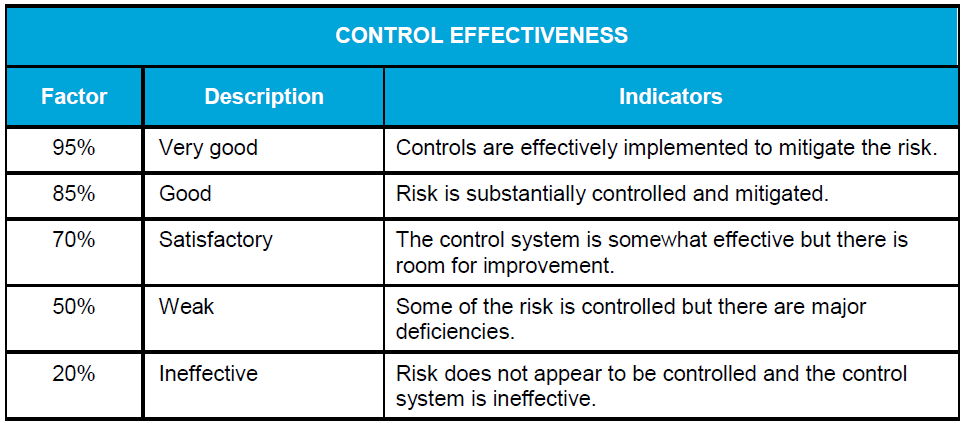
[suggested, adapt to organisation needs]

* 5 Almost Certain > 1 in 10. Description: likelihood of occurring every year
* 4 Likely 1 in 10 – 100. Description: likelihood of it occurring several times within the next ten years
* 3 Possible 1 in 100 – 1,000. Description: could occur more than once within the next ten years
* 2 Unlikely 1 in 1,000 – 10,000. Description: would be surprising if it occurred
* 1 Rare 1 in 10,000 – 100,000. Description: has not occurred to date

# Controls effectiveness scale

[suggested, adapt to organisation needs]

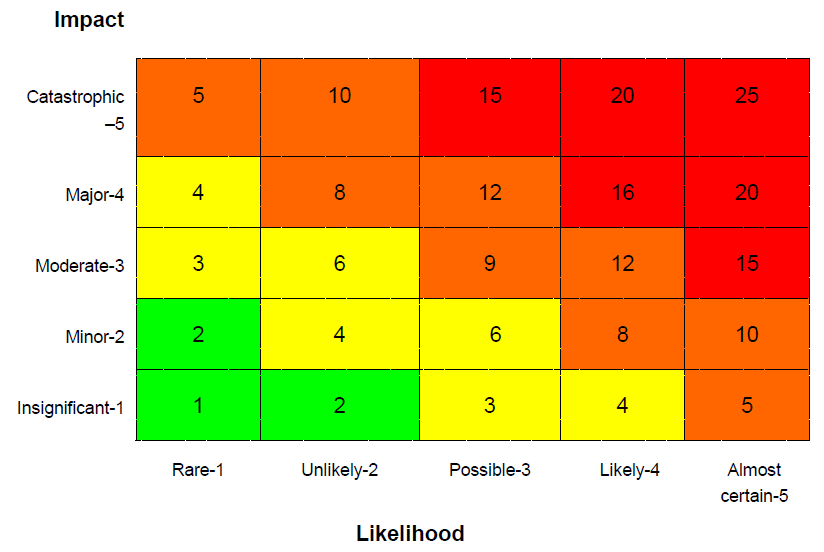
Table 4 Control effectiveness



# Overall risk scoring matrix

[suggested, adapt to organisation needs]

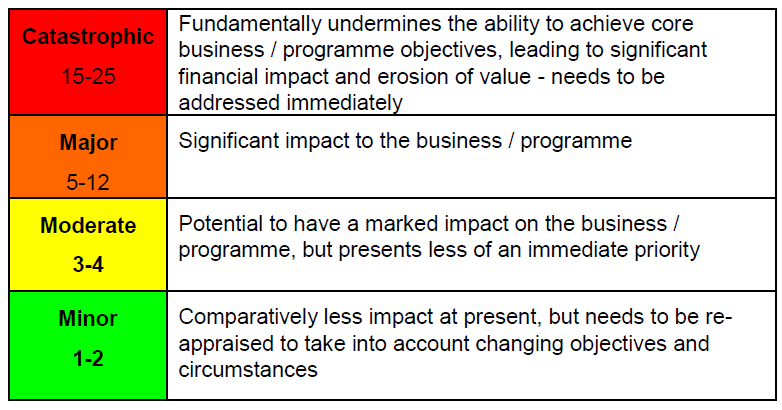
Table 5 Overall risk scoring



# Overall risk category

[suggested, adapt to organisation needs]

Table 6 Overall risk category



# Summary of risks identified

Note: This table represents an interim assessment prior to the implementation of the remedial action plan which has been recommended.

The ratings in columns C through F of table 7 will need to be reviewed after the remediation actions have been implemented to validate the current ratings and where possible:

* Decrease the impact rating (column C)
* Decrease the likelihood rating (column D)
* Decrease the overall risk rating (column E)
* Increase the control effectiveness rating (column F)

Table 7 Risk assessment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** |
| **Assessment tool used** | **Risks identified** | **Impact rating**  **(1 to 5)** | **Likelihood**  **Rating**  **(1 to 5)** | **Overall risk rating**  **(Minor,**  **Moderate,**  **Major,**  **Catastrophic)** | **Interim Control effectiveness rating**  **(20% to 95%)** |
| Business Continuity |  |  |  |  |  |
| Cloud Services |  |  |  |  |  |
| Compliance Assessment Tool (37 questions - alignment with the Act) |  |  |  |  |  |
| Data Protection Assurance |  |  |  |  |  |
| Digital Devices |  |  |  |  |  |
| Direct marketing |  |  |  |  |  |
| Existing contracts and policies |  |  |  |  |  |
| Incident response capability |  |  |  |  |  |
| Information security |  |  |  |  |  |
| Information Sharing & Data Subject Access |  |  |  |  |  |
| Personal Information Diagnostic |  |  |  |  |  |
| Physical security and site access |  |  |  |  |  |
| POPI Governance |  |  |  |  |  |
| Records Management |  |  |  |  |  |
| Social media |  |  |  |  |  |
| Supplier Selection matrix |  |  |  |  |  |
| Web site |  |  |  |  |  |

# Next steps

This Risk Appetite Report must be reviewed and approved as the basis for decision making before the final Translate / remediate phase of the project.