

**iSelect**

# **Risk Management Framework**

**Version: 2023.1**

**May 2023**

## 1. Introduction

The following document provides a structured and transparent approach to the Risk Management Framework across iSelect.

The Framework provides a detailed risk management process that complies with the Australian Risk Management Standard (AS/ANZ 31000:2018). This methodology provides systematic and consistent identification, assessment and management of risk across iSelect.

**Risk** is defined as:

*"...anything that may impede a company from achieving its objectives". (AS/ANZ 31000:2018)*

**And encompass:**

- Risk as an opportunity: The possibility of good things not happening;
- Risk as a hazard: The threat of bad things happening; and
- Risk as uncertainty: The potential that actual results will not equal anticipated outcomes.

Risk not only includes the possibility of economic or financial loss or gain but also includes personal injury, death, physical damage, business interruption and reputational and image damage.

**Risk management** is defined as:

*"The coordinated activities to direct and control an organisation with regard to risk" (AS/ANZ 31000:2018)*

Risk Management encompasses the application of management policies and processes to enable systematic identification, analysis, treatment and monitoring of risk.

*"Risk management is an integral part of good management practice. It is an iterative process consisting of steps, which, when undertaken in sequence, enable continual improvement in decision making."*

The objectives of a robust risk framework is to assist the organisation in integrating risk management into significant activities and functions. The effectiveness of risk management will depend on its integration into the governance of the business, including decision-making and requires support from stakeholders, particularly top management.

This Risk Management Framework is applicable to all verticals and operations of iSelect.

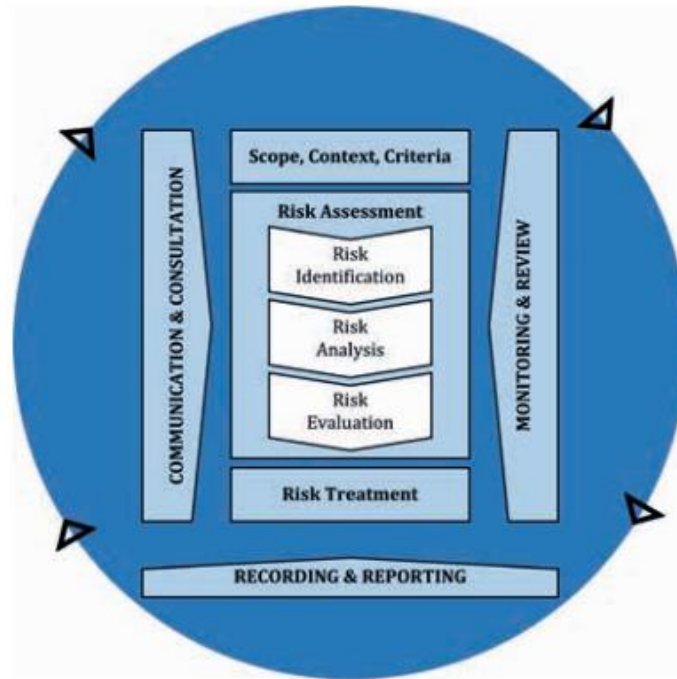
## 2. Risk Management Process Overview

The risk management process, based on the Australian Standard for Risk Management (AS/ANZ ISO 31000:2018), involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

AS/ANZ ISO 31000:2018 is separated into three key core areas:

1. Risk Management Principles (8 principles for managing risk) – Clause 3
2. Risk Management Framework (5 components to the framework for managing risk) – Clause 5
3. Risk Management Process (6 processes for managing risk) – Clause 6

## The Risk Management Process Overview



### 2.1 Risk Management Principles (Clause 3)

For risk management to be effective, iSelect should at all levels comply with the principles described in clause 3 which includes:

- a) **Integrated** - Risk management is an integral part of all organisational activities.
- b) **Structured and comprehensive** - A structured and comprehensive approach to risk management contributes to consistent and comparable results.
- c) **Customised** - The risk management framework and process are customised and proportionate to the organisation's external and internal context related to its objectives.
- d) **Inclusive** - Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.
- e) **Dynamic** - Risks can emerge, change or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.
- f) **Best available information** - The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.
- g) **Human and cultural factors** - Human behaviour and culture significantly influence all aspects of risk management at each level and stage, and;

- h) **Continual improvement** - Risk management is continually improved through learning and experience.

## **2.2 Risk Management Framework (Clause 5)**

### **2.2.1 Leadership and commitment (5.2)**

Sustained commitment and strategic planning is required to maintain the effectiveness of risk management processes. Management should define and endorse the risk management policy and ensure that the organisational culture and risk management policy are aligned to enable the dual achievement of risk management and organisational objectives.

iSelect assigns management accountabilities and responsibilities at appropriate levels of the organisation and ensures that the necessary resources are allocated to risk management, to communicate the benefits of risk management to all stakeholders.

The iSelect Risk Management Framework ensures legal and regulatory compliance, and ensures that the framework for managing risk remains appropriate.

### **2.2.2 Integration (5.3)**

Integrating risk management is reliant upon organisational structure, context and governance. iSelect integrates risk management into the needs and culture of the organisation by ensuring it is part of the purpose, governance, leadership, objectives and strategy to achieve sustainable performance and long term viability.

### **2.2.3 Design (5.4)**

In designing the framework for managing risk, management have considered the internal and external context of the organisations such as the cultural, legal and regulatory, competitive and technological contexts. Evaluating iSelect's internal context may include governance, structures and roles, responsibilities and capabilities understood in terms of resources and knowledge.

Establishing the Risk Management Framework clearly highlights iSelect's rationale for managing risk and assigns the accountability and responsibilities for managing risk. Accountability for risk is assigned by identifying risk owners, responsible parties for risk management at all levels and establishing performance management measurement and escalation processes.

Risk management is embedded in all practises and processes in a way that is relevant, effective and efficient. In particular, risk management is embedded into the policy development, business and strategic planning and review and change management.

iSelect have established internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk. This will include mechanisms to consolidate risk information from a variety of sources. iSelect has developed and implemented plans to communicate and engage with external shareholders ensuring an effective exchange of information. This process facilitates an effective framework for communication with our legal, regulatory and governance requirements and communicating with stakeholders in the event of a crises or contingency.

## **2.2.4 Implementation (5.5)**

In implementing the risk management framework for managing risk, an appropriate strategy and timing for implementation has been established and applicable business processes for inclusion in the framework has been identified.

This risk framework enables compliance with legal and regulatory requirements externally and internally and forms the basis for consultation with stakeholders to ensure that the risk framework remains appropriate and reflective at all levels of the organisation.

## **2.2.5 Evaluation (5.6)**

To ensure that risk management is effective and continues to support organisational performance, iSelect established performance indicators to measure performance of the risks against, that will be periodically reviewed for its appropriateness. The internal and external content will also be reviewed to determine whether the risk management plan in use remains relevant.

## **2.2.6 Improvement (5.7)**

Based on results of monitoring and reviews, actions will be taken on how risk management can be improved. These improvements should lead to improvements in the organisations' management of risk and its risk culture.

## **2.3 Risk Management Process (Clause 6)**

### **2.3.1 Communicate & Consult (6.2)**

Ensure effective communication of all iSelect stakeholders as and when is appropriate. Provide regular reports internally to Business Vertical Managers, the Executive Management Team, and the Board at each phase of the risk management process.

### **2.3.2 Scope, Context and Criteria (6.3)**

It is important to understand and define the scope of risk management activities to determine what risk management process will be applied at different levels (e.g. strategic, operational, project, or other activities).

The establishment of context sets the scope and parameters for the remainder of the risk management process. The context must be defined after the organisation's overall objectives and strategies have been taken into consideration. This involves focussing on the environment in which the business operates and identifying relevant components that may impact on risk management, for example, financial, operational, competition, political, legal etc.

It is important to achieve equilibrium between costs, benefits and opportunities in the risk management context.

Criteria should be defined to evaluate the significance of risk and to support decision making processes. Risk criteria should reflect iSelect's values, objectives and resources, and be consistent

with existing policies. Risk criteria should be established at the beginning of the risk assessment process, however given they are dynamic, they should be continually reviewed and amended.

### **2.3.3 Risk Assessment 6.4 – Risk Identification (6.4.2)**

This is the process of identifying the risks that need to be managed in order to ensure iSelect achieves its goals and objectives. The identification of risk is a continual process and may occur during day-to-day activities. Risks may result from a number of instigators. For example, they may be inherent to the normal operations of the business; they may arise in the pursuit of new growth, profit or business opportunities or from changes to the fundamental environment in which the organisation currently exists.

Formulating the wording of the risk description is a task that requires careful consideration. A poorly defined risk will lead to difficulties in estimating the potential impact to iSelect. It will also complicate the identification of appropriate mitigating controls to eliminate the risk. Categorisation of risks is used to “group” various risks together where it can prove helpful for measuring and reporting (see Appendix A).

### **2.3.4 Risk Analysis (6.4.3)**

Analysis of risks is the process of determining why, how and where the possible incident might occur. Further, by identifying the source of the risk, management will be better able to measure the risk and determine an appropriate strategy for managing it to an acceptable level.

Analysis involves estimating the likelihood of occurrence and the consequence that such an occurrence might have on the organisation. Existing controls and management procedures should be identified and an assessment made as to the effectiveness of controls. The likelihood of the event occurring and the subsequent impact should then be reassessed in light of the review of the existing controls. These two criteria are then combined to provide a level of risk. Risks are analysed in three stages:

- **Inherent Risk Rating (worst case/do nothing)**

The risk rating without any mitigating strategies or controls implemented. Should represent the worst probable case scenario for a particular risk.

- **Residual Risk Rating (where we are today)**

The risk rating as it stands today, taking into account the progress in implementing the identified risk mitigation strategies.

- **Risk Appetite Rating (where we want to be)**

The risk rating that an organisation is prepared to take.

### **2.3.5 Risk Evaluation (6.4)**

Risk evaluation involves comparing the level of risk with previously established risk criteria. This phase of the risk management process is required in order to determine which risks should be brought to the attention of management for priority treatment.

### **2.3.6 Risk Treatment (6.5)**

Risk treatment involves identifying the range of options for mitigating risk, assessing those options, preparing risk treatment plans and implementing them. Low risks may be accepted with minimal further treatment; however, risks evaluated as moderate, high or extreme should be managed to an acceptable level through the process of a treatment plan.

Treatment plans should identify responsible persons, timing, expected outcomes, resources, and the review process to be set in place. Such plans will require approval from the relevant management prior to implementation. The plan should also include a mechanism for monitoring critical implementation milestones. Generally, the treatment plan will involve one of the following strategies:

- **Risk avoidance** – this involves deciding not to become involved in, or to withdraw from, an activity based on the level of risk (if this is practical). It should be noted that risk avoidance might well increase the significance of other risks.
- **Reducing the likelihood of occurrence** – this involves modifying the environment through implementing or strengthening controls to minimise the identified risk(s). When potential risk situations are identified, alternative courses of action should be evaluated to determine if the undesirable outcome could be avoided at reasonable cost. As a general guideline, the controls should cost less than the expected value of exposure and/or less than the cost of the contingency action.
- **Reducing the consequences** – this involves implementing a contingency plan. A contingency plan should be developed for contingency actions addressing significant unavoidable risk when preventative action is either unavailable, the cost of prevention is prohibitive or the preventative action fails. The contingency plan must be realistic and achievable.
- **Risk transfer** – this involves obtaining insurance to cover financial loss should a particular circumstance eventuate or through contractual arrangements with third parties.
- **Risk retention** – where it is not feasible or economical to treat in any other way, it may be appropriate to accept the residual risk.

Treatment options, assessment and implementation progress should be clearly documented in a Risk Management Database or repository.

### 2.3.7 Monitoring and Review (6.6)

It is imperative that the mitigation and/or elimination actions, as defined in the risk treatment stage, are actively managed, monitored and communicated on an ongoing basis.

Risks need to be regularly reviewed to ensure that previously identified management controls remain effective in the mitigation of the risk. It is also necessary to ensure that changing circumstances do not alter risk assessment and priorities. There is a need to ensure that the management treatment plan remains relevant. The status of all open risks is updated on a regular basis at an interval determined appropriate by management.

### 2.3.8 Recording and Reporting (6.7)

Recording and reporting aim to communicate risk management activities and outcomes across the business, provide information for decision making, improve risk management activities, and to assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

### 3. Detailed Guidance on Risk Ratings and Risk Treatment

In applying a consistent approach towards risk rating across iSelect, a list of qualitative and quantitative factors have been identified for likelihood, consequence and mitigating controls. These attributes have been regularly reviewed by the The Risk and Compliance Manager and approved by the Executive – Legal, Risk and Compliance and the Board. The guidance and tables below highlight the attributes that must be evaluated when determining the level of inherent and residual risk.

#### 3.1 Risk Likelihood Rating

Some events happen once in a lifetime. Others can happen almost every day. Analysing risks requires an assessment of their frequency of occurrence. The following table provides broad descriptions used to support likelihood ratings. The occurrence should be judged without reference to known management practices since these are assessed in step 3 of the risk management process overview.

Likelihood Rating	Descriptor	Qualitative description	Quantitative Description
5	Almost Certain	The event is <b>almost certain to occur</b> within the time horizon	The event almost certain to occur more than one time this year (2:1)
4	Likely	The event is <b>likely to occur</b> within the time horizon	The event should occur once this year (1:1)
3	Possible	The event <b>may occur</b> within the time horizon	The event will occur once in the next two years (1:2)
2	Unlikely	The event is <b>not likely to occur</b> within the time horizon	The event will occur once in the next three years (1:3)
1	Rare	The event is <b>will occur in exceptional</b> circumstances during the time horizon	The event will occur once in five years or greater (1:5)

#### 3.2 Guidance to assist assessment of the likelihood of occurrence for any given risk event:

The following questions are considered when assessing “likelihood” for each identified risk:

- **Complexity** – Consider the complexity of the underlying processes or environment in which iSelect operates.
- **Susceptibility** – How vulnerable (speed of onset and velocity) is iSelect to the identified risk?
- **History** – To what extent is the risk known to have occurred?



### 3.3 Risk Consequence Rating

The outcome or impact of a risk event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. Consequence represents the severity or impact of a risk event based on quantitative or qualitative analysis of the loss, injury, damage, disruption, opportunity cost or gain which may result.

Consequence is assessed on a 1-5 scale (“low” to “extreme”) using guidance across various potential impact areas. It is important to consider consequences as more than just financial as risks often have other non-financial impacts which may be of concern to iSelect (e.g. Reputation, staff injury etc.).

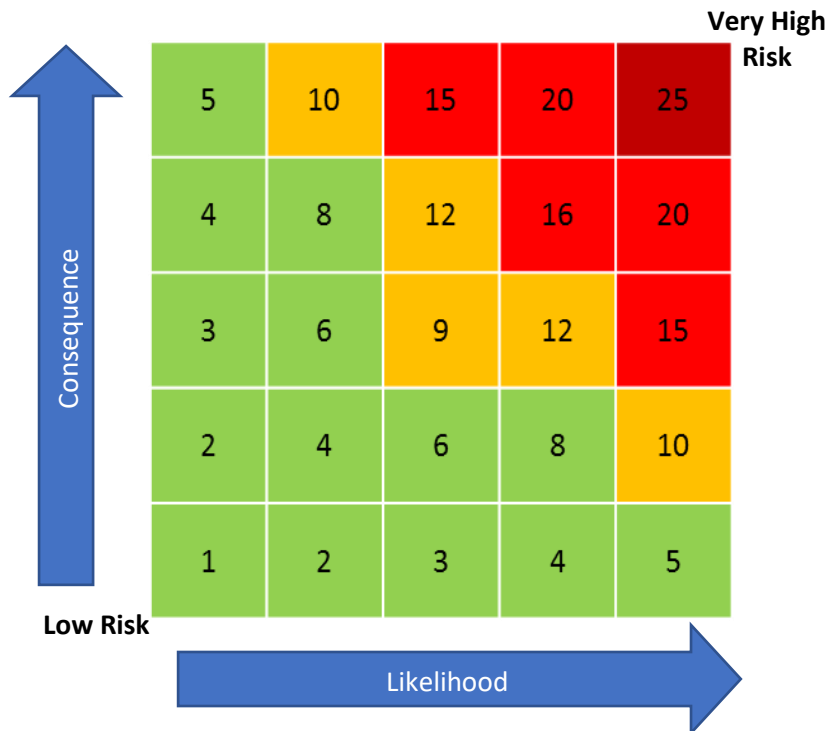
To assist with rating consequence, the detailed consequence table on the following page provides descriptions of possible impacts, incorporating:

- Financial
- Reputation and Market Perception
- Customer Service
- Legal and Regulatory
- Human Resources
- Health and Safety

Rating	Financial	Reputation & Market Perception	Customer Service	Legal & Regulatory	Human Resources	Occupational Health & Safety
<b>Extreme 5</b>	Greater than <b>\$12.5 m</b>	Enduring ( <b>&gt;2 months</b> ) impact on market perception of iSelect. Saturated national media coverage by credible financial media that spilled over to consumer media	Significant impact on key customer metrics including dialler, e-mails and website for <b>more than 3 days</b>	<b>Imposition of significant</b> sanction / operating restriction by regulator.  <b>Loss of AFSL License</b>	Unexpected / unplanned loss of <b>several key</b> executives including the <b>CEO</b>	<b>Death</b> or total permanent <b>disability</b> of one or more staff
<b>Major 4</b>	Greater than <b>\$7.5m</b> but less than <b>\$12.5m</b>	Sustained ( <b>1-2 months</b> ) impact on market perception of iSelect. Sustained national media coverage	High Impact on key customer acquisition and service channels including dialler, e-mails and website for between <b>1 and 3 days</b>	<b>Imposition of penalty</b> or restitution action by regulator	Unexpected / unplanned loss of <b>two or more key</b> executives  Unexpected /unplanned loss of the CEO	<b>Serious injury</b> to one or more members of staff requiring lengthy hospitalisation / rehabilitation
<b>Moderate 3</b>	Greater than <b>\$2.5m</b> but less than <b>\$7.5m</b>	Short term ( <b>2 - 4 weeks</b> ) impact on market perception of iSelect. Isolated national media coverage	Impact on key customer acquisition and service channels for more than a <b>day</b>	Imposition of <b>moderate penalty</b> or restitution action by regulator	<b>Unexpected</b> / unplanned loss of a key executive / <b>two or more</b> key personnel	<b>Injury</b> affecting one or more members of staff requiring medical attention and hospitalisation
<b>Minor 2</b>	Greater than <b>\$500k</b> but less than <b>\$2.5m</b>	Brief ( <b>1 – 2 weeks</b> ) impact on market perception of iSelect. Limited media interest or coverage	Impact on key customer acquisition and service channels for <b>more than 3 hours</b>	Imposition of a <b>minor</b> penalty or restitution action by regulatory body	Unexplained / unplanned loss of <b>key</b> personnel.	Minor injury or illness affecting a member of <b>staff</b> requiring medical attention
<b>Low 1</b>	Less than <b>\$500k</b>	Brief impact of a week on market perception of iSelect. Isolated media interest ( <b>1 day</b> )	Impact on key customer acquisition and service channels for less than <b>3 hours</b>	<b>Threat</b> on minor sanction / penalty	<b>Unexpected</b> / unplanned loss of a <b>senior</b> staff member.	Minor injury or illness affecting a member of <b>staff</b> , a visitor, or a contractor

### 3.4 Inherent Risk Assessment (Pre-control Assessment)

Inherent risk is measured by evaluating the exposure to the consequence, given the likelihood of a risk event occurring, where there are no management controls or mitigating practices in place. The ratings for likelihood and consequence for each risk are combined in the matrix below to determine the overall inherent risk ranking.



- Very High risk** – must complete control evaluation
- High risk** – must complete control evaluation
- Moderate risk** – management responsibility must be defined
- Low risk** – examination of controls is not specifically required

### 3.5 Inherent Risk – Response Plan

Inherent Risk Group	Priority & Response Required	Organisational Involvement	Monitoring & Reporting	Integration with planning activities
<b>Very High Risk</b>  <b>Rating 25</b>	<ul style="list-style-type: none"> <li>Immediate evaluation required.</li> <li>Identify and critically evaluate existing management strategies and controls.</li> <li>Determine additional strategies and actions necessary to manage the risks to an acceptable level within an agreed timeframe.</li> <li>Assign specific accountability to Executive Group members or designated taskforce</li> </ul>	<ul style="list-style-type: none"> <li>Chief Executive Officer (“CEO”)</li> <li>Relevant Executive Group members</li> <li>Board of Directors (at the discretion of the CEO)</li> <li>Head of Corporate Affairs / Head of Risk</li> </ul>	<ul style="list-style-type: none"> <li>Formally reported to the CEO each quarter</li> <li>Formally reported to the Board each quarter</li> <li>More frequent reporting may occur at the discretion of the CEO</li> </ul>	<ul style="list-style-type: none"> <li>Consideration of extreme risks occurs as part of group Strategic Planning</li> </ul>
<b>High Risk</b>  <b>Rating 15 to 20</b>	<ul style="list-style-type: none"> <li>Priority evaluation required</li> <li>Identify and critically evaluate existing management strategies and controls.</li> <li>Determine additional strategies and actions necessary to manage the risks to an acceptable level.</li> <li>Reconfirm specific accountability to Executive Group members and their direct reports</li> </ul>	<ul style="list-style-type: none"> <li>Relevant Executive Group members</li> <li>Direct reports of the relevant Executive Group members</li> <li>Head of Corporate Affairs / Head of Risk</li> </ul>	<ul style="list-style-type: none"> <li>Reported to the CEO each quarter</li> <li>Reported to the Board each quarter</li> </ul>	<ul style="list-style-type: none"> <li>Consideration of significant risks occurs as part of group or business unit Strategic Planning</li> </ul>
<b>Moderate Risk</b>  <b>Ratings 9 to 12</b>	<ul style="list-style-type: none"> <li>Identify and critically evaluate existing management strategies and controls.</li> <li>Critically assess the commerciality of improving management strategies based on the cost and effort required and the priority of other risks to be addressed.</li> <li>Monitor the level of risk on a periodic basis and escalate the management response if the risk escalates.</li> <li>Identify management accountabilities</li> </ul>	<ul style="list-style-type: none"> <li>Relevant Executive Group members</li> <li>Direct reports of the relevant Executive Group members</li> <li>Head of Corporate Affairs / Head of Risk</li> </ul>	<ul style="list-style-type: none"> <li>Monitored periodically by the relevant Executive Group member and their direct reports</li> </ul>	<ul style="list-style-type: none"> <li>Incorporated into business unit plans</li> <li>Considered as a part of business process design</li> </ul>
<b>Low Risk</b>  <b>Ratings 1 to 8</b>	<ul style="list-style-type: none"> <li>No formal evaluation of mitigating strategies and controls required.</li> <li>Monitor the level of risk on a periodic basis and escalate the management response if the risk escalates.</li> </ul>	<ul style="list-style-type: none"> <li>Relevant Executive Group members</li> <li>Direct reports of the relevant Executive Group members</li> </ul>	<ul style="list-style-type: none"> <li>Monitored infrequently by the relevant Executive Group member and their direct reports</li> </ul>	<ul style="list-style-type: none"> <li>Considered as a part of business process design</li> </ul>

### 3.6 Risk Appetite Assessment and Rating

Risk appetite is a measure of how much risk an organization is prepared to take, from being risk avoidance to tolerating higher level of risk (temporarily or on a long-term basis) in exchange for potential benefits. Management team is responsible for assessing its risk appetite for the Very High and High inherent risks.

Risk management's role is to establish internal controls and other measures necessary to ensure that residual risk (or the level of risk remaining after the inherent risk has been mitigated by internal controls) falls within the risk appetite.

Risk tolerance represents the application of risk appetite to specific objectives. Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that it will achieve its objectives. While risk appetite is broad, risk tolerance is tactical and operational. Risk tolerances guide operating units as they implement risk appetite within their individual sphere of operation.

Risk appetite should be expressed in the same form as the severity of the inherent and residual risks, as being a product of likelihood and consequence.

### 3.7 Risk Treatment Options

Risk treatment involves identifying the range of options for treating risks, assessing these options and the preparation and implementation of treatment plans. For risk above iSelect's risk tolerance, appropriate treatment plans should be agreed, assigned and actioned.

It is important to assess the organisational wide risk tolerance and provide adequate guidance. The following options may be considered in treating risks.

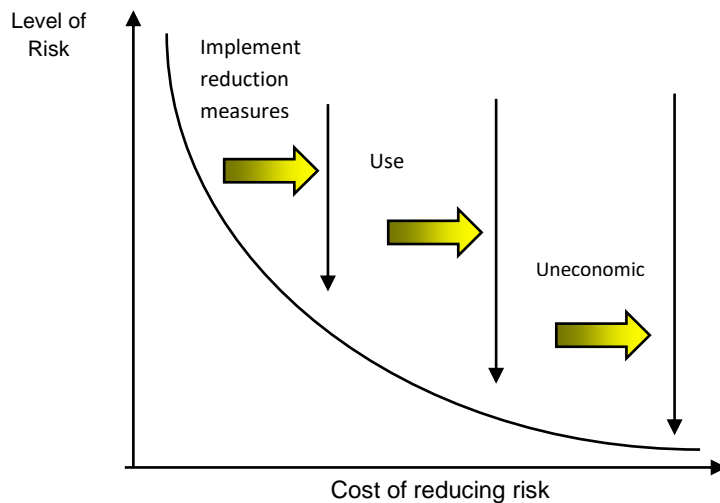
Option	Positive Risk	Negative Risk
<b>Avoid</b>	Avoid and abstain from an activity when the accumulative opportunity for gain is outweighed by the accumulative opportunity for loss.	
<b>Seek</b>	Seek and perform an activity when the opportunity for gain outweighs the opportunity for loss.	
<b>Manage (Enhance/Mitigate)</b>	Change the likelihood and/or consequence of risk to maximise the opportunity impact on iSelect.	Change the likelihood or consequence of risk to minimise the impact on iSelect.
<b>Transfer</b>	Transfer the potential gain or loss to a third party (e.g. insurer) to reduce iSelect exposure to the risk or set of risks associated with particular activities.	
<b>Accept</b>	After establishing appropriate controls, iSelect needs to accept the residual risk within the decision/activity and monitor those controls in place to maximise the opportunity for positive outcomes.	After establishing appropriate controls, iSelect will accept the residual risk within the decision/activity and monitor those controls in place to minimise negative outcomes.

### 3.8 Selecting Risk Treatment Options

Selecting the most appropriate option involves balancing the costs of implementing each option against the benefits derived from it.

In general, the cost of managing risks needs to be commensurate with the benefits obtained. When making such cost versus benefit judgements, the context should be taken into account.

It is important to consider all direct and indirect costs and benefits whether tangible or intangible, and measured in financial or other terms.



### 3.9 Control Assessment and Rating (determining residual risk)

To determine the level of residual risk, mitigating practices and controls such as policies, procedures, practices and processes must be assessed and evaluated.

Where mitigating practices / controls exist but are not being followed and monitored, then adequate control does not exist, as in order for mitigating practices / controls to be effective they also must be communicated, actioned and monitored. Below is the rating table to describe assessment results of controls.

	Number	Rating *	Description
← Adequate →	Excellent	1 or 2	<b>Risk Exposure is effectively managed</b> Highly effective and proven strategies, actions, systems and processes exist to manage the risk and management accountability is clearly assigned. The systems, processes and actions are well documented and monitored regularly for continued effectiveness in mitigating the risk.
	Good	3 or 4	<b>Majority of Risk exposure is effectively controlled and managed</b> Effective strategies, actions, systems and processes exist to manage the risk and management accountability is defined. Some opportunities exist to marginally improve effectiveness of the mitigating strategies and controls however these may not yet be actioned or may not be justifiable (e.g. not cost effective).
← Inadequate →	Marginal	5 or 6	<b>There is room for improvement</b> Partially effective strategies, actions, systems and processes exist to manage the risk. Opportunities exist to improve the effectiveness of mitigating strategies and controls however these have not yet been actioned (e.g. re-alignment of accountability, refinement of processes due to changes in operations, improved monitoring of effectiveness).
	Poor	7 or 8	<b>Negligent risk exposure appears to be controlled, but there is major risk exposure</b> Ineffective strategies, actions, systems and processes are currently in place to manage the risk. Substantial changes in the design and operation of mitigating controls need to be implemented and management accountability determined in order to manage the risk effectively.
	Unsatisfactory	9 or 10	<b>Control measures are ineffective</b> No strategies, actions, systems or processes have been identified and implemented to manage the risk.

\* Range of rating allows for strength of the statement to be varied.

Upon control assessment, Residual Risk is determined and expressed in the same form as the severity of the inherent risk and risk appetite, as being a product of likelihood and consequence. The Company should ensure that residual risk falls within the risk appetite, or else the additional risk treatment plans are required to be developed.

### 3.10 Monitor and Review

Ongoing review is essential to ensure that risk profiles are complete and reflect prevailing strategies, marketing conditions, operational and management plans. Treatment plans should be continuously updated to ensure that it remains relevant. Factors that may affect the likelihood and consequences of risks change over time, as do factors that affect the suitability of management strategies or cost of the treatment options. Therefore, it is necessary to undertake the risk management cycle regularly at each level of iSelect. Implementation of risk treatment plans should be monitored regularly and provide an important performance measure.

### 3.11 Communicate and Consult

Communication will involve dialogue with stakeholders (the CEO, the Executive Group and the Board of Directors) with efforts focused on creating a consultative atmosphere. Effective internal and external communication is important to ensure that responsibility for implementing risk management, and those with a vested interest, understand the basis on which decisions are made and particular actions required. In particular, the provision of information to the Executive Team will allow them to make the necessary business decisions with greater certainty.

Stakeholders are likely to make judgments about risk based on their perceptions. These can vary due to differences in values, needs, assumptions, concepts and concerns as they relate to the risks or the issues under discussion. Since the views of stakeholders can have a significant impact on the decisions made, it is important that their perceptions of risk be identified and recorded and integrated into the decision-making process.

The consultative approach allows management to take 'ownership' and appreciate the benefits of particular controls and the need to endorse and support a treatment plan.

## 4. Risk Management Leadership and Responsibilities

### 4.1 Board

The Board has responsibilities in relation to financial reporting, risk management and internal control, and also monitors compliance with relevant requirements of other laws and regulations. In relation to risk management and internal control, the Board assumes responsibility over:

<ul style="list-style-type: none"><li>• Review and endorse risk profile in the Corporate Plan</li><li>• Review risk assessments</li><li>• Review major risk management project</li></ul>	<ul style="list-style-type: none"><li>• Approve risk policy and framework</li><li>• Review major fraud reports</li><li>• Review quarterly risk management report and profile</li></ul>	<ul style="list-style-type: none"><li>• Review the internal audit program and report</li><li>• Review external audit reports in relation to internal controls</li><li>• Review moderate or higher incidents</li></ul>
--	--	---

### 4.2 Executive Management Team



The Executive Management Team are responsible for:

- overall design and management of the Risk Management Process at all levels within iSelect
- setting risk appetite
- providing assistance to management to fulfil Risk Management responsibilities under the risk management program including risk assessments
- raising risk awareness
- risk reporting to the Board.

### 4.3 Risk & Compliance Manager & Risk and Compliance Consultant

The Risk and Compliance Manager is responsible for implementation and coordination of the risk management program including:

<ul style="list-style-type: none"><li>• Risk system management and training</li><li>• Coordinating quarterly business area risk updates</li></ul>	<ul style="list-style-type: none"><li>• Risk profile management</li><li>• Reviewing strategic plan risks and mitigating strategies</li></ul>	<ul style="list-style-type: none"><li>• Board Reporting</li></ul>
---	--	---

Risk and Compliance Consultant is operationally responsible for the Risk Management Framework that includes the following information:

<ul style="list-style-type: none"><li>• Terminology and definitions</li><li>• Roles of participants</li></ul>	<ul style="list-style-type: none"><li>• Risk Submission and approval</li><li>• Risk reporting</li></ul>	<ul style="list-style-type: none"><li>• Tools and forms</li><li>• Risk identification</li></ul>
---	---	---

### 4.4 Risk Owner

The Risk Owner is responsible for:

- managing risk through to an acceptable level
- the accuracy of the documentation of the risk
- allocation of strategy ownership
- obtaining approval for any suggested risk treatment strategies prior to implementation
- monitoring and reviewing the progress of the risk, until it is managed to an acceptable level
- reporting the progress of the risk.

### 4.5 Mitigating Strategy Owner

For each risk one or more mitigating strategies can be developed. Each mitigating strategy has a responsible officer assigned. The responsible staff member is accountable for:

- implementation of the mitigating strategy within the required timeframe

- monitoring progress of the mitigating strategy implementation
- reporting to the risk owner the progress of mitigating strategy implementation in line with the Update schedules.

#### **4.6 All Staff**

Risk Management is essentially everyone’s responsibility. All staff are responsible for staying alert to incidents or events that might impact management’s assessment of the risks and should immediately escalate the information on those incidents or events to their managers or the Risk and Compliance team.







## **5. Risk Management Reporting**

Risk Management reporting takes the form of a fully detailed risk assessment report that can be used by management to continue to manage risks identified and assign accountabilities and processes to ensure sustainability. Sample risk management reporting components are noted below.

### **5.1 Summary Risk Information**





For moderate or lower risks, inherent risk ratings are assessed and updated. For high and very high risks, in addition to inherent risks, control effectiveness, residual risk rating and risk appetite are also assessed, in order to determine whether they have been properly managed – residual risk falls within risk appetite. The following table provides a summary of the high and very high risks facing iSelect (only as an **example**)

ID	Risk Category	Risk Description	Inherent risk rating		Control rating		Residual risk rating	Risk Appetite	Management Action Planned?
			Score	Level	Score	Level			
A	Compliance	Increased regulation imposes higher risks of non-compliance	25	V	5	IN	M	L	Y
B	Human Resource	Failure to attract and retain appropriate talent	20	H	6	IN	M	L	Y
C	Information Technology	Dependency on third party providers to operate key business systems (Third Party Agreement)	16	H	8	IN	H	L	Y
D	Strategic	Inability to scale existing verticals	20	H	4	A	M	M	N
E	Financial	Inappropriate execution of revenue assurance	25	V	5	IN	M	L	Y

RISK RATINGS			
	Very High risk		Moderate risk
	High risk		Low risk
CONTROL RATINGS			
	Adequate control		Inadequate control

## 5.2 Detailed Risk Information – example only

The following information supports risk management summary information provided to key executives.

<b>Reference:</b>	ABC123		
<b>Risk Description:</b>	Failure to attract and retain appropriate talent		
<b>Risk Category:</b>	Human Resources		
<b>INHERENT RISK ASSESSMENT</b>			
<b>Contributing Factors (<i>what causes the risk to exist</i>):</b>			
<ul style="list-style-type: none"> <li>Dependency on small number of individuals who possess hard to replace corporate knowledge or industry skills</li> </ul>	<ul style="list-style-type: none"> <li>Limited career progression in a small organisation</li> <li>Lack of sufficient career flexibility</li> </ul>		
<b>Likelihood Rating:</b>	5	<b>INHERENT RISK RATING:</b>	
<b>Consequence Rating:</b>	4	20	
<b>CURRENT CONTROLS / MITIGATING PRACTICES</b>			
<ul style="list-style-type: none"> <li>Dedicated HR processes</li> <li>Workforce plan prepared – recruitment needs identified in advance of having to recruit</li> </ul>	<ul style="list-style-type: none"> <li>Positive work / life balance / family friendly policies, etc.</li> <li>Organisational structure provides increased opportunities for existing staff</li> </ul>		
<b>Control Rating</b>	6		
<b>RESIDUAL RISK RATING</b>	12		
<b>RISK APPETITE RATING:</b>	5		
<b>MANAGEMENT ACTION PLAN</b>			
<b>Activity</b>	<b>Responsibility</b>	<b>Timing</b>	
<ul style="list-style-type: none"> <li>Development of training plans</li> <li>Long-term incentive plans for key personnel</li> </ul>	<ul style="list-style-type: none"> <li>Tom</li> </ul>	<ul style="list-style-type: none"> <li>February 200x</li> </ul>	

### 5.3 Risk Reporting to CEO and Board

iSelect encourages an environment in which risks or concerns can be reported and in a timely manner. All personnel have an ongoing responsibility to manage risk at iSelect and report risk events to either their direct line manager or the Risk and Compliance Team.

Risk management is one of its key areas discussed and it is a standing agenda item at Board meetings. The approval of the overarching Risk Management Framework document is executed by the Board and relies on Executive Team to disseminate throughout the iSelect business.

The table below illustrates the various responsibility levels at iSelect, their interaction with Risk Management including key documents that reflect the risk activity undertaken at iSelect.

To	Report(s)	Prepared By	Frequency	Content / Purpose
Board of Directors	Risk Framework Summary Risk Reports	Risk and Compliance Manager	Annually Quarterly	Review and approval of Risk Framework Update of changes to iSelect risk profile. This may include status of outstanding or untreated risks and due action items
CEO	Summary Risk Reports	Risk and Compliance Manager	Quarterly	The risk reports may include confirmation that controls are operating and report on any current risk/compliance matters
Executive Management Team	Corporate Risk Register Summary Risk Reports Risk Event Summary and Action Plans	Risk and Compliance Manager & Risk Owners	Quarterly	Summary Risk reports and risk registers provides Executive Team with an update on the ranking of risks together with agreed treatment plans. Other supporting Risk Management initiatives can be tabled via the reporting and monitoring process.
Risk and Compliance Manager	Detailed Risk Registers (Risk Assessments) Risk Event Summary and Action Plans	Risk and Compliance Consultant & Risk Owners	Ongoing	General managers need to continually monitor risk at the operational levels. Any material risk events should be immediately reported and included into the Corporate Risk Register. It is also their responsibility to ensure delegates are aware of iSelect risk framework.
Risk and Compliance Team	Escalation of Risk Events and management of Action Items	Operational Personnel	Ongoing	Personnel have a responsibility to report / escalate risk events which may or have occurred. Action Items may fall under their responsibility and should be actioned and reported within due dates.

## 6. Document Control

### 6.1 Purpose

This Framework specifies a detailed risk management process that provides systematic and consistent identification, assessment and management of risks across iSelect, that complies with the Australian Risk Management Standard (AS/ANZ 31000:2018).

### 6.2 Scope

This Framework applies to all employees of iSelect.

### 6.3 Policy Information

<b>Policy Department:</b>	Risk and Compliance	<b>Next review date:</b>	May 2024
<b>Owner:</b>	Compliance and Risk Manager	<b>Review Period:</b>	Annual
<b>Approver:</b>	Executive of Legal, Risk and Compliance	<b>Last Author</b>	Katie Baines

### 6.4 Document History

Version	Date Approved	Author	Description
1	14 Aug 2013		Policy developed
2023.1	1 June 2023	K Baines	Reformatted and review of framework.

### 6.5 Related documents

- Risk Register (housed within Riskware software)

## Appendix A – Risk Categories

Based on iSelect current strategy and operations, a list of risk categories, category descriptions and an example of contributions has been listed below to aid risk identification.

<b>Assets</b> - Risks relating to the management or maintenance of iSelect key assets including property, plant, inventory and environment (e.g. buildings, security documentation and money)	
<ul style="list-style-type: none"> <li>• security of assets</li> <li>• records management</li> <li>• asset maintenance</li> </ul>	<ul style="list-style-type: none"> <li>• capital planning / replacement strategy</li> <li>• capacity and function</li> </ul>
<b>Customer Service</b> - The management and servicing of obligations to customers	
<ul style="list-style-type: none"> <li>• Sales accuracy</li> <li>• relationship management</li> </ul>	<ul style="list-style-type: none"> <li>• complaints handling</li> <li>• dispute resolution</li> </ul>
<b>Business Continuity</b> - The planning and processes required to maintain the continuity of business activities or recovery response to a disastrous event, which may impact the effectiveness of business operations. This includes internal and external activities and processes (e.g. system failures, critical staff dependencies, fire, flood, etc)	
<ul style="list-style-type: none"> <li>• knowledge of critical activities</li> <li>• resilience to disruption</li> <li>• single points of failure</li> <li>• alternate processing capabilities</li> </ul>	<ul style="list-style-type: none"> <li>• reliance on key suppliers</li> <li>• communication of roles, responsibilities &amp; training</li> <li>• maintenance/testing of plans</li> </ul>
<b>Regulatory</b> - Risks relating to non-compliance with legislation, regulations, supervision or internal policies and procedures. This also includes all regulatory issues impacting iSelect	
<ul style="list-style-type: none"> <li>• regulatory compliance</li> <li>• regulator relationships</li> <li>• external environmental issues</li> <li>• competition law</li> </ul>	<ul style="list-style-type: none"> <li>• Australian Competition &amp; Consumer Commission</li> <li>• Intellectual property, copyright</li> <li>• Whistleblowing</li> </ul>
<b>Legal &amp; Contractual</b> - Risks associated with developing, managing and monitoring contracts as well as compliance with required service levels and cost arrangements as specified within the terms of service agreements	
<ul style="list-style-type: none"> <li>• adequacy of legal agreements</li> <li>• KPIs and contractual performance</li> <li>• roles and responsibilities</li> <li>• adequacy of contract management systems</li> </ul>	<ul style="list-style-type: none"> <li>• service and renewal requirements</li> <li>• completeness and accuracy of contracts register</li> <li>• profitability of contractual arrangements</li> <li>• licensing agreements</li> </ul>
<b>Corporate Governance</b> - Risk associated with Governance requirements and Board governance processes and practices	
<ul style="list-style-type: none"> <li>• monitoring</li> <li>• independence</li> <li>• company Code of Conduct</li> </ul>	<ul style="list-style-type: none"> <li>• composition of members and skill mix</li> <li>• reporting</li> </ul>

<b>Finance</b> - Risks associated with the development, collection, storage and reporting of financial information vital to sustaining the management of iSelect operations. This category also includes risks associated with budgeting, management reporting and cost management	
<ul style="list-style-type: none"> <li>• taxation (legacy and current issues)</li> <li>• procurement cost effectiveness</li> <li>• accounting policy</li> <li>• debt management</li> <li>• supplier payment</li> <li>• investments</li> <li>• capital expenditure</li> </ul>	<ul style="list-style-type: none"> <li>• budget setting</li> <li>• cash reserve management</li> <li>• insurance</li> <li>• fraud</li> <li>• hedging/use of derivatives</li> <li>• financial reporting</li> </ul>
<b>Human Resources</b> - Risks associated with recruitment, remuneration, retention and industrial relations, including supporting systems, processes and procedures	
<ul style="list-style-type: none"> <li>• equal opportunity</li> <li>• availability of skilled staff</li> <li>• staffing mix</li> <li>• succession planning</li> <li>• performance management</li> </ul>	<ul style="list-style-type: none"> <li>• remuneration framework</li> <li>• career development</li> <li>• stress</li> <li>• training and development</li> </ul>
<b>Information Technology</b> - The risks arising from the use and reliance on information by the organisation or other external entities, which may impact operations (e.g. internal systems, external service providers systems, Internet)	
<ul style="list-style-type: none"> <li>• data management</li> <li>• data security</li> <li>• systems development /new systems</li> <li>• process improvement &amp; enablement</li> </ul>	<ul style="list-style-type: none"> <li>• systems maintenance</li> <li>• availability</li> <li>• data integrity</li> <li>• service delivery</li> </ul>
<b>Occupational Health and Safety (OH&amp;S)</b> - Risks associated with complying with OH&S legislation, internal policies and accreditation requirements & workers compensation	
<ul style="list-style-type: none"> <li>• internal practices and procedures</li> <li>• staff guidance and training</li> <li>• incident reporting</li> </ul>	<ul style="list-style-type: none"> <li>• organisational response to legislative requirements</li> <li>• OH&amp;S audits</li> </ul>
<b>Strategic</b> - Risks associated with the strategic direction of the business. Including market conditions, legal and regulatory frameworks, competitor activity, strategy development, strategic alliances, business planning and performance targets	
<ul style="list-style-type: none"> <li>• brand management</li> <li>• customer segmentation strategy</li> <li>• research and development</li> <li>• acquisition and integration</li> <li>• strategic alliances</li> </ul>	<ul style="list-style-type: none"> <li>• business planning</li> <li>• exploring new opportunities for growth in the business units</li> <li>• performance targets</li> <li>• customer relationship management</li> </ul>