Risk Management Policy

Last Updated 15 June 2016

Contents

1 Introduction

As a publicly listed company and provider of financial products and services, DomaCom Limited and its related entities (DomaCom) operates in a highly regulated environment.

DomaCom is committed to the effective management of risk, which is central to its continued growth and success and the achievement of the Company's corporate objective and strategy.

1.1 Key obligations under this policy

DomaCom has adopted a Risk Management Policy for the oversight and management of material business risks and manages risk within a comprehensive risk management process which is based on the principles and guidelines outlined in ISO 31000 - Risk Management and from Australian New Zealand Standard AS/NZ 4360:2004

A key element of this risk management process is the Board's assessment of risk, which is based on the level of risk DomaCom is able to sustain in achieving its corporate objective of delivering value to shareholders. Risks are identified, analysed and prioritised using common methodologies and risk controls are designed and implemented having regard to the overall corporate strategy.

The Board is responsible for reviewing and approving the overall management of risk and internal controls.

The Board monitors DomaCom’s risk profile, risks and mitigating strategies primarily through a combination of the Board and receipt of regular reports from management on the effectiveness of DomaCom’s risk management process.

DomaCom Management, through the CEO, COO/CFO, Legal Counsel, Chief Compliance and Risk Officer, Financial Controller and Company Secretary is responsible for the overall design, implementation, management and coordination of the Company's risk management and internal control system.

Each business unit has responsibility for identification and management of risks specific to their business. This is managed through an annual risk workshop within each business unit and a regular self-assessment of the risk register as part of regular management reporting.

The outcomes of the business unit risk workshops are integrated in the Corporate Risk Register and presented to the Board on an annual basis, and management is required to present regular updates to the Board on material business risks.

In addition, the Chief Compliance and Risk Officer independently monitors the Corporate Risk Register and internal control framework and provides written reports to the Board on the effectiveness of the management of risk and internal controls.

1.2 Updating of Policy

The Chief Compliance and Risk Officer will be responsible for updating this policy. The policy will be reviewed and updated (if necessary) at least annually and whenever there is a change in law or business activities.

2 Background

(a) DomaCom will take all appropriate actions to help ensure that it complies with its risk management obligations under this policy.

(b) DomaCom is required to have adequate risk management systems which:

(i) identify, analyse, evaluate, treat and communicate risks in its business, and monitor and report on risk management issues;

(ii) assesses risks associated with its business and the probability of those risks occurring; and

(iii) provides risk management training to all Staff.

(c) DomaCom's risk management system is:

(i) based on a structured and systematic process that takes into account the DomaCom regulatory obligations;

(ii) identifies and evaluates risks faced by its business, focusing on risks that adversely affect clients or market integrity (this includes risks of non-compliance with regulatory obligations);

(iii) establish and maintain controls designed to manage or mitigate those risks; and

(iv) fully implement and monitor those controls to ensure they are effective.

(d) The Australian and New Zealand standard on risk management systems, AS/NZ 4360:2004, provides a guide in planning and implementing risk management systems.

3 Strategy

(a) The risk management function for DomaCom will be overseen by the Chief Compliance and Risk Officer who reports to the Legal Counsel and ultimately to the Board.

(b) DomaCom's risk management strategy will be approved by the Board. The Chief Compliance and Risk Officer will brief the Board on changes to, or breaches of, the risk management systems.

(c) Compliance procedures will also be developed by the Chief Compliance and Risk Officer that will address the regular regulatory reporting and the monitoring of the day to day management of the Company. The compliance procedures will be established to ensure compliance with the relevant regulatory requirements. Implicit in the concept

of the compliance procedures is that they manage and, where possible, reduce the inherent risks involved in the Company's business.

(d) DomaCom has identified a number of risks which are described in the live Corporate Risk register. The Risk Register identifies:

(i) the risks to DomaCom;

(ii) the likelihood that each individual risk will arise;

(iii) the impact on the business of the risks, including consideration for any mitigating systems DomaCom has in place; and

(iv) what risk prevention measures are available.

(e) Individual risks are identified on the basis of both the likelihood that they will occur and their impact in the event they occur.

(f) DomaCom undertakes a detailed Risk Analysis which includes for each risk identified in the Risk Register the following:

(i) a description of the risk;

(ii) the cause of the risk;

(iii) the consequences of the risk;

(iv) the inherent risk rating;

(v) a description of the controls to address the risk;

(vi) the residual risk rating allowing for the mitigating controls that have been implemented; and

(vii) action plans where necessary.

4 Treatment of Risks

Where DomaCom identifies a risk it will impose appropriate procedures to, so far as possible, reduce the potential impact of, or likelihood of, the occurrence of that risk.

Where DomaCom identifies a risk that is likely to have either a high or extreme impact upon the business, even after organising appropriate procedures to mitigate against it, DomaCom has identified 4 potential approaches:

(a) Terminate the risk

This is achieved by, for example eliminating the business area or significantly altering it. DomaCom will choose this course of action for risks that could have catastrophic impact on the business and where the costs of otherwise regulating the risk outweigh the potential business benefit.

(b) Manage and reduce the risk

DomaCom can seek to reduce a risk by taking specific action focused at the risk itself, for example seeking to reduce the likelihood the risk will occur or reducing the potential impact if the risk occurs.

(c) Accept the risk

DomaCom recognises that all businesses involve a degree of risk. Accordingly, there may be some risks that DomaCom acknowledges and agrees to accept.

(d) Pass on the risk

DomaCom can choose to pass on all or part of a certain risk to another party.

5 Rating of Risks

Risks are assigned an overall risk rating of Low, Moderate, High or Extreme. Each risk rating represents a combination of the likelihood that the risk will eventuate combined with the potential impact of the risk if it eventuates. Refer to Annexure A for Risk Rating matrix.

6 Risk Register and Risk Analysis

A live Corporate Risk Register will represent a summary of the most significant risks identified by DomaCom and this will be reported to the Board on a monthly basis.

7 Details of role, seniority and capabilities of risk management personnel

7.1 Board of Directors

The board of directors (**Board**) is accountable for ensuring that a risk management system is established, implemented and maintained in accordance with this policy. Assignment of responsibilities in relation to risk management is the prerogative of the Board.

7.2 Responsible Managers

Responsible Managers are accountable for strategic risk management within the business areas under their control, including the devolution of the risk management process to staff.

7.3 Chief Compliance and Risk Officer

The Chief Compliance and Risk Officer will be accountable to the Board for the implementation of the risk policy in key areas of DomaCom, and for maintaining a programme for risk reassessment and the Risk Registers. The Chief Compliance and Risk Officer will provide staff with initial training and ongoing advice in risk management matters. The Chief Compliance and Risk Officer is responsible for the DomaCom's ongoing compliance procedures. Implicit in the concept of these procedures is that they manage and, where possible, reduce the inherent risks involved in DomaCom's business.

8 Risk Review Process

(a) An annual review of the DomaCom's risk management processes will be conducted by the Chief Risk and Compliance Officer in conjunction with the Executive Team and the Board.

(b) The Chief Compliance and Risk Officer will provide a report to the Board detailing the findings of the annual review.

(c) If necessary, a third party will be engaged to provide an independent review of the DomaCom's business risks and controls.

9 Adoption of policy

This policy was adopted by the Board on 15 June 2016.

ANNEXURE A - RISK RANKING MATRIX

Likelihood (not taking into account existing controls) within the next 12 months

Level	Descriptor	Description
5	Almost Certain	Is expected to occur
4	Likely	Will probably occur based on previous experience
3	Possible	May occur
2	Unlikely	Could occur but chances remote
1	Rare	May occur only in exceptional circumstances

Consequences

Level	Consequence	Example
5	Extreme	High regulatory impact, high client impact, financial loss in excess of $200k, major effect on operations and on-going viability, greater than 10% impact on targets, adverse media attention, continuation of business jeopardised
4	Major	High regulatory impact, enforcement action by regulator, medium client and staff impact, potential for legal action, financial loss up to $200k, major effect on operations, up to 10% impact on targets.
3	Moderate	Regulatory impact, medium client and staff impact, financial loss up to $50k, some effect on operations, up to 5% impact on targets.
2	Minor	No regulatory impact, low client impact, financial loss up to $10k, no effect on operations, up to 1% impact on targets
1	Insignificant	No regulatory impact, no client or staff impact, no financial loss, no impact on targets

Existing Control Rating

Level	Descriptor	Description
4	Excellent	System is effective in reducing risk to an acceptable level, responsibility clear, well documented, regularly reviewed
3	Good	Systems and documentation in place but room for improvement
2	Fair	Some controls in place but incomplete
1	Poor / Unsatisfactory	Ad hoc and poorly documented processes, or no controls at all

Risk Priority Rating

Level	Descriptor	Description
H	High	Immediate action required with ongoing active management
S	Significant	Review of existing controls required
M	Medium	Controls in place but require regular review
L	Low	Risk of little concern and/or effective controls in place

Inherent Risk Rating Matrix

	Consequences					
Likelihood	Ratings	1	2	3	4	5
	5	**S**	**H**	**H**	**H**	**H**
	4	**S**	**S**	**H**	**H**	**H**
	3	M	M	**S**	**S**	**H**
	2	L	L	M	**S**	**S**
	1	L	L	L	M	**S**

Residual Risk Rating Matrix

	Existing Controls				
Inherent Risk	Ratings	1	2	3	4
	H	**H**	**H**	**S**	M
	S	**S**	**S**	M	L
	M	M	M	M	L
	L	L	L	L	L