**NUCHEV LIMITED**
**ACN 163 225 090**
**(Company)**

# RISK MANAGEMENT FRAMEWORK

(Approved by the Board on 29 August 2023)

## 1 Objectives

The Group Risk Management Framework is designed to:

- Provide an integrated enterprise-wide approach to business risk, including a common business risk language;
- Ensure that key risks currently faced by the business are understood, monitored and managed in accordance with the risk appetite of the business;
- Heighten risk awareness risk throughout the organisation and ensure that risk is considered in all decision-making processes;
- Ensure that all staff are aware of their responsibilities in relation to managing and taking risk; and
- Develop a mechanism and format for reporting and assessment of risks, how they are treated or managed, an escalation process and the methodology for ratings risks.

## 2 Roles and Responsibilities

### 2.1 The Board

The Board is ultimately responsible for the overall system of internal control and ensuring the Group has the right balance between taking risk and mitigating risk.

The Board sets the level of business risk that is acceptable for the Group (referred to as the company's risk appetite) and both oversees and monitors the operations of the risk management system. The Board is also responsible for reviewing new risks as they emerge and establishing the best structure for undertaking risk management activities, including practices that allow the Board to stay informed about risk within the business, and for providing Board oversight of risk matters. The Board also has a key role to play in managing risk in an emergency or crisis situation.

### 2.2 The Audit & Risk Committee

The Board has delegated responsibility for ensuring that the Group maintains effective risk management and internal control systems and processes to the Audit and Risk Committee. The Audit and Risk Committee reviews the risk profile including material business risks. It is important to note that, in appointing the Audit and Risk Committee, the Board has not delegated its responsibilities, as the Board retains accountability for risk management within the Group.

The Audit and Risk Committee reports to the Board on regular (quarterly) basis on the activities it has undertaken to review and monitor the effectiveness of the Group's risk management systems and specific risks identified by Management. The Audit and Risk Committee also periodically assesses the adequacy of the Framework and the resources that are available to implement this framework.

The Board formally reviews the Charter, membership and performance of the Audit and Risk Committee annually.

## 2.3 The Chief Executive Officer (CEO)

The CEO is responsible for implementing a strong risk management culture and embedding the Framework throughout the Group. In particular, the CEO is responsible for ensuring the Group is committed to managing its risks and that the availability of resources, as well as the performance of these resources, is sufficient to effectively manage the business' risks.

## 2.4 Management

Effective risk management is central to Nuchev's approach to driving sustainable, profitable growth. Management are responsible for designing and implementing risk management and internal control systems which identify material risks for the Group and aim to provide the Company with warnings of risks before they escalate.

Management implements the action plans developed to address material business risks across the Company.

Management regularly monitors and evaluates the effectiveness of the action plans. In addition, management promotes and monitors the culture of risk management within the business as well as ensuring compliance with the internal risk control systems and processes.

Management reports regularly to the Audit and Risk Committee and the Board regarding the status and effectiveness of the risk management program.

The Executive Leadership Team (ELT) must be satisfied that processes are in place to establish, implement and maintain the Risk Management Framework.

In addition, they must be satisfied that the roles and responsibilities that their staff and other stakeholders are expected to undertake in relation to risk management are well understood throughout the organisation. The ELT are responsible for:

- Identifying and evaluating current and emerging risks within their business area;
- Confirmation and assignment of ownership for specific risks; and
- Regular (at least six monthly) review and update of the risk assessments, risk profiles and key risks within their business area.

While the ELT has primary responsibility for risk management within their business area, the broader Management teams are also responsible for:

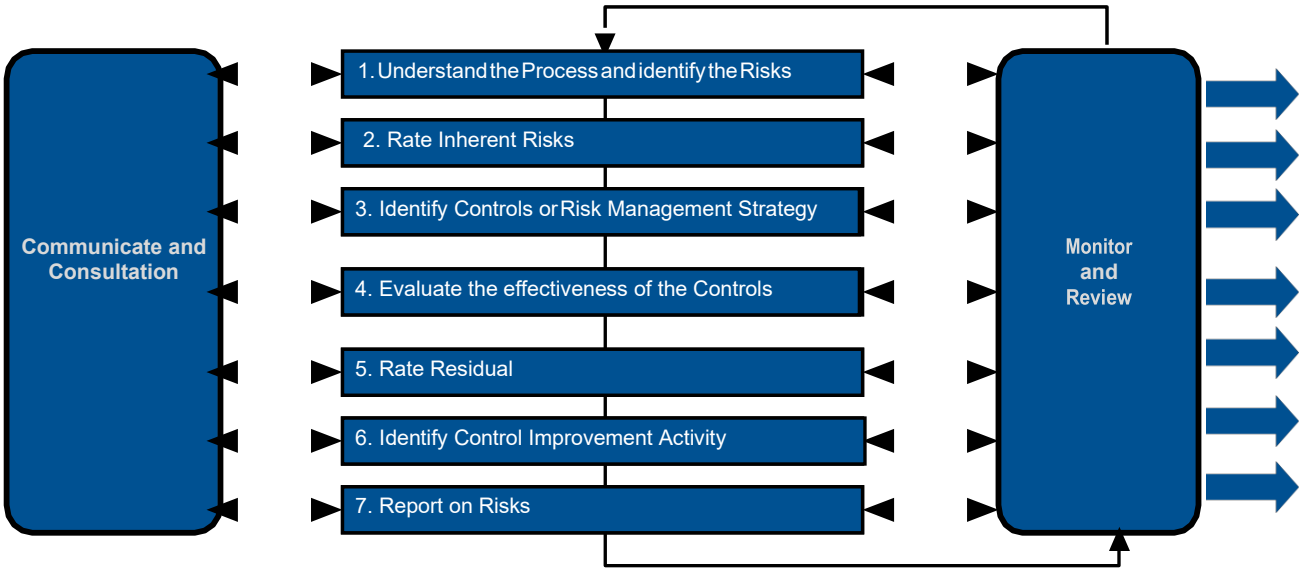
- Developing the environment within which risk management processes and procedures are implemented;
- Adequately training and developing staff so that risk management objectives may be achieved;
- Promoting a culture where risks are identified, as they emerge, and are managed appropriately;
- Reporting on risk events including near misses, incidents and breaches to the ELT;
- Ensuring that sufficient resources are available to effectively manage risks;

- Ensuring that the roles their teams are expected to undertake to implement risk management procedures and control activities are well understood throughout the organisation; and
- Implementing measures to manage operational risks and incorporating them into business procedures.

## 3 Risk Management Process

### 3.1 A Seven Step Approach

The risk management process adopted by the Group is aligned to good practice and is summarised in the following diagram:




The main elements of the risk management process include:

***Step 1: Understand the Process and Identify the Risks:***

The core objectives, processes and procedures of each department or business unit must firstly be understood. Then the major risk areas in each department are identified and discussed via workshops with management.

***Step 2: Rate Inherent Risk:***

The process by which the major risk areas in each department or business unit are given an inherent rating, which involves considering the likelihood of occurrence and the impact of the risk if it materialises. An inherent risk rating is a rating that does not consider the effect of controls or risk mitigation strategies.

***Step 3: Identify Controls:***

Risk mitigation strategies, and measures or controls that are in place to manage risk are identified by the business process owners.

***Step 4: Evaluate the Effectiveness of Controls:***

The efficacy of the controls that are in place to mitigate and/or eliminate the risk is then determined by management. For key controls, Management are required to provide evidence that the control is in place or the results of their review of the effectiveness of the control.

***Step 5: Rate Residual Risk:***

The risk is then re-rated at a residual level.

The residual risk rating is the rating that is applied to the risk after considering the adequacy and effectiveness of the controls that are in place to manage the risk.

The objective of this phase in the risk management process is to separate the key (or material/significant) risks, which require further attention, from the risks that are managed to an acceptable level by the existing controls or risk mitigation strategies.

The residual risk rating is determined by using the same qualitative measures used to assess inherent risk in step 2, namely the likelihood of an event occurring and the consequences on the Group if it did occur.

***Step 6: Identify Control Improvement Activity:***

The residual risks are compared to the Risk Appetite that has been set by the Board, or other pre- established criteria. Appropriate action plans or control improvement activities required to further mitigate risks to an acceptable level are agreed with departmental managers.

Not all major risks will be further reduced, as management may decide to accept certain risks.

This is a valid approach provided the acceptance of the risks is aligned to the Risk Appetite set by the Board.

Other risks may have a higher residual rating than the business would like, that cannot be reduced further, perhaps because of external factors out of their control (e.g. currency movements or competitor activity).

It is important that these risks are closely monitored, and action plans should be put in place to quickly respond to changes or if it seems that the risk may materialise.

***Step 7: Report on Risks:***

Reporting of key risks and the performance of the applicable mitigation strategy is undertaken on a quarterly basis to the Audit and Risk Committee, and on a six-monthly basis to the Board.

Quarterly to six monthly reviews are held with departmental heads to re-evaluate their risks and as such the risk management process described above recommences, becoming cyclical.

### 3.2 The Risk Management System

The Group's risks, current control environment, risk assessments (inherent and residual), actions required, and risk owners are recorded in the Group Risk Register, which is centrally maintained by the Chief Financial Officer (CFO).

The quarterly risk report provided to the Audit and Risk Committee and, on a six-monthly basis, to the Board is extracted from the Group Risk Register – highlighting the top 10 risks identified by management and providing an overview of changes in the Group's risk profile/key risk ratings.

### 3.3 The Risk Profile

The Risk Register contains the business risk profiles, which are prepared in accordance with the Seven Step approach. The risk profiles are "living" and non-static because they are regularly updated based on analysis and feedback.

Each risk profile contains the following components:

- Key risk area and associated risks;
- Key objective threatened (i.e. the risk definition and effect);
- Risk owner(s) and responsibilities;
- Inherent risk rating;
- Control or other mechanisms in place to reduce the risk and their effectiveness;
- Residual risk rating; and
- Control improvement plans and action items.

It is important to note the difference between inherent risk and residual risk ratings.

An inherent rating is the likelihood and consequence of a risk event occurring in the absence of any action to control or modify the circumstances.

A residual rating signifies the exposure to loss remaining after a risk has been countered, controlled, mitigated or eliminated.

## 4 Risk Identification, Evaluation & Rating Procedures

### 4.1 Understanding the Process and Risk identification (Step 1)

The Framework applies to all categories of risk that may affect the Group.

Risk identification involves analysing factors, circumstances and events that could give rise to a company's objectives not being achieved. Risks may include both adverse events and lost opportunities. The following steps are applied to facilitate the risk identification process:

- Identify the objectives of the company as a whole and the objectives of supporting operational departments and processes (business objectives); and

- Identify the events that, should they occur, could lead to the objectives not being achieved.

During the risk identification process, the Group categorises risks as follows (and in no particular order of priority):

| Category | Risk Definition |
|---|---|
| **Strategic** | Risks affecting determination of the Group strategy and objectives and the ability to achieve them. Including risks exposing the Group to loss of distribution partners, major customers or inadequate distribution channels and/or inappropriate products and marketing. |
| **Reputational** | Risks around the brand or reputation of the Company |
| **Operational** | Risks resulting from the operations or processing activities of the business. They are directly affected by supply chain failures and/or product quality issues. |
| **Environmental** | Risks affecting the company's ability to continue operating in a manner that does not compromise the health of the ecosystems in which it operates over the long term, including the environmental risks of major suppliers and manufacturers used by the Group in its supply chain. |
| **Work Health & Safety (WHS)** | Risks resulting from workplace incidents or events that expose staff (including contractors working for the Company) to serious injuries and/or potentially death. This includes physical and non-physical (eg mental health) risks and the Group's exposure to WHS fines and/or other regulatory actions. |
| **People** | Risks arising from inadequate Human Resource practices, policies and procedures, leading to the inability to attract and retain competent resources that perform properly to achieve the Group's objectives. |
| **Financial** | Risks relating to the documents prepared for external parties and management, including external financial reporting (ASX, ASIC, ATO etc). These risks are affected by the information contained within the Group's financial accounting and reporting systems and by the application of generally accepted accounting and regulatory principles and/or requirements. Risks around the way in which financial information is presented and communicated throughout the Group and externally to suppliers, customers, shareholders, and other key stakeholders, such as regulatory authorities. |
| **Information Technology** | Risks relating to Group reliance on information technology and systems, including the functionality and availability of the computer and communication systems used by the Group. |
| **Regulatory** | Risks around the way in which the Group manages its exposure to regulatory obligations in the markets and geographies it operates (for example food safety standards, licencing and compliance with import/export of goods for sale in foreign markets). |
| **Legal** | Risks around the way in which the Group communicates information to shareholders and the ASX and complies with its legal obligations (including ongoing disclosure obligations). |

## 4.2 Risk Rating Criteria (Steps 2 and 5)

Risk evaluation and rating procedures provide an analysis of each risk to determine the overall effect the risk is likely to have on the Group's financial performance, strategy, reputation and operations. This is defined by the

assessment of the risk against the likelihood that the risk event will occur; and the consequential impact or effect that the risk will have if the event actually occurs. The approach for analysis and evaluation is essentially qualitative, using manager experience, judgment and intuition to make decisions.

Two steps in the Risk Management Process require the risk to be rated:

**Step 2 – Rate the Inherent Risk** which involves assessing the likelihood that the risk events could occur and their resulting impact on the business, assuming no controls or risk management strategies are in place; and

**Step 5 – Rate the Residual Risk** which involves assessing the probability and impact of the risk having considered the existence and effectiveness of the control or risk management

The risk rating is a combination of Likelihood and Consequence. This is discussed further in sections 6.2.1, 6.2.2 and 6.2.3 below.

4.2.1 Determining the Likelihood

In order to assess the level of risk, the likelihood of the risk occurring needs to be determined.

The Group adopts classifications with generally understood meanings such as “Rare”, “Possible”, “Likely” etc. The following scale is used during the risk rating process to record the likelihood of a risk event occurring.

| Rating | Description | Frequency |
|---|---|---|
| **Almost Certain** | Expected to occur in most circumstances | May happen several times a year |
| **Likely** | Will probably occur in most circumstances | Approximately once per year |
| **Possible** | Should occur at some time | Approximately once per 5 years |
| **Unlikely** | Could occur at some time | Approximately once per 5 to 10 years |
| **Rare** | May occur in exceptional circumstances | Approximately once every 20 years or less |

## 4.3 Assessing the Consequence

The consequence or impact to the business of the risk materialising is defined as Insignificant through to Catastrophic. The matrix on the following page provides a definition for Insignificant, Minor, Moderate, Major and Critical, in terms of financial impact, legal, regulatory and contractual impact as well as impact on our employees, customers, brand, reputation and operations.

The impact or consequence of each risk should be assessed separately as well as an overall picture of all consequences together. For example, a risk that may

have multiple financial consequences might also have a regulatory impact that should be assessed together to determine the overall level of consequence. Particular care must be taken with quantitative analysis when examining consequences that are intangible or difficult to quantify, such as brand and reputational impacts.

### 4.4 Rating the Risk – Combining Likelihood and Consequence

Each risk is then given an overall rating by combining the likelihood and consequence rating. Senior Managers assess and evaluate each risk and develop treatment plans based upon the overall rating.

| Risk Matrix | | Consequence (Severity) | | | | |
|---|---|---|---|---|---|---|
| | | Insignificant | Minor | Moderate | Major | Critical |
| Likelihood | Almost Certain | Medium | High | High | Extreme | Extreme |
| | Likely | Medium | Medium | High | High | Extreme |
| | Possible | Low | Medium | Medium | High | High |
| | Unlikely | Low | Low | Medium | Medium | High |
| | Rare | Low | Low | Low | Medium | Medium |

## 5 Risk Treatment and Mitigation

### 5.1 Identify the Controls or Risk Management Strategies (Step 3)

There are a number of ways that an organisation can manage risk. Implementing controls within business processes is a common technique. Controls are activities that:

- Reduce the frequency of risk events;
- Reduce the impact of risk events;
- Indicate the occurrence of a risk event (“indicators”), so the necessary actions can be taken to reduce the impact of that event, or improve existing controls to reduce the impact or frequency of future events; and
- Give warning of circumstances that indicate that the likelihood of occurrence of a risk event has increased (“predictive controls”).

The Group implements a number of control activities to manage risks within its businesses. These control activities encompass both preventative and detective controls, manual and automated controls.

A strong control environment is one where there are a greater number of preventative automated controls and less detective or manual type controls.

Controls typically include: system access controls; inbuilt limits and parameters within systems; written procedures; verification and authorisations; reconciliations; checklists; exception reporting; and segregation of duties.

In addition to controls, management may use specific strategies to manage risk.

These may include: transferring risk using insurance, re-insurance or hedging; avoiding the risk by changing the process or strategy; taking risk in other areas (e.g. expansion into new markets to reduce dependence on one market or customer); various relationship management techniques; and succession planning or retention strategies to retain talent.

### 5.2 Evaluating the Effectiveness of the Controls (Step 4)

A risk's residual rating largely depends on the risk mitigation measures, including the key controls that are in place and their effectiveness. The Board would generally expect the residual rating of most operational and financial risks to be at a low to medium level.

Management are responsible for confirming the effectiveness of the controls or risk management strategy on a monthly, quarterly or annual basis, depending on the type of control.

Depending on the control or risk management strategy, management may want to conduct testing to confirm it is operating as intended. This would be appropriate where they do not have visibility that it is completed or where they do not ensure on an ongoing basis that it is in place.

### 5.3 Identify Control Improvement Strategies (Step 6)

Often the residual risk is still deemed too high. For example where the controls, or risk management strategies, that are in place are only partially effective or are not sufficient to manage the risk. As a result management need to identify further action to improve the control environment. This further action involves the design and implementation of plans to ensure that the level of residual risk aligns to the Group's strategy and risk appetite.

## 6 Risk Reporting (Step 7)

Much like the risk evaluation procedures, risk reporting is an on-going cyclical process. The reports are produced by the CFO and are based on summarised discussions with the various risk owners and/or departmental heads.

Organisation-wide “top ten” risks are reported to the Audit and Risk Committee on a quarterly basis.

Each quarterly report requires management to certify to the Audit and Risk Committee that the Risk Management Framework continues to provide effective risk oversight and management of the entity’s material business risks.

## 7 Review of the Risk Management Framework

Led by the CFO, the ELT undertakes a comprehensive review of the Risk Management Framework annually, or when a material change to operations, risk appetite and/or external environment occurs.

This review ensures that the Risk Management Framework remains appropriate, effective and adequate with regards to Group’s size, business mix and complexity of the business operations. The scope of the review includes:

Whether the risk management framework remains appropriate for the business operations;

The specific resources utilised, at a minimum, to undertake risk management activities;

- The risk appetite statement;
- All risk management processes and procedures; and,
- Internal control systems and testing plans.

As per Recommendation 7.2 of the ASX Corporate Governance Principles, the Audit & Risk Committee reviews the Risk Management Framework at least annually to satisfy itself that it continues to be sound and discloses in relation to each reporting period, whether such a review has taken place.