Risk Management Guideline

[Selected Pages]

Version 5.0 (June 2015)

1 Objective

The Risk Management Guideline ("Guideline") outlines the processes used at Panoramic Resources Limited ("Panoramic") to identify and manage risk and opportunities.

It is recognised that implementation of this Guideline may require additional project specific training, procedures, plans, guidelines, forms, checklists and/or registers to ensure compliance with specific statutory, legal or other requirements.

It is expected that it will be the responsibility of Senior Management, under the direction and supervision of the Chief Financial Officer (CFO), to ensure that, where required, these additional documents are developed to meet and/or exceed the requirements stipulated in this Guideline.

2 Scope

This Guideline applies to all activities and processes undertaken at Panoramic and in which Panoramic has control and influence.

3 Responsibilities/Accountabilities

Role/Function	***Responsibilities/Accountabilities***
Board	• On a bi-annual basis, to review and approve the Guideline. • On a bi-annual basis, to review and approve the Panoramic Risk Management Policy (as signed by the MD) • On a bi-annual basis, to review and approve the Panoramic Risk Appetite Statements. • On a bi-annual basis, to review and approve the Qualitative Risk Matrix Definitions, Likelihood and Impact. • As required and if there are directors on the Board that are not members of the Committee, take advice and necessary action to relation to the findings of the Committee in relation to the review of significant risks across the Panoramic Group. • On an annual basis as required under ASX Listing Rules *Appendix 4G* and as pronounced in Recommendation 7.2 of the *Corporate Governance Council Principles and Recommendations,* to be satisfied that Panoramic's Risk Management Framework ("RMF") was (for the previous reporting period) and continues to operate on a sound basis.
Environment, Safety and Risk Committee("Committee"), noting that as at the date of this Guideline all directors are also members of the Committee)	• To supervise the operation of the Guideline, RMF and the Risk Management Policy ("RMP"). • On a bi-annual basis, to review the Guideline (including the RMP, Risk Appetite Statements and the *"Qualitative Risk Matrix Definitions, Likelihood and Impact"*) and to propose amendments as required to the Board. • On an annual basis, review the level of compliance of internal and external stakeholders to the RMP and to give the necessary assurance to the Board.

Job Title	Responsibilities/Accountabilities
Managing Director (MD)	• Together with senior management, to provide the necessary resources to enable the RMF and RMP to be applied and carried out across the Panoramic Group. • Together with the COO and CFO, on a regular basis, to identify, assess and review the significant risks (and opportunities) across the Panoramic Group and the steps taken and/or proposed to manage these risks/hazards using the appropriate risk matrix for impact, tolerance and opportunity. • To complete the Senior Management Risk Appetite Questionnaire every two years. • To provide to the Board on a semi-annual basis, Written Certification together with the CFO, certifying after obtaining adequate assurance from the CFO, that the Company's financial reports are based on a sound system of risk management and internal control and that the system is operating effectively (in accordance with *Section 295A of the Corporations Act 2001*).
Chief Financial Officer (CFO)	• To be ultimately responsible and accountable for the maintenance and update of the Guideline and for the presentation of the Guideline, every two years, for review and approval by the MD, the Committee and the Board. • On a regular basis, to identify, assess and review the significant strategic, financial and corporate/legal/governance risks and the steps/processes taken and/or proposed to manage/mitigate these risks using the appropriate risk matrix for impact and tolerance. • Together with the COO, on a bi-annual basis, to conduct and supervise the undertaking of risk assessments across the Panoramic Group in order to facilitate the storage of the risk assessments/profiles/hazards using the Bow-Tie ™ Software. • To complete the Senior Management Risk Appetite Questionnaire every two years. • To tabulate the results of the Senior Management Risk Appetite Questionnaire. • Using the results of the Senior Management Risk Appetite Questionnaire(s), review and amend if required the Panoramic Risk Appetite Statements and RMP for presentation to the MD, Committee and the Board. • On a bi-annual basis, to review the Qualitative Risk Matrix Definitions, Likelihood and Impact and to propose amendments as required to the MD, Committee and the Board. • To provide to the Board on a semi-annual basis, after a review on the effectiveness of the RMF and the level of compliance against the RMP, a Written Certification together with the MD, certifying that the Company's financial reports are based on a sound system of risk management and internal control and that

	the system is operating effectively (in accordance with *Section 295A of the Corporations Act 2001*).
Job Title	***Responsibilities/Accountabilities***
Chief Operating Officer (COO)	• To lead, manage and provide the necessary resources to enable the RMF and RMP to be applied and carried out at operational level. • On a regular basis, together with the Operations Managers, to identify, assess and review the significant operational risks/ hazards and the steps/processes taken and/or proposed to manage these risks/hazards using the appropriate risk matrix for impact, tolerance and opportunity. • Together with the CFO, on a bi-annual basis, to conduct and supervise the undertaking of risk assessments across the Panoramic Operations in order to facilitate the storage of the risk assessments/profiles/principal hazards using the Bow-Tie ™ Software. • To complete the Senior Management Risk Appetite Questionnaire every two years.
Other Senior Management (including Operation Managers)	• To manage the level of risk within their individual area(s) of authority and to coordinate RMF training and support. • As required, to report all new risks that have been determined to be unacceptable to the Operation Managers, COO, CFO and MD for assessment. • As required, to develop and manage plans, assessment procedures and other tools as detailed in *Section 8: Risk Management and Response* to reduce risks to an acceptable level as stipulated under the RMF. • As required, to monitor and assess associated risk profiles/principal hazards and to update or delegate the update using the Bow-Tie ™ Software. • As required and on at least an annual basis, conduct a risk and opportunity assessment against department/Operation Business Plans. • On a bi-annual basis, to conduct risk assessments under the direction and supervision of the CFO and COO and to review Department/Operations Risk/Hazard Registers and to make any changes to the risk profiles as required. • To conduct a documented annual review of core work processes within their department/function area/accountability to determine the level of compliance (*from zero to 100%)* using the agreed risk matrix score for impact, tolerance and opportunity against the applicable standard, statutory legislation and/or contract requirements. • On an annual basis, each Operation Manager, upon written advice from each of their Department Heads, to provide a *Project Risk Summary and Compliance Report* to the COO

	(copy CFO) outlining the level of compliance (*from zero to 100%*) of each department using the agreed Qualitative Risk Matrix Definition, Likelihood and Impact score against the applicable standard, statutory legislation, and/or contract requirements and of any corrective action(s) proposed, if required. • To complete the Senior Management Risk Appetite Questionnaire every two years.

Job Title	***Responsibilities/Accountabilities***
Risk Owner	• To be accountable for the application of the RMF and RMP in respect to a risk and opportunity associated with a task or activity.
Risk Work Team	• To participate in the risk assessment process in accordance with the RMF.
All Employees	• Ensure that the procedures, tools and resources of the RMF are applied and complied with in accordance with the RMP.

4 Guideline

4.1 Risk Management

Justice Owen in the 2003 HIH Royal Commission defined “Corporate Governance” as “the framework of rules, relationships, systems and processes within and which authority is exercised and controlled within corporations. It encompasses the mechanisms by which companies and those in control, are held to account”.

Risk and opportunity management contributes to good Corporate Governance by providing reasonable assurance to boards, managers and employees that the organisational objectives, strategy and goals will be achieved within a tolerable degree(s) of residual risk.

Risk and opportunity management is a comprehensive process, supported by appropriate strategies, frameworks and processes that are designed to identify, analyse, evaluate, treat, monitor and communicate those risks that could prevent a department, project or work group from achieving its objectives. It covers strategic as well as operational, economic and non-economic risks.

4.2 Risk Management Framework

In order to implement an integrated approach to risk management and ensure a high-quality and uniform risk management process, since 2011/12, Panoramic has had in place an enterprise-wide Risk Management Framework (“RMF”).

***Figure 1*: Panoramic RMF**

5 RMF Components

The Panoramic RMF consists of eleven interrelated Components that are grouped into three core stages, namely (1) Establishing Context; (2) Risk Identification analysis and evaluation and (3); Risk Response and Management. The RMF Components are:

- ***Risk Context and Risk Identification***
  - Internal Environment
  - Risk Culture
  - Risk and Opportunity Assessment
  - Risk Methodology
  - Assessment Tools
  - Risk Data (Repository)
  - Risk Analysis and Evaluation
- ***Risk Response and Risk Management***
  - Respond to Events
  - Report and Review
  - Manage Activities
  - Risk Recording
  - Communicate Risk

6 Risk Leadership

6.1 Internal Risk Environment

The internal risk environment of a Company influences the risk consciousness and culture of its people, and is the basis for the components of a RMF, providing discipline and structure.

The internal risk environment and philosophy of Panoramic are outlined within the following structures of the RMF:

- Risk Management Guideline;
- Risk Management Policy;
- Risk Appetite Statements;
- Senior Management Risk Appetite Questionnaire;
- MD and CFO Certification to the Board on risk and control compliance;
- Oversight by the Committee and Board and satisfaction that Panoramic's Risk Management Framework ("RMF") was (for the previous reporting period) and continues to operate on a sound basis;

- The integrity, ethical values, and competence of the Panoramic employees (under Panoramic's *Code of Conduct*); and
- The way management assigns authority, responsibility and organises and develops its people.

6.1.1 Risk Management Philosophy

Panoramic's risk management philosophy and culture is articulated through the Panoramic Risk Management Policy ("RMP") (*Attachment A*).

The Panoramic RMP shall be reviewed on a bi-annual basis by the Environment, Safety and Risk Committee ("Committee") and authorised by the Board. The RMP shall be reviewed on a bi-annual basis and amended if required.

The RMP shall be communicated to all employees via Panoramic's internal intranet, displayed in prominent areas throughout each site and shown on the Panoramic Web Site (www.panoramicresources.com.au).

6.1.2 Risk Appetite

Risk appetite can be broadly defined as "the amount of risk an organisation is willing to take in the pursuit of its goals".

Risk appetite is a key component of the RMF as it sets the boundaries within which management and employees are expected to operate in order to deliver strategic and operational objectives.

A clearly understood and clearly articulated statement(s) of risk appetite can assist in unlocking value by better aligning decision-making and risk taking between the Board and management.

An organisation's risk appetite is at the heart of how it goes about its business and represents to all stakeholders how it wishes to be perceived internally and externally.

Panoramic's risk appetite is detailed in the Board approved *Panoramic Resources Risk Appetite Statements (Attachment C)*.

The Senior Management of Panoramic complete, on a bi-annual basis, a *Senior Management Risk Appetite Questionnaire (Attachment B)*, which involves each executive answering questions on various types of organisational risks the Company faces.

The Company's Risk Appetite Statements are reviewed and amended if required after consideration of the questionnaire results by the CFO and a draft set of statements are presented for review, discussion and approval by the Committee and / or the Board [*noting that all directors of the Panoramic Board are currently also members of the Committee and as such the review and approval process can be done simultaneously at the one meeting of directors*].

Panoramic's risk appetite is further defined within the *"Qualitative Risk Matrix and Definitions of Likelihood and Impact" (Attachment D*). To calculate the level of risk, Panoramic has established a *Risk (Opportunity) Appetite Hierarchy* associated with the Risk Appetite Statements.

6.1.3 Risk Tolerances

Risk tolerance is the tolerable deviation from the level set by the Company's risk appetite and business objectives.

Panoramic promotes agility and innovation to exploit new business opportunities, while focusing on adequately managing unacceptable risks as required.

For example, the Executive General Manager–Business Development and General Manager Exploration shall include a risk component in every new initiative/project, so that Senior Management and the Board can have the discretion to pursue new opportunities up to the agreed level of risk appetite.

From the results of the latest *Senior Management Risk Appetite Questionnaire,* Panoramic generally has a zero risk tolerance when complying with situations that require specific legal, regulatory or industry requirements.

On an annual basis, each Operation Manager shall, upon written advice from each Department Head, provide a *Project Risk Summary and Compliance Report* to the COO (copy CFO) outlining the level of compliance (*from zero to 100%*) of each department using the appropriate "*Qualitative Risk Matrix Definition, Likelihood and Impact"* and against any applicable external or internal standard, statutory legislation, and/or contract requirements and of any monitoring and/or corrective action(s) proposed, if required. Corrective action plans shall be developed for any identified non-compliances and non-conformances.

At the operational level, exceptions can be tolerated (or different thresholds defined) so long as at that level, the overall exposure does not exceed the set risk appetite.

Panoramic recognises that there may be circumstances where the cost/business impact of risk mitigation options exceeds Panoramic's capabilities/resources, thereby leading to higher tolerance levels in these particular risk conditions.

Where possible, when the cost/business impact of risk mitigation can be identified with a high degree of certainty, those circumstances where risk conditions exceed defined risk tolerance levels shall be reviewed and authorised by the Committee and or Board prior to proceeding with the risk mitigation option(s).

In those circumstances where the level of risk exceeds Panoramic's tolerance levels, but the 'opportunity versus risk' ratio significantly favours value accretion, the Board decision to proceed shall be minuted in the Board meeting minutes, including the justifications for proceeding.

Risk tolerance levels shall be defined for events, activities and tasks using Panoramic's "*Qualitative Risk Matrix Definition, Likelihood and Impact" (Attachment D)*. Risk Tolerances Indicators shall be identified and regularly monitored and reported on by each Risk Owner.

6.1.4 Board Annual Effectiveness Review of the RMF and MD and CFO Written Certification

Recommendation 7 ("Recognise and Manage Risk") of the Australian Stock Exchange (ASX) Corporate Governance Council's July 2014 *"Corporate Governance Principles and Recommendations (Third Edition)"* states that a listed entity should establish a sound risk management framework and periodically review the effectiveness of that framework. ***Recommendation 7.2* requires the Committee or Board to review the RMF at least annually "to satisfy itself that it (the RMF) continues to be sound**. Moreover, listed entities are to include in the annual *Corporate Governance Statement* a statement on whether, in relation to each reporting period, whether such a review has taken place in addition to disclosing the extent to which the listed entity has followed the other Principle 7 recommendations on having in place a risk management framework in identifying risks and the appropriate risk management internal controls, systems and response procedures to mitigate their impact on strategic, operational and financial performance.

Included in Principle 7 and in accordance with *Section 295A* of the *Corporations Act, 2001,* **the MD and the CFO are also required to provide to the Board, on least an annual basis, a Written Certification certifying that the Company's financial reports are based on a sound system of risk management and internal control and that the system is operating effectively**.

6.1.5 Oversight by the Panoramic Board

In order to achieve an opinion on the effectiveness of the Panoramic RMF, the Board shall:

- **Understand, review and authorise the Panoramic RMP, the Panoramic Resources Risk Appetite Statements and the Panoramic Risk Management Guideline;**
- **Periodically challenge Senior Management to demonstrate the effectiveness of risk processes in identifying, assessing and managing Panoramic's most significant enterprise-wide risk exposures;**
- **Annually review Panoramic's risk exposures and consider the current risk exposures against the approved Risk Appetite Statements; and**
- **Request regular updates by Senior Management of key risk indicators of the key risk exposures as contained in a *Risk Summary Report* and a *Project Risk Summary and Compliance Report* discussed in section 8.3.**

6.1.6 The Panoramic Code of Conduct

The effectiveness of risk management is a function of the integrity and ethical values of those who create, lead, administer and monitor organisational activities.

Integrity and ethical values are essential elements of Panoramic's internal risk environment, affecting the design, administration and monitoring of the RMF.

In order to support a strong foundation of integrity and ethics, Panoramic has developed and implemented a formal *Code of Conduct*, which addresses integrity, ethics, acceptable behaviours and conflicts of interest inside and outside the work place.

6.2 Risk Culture

A strong *Risk Culture* characteristically offers a setting in which the components of risk are discussed openly, and acceptable levels of risk are understood and maintained.

Risk Culture consists of three core components, which drive behaviours within an organisation.. These components include:

- *Behaviour towards taking risk* – How much risk does Panoramic feel it can absorb and which risks is it willing to take?
- *Behaviour towards following policy* – An element of Risk Culture is the extent to which people will, or will not embrace and/or comply with a policy.
- *Behaviour towards negative outcomes* – How does Panoramic deal with expected or unexpected adverse outcomes. For example, material loss events and missed value accretive opportunities.

A strong *Risk Culture* begins at the top, with the Board and Senior Management who together set the direction backed-up with policy, communicate on processes under the RMF, acknowledge and if appropriate, reward effective risk management behaviours.

In order to promote a strong *Risk Culture*, Panoramic shall promote the importance of a culture of collaboration throughout the Company to foster a climate of mutual trust in which personnel adopt a team approach to solving problems and to preventing the recurrence of serious incidents.

To foster its inherent *Risk Culture*, Panoramic shall implement processes to appropriately investigate material loss events and missed value accretive opportunities, identifying the major causes and recording potential learning(s) from these incidents.

7 Risk and Opportunity Assessment

Risk and opportunity assessment allows the Company to consider the extent to which potential events have an impact on the achievement of its organisational objectives.

Risk and opportunity assessment shall be conducted in *Four Key Business Areas*:

1. *Planning* - Risk assessments on strategic and operational objectives.
2. *Processes* - Risk assessment on core work activities and tasks.
3. *New Projects / Initiatives / Suppliers* - Risk and opportunity assessments on new ventures, implementation of major projects and the use of new contractors or suppliers.
4. *Ongoing Operations* - Risk assessments conducted on work areas.

Panoramic uses numerous methods and tools to conduct risk assessments in either of the *Four Key Business Areas*. Specific Risk assessments tools include, but a not limited to, Job Hazard Analysis (JHA), "Take 5"/"SHEDs", Prestart Checks / Inspections, Planned Task Observation, Hazard Reports and "Hazid" Workshops/ Planned Safety Action Planning and post incident audits.

In consultation and guidance from the COO, each Operation Manager shall provide sufficient and appropriate resources to implement the use of risk assessment methods and tools across all departments.

Risk assessments, as the need arises, shall be undertaken individually (Risk Owner) or as a group (Risk Work Team) and are owned by the applicable authority or manager.

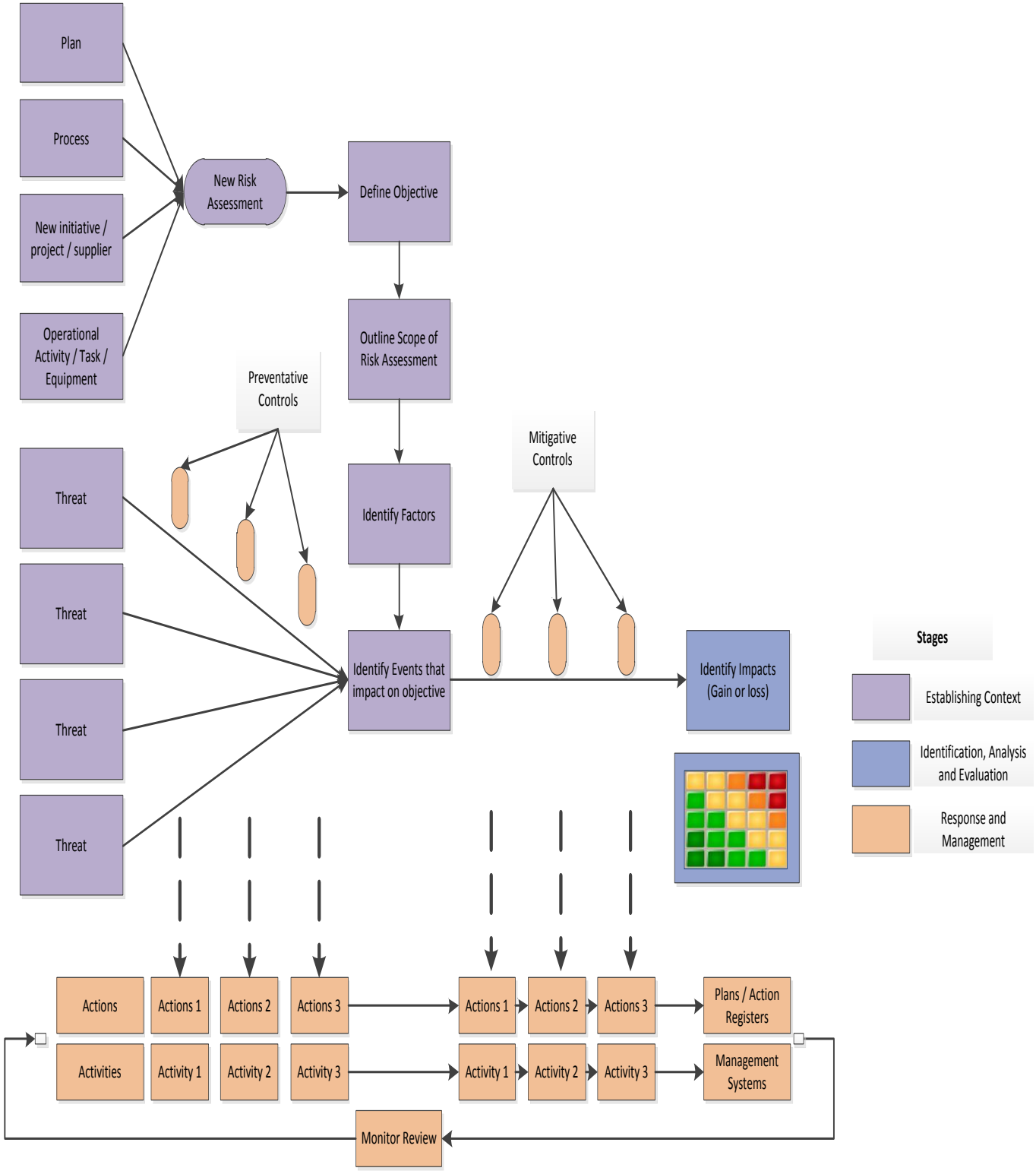
7.1 Risk Assessment Methodology

Panoramic's Risk Assessment Methodology conforms to *AS/NZS ISO 31000:2009 Risk Management - Principles and guidelines* and the *COSO Model*. It consists of *3 core stages:*

1. Establishing context
2. Risk identification, analysis and evaluation
3. Risk response and management.

The individual steps and the relationships between each stage are shown in Figure 2.

***Figure 2*: Panoramic Resources Risk Methodology Stages**



7.2 Establishing Context

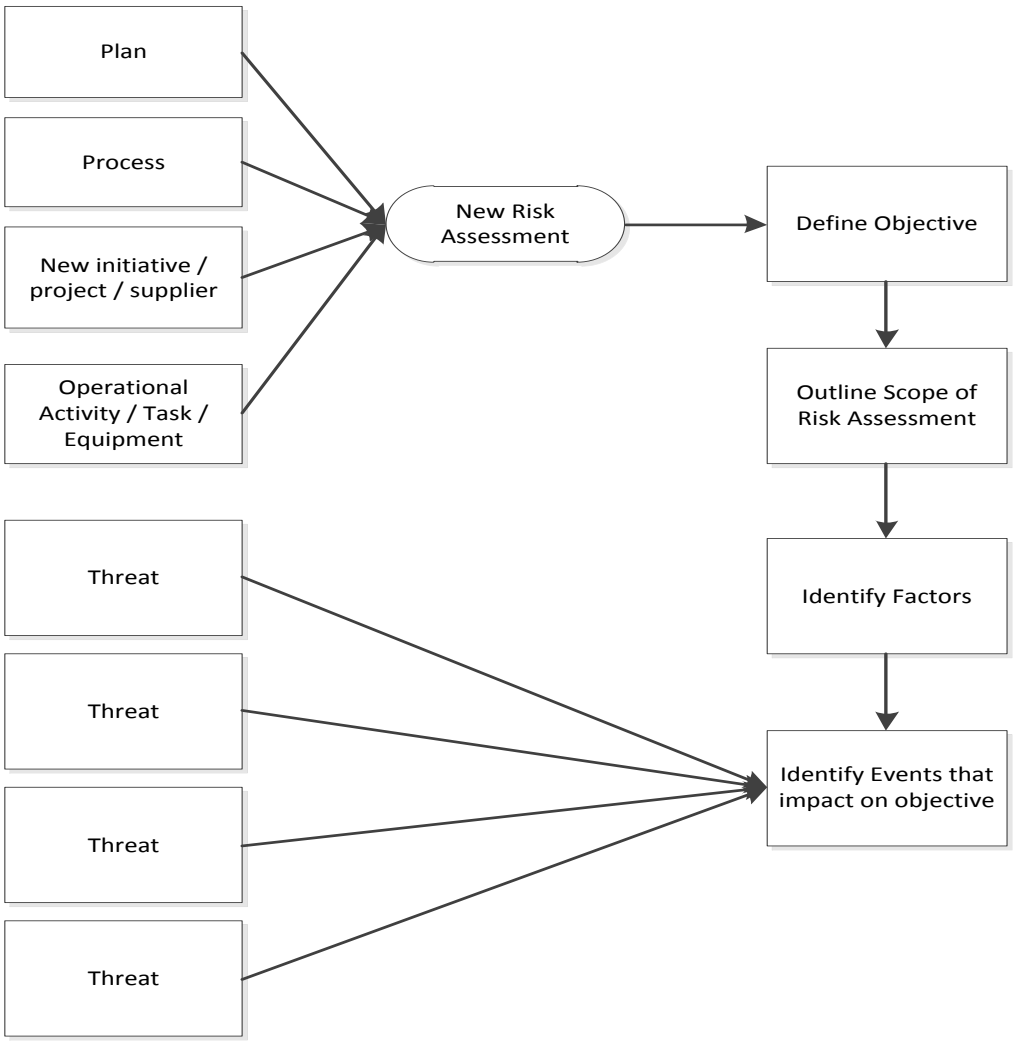


***Figure 3*: Establishing Context Steps**.

By establishing the context or the environment in which an organisation seeks to achieve its objectives, an organisation can articulate the objective and identify potential events to be taken into account when assessing a specific risk or threat.

The context of the risk management process will vary according to the type of risk assessment and the needs of the Risk Owner.

When establishing a context of the risk assessment process, the Risk Owner shall consider, but not be limited to, the following:

- Defining the specific objectives to be risk assessed;
- Defining accountabilities/responsibilities for and within the risk management process;
- Defining scope, as well as the depth and breadth of the risk assessment activities to be carried out, including specific inclusions and exclusions;

- Defining process, project, event, activity, task, function or asset in terms of time and location;
- Defining the relationship between a particular process, project, event, activity, task and other processes, projects, events, activities or tasks;
- Defining the risk assessment methodology and tool to be utilised; and
- Identifying and specifying the decisions that are required to be made.

The Risk Context information shall be recorded by the Risk Owner within the chosen Risk Assessment Methodology.

7.2.1 Event Identification

An event is defined as an incident or occurrence from internal or external factors or drivers that affect objectives. Events can have a negative impact, a positive impact, or both. Events with negative impacts represent risks while events with positive impacts may offset negative impacts and or present opportunities.

Events are identified firstly from identifying internal and external factors. A myriad of external and internal factors drive events that affect objectives.

External factors that should be considered when identifying events, along with examples and implications are described in Table 3.

***Table 3*: Examples of External Factors and Events**

External Factor	***Events – Example***
Economic	Events include commodity, currency and interest rate price movements, capital availability (equity and debt), the barriers to competitive entry.
Natural Environment	Events include flood, fire, or earthquake that result in damage to plant or buildings, restricted access to raw materials, or loss of human capital.
Political / Legal	Events include the election of a new government with different political agendas, new laws, taxes and a changing regulatory landscape.
Social	Events include changing demographics, social morals, family structures, and work/life priorities, terrorism activity that result in a change in the supply and demand of goods and services.
Technological	Events include new electronic methods for facilitating commerce that result in expanded availability of data, reductions in hardware and software costs, and increased levels of demand for technology-based services

Events are also influenced by internal factors as an organisation's capability and capacity reflect previous choices, influence future events and drive management decisions.

Internal factors, along with examples of related events and their implications are described in Table 4.

***Table 4*: Examples of Internal Factors and Events**

Internal Factor	***Events – Example***
Infrastructure, Plant and Equipment	Events include increased capital cost, unscheduled maintenance, equipment availability / downtime and increased operating costs.
Personnel	Events include personnel and or skills shortage, workplace accidents, fraudulent activities, expiry of employee agreements, strike or union action (if applicable).
Materials	Events include a supplier going into administration/receivorship, shortage of critical spares, significant price increases.
Process	Events include process modification without adequate change management protocols, process execution errors, lost time, waste.
Information Technology	Events include volume volatility, system downtime, and security breaches.
Work Environment	Events include excessive heat, cyclones activity, floods etc.

The identification of external and internal factors or drivers that influence events is required in order to choose the appropriate risk management method. Once the major contributing factors have been identified, the Risk Owner is able to consider their significance and focus on those events that can affect the achievement of goals and objectives.

A Risk Owner shall select the best method to fit the event and the need, size and scope of the risk assessment exercise and to ensure that the involved personnel have the applicable Event Identification capabilities and the supporting tools in place before commencing Event Identification.

1.1.1 Event Identification Methods

Event Identification methods and tools consider both past and future events.

Event Identification methods and tools vary in terms of where they are used. Some tools focus on detailed data analysis and create a “bottom-up” view of events, while other methods have a “top-down” focus.

The key types of Event Identification methods and tools used in the Company are described in Table 5.

***Table 5*: Panoramic Resources’ Event Identification Methods and Tools**

Method/Tool	***Description***
Risk Workshops and Interviews (HAZID)	These methods identify events by drawing the on accumulated knowledge and the experience of the Risk Work Team members and other internal and external stakeholders through structured discussions.
Process Analysis & Business Impact Analysis	This method analyses the inputs, tasks, responsibilities and outputs that form a process. By reviewing the internal and external factors that affect the elements within a process, events can be identified that could affect outcomes and objectives.
Leading Event Indicators	By monitoring output data correlated to events, the Risk Owner can identify the existence of conditions that could give rise to an event.
Loss event data registers(Incident Analysis)	The collection and storage of historical data on loss events in registers are a useful source of information for identifying similar trends and causes. Once a cause(s) of an incident has been identified and retained, the Risk Owner is able to recall the learning from previous incidents to more effectively assess and treat a new event.
Event Inventories (Risk Registers)	These are detailed registers of potential events common within a particular project or department, or to a particular process or activity common across the Company.
Internal Analysis	This may be done as part of a routine business planning cycle process, typically via regular scheduled meetings. If applicable, internal analysis can utilise information from other stakeholders (customers, suppliers, other departments) or from external advice.
Escalation and Threshold Triggers	These triggers alert the Risk Owner to potential hazards or events with predefined criteria and or thresholds. Once triggered, an event may require further assessment or an immediate response.

1.1.2 Interdependencies

Historically, one event can trigger another, and events can occur concurrently.

In Event Identification, a Risk Owner shall assess the relationships between other events and risks to determine if events relate to each other and what Components of Risk Management are best suited in that instance.

Overall, Event Identification needs to be robust, as it forms the basis for the Risk Assessment and Risk Response Components.

1.1.3 Threats (Causes) Identification

Events may be caused by any number of threats. In order to implement specific risk mitigation controls, a Risk Owner is required to identify specific threats (causes) of that particular event.

Threat (Cause) Identification provides the Risk Owner with a greater understanding of the likelihood of the event occurring again and the likely impact. Threats also provide the basis for identifying applicable preventative and mitigating controls.

The Risk Owner shall endeavour to identify the number of related events and the associated threats (causes) as is reasonably possible.

7.3 Risk Analysis and Evaluation

Risk Analysis and Evaluation involves developing an understanding of the level of risk, the quantity of the risk (or opportunity) and what controls can be used to mitigate and lower the threat or risk (residual risk). Risk Analysis enables decisions to be made on whether risks need to be treated or controlled, and the most appropriate Risk Management methods and tools to be used.

Risk analysis and evaluation also provides inputs into the different types and levels of risk.

The process and steps to undertake risk analysis and evaluation are outlined in Figure 2.

1.1.4 Distinguishing Between Risks and Opportunities

Events have either a negative and positive impact, or both. Events with a negative impact represent risks which require the Risk Owner’s assessment, response and treatment.

Events that have a positive impact represent opportunities to channel back positive learning into business plans (goals and objectives).

Events shall be analysed and evaluated for both risks and opportunities.

1.1.5 Qualitative Risk Analysis

Panoramic uses qualitative risk analysis to view the potential likelihood and consequence of future events. The qualitative risk analysis methodology used is the *Panoramic Resources Qualitative Risk Matrix and Definitions of Likelihood and Impact* (*Attachment D*).

The likelihood and impact of each identified risk in an activity or task shall be assessed using this methodology and each risk shall be classified and prioritised using the Board approved risk acceptance threshold levels.

Inherent Risk is the level of risk assuming that no risk management mitigation controls are in place. Residual Risk is the level of risk assuming that identified risk management mitigation controls are in place and are effective**. A Risk Owner shall determine both Inherent Risk and Residual Risk when conducting a Risk Assessment of an activity or task.**

The impacts / consequences identified during the Risk Assessment process are classified as being either Economic or Non-economic.

Economic consequences shall be scaled when determining the level of risk acceptance according to sensitivity.

All Risk Owners when undertaking a Risk Assessment of an activity or task within one of the *Four Key Business Areas* shall consider, as a minimum, the following three types of economic risk/opportunity:

- *Production* - What could disrupt the delivery of products?
- *Quality* – What could impact on the quality of products?
- *Loss or Damage* – What could cause financial loss or damage?

Non-economic consequences are more difficult to scale. All Risk Owners when undertaking a Risk Assessment of an activity or task within one of the *Four Key Business Areas* shall consider the following three types of Non-economic consequences:

- *Health, Safety, Environment and Community* – What could harm people, the environment or the local community in conducting this activity?
- *Legal* – What could cause an enforcement/prohibition notice or prosecution in conducting this activity?
- *Reputation* – What could cause a loss of reputation in relation to conducting this activity?

1.1.6 Risk Evaluation

Risk Evaluation shall be undertaken by a Risk Owner with the relevant experience and expertise and will have, as a minimum, a very good understanding of the activity or task being analysed in the *Key Business Area*. The Risk Owner shall be able to judge the likelihood and impact on the business and operational context, but if considered necessary, the views of relevant internal and external experts shall be obtained to assist in the evaluation of particular risks.

Special attention shall be given to any risks assessed as having a very high negative consequence and/ or a very low likelihood of occurring. These are *Major Risks* in which the Economic or Non-economic consequences can include one or multiple fatalities, major plant or mine / project failure resulting in a severe business interruption event.

Consideration shall also be given to aggregation of risks arising from a number of interrelated causes. Where such risks are identified, they shall immediately be noted in the applicable *Risk Register* as *Special Cases* and each risk shall have sufficient controls to mitigate the likelihood and impact to an acceptable *Risk Residual Level*.

The results of a Risk Evaluation shall be recorded in the applicable Risk Registers, Plans and Reports.

Panoramic has established *Four Residual Risk Levels*. These Include:

- *Critical* - Risks that significantly exceed the risk acceptance threshold and need urgent and immediate attention. These risks are to be reported to the Operations Manager and or the COO, CFO and MD.
- *High* - Risks that exceed the risk acceptance threshold and require proactive Risk Management. Includes those risks for which proactive actions have been taken, but further risk reduction is impossible or impracticable. However, active monitoring is required and the latter requires the sign-off from Operational Managers or Department Heads.
- *Moderate* - Risks that lie on the risk acceptance threshold and require active monitoring. The implementation of additional measures could be used to mitigate and control the risk further.
- *Low* - Risks that are below the risk acceptance threshold and do not require active risk management. Certain risks could in time require active monitoring.

A Risk Owner shall allocate a *Residual Risk Level* to the risk relating to each event, activity or task. Where risks are determined to be *Critical* or *High*, which is unacceptable, the Risk Owner shall identify, record and report the risk(s) to the appropriate Authority Level in order for action to be initiated, such as immediately stopping the event, activity or task, or introducing mitigation controls (if available).

8 Risk Management and Response

Within the RMF and as a matter of course, Panoramic shall manage risk in the following ways:

1. Risks with negative consequences / impacts shall be avoided, transferred or minimised.
2. Risks with positive consequences / impacts shall be exploited, shared or enhanced as an opportunity.
3. In those cases where active risk responses are not possible, *Residual Risks* must be reduced to an acceptable risk threshold level after approval from the required Authority Level.

8.1 Risk Treatments / Controls

Risk Treatments / Controls are any process, policy, device, practice or other measure that is intended to minimise risk. Risk treatments / controls are the key to Risk Management as they reduce or eliminate the level of risk the event will face in the achievement of the identified business objective. Treatment and or Controls and their associated actions are shown in Figure 2.

Panoramic uses *Two Types of Risk Treatments / Controls*, namely (1) Preventative controls; and (2); Mitigation controls. Preventative controls reduce the level of risk by preventing the event from occurring and thereby reducing the "likelihood" of the event. Mitigation controls are used to reduce the level of risk by reducing the "consequence/impact" of the event. Mitigation controls include but are not limited to fire extinguishers, seatbelts, insurance, legal advice, and hedging derivatives.

Risk treatments / controls are graded in accordance with their effectiveness in controlling the risk. Panoramic uses a hierarchy of treatments / controls. These include:

- *Elimination* – Complete removal of the Factor / Hazard.
- *Substitution* – Replacement with a more effective control alternative.
- *Engineering Controls* – Isolation, Segregation, Containment or Limitation. All these controls involve physical separation.
- *Administration Controls* – Establishing appropriate policies and guidelines to control exposure to events.
- Personal Protective Equipment (PPE).

Risk treatment involves identifying the range of options for treating risks, assessing those options, preparing risk treatment plans and implementing these plans as soon as practical. Risk treatment shall always consider the effectiveness hierarchy of controls and to optimise the level of risk exposure to "as low as is reasonably practicable" ("the ALARP Principle").

When significant risks have been determined and prioritised, risk treatment / controls identification shall be undertaken to determine what control measures are required and what actions are to be taken to eliminate or minimise the consequence/impact.

As a minimum, a Risk Owner shall ensure that the appropriate action to reduce the identified risk to an acceptable level for those activities and processes that have or may have significant consequence/impact is undertaken as soon as practical.

Project, process or other work activities shall not commence until appropriate treatments / controls have been implemented, monitored and deemed effective by the relevant Authority Level.

8.2 Risk Assessment and Analysis Recording

Where applicable, all Risk Analysis information on future planned projects shall be entered into each Project/Business Plan.

All risk assessment and risk analysis information shall be entered into the appropriate department/function Risk Register using the BowTie™ Software Risk Assessment Database. Information shall include identified risks with their evaluations and agreed treatment/controls.

As required, other risk reporting formats may be developed for specific purposes.

8.3 Risk Analysis Updates and Compliance Reporting

A new Risk Analysis shall be conducted on an existing risk if the circumstances have changed or there have been new developments. The update shall reflect the results of Risk Responses that have been previously implemented, and they must identify and record additional risks that have emerged since the last update.

On an annual basis, each Department Head/Function Manager shall review their department/function Risk Registers print-out taken from the Bow-Tie™ Software Risk Assessment Database. All risks shall be reviewed to determine the level of compliance (*from zero to 100%)* using the agreed risk matrix score for impact, tolerance and opportunity against the applicable standard, statutory legislation and/or contract requirements thereby ensuring that either (1) a risk(s) has not developed a higher risk profile, or (2) outlining monitoring and corrective measures to reduce the risk(s) to an acceptable level.

A *Risk Summary Report* detailing on the significant risks and status and the level of compliance (*from zero to 100%*) for their department/function against the RMF and RMP shall be developed and maintained by each Department Head/Function Manager and shall be provided on an annual basis to their Operation Manager/Next Authority Level.

On an annual basis, each Operation Manager shall complete and provide a *Project Risk Summary and Compliance Report* to the COO (copy CFO) for review.

The CFO shall provide to the Board on a semi-annual basis in February and August, after reviewing the effectiveness of the RMF and the level of monitoring/compliance against the RMP with Senior Management, a Written Certification (together with the

MD after giving reasonable assurance to the MD), certifying that the Company's financial reports are based on a sound system of risk management and internal control and that the system is operating effectively (in accordance with *Section 295A of the Corporations Act 2001*).

8.4 Risk Assessment and Analysis Software

Panoramic has chosen to use the BowTie™ Software Risk Assessment Database to analyse and record risk assessments on identified events, activities and tasks within the *Four Key Business Areas* for each department/function across the organisation.

8.5 Training and Awareness

Risk Management Awareness and Training Programs will be identified, developed and implemented where appropriate and when time permits as outlined in Table 6.

***Table 6*: Panoramic Resources Risk Training Requirements**

Training Program	***Area***	***Proposed Attendees***
Board Risk Awareness	Board	Directors/CFO/COO
Management Risk Awareness	Corporate, Operations, Projects	Senior Management/Department Heads/Function Managers
Risk Management Framework/ RMF Guideline	Corporate, Operations, Projects	Managers, Supervisors, OHS And Environmental Officers
Risk Management Awareness RMF/RMP Induction	Corporate, Operations, Projects	All employees
BowTie™ Software	Corporate, Operations	As required
Data Recovery (DR) and Business Continuity (BC) Workshops	Corporate, Operations	As required
JHA	Operations, Projects	All personnel
Take 5	Operations, Projects	All Personnel
SHEDs	Operations, Projects	All Personnel

Definitions and Abbreviations

- Definitions

Term	Definition
ALARP ("As low as reasonably practicable")	Risk that is tolerable on the basis that the risk is acceptably low and cannot be further reduced effectively considering the cost, time and resources involved.
Aspect	An element of an organisation's activities, products or services that can interact with the environment. For environmental risk purposes, "aspect" is a synonym for "hazard".
Consequence	The impact of an event expressed qualitatively or quantitatively, being a loss, harm, disadvantage or gain.
Communication and Consultation	Continual and iterative processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders.
Control	Any process, policy, device, practice or other measure that is intended to minimise risk.
Event	An event is defined as an incident or occurrence from internal or external sources that affects achievement of objectives.
External Context	External environment in which the organisation seeks to achieve its objectives.
Hazard	A source of potential harm or a situation with the potential to cause actual or perceived loss or damage to people, the environment, plant, equipment, customer expectation or product quality.
Hazard Identification	The process of identifying threats (risks with a negative consequence) or enhancement measures for opportunities (risk with potential positive consequences).
Impact	The harm that has or could occur if the controls are absent or fail.

Term	Definition
Internal Context	Internal environment in which an organisation seeks to achieve its objectives
Inherent Risk	The risk remaining if proposed that no controls are put in place / implemented.
Likelihood	The most realistic or credible chance that a particular event will occur, resulting in the 'maximum reasonable consequence', expressed as a qualitative or quantitative description of probability or frequency.
Maximum Reasonable Consequence (MRC)	The largest realistic or credible consequence from an event, considering the location of and population encountering the event as well as the credible failure of current controls.
Monitoring	Continually checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.
Maximum Reasonable Outcome (MRO)	The outcome for an incident or risk, based on its maximum potential consequence and the likelihood of that consequence occurring after applying the *Panoramic Resources Qualitative Risk Matrix and Definitions of Likelihood and Impact*. The Maximum Reasonable Outcome is classified as Low, Moderate, High or Critical.
Opportunity	Opportunity is the possibility that an event will occur and positively affect the achievement of objectives.
Predicted Risk	The predicted risk remaining if proposed controls are implemented.
Qualitative Risk Assessment	Qualitative assessments assess the maximum reasonable consequence of a hazard / aspect or opportunity against its expected likelihood using predefined consequence and likelihood descriptors in the *Panoramic Resources Qualitative Risk Matrix and Definitions of Likelihood and Impact*.
Residual Risk	Risk remaining after risk treatment(s) has been implemented. If controls are implemented, it reflects current risk. If controls have not yet been implemented, it reflects predicted risk levels.

Term	Definition
Risk	An uncertain event or condition that if it occurs will affect the achievement of one or more objectives. It is measured in terms of the likelihood of occurrence and its potential consequences, and assigned an overall risk classification.
Risk Appetite	An organisation's approach to assess and eventually pursue, retain or turn away from risk.
Risk Acceptance Threshold	A measure (or criteria) of the level of risk above which proactive actions must be taken to manage threats and maximise opportunities and below which risks may be accepted.
Risk Analysis	The overall process of risk identification and risk assessment.
Risk Assessment	The method of evaluating the consequence and likelihood of identified hazards, aspects or opportunities and comparing these against a defined risk acceptance threshold relevant to the level of assessment.
Risk Capacity	The overall maximum level of risk that Panoramic Resources can bear and the types of risk Panoramic Resources desires or is prepared to accept in order to achieve its strategic, operational and financial objectives in both the short and long term.
Risk Management	The process of making informed decisions and implementing appropriate actions, based on a hierarchy of controls, in response to risk analysis results.
Risk Management Framework (RMF)	The set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk Owner	Person accountable for the overall management of a hazard and contributing risk scenarios within the work area. This person is also accountable for ensuring controls are in place and effective and that the risks are reviewed appropriately.
Risk Profile	Description of any set of risks.

Term	Definition
Risk Management Policy (RMP)	Statement of the overall intentions and direction of an organisation related to risk management.
Risk Treatment	Process to modify risk
Risk Tolerance	The quantum or degree of risk that the Company is prepared to accept for each category of risk (operating within its overall risk capacity), where possible expressed in terms of the degree of confidence required so that specific objectives will not be compromised or the tolerance threshold will not be breached.
Risk Rating	The classification of risk based on its likelihood of occurrence and potential consequence(s). Risks undergoing Level 2 assessments are rated in the descriptive terms: Critical, High, Moderate and Low.
Risk Scenario	A description of how the hazard / aspect could potentially result in an impact.
Significant Risk	Risks with a risk rating of *Critical* or *High*.
Stakeholder	Person or organisation that can affect, be affected by, or perceives themselves to be affected by a decision or activity.
Standard Operating Procedure (SOP)	A procedure written at the task level, clearly describing the sequential steps that result in the best known way to complete a task. It does not contain complex decision making.
Work Area	Part of a hierarchical structure that represents the physical location where work is conducted. The hierarchy breaks sites down further, into logical physical sections.