Royal Australasian College
of Dental Surgeons

Let knowledge conquer disease

RISK MANAGEMENT FRAMEWORK

October 2018

Table of Contents

1. PURPOSE

The purpose of the RACDS Risk Management Framework is to provide a robust and effective implementation of risk management as a crucial part of the College's operating practices at a corporate, strategic, and operational as well as a means of improving organisational activities. The Risk Management Framework has been developed based on the elements as presented in the Risk Management Standard ISO 31000:2009.

2. SCOPE

The Risk Management Framework defines the organisational processes and structure for managing risk to assist with the achievement of strategic objectives, operational objectives, and contribute to the College's sustainable growth and continued development. The Risk Management Framework is applicable to all Council members, 'office holders', examiners, lecturers and all employees of the College.

3. FRAMEWORK STATEMENT

The College is committed to the ongoing development of a consistent approach to risk management, underpinned by a risk-aware and responsive culture.

Every employee, Councillor and office bearer in the College has a role in managing risk by exploring and enhancing opportunities and minimising threats. Risk management contributes to good corporate and operational governance by providing assurance to the Council that College objectives will be achieved within an acceptable degree of residual risk, recognising that effective risk management is about ensuring strategically balanced and defensible decision making processes.

4. IMPLEMENTATION

4.1 Policy Setting

The College has a range of high level documents associated with risk. Within the organisation all policies in respect of risk are approved by Council whilst Procedures in respect of risk are approved at the operational level.

4.2 Risk Management Principles

The effective management of risk is vital to the continued development and success of the College. Risk management must be embedded in the College culture to assist the College in making well informed decisions. For risk management to be effective, all College operations must adhere to the following principles:

4.2.1 Understand the nature of the risks that the College faces

4.2.2 Ensure that risk management is integrated into all College processes;

4.2.3 Focus on the sources of uncertainty that impact on the achievement of College activities and objectives;

4.2.4 Explicitly address uncertainty and how such occurrences can be managed.

4.2.5   Provide a systematic, structured and timely approach in assessing risk whilst providing a mechanism to reliably document current or potential risks to compare with past results.

4.2.6   Use best current available information from a wide range of sources.

4.3   Risk Management Framework

The RACDS Risk Management Framework has been adapted from the Australian and New Zealand Standard ISO 31000-2009. The following components of risk management, identified in the diagram below, work together to help achieve the best outcomes for the College. These components set the structure of the risk management framework for the College. The framework includes the Risk Management Policy, other College policies, procedures, tools, templates, and reports which will be continually developed and implemented as appropriate for different levels within the College.
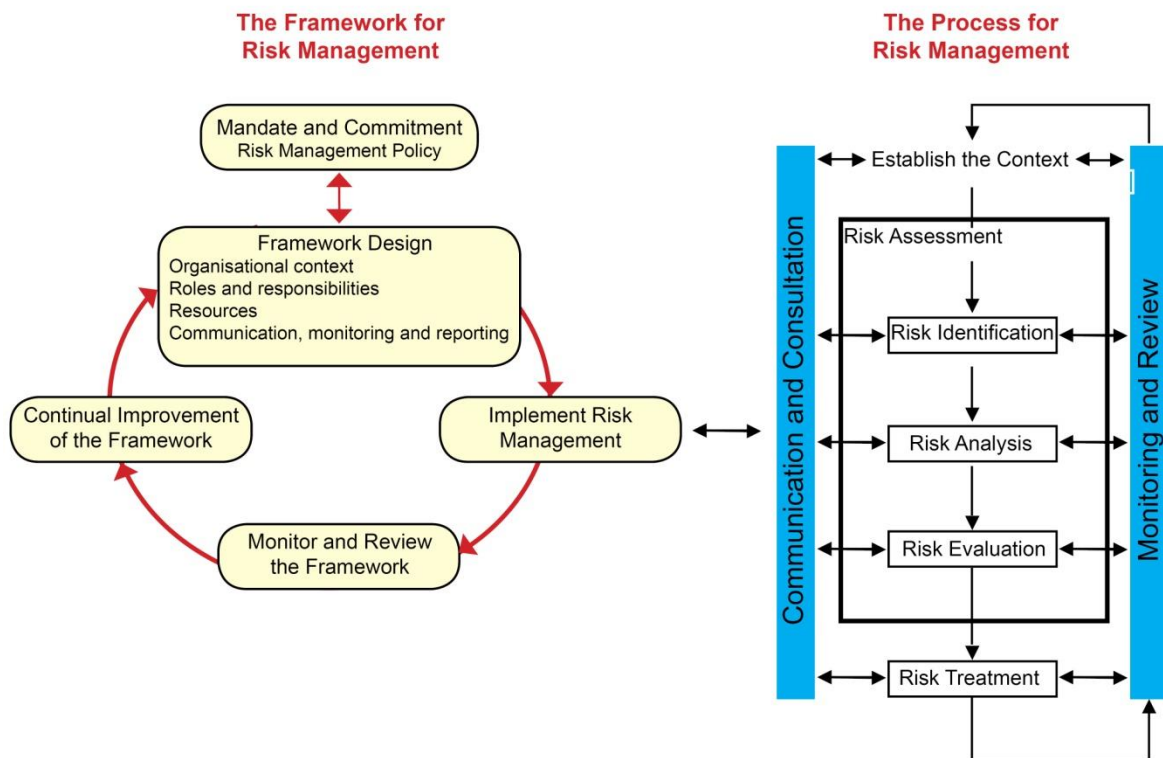
The Risk Management Framework is a set of components that provides the arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the College.

4.4   Risk Management Processes

The risk management process is an integral part of RACDS management philosophy. It is embedded in College culture and practices; and tailored to suit the specific needs of the College. The process is in accordance with the Australian New Zealand Standard ISO 31000-2009.   The diagram below presents a summary of the risk management process which includes activities of communications and consulting;

establishing internal and external contexts, identifying, analysing and evaluating risks; formulating plans; and monitoring, reviewing and reporting risks.
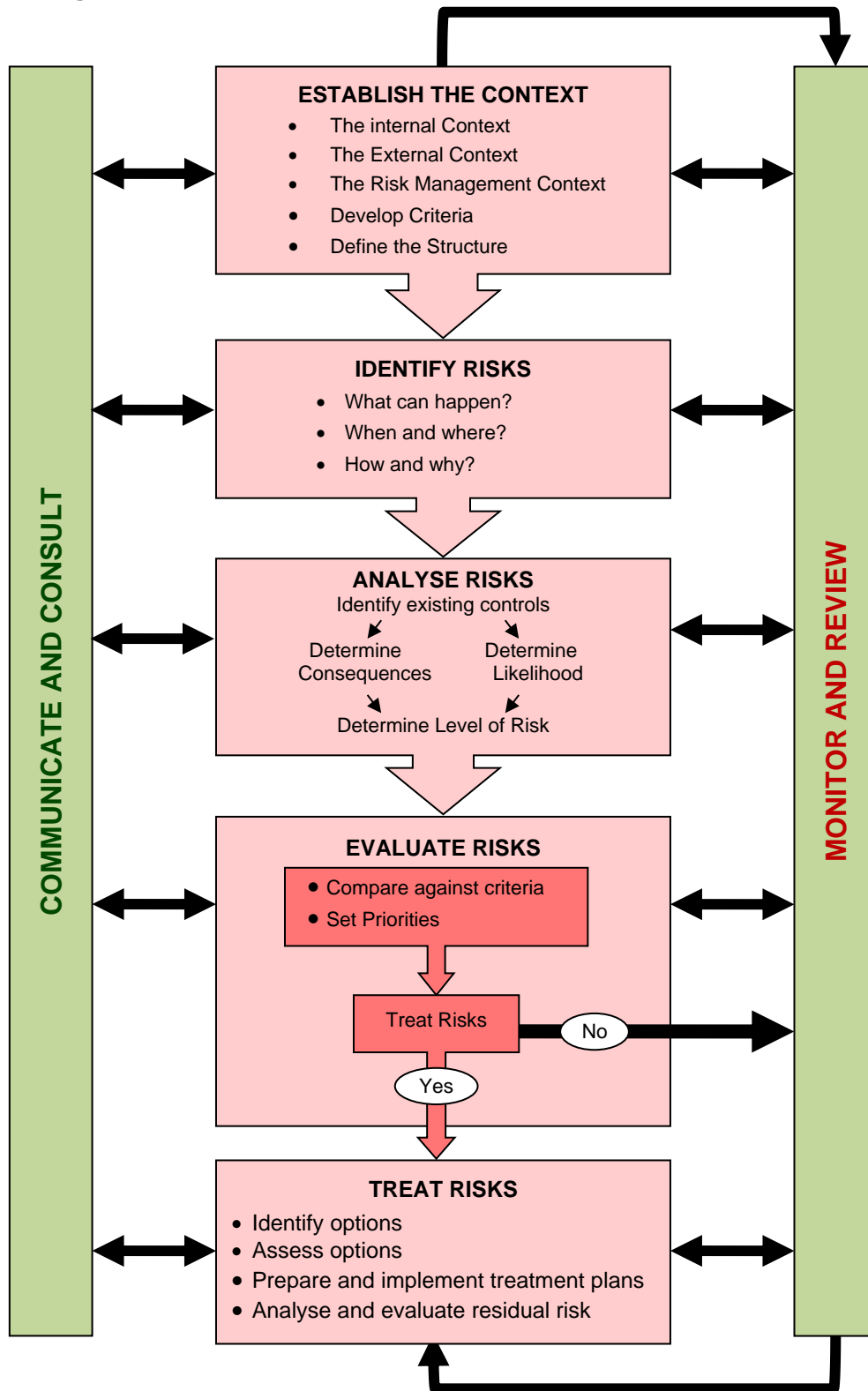
The diagram reinforces that the College needs to identify, assess and treat or manage risks. This includes any risks which may impact on the strategic objectives of the College, such as financial, operational, or major hazard risks.

The management of these risks are monitored and reviewed for effectiveness in dealing with and in developing mitigation strategies. This process will be undertaken with clear communications and consultation throughout the all relevant areas of the College.

The Australian Standards ISO 31000-2009 defines the risk management process as *"The culture, processes, and structures that are directed towards the effective management of potential opportunities and adverse effects."*

The diagram also identifies that the first step in the risk management process and decisions that may be made need to take into account the current College context. As the College context changes, or the circumstances that a College faces or operates in changes, so the risk profile of the College may also change.

Risk Management Process

COMMUNICATE AND CONSULT

MONITOR AND REVIEW

ESTABLISH THE CONTEXT
- The internal Context
- The External Context
- The Risk Management Context
- Develop Criteria
- Define the Structure

IDENTIFY RISKS
- What can happen?
- When and where?
- How and why?

ANALYSE RISKS
Identify existing controls

Determine Consequences   Determine Likelihood

Determine Level of Risk

EVALUATE RISKS
- Compare against criteria
- Set Priorities

Treat Risks — No

Yes

TREAT RISKS
- Identify options
- Assess options
- Prepare and implement treatment plans
- Analyse and evaluate residual risk

RISK MANAGEMENT PROCESS – IN DETAIL AS/NZS ISO 31000:2009

4.5　Communication and Consultation

Communication and consultation is required between all stakeholders throughout the risk management process. This ongoing activity is used to gather information to assist in each step of the risk management process as well as notifying stakeholders both internally and, if appropriate, externally, of the status of risks and risk mitigation treatments. Effective and clear communications are also essential when risks are to be escalated to the next level within the College. Risk management deals with actual and perceived risks. It is important that differences between actual and perceived risk are clarified for all stakeholders. This way risk management discussions can be enhanced in a manner that offers clarity of the issue enabling a clear understanding by all stakeholders.

4.6　Risk Responsibilities and Accountabilities at RACDS

The risk management and accountabilities identify the channels of communication and consultation of how risks are managed through clear reporting and escalation lines and how decisions and directions are managed. These lines of communication and consultation also act as lines of defence which are used to structure roles, responsibilities and accountability for the management and reporting of risks. These are described below.

4.6.1　First Line of Defence
　　　　The first line of defence are the College employees whose role is to identify and manage hazards and report incidents to their Managers when the risks are outside of their capabilities. Everyone within the College community has a responsibility to identify and report risk to the College CEO.

4.6.2　Second Line of Defence
　　　　The second line of defence consists of the Chief Executive Officer and Senior Management Team who have the responsibility to formulate risk management strategies, tolerance limits and structures. The Senior Management Team also coordinate, oversee and objectively challenge the execution, management, control and reporting of risks.

4.6.3　Third Line of Defence
　　　　The third line of defence is risk auditing, carried out by the Finance, Audit and Risk Committee whose role is to review and assess and update the College's risk profile and ensure an effective risk management system is in place. This Committee operates on the delegated authority of the Council in accordance with the Finance, Audit and Risk Committee Terms of Reference.

4.6.4　Fourth Line of Defence
　　　　The fourth line of defence are the external auditors whose roles are to inform and support the Finance, Audit and Risk Committee and the Council, and provide independent assurance on the design and effectiveness of the overall systems of internal financial control, and processes which include risk and compliance.

　　　　The Council are the ultimate owners of risk for the College and have a responsibility to monitor the College's overall risk profile and ensure that adequate resources are available to address the risks.

4.7 Establishing the Context

By establishing the context, the Council will articulate its objectives and define the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process (AS/NZS ISO 31000:2009).

Establishing the context defines the scope for the risk management process and sets the criteria against which the risks will be assessed. The scope should be determined within the context of the College's objectives. Risks are uncertainties that affect the achievement of the College's objectives, so risks cannot fully be identified if these objectives and strategies are unclear.

The selections of key objectives of the College risk management framework are driven by an evaluation of the external and internal factors that may currently impact the College. A review of both the external and internal context at the commencement of the risk assessment planning assists in identifying the processes which may be subject to increased risks and, as such, would derive the greatest value from the risk assessment. Risks can arise due to external or internal influences:

4.7.1 External Risks

External risks are exposures that result from environmental conditions that RACDS is unable to influence, such as the regulatory environment and economic conditions. Consideration should be given to the following inputs as they relate to the organisation, social, regulatory, legislative, cultural, competitive, financial, and the political environment. It is also essential to include the consideration of the College's external relationships such as the perceptions and values of external stakeholders.

4.7.2 Internal Risks

Internal risks are exposures that arise from the decision-making processes and the use of internal and external resources. The internal context is the internal environment in which the College functions and seeks to achieve its objectives. Consideration should be given to factors such as:

a) Strategies and plans are in place and monitored to achieve objectives;
b) Governance, structure, roles and accountabilities;
c) Capability of College employees, systems and processes;
d) Changes to processes or compliance obligations;
e) The risk tolerance and appetite of the Council.

4.7.3 The following key strategic areas will be considered:

- **Growing the College Community**
- **Enhancing Education Leadership and Professionalism**
- **Strengthening Organisational Excellence**
- **Improving Stakeholder Engagement**

The approach that RACDS will take to ensure effective risk management will incorporate:

a) Being open to accepting an appropriate level of risk if that is what is necessary to achieve the College objectives, this will be achieved by understanding the College's appetite and tolerance for certain risks.

b) Identifying and assessing what can go wrong in delivering on objectives or, conversely, what opportunities for improvement or refinement exist in program or project development.

c) Designing and implementing corrective mechanisms to lower the likelihood of negative events or reduce the consequences of risks when they occur.

4.8   Risk Assessment

In undertaking risk assessments the College will use the best available information, data and research available. Risk assessment will involve three steps: risk identification; risk analysis; and risk evaluation.

4.9   Risk identification

Risk identification is the process of identifying key risks facing the College. This involves analysing the sources of risks, potential hazards, possible causes and the potential exposure. Risk identification activities will be planned and structured, and focused on different levels within the College.

4.10 Risk Analysis

Once key risks have been identified, they are then analysed.   The purpose of the risk analysis is to achieve an understanding of the risk and to consistently rank and prioritise these for attention based on the residual risk to the College. Risk assessment involves consideration of the source of the risk, determining the consequence of the outcome of the risk, and the likelihood that those consequences may occur, and then understanding the controls that are currently in place and how effective they are.

The following table is a model used by College for assessing the consequence and likelihood of risks.

RISK AREAS	CONSEQUENCE				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
	1	**2**	**3**	**4**	**5**
PEOPLE EFFECTS	Injury or illness from adverse event, not requiring medical treatment. Insignificant loss of productivity.	Injury or illness from adverse event requiring first aid or medical treatment and/or minor Workcover claim. Minor loss of productivity.	Injury or illness from adverse event or work related illness causing hospitalisation and/or ongoing personal leave and/or Workcover. Moderate loss of productivity. Short term disability to one or more persons	Life threatening injury or illness from adverse event or work related illness causing hospitalisation and/or ongoing Workcover. Major loss of productivity. Extensive injury or impairment to one or more persons	Death or multiple life threatening injuries from adverse event or work related illness. Service delivery ceased.
FINANCIAL	Up to $10 K reduction in annual budgeted net cash flow.	$10 K - $149K reduction in annual budgeted net cash flow	$150 K - $400 K reduction in annual budgeted net cash flow	$400,000 - $699,000 reduction in annual budgeted net cash flow	Over $700,000 reduction in annual budgeted net cash flow
SERVICE OUTPUTS	Minimal disruption	Some service disruption in the area	Total cessation of one service for a few weeks	Disruption of multiple services for several months	Total cessation of multiple services for many months
REPUTATION	No Media coverage; complaint to employee; minor reputational impact in clinical and professional arena	Local media coverage, and complaint to management	Local media coverage over several days; senior managers depart and members affected	State media coverage; CEO departs affecting business continuity and members lost; major reputational impact in clinical and professional arena	National media coverage; wide social media coverage; significant impact on funding for several years; long term loss of members
LEGAL and COMPLIANCE	Minor legal issues or breach of regulations	Breach of regulations; minor litigation	Breach of regulation with investigation by authority and possible moderate fine, and litigation and legal costs up to $999k	Major breach of regulation with punitive fine, and significant litigation involving many weeks of senior management time and up to $3m legal costs	Major litigation costing $>3m; Investigation by regulatory body resulting in long term interruption of operations
MANAGEMENT IMPACT	Will require some management attention over several days	Will require some senior management time over many days	Disruption that will require senior management time over several weeks	Disruption that will require senior management time over several weeks	Restructuring of organisation with loss of many senior managers

4.10.1 **Likelihood Criteria**

Likelihood of potential adverse risk events will be assessed against five criteria, ranging from Insignificant to Rare to Almost Certain, as set out in the table below.

RISK SCORING MATRIX			CONSEQUENCE				
			Insignificant	Minor	Moderate	Major	Catastrophic
			1	2	3	4	5
LIKELIHOOD	Certain	5	Medium	High	High	Extreme	Extreme
	Likely	4	Medium	Medium	High	High	Extreme
	Possible	3	Low	Medium	Medium	High	High
	Unlikely	2	Low	Low	Medium	Medium	High
	Rare	1	Low	Low	Low	Medium	Medium

4.10.2 **Risk ratings are defined as:**

LOW RISK	No specific further actions required other than compliance with established procedures.
MEDIUM RISK	Additional actions need to be assessed, approved and actioned in a routine manner to minimise risk event. Action at office team level.
HIGH RISK	Priority action plan needs to be formulated and additional control needed to minimise event. Action at senior management level required.
EXTREME RISK	Immediate action required to mitigate event. Action at senior management and Council level required.

Risk acceptability is to be evaluated, dependant on the level of risk. The Risk Response in the table above shows the rate of response, and authority level for each level of risk.

4.10.3 **Evaluation and Responsibility**

Risk evaluation is the *"process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable."* (AS/NZS ISO 31000:2009). An evaluation of each risk is undertaken to determine those risks that are acceptable and those that require further management. In order to figure out the risk levels after controls are applied an examination will be undertaken of what controls are in place and how effective they are in managing the likelihood of the risk occurring and or the consequences if the risk eventuates.
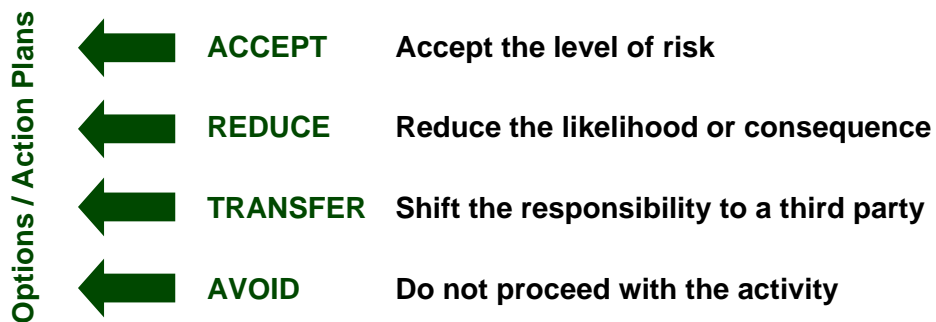
Some risks may be so low that the College may decide to carry the risk whilst other risks may be so extreme that the College will not accept it. Dependent on the level of inherent risk, management strategies will vary.

4.10.4 Some reasons why a **risk may be acceptable** include:

- The level of risk is so low that specific management is not necessary;

- There are no effective management strategies available;

- The costs of management outweighs the potential benefit;

- Opportunities presented outweigh the threats to such an extent that the risk is acceptable.

4.11 Risk Management

Risk management involves identifying the range of options for addressing unacceptable risks, assessing those options, preparing risk management plans and implementing them. Risk management options include:

Options / Action Plans

ACCEPT   **Accept the level of risk**

REDUCE   **Reduce the likelihood or consequence**

TRANSFER   **Shift the responsibility to a third party**

AVOID   **Do not proceed with the activity**

D Clark, Risk Management 2007

4.12 Risk Reporting

The Council require informed and summarised risk reporting whilst operational staff require more detailed risk reporting. The development of reporting protocols and compliance monitoring should include:

- Timely risk reporting responsive to the organisation's Risk Appetite.
- Clear documentation of reported risks understandable by all staff.
- Risk reporting must include feedback through to the Council and the individual who identified the risk.

4.13 Monitor and Review

The College maintains a Risk Register which is used as the basis to monitor and review risks. Monitoring and reviewing activities identify changes in context, likelihood, new and emerging risks and issues. Feedback from this process is used to modify risk assessment and management options.

The Council oversees and monitors the College risk management process while management and staff are responsible for reviewing and updating the relevant risk profiles within their jurisdiction.

4.14 Records and Documentation

Risk identification, assessment and management plans will be documented in the Risk Register.

It is important to document the process and be able to:

- provide an audit trial
- provide evidence of a systematic approach to risk identification and analysis;
- enable decisions or processes to be reviewed;
- provide a record of risks and to develop the College risk knowledge database;
- provide Council with a risk management plan for approval and subsequent implementation;
- provide an accountability mechanism and tool;
- facilitate continuing monitoring and review;
- share and communicate information.
- demonstrate to the College community and auditors that the process has been conducted properly.

4.15 Continuous Improvement

To ensure that the risk framework is effective and continues to support College activities and performance, the College will:

- monitor the impact of risk management strategies implemented;
- periodically review whether the risk management framework and policy are still appropriate, given the College's internal and external context.

5. LEGISLATIVE AND OTHER REFERENCES

- AICD Company Directors Module 3: Risk: Issues for Boards 2008
- Australian New Zealand Risk Management Standard ISO 31000:2009
- BWise Nasdaq: Assessing risks: Inherent or Residual 2012
- Deloitte - Risk Intelligence Series, Issue No.5 2007
- FWK-030 Risk Management Framework
- IS Handbook 2012
- POL- 027 Local Risk Management Policy
- Strategic Performance Management, Bernard Marr 2006

GLOSSARY OF TERMS

Consequence: the outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Cost: of activities, both direct and indirect, involving any negative impact, including money, time, labour, disruption, and goodwill, political and intangible losses

Event: an incident or situation, which occurs in a particular place during a particular interval of time.

Hazard: a source of potential harm or a situation with a potential to cause loss.

Inherent: the risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk)

Likelihood: used as a qualitative description of probability or frequency.

Loss: any negative consequence, financial or otherwise.

Monitor: to check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change.

Probability: the likelihood of a specific event or outcome.

Residual risk: the risk left over after you have implemented a risk management option or after the controls are taken into account.

Risk: the effect of uncertainty on objectives. It is measured in terms of consequences and likelihood.

Risk Appetite: amount and type of risk that an organisation is willing to pursue or retain.

Risk acceptance: an informed decision to accept the consequences and the likelihood of a particular risk.

Risk analysis: a systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.

Risk assessment: the overall process of risk analysis and risk evaluation.

Risk control: is any measure or action that modifies risk. Controls include policies, standards, procedures and physical changes to eliminate or minimise adverse risks.

Risk identification: the process of determining what can happen, why and how.

Risk management: the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

Risk management process: the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

Risk reduction: a selective application of appropriate techniques and management principles to reduce either likelihood of an occurrence or its consequences, or both.

Risk retention: intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the organisation.

Risk transfer: shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means. Risk transfer can also refer to shifting a physical risk or part thereof elsewhere.

Stakeholders: those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.

NOTE: The term stakeholder may also include interested parties as defined in ISO 14050:1998 and AS/NZS ISO 14004:199