



RISK MANAGEMENT POLICY
2024/2025

"Service Delivery through Integrity"

Tel : 035 874 5500 • 400 Ugagane Street, Ulundi, 3838 • Private Bag X76, Ulundi, 3838
www.zululand.org.za

TABLE OF CONTENTS

1.	INTRODUCTION	3
2.	PURPOSE	3
3.	OBJECTIVES	3
4.	SCOPE	4
5.	LEGISLATIVE REQUIREMENTS	4
6.	THE POLICY STANCE	4
7.	BENEFITS OF RISK MANAGEMENT	5
8.	RISK MANAGEMENT PROCESS	6
8.1	Risk Identification	6
8.2	Risk Evaluation	7
8.3	Risk Response	7
9.	RISK MANAGEMENT RESPONSIBILITIES	8
10.	MONITORING & REPORTING	10
11.	IMPLEMENTATION OF THE POLICY & REVIEW	11
12.	APPROVAL	11
	APPENDIX A - DEFINITIONS	12
	APPENDIX B - RATING TABLES	14
	APPENDIX C – RISK CATEGORIES	18

1. INTRODUCTION

The Accounting Officer with the support from the Municipal Council (Executive Authority) of Zululand District Municipality (ZDM) is committed to a process of risk management that is aligned to the principles of good corporate governance, as required by Municipal Finance Management Act (MFMA), Act no 56 of 2003 and King IV report on corporate governance

2. PURPOSE

The purpose of this policy document is to provide a risk management framework and guidelines to be followed within the Zululand District Municipality (hereafter referred to as "ZDM").

This document sets out ZDM's Enterprise Risk Management Policy Framework. It describes ZDM's Risk Management: Policy, Objectives, Benefits, Principles, responsibilities, and guidelines.

3. OBJECTIVES

The objectives of this Risk Management Policy are to:

- i) Provide a level of assurance that current and emerging significant risks are effectively managed;
- ii) Improve municipality's performance by assisting and improving decision making and planning;
- iii) Promote a more innovative, less risk averse culture in which the taking of calculated risks in pursuit of opportunities to benefit the organisation is encouraged;
- iv) Provide a sound basis for integrated risk management and internal control as components of good corporate governance;
- v) Establish a culture of Risk Management within the Municipality;
- vi) Effectively manage specific risks within the Municipality such as security and fraud and corruption;
- vii) Ensure that the Municipality complies with legislation, policies, and regulatory requirements;
- viii) Embed risk management into the culture and language of the Zululand District Municipality; and
- ix) Delineate boundaries regarding risk management within the Zululand District Municipality.

4. SCOPE

This policy document applies to all personnel within the Zululand District Municipality. It does not apply to any local municipality falling under the Zululand District Municipality.

5. LEGISLATIVE REQUIREMENTS

The Municipal Finance Management Act stipulates in section 62 that:

“The Municipal Manager....has and maintains effective, efficient and transparent systems:

- (i) of financial and risk management and internal control; and*
- (ii) of internal audit operating in accordance with any prescribed norms and standards”*

The extension of the general responsibilities, in terms of section 79 of the MFMA, to all Top Management is a cornerstone in the institutionalization of risk management in the public service. It establishes responsibility for risk management at all levels of management, extending beyond the roles of the Accounting Officer, the internal audit unit, or the Audit Committee in this regard.

The King IV Report on Corporate Governance also reflects on risk management as an integral part of strategic and operational activities.

King IV Report states “The Board is responsible for the total process of risk management, as well as for forming its own opinion on the effectiveness of the process.”

6. THE POLICY STANCE

At ZDM, we are committed to optimal management of risk in order to achieve our vision, our key objectives and to protect our core values.

The council of the ZDM has committed the organisation to a process of risk management that is aligned to the principles of the King iv Report and the Municipal Finance Management Act 56 of 2003 (MFMA). The features of this process are outlined in this document. It is expected that all departments, operations, and processes within the municipality will be subject to the prescripts of this risk management policy.

The council recognises that at ZDM, risk management is a complex and a diverse concept, and that there are many departments of the municipality

working at managing risk exposures. It is the intention that these departments / divisions will work together in a consistent and integrated manner, with the overall objective of reducing risk, as far as reasonably practicable.

Different risk related or assurance provider functions will align their various goals and reporting processes into one cohesive and structured framework. All the ZDM's business, financial, technological, legal, and operational risk exposures, whether they are insurable or not, will be identified, assessed, and appropriately managed.

All risk management efforts will be focused on supporting the ZDM's objectives. Equally, they must ensure compliance with relevant legislation, and fulfil the expectations of employees, communities, and other stakeholders in terms of corporate governance.

Effective risk management is imperative to an organisation with our risk profile. The realisation of our Integrated Development Plan depends on us being able to take calculated risks in a way that does not jeopardise the direct interest of stakeholders. Sound management of risk will enable us to anticipate and respond to changes in our environment, as well as make informed decisions under conditions of uncertainty.

Every employee has a part to play in this important endeavour.

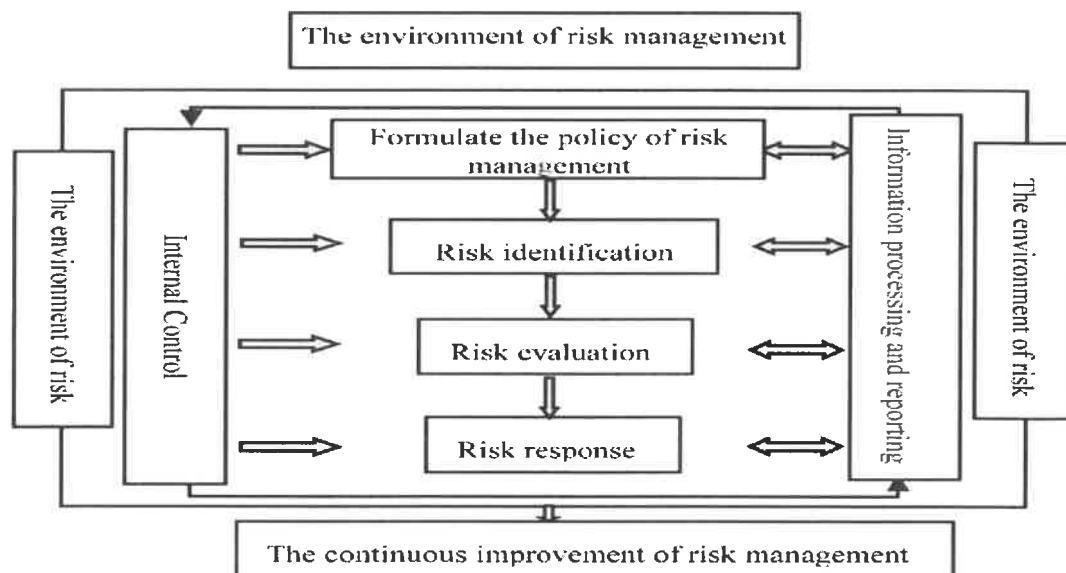
7. BENEFITS OF RISK MANAGEMENT

The benefits of municipality risk management to ZDM encompass:

- ✓ **Enhancing risk response decisions** - Municipality's Risk Management provides the rigour for management to identify alternative risk responses- risk avoidance, reduction, sharing and acceptance.
- ✓ **Reducing operational surprises and losses** – ZDM faces a myriad of risks affecting different parts of the organisation. Municipality risk management facilitates effective responses to the interrelated impacts and enhances an integrated response to multiple risks.
- ✓ **Seizing opportunities** – By considering a full range of potential events, Management is positioned to identify and proactively realize opportunities.

- ✓ **Improving deployment of capital** – Obtaining robust risk information allows Management to effectively assess overall funding requirements and enhance allocation.
- ✓ **Ensuring compliance with laws and regulations** - Municipality Risk Management contributes to effective reporting and monitoring of compliance with laws and regulations and assists with the limitation of damage to ZDM's reputation and associated consequences.
- ✓ **Increasing probability of achieving objectives** – Municipality's Risk management seek to achieve ZDM's performance and financial targets and assist with the prevention of loss resources. Control and risk interventions will be chosen on the basis that they increase the likelihood that ZDM will fulfil its intentions/ commitments to its stakeholders.

8. RISK MANAGEMENT PROCESS



8.1 Risk Identification

- ✓ The objective of risk identification is to understand what is at risk within the context of the Municipality's explicit and implicit objectives and to generate a comprehensive inventory of risks

based on the threats and events that might prevent, degrade, delay or enhance the achievement of the objectives.

- ✓ Annually and for each strategic business objective contained in the IDP adopted by Council of ZDM, Managers will identify the key risks that might impede the achievement of the respective business objectives.
- ✓ Risk identification will be performed as part of all major decision making processes.
- ✓ The risk identification process should cover all significant risks, regardless of whether or not such risks are within the direct control of the Municipality.

8.2 Risk Evaluation

- ✓ Assess the significance of risks to enable the development of Risk Responses
- ✓ All risks will be evaluated on a quantitative basis and if this is not appropriate, qualitative factors will be adopted
- ✓ Once the risks have been identified, the likelihood of the risk occurring and the potential impact if the risk does occur must be assessed using a risk-rating table during the risk assessment ***(refer to rating tables on Annexure A below)***

8.3 Risk Response

- ✓ Once risks have been analyzed appropriate, risk responses will be determined to mitigate risks to unacceptable level within reasonable costs.
- ✓ Risk can be dealt with in various ways. The risk response options encompass all possible management responses to risk, whether viewed as opportunities, uncertainties or hazards. The risk response options and examples of activities under each option are outlined below:
 - Mitigate (steps taken to reduce either the likelihood or impact e.g., policies, procedures, registers (etc).
 - Transfer (steps taken to shift the loss or liability to others i.e., Insurance covers on vehicles, computers, etc.
 - Exploit (steps taken to leverage opportunities e.g., strengthening relations with other department etc).
 - Avoid (steps taken to prevent the occurrence of hazards e.g., deciding not to embark on a project, activity because it is too risk and has highly hazardous impact); or
 - Acceptance (an informed decision to accept both the impact and likelihood of risk event e.g., risk that ZDM can do nothing

about but live with them and just keep monitoring).

9. RISK MANAGEMENT RESPONSIBILITIES

All personnel have a responsibility for maintaining good internal control and managing risk to achieve strategic objectives.

Collectively, staff at operating units needs to have appropriate knowledge, skills, information, and authority to establish, operate and monitor the system of risk control. This requires a good understanding of the municipality, its objectives, the risks it faces and the people we deal with. Everyone should be aware the risks they are empowered to take, which should be avoided and reported upwards.

Notwithstanding the participatory approach in risk management, the ultimate responsibility for managing risk lies with Zululand Municipality's Council and the Accounting Officer

In the table below the various role players are identified and their roles in the risk management process is discussed.

Role Player	Role
Council	<ul style="list-style-type: none"> • They define the mission, vision and strategic objectives • They approve the risk management policy • They approve the fraud prevention policy • Obtain assurance from management that the ZDM's strategic choices were based on a rigorous assessment of risk • Obtain assurance that key risks inherent in the ZDM's strategies were identified and assessed, and are being properly managed • Assisting the Accounting Officer to deal with fiscal, intergovernmental, political and other risks beyond their direct control and influence • They report on the effectiveness of risk management in the annual report.
Accounting Officer	<ul style="list-style-type: none"> • The Accounting Officer is the ultimate Chief Risk Officer of the municipality and is accountable for the municipality's overall governance of risk. • By setting the tone at the top, the Accounting Officer promotes accountability, integrity and other factors that will create a positive risk and control environment. • Delegating responsibilities for risk management to Management

	<p>and internal formations such as the Risk Management Committee, Finance Committee, ICT Steering Committee, etc.</p> <ul style="list-style-type: none"> • Holding Management accountable for designing, implementing, monitoring and integrating risk management into their day-to-day activities • A report on the effectiveness of the risk management should be included as part of the periodic management and financial reporting process to Council.
Audit Committee	<ul style="list-style-type: none"> • The detailed responsibilities of the Audit Committee with respect to risk management should be formally defined in its charter • The Audit Committee provides an independent and objective view of the municipality's risk management effectiveness by reviewing the outcome of the risk management processes. • Reviewing and recommending disclosures on matters of risk in the annual financial statements and annual report • Providing regular feedback to the Accounting Officer and the Council on the adequacy and effectiveness of risk management in the ZDM, including recommendations for improvement • Ensuring that the internal and external audit plans are aligned to the risk profile of the Municipality.
Municipal Risk Management Committee	<ul style="list-style-type: none"> • Assist the Accounting Officer in monitoring the execution of the municipal risk management. • Review the risk management progress and maturity of the municipality, the effectiveness of risk management activities, the key risks facing the municipality, and the responses to address these key risks. • Provide timely and useful reports to the Audit Committee and the Accounting Officer on the state of risk management, together with accompanying recommendations to address any deficiencies identified by the Committee. • Additional responsibilities of the Risk Management Committee are formally defined in its charter.
Management	<ul style="list-style-type: none"> • Identify key risks to departmental objectives as an integral part of the business planning process, • Ensure that management plans are in place and reviewed to mitigate the key risks identified during the business planning risk assessment process, • Devote personal attention to overseeing the management of key risks within their area of responsibility • Provide risk management reports to the Risk Management Committee, presenting to the Risk Management and Audit

	<p>Committees as requested</p> <ul style="list-style-type: none"> • Maintain the proper functioning of the control environment within their area of responsibility • Ensure that risk to objectives is a standing item on the agenda for senior management team meetings. • Hold officials accountable for their specific risk management responsibilities.
Chief Risk Officer	<ul style="list-style-type: none"> • The AO may appoint a member of the municipal staff as the Chief Risk Officer to perform the day-to-day risk management duties. • The CRO manages, initiates, drives, advise on and coordinate all risk management activities. • Ensure effective information system exist to facilitate overall risk management improvement within the municipality.
Other Officials	<ul style="list-style-type: none"> • Other officials are responsible for integrating risk management into their day-to-day activities. • They must ensure that their delegated risk management responsibilities are executed and continuously report on progress. • Inform their supervisors and/or the Risk Management Committee of new risks and significant changes in known risks
Internal Audit	<ul style="list-style-type: none"> • The role of the Internal Auditing in risk management is to provide an independent, objective assurance to the Accounting Officer on the effectiveness of the municipality's system of risk management. • Prepare a risk-based audit plan and an internal audit program for each financial year.
External Audit	<ul style="list-style-type: none"> • The external auditor (Auditor-General) provides an independent opinion on the effectiveness of risk management.
Risk Owner /Action Owner	<p>Each key risk will have a nominated risk owner, who will be responsible for the following</p> <ul style="list-style-type: none"> • Updating the risk information; • Providing assurance regarding the risk's controls; • Co-ordinate the implementation of action plans for the risk; and • Reporting on any developments regarding the risk.

10. MONITORING & REPORTING

- ✓ All new risks and changes to existing risks will be captured into the risk management system in the period they are identified.

- ✓ The members of the Risk Committee, will collect and aggregate the information from their respective departments and report to the Risk Management Committee during the quarterly meetings regarding the changes in risk profile of the Department.
- ✓ The Municipal Manager will report to the Council on a regular basis, both the current risk profile of the Municipality and a summary of any major changes since the last report.

11.IMPLEMENTATION OF THE POLICY & REVIEW

The risk management policy should be communicated to all incumbent officials and arrangements should be made for communicating the policy to all new recruits.

This Policy shall be reviewed annually by the Risk Management Committee to reflect the current stance on risk management.

12.APPROVAL

Approval by Council Committee

The Risk Management Policy was adopted by the Council of Zululand District Municipality on **27th** day of **June 2024** by way of a council resolution **ZDMC: 24/445**.

Signature of the Hon. Speaker of Council

Cllr. D.T Memela:  Date: 27/06/2024

APPENDIX A - DEFINITIONS

Word	Meaning
<i>“Risk”</i>	<p>An unwanted outcome, actual or potential, to the Institution’s service delivery and other performance objectives, caused by the presence of risk factor(s).</p> <p>A chance of something happening or not happening that will have an impact upon the objectives of ZDM and/or individual business units.</p> <p>Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. This definition of “risk” also encompasses such opportunities.</p> <p>Risk is often created by:</p> <ul style="list-style-type: none"> • Changes that takes place within the Municipality (i.e. people, systems, processes, technology, legislation and regulations); • External influences (i.e. economics, availability of human resources and damages); • Operations and complexity of processes; • Volume of activities within a Municipality; and • The nature of the control environment.
<i>“Risk Management”</i>	Systematic and formalised processes to identify, assess, manage, and monitor risks.

<i>“Risk Assessment “</i>	The overall process of identifying, analysing and evaluating risk. The risk assessment process should consider risks that are significant to the achievement of the Municipality’s objectives. This is a continuous process, requiring regular reviews, as and when internal and external changes influence the Municipality’s strategies and objectives.
<i>“Strategic risk assessment”</i>	Strategic risk identification is to identify risks emanating from the strategic choices made by the Municipality, specifically with regard to whether such choices weaken or strengthen the Municipality’s ability to execute its Constitutional mandate.
<i>“Operational risk assessment”</i>	Operational risk identification identify risks concerned with the Municipality’s operations. Operational risk identification seeks to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities, and external events
<i>“Inherent Risk”</i>	The exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors.
<i>“Likelihood/Probability”</i>	The probability refers to the chances of a risk occurring which could cause adverse effect on the municipality’s business. The probability is measured on a scale of 1 to 5
<i>“Impact”</i>	The severity is the consequence or damage the risk can cause if it materializes or is the material loss to the municipality (financially and non-financially), if the risk materialises. Impact is also measured on a scale of 1 to 5
<i>“Control Activities”</i>	Organization’s structure, work and authority flows, people and management information systems, designed to help the organization accomplish specific goals or objectives. Internal controls are actions, systems, policies, methods and procedures

	implemented by management to manage or reduce the likelihood and impact of the inherent risk. Internal controls are embedded in the daily activities of our municipality.
<i>“Residual Risk”</i>	The remaining exposure after the mitigating effects of deliberate management intervention(s) to control such exposure (the remaining risk after Management has put in place measures to control the inherent risk).
<i>“Risk Appetite”</i>	The amount of residual risk that the Institution is willing to accept.
<i>“Risk Tolerance”</i>	The amount of risk the Institution is capable of bearing (as opposed to the amount of risk it is willing to bear)
<i>“Risk Management Committee”</i>	A committee appointed by the Accounting Officer to review the Institution’s system of risk management.
<i>“Risk Owner/Action Owner”</i>	The person accountable for managing a particular risk.
<i>“King IV”</i>	The King Code of Corporate Governance for South Africa
<i>“MFMA”</i>	Municipal Finance Management Act (Act No. 56 of 2003).
<i>“IRMF”</i>	Integrated Risk Management Framework

APPENDIX B - RATING TABLES

a) Impact

This is the potential magnitude of the impact on your objectives, should the risk actually occur. This must be assessed on the basis that management has no specific controls in place to address the risk, i.e. without any controls in place, what will the impact of this risk be on the Organisation?

The table below is to be used to assist management in quantifying the impact of specific risk:

Impact Rating	Qualification Criteria
Catastrophic 5	<ul style="list-style-type: none"> • Negative outcomes or missed opportunities that are of critical importance to the achievement of the objectives • Significant over-expenditure, unauthorised expenditure, non-compliance with prescripts, effect on revenue and asset base • Use of unproven technology for critical system / project component • High level of technical interdependencies between system / project components • Major environmental damage • Serious injury (permanent disability) or death of personnel or members of the public • Major negative media coverage • Major disruption to mission critical activities • Termination of Projects
Major 4	<ul style="list-style-type: none"> • Negative outcomes or missed opportunities that are likely to have a major impact on the ability to meet objectives • Major non-compliance implications with PFMA and other legislation, significant overspending, non-availability of financial resources, major effect on revenue and asset base • Use of technology not previously utilised for critical systems / project components • Significant injury of personnel, visitors or public • Significant environmental damage • Significant negative media coverage • Reduction in supply of goods and / services for a period 24 & 48 hours over mission critical services • Major disruption to critical activities
Moderate 3	<ul style="list-style-type: none"> • Negative outcomes or missed opportunities that are likely to have a relatively substantial impact on the ability to meet objectives • Moderate impact on revenue and assets • Use of unproven or emerging technology for systems / project components • Minor environmental, safety or health impact • Negative media coverage • Reduction in supply of goods or services for a period between 24 & 48 hours over critical services and significant disruption to activities

Impact Rating	Qualification Criteria
Minor 2	<ul style="list-style-type: none"> • Negative outcomes or missed opportunities that are likely to have a relatively low impact on the ability to meet objectives • Minor impact on revenue or asset base • Use of unproven or emerging technology for systems/project components • Minor environmental, safety or health impact • Minor negative media coverage • Loss of an asset with minor impact on operations
Insignificant 1	<ul style="list-style-type: none"> • Negative outcomes or missed opportunities that are likely to have a negligible impact on the ability to meet objectives • Insignificant financial loss • No environmental, safety or health impact • Zero negative/media coverage • No impact on business or core systems • Use of unproven or emerging technology for non-critical systems/project components

b) Likelihood of occurrence

This is the likelihood that the identified risk will occur within a specified period of time (between 1 and 3 years) on the basis that there are no specific controls in place to address the risk. The table below is to be used to assist management in quantifying the probability of specific risk occurring.

Likelihood Rating	Measurement Criteria	Qualification Criteria
Almost Certain 5	The risk is already occurring, or has a high likelihood of occurring more than once during the next 12 months.	The risk is almost certain to occur in the current circumstances.
Likely 4	The risk will easily occur, and is likely to occur at least once during the next 12 months.	More than an even chance of occurring.
Possible 3	There is an above average chance of the risk occurring at least once during the next 3 years.	Could occur often.
Unlikely 2	The risk has a low likelihood of occurring during the next 3 years.	Low likelihood, but could happen.
Rare	The risk is conceivable but it is only	Not expected to

1	likely to occur in extreme circumstances.	happen - event would be a surprise.
---	---	-------------------------------------

c) Inherent risk exposure

Inherent risk is defined as the exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such risk factors. *Inherent risk rating = impact x likelihood* (in the absence of mitigating controls). This indicator may be used to assign the level of management resources required to control the relevant risks.

Inherent risk exposure	Factor
Maximum	³ 20
High	³ 15 < 20
Medium	³ 10 < 15
Low	³ 5 < 10
Minimum	< 5

d) Control Adequacy Assessment

Having established which controls are in place to manage the risk in question, it is necessary to assess the effectiveness of the controls. This is a measure of how well management perceives the identified controls to be working and effectively managing the risks

The table below was used to assist management in quantifying the adequacy of existing risk mitigating controls, in order to determine the residual risk:

Control Adequacy Factor	Qualification Criteria
Very Good 90%	The risk is effectively controlled and managed, but in some regards over-controlled.
Good 70%	Majority of risk exposure is effectively controlled and managed.
Satisfactory 50%	Some of the risk exposure appears to be controlled, but there is some room for improvement in the internal control system.
Weak	Some of the risk exposure appears to be controlled, but there

20%	are major deficiencies.
Unsatisfactory 10%	Control measures are ineffective.

e) Residual Risk exposure

Residual risk is defined as the remaining exposure after the mitigating effects of deliberate management intervention(s) to control such exposure (the remaining risk after management has put in place measures to control the inherent risk).

Residual risk = Inherent risk – control adequacy rating

Description	Thresholds	Suggested Action	Suggested Timing
High	between 15 and 25 – Unacceptable	Management should take immediate action to reduce risk exposure to an acceptable level.	Immediate action required.
Medium	between 8 and 14 - Cautionary	Management should constantly monitor the risk exposure and related control adequacy.	Medium-term, within three months.
Low	between 1 and 7 - Acceptable	Management may consider reducing the cost of control.	Monitor, no action required.

APPENDIX C – RISK CATEGORIES

The following are some of the risk categories:

a) Some external factors to be considered:

- Political: the influence of local and international governments and other governing bodies;
- Economic: international, national markets and globalisations;
- Social: major demographic and social trends, level of citizen engagement; and
- Technological.

b) Internal factors reflect management's choices and include such matters as:

- The overall management framework;
- Governance and accountability frameworks;
- Level of transparency required;
- Values and ethics;
- Infrastructure;
- Policies, procedures and processes;
- Human resource capacity; and
- Technology

c) Possible sources of risk may include:

- New activities and services;
- Disposal or cessation of current activities;
- Outsourcing to external service providers;
- Commercial / legal changes;
- Changes in the economic conditions;
- Socio-political changes, like elections;
- National and international events;
- Personnel / human behaviour;
- Behaviour of contractors / private suppliers;
- Financial / market conditions;
- Management activities and controls;
- Misinformation;
- Technology / technical changes, i.e. new hardware and software implementations;
- Operational (the activity itself) changes;
- Business interruption / Business Continuity;
- Occupational health and safety;
- Property / assets;

- Security (including theft /impersonation);
- Fraud / corruption;
- Natural events; and
- Public liability.