SHIRE OF KONDININ

RISK MANAGEMENT PLAN

December 2021~~November 2019~~

CONTENTS PAGE

REVIEW OF RISK MANAGEMENT, INTERNAL CONTROL & LEGISLATIVE COMPLIANCE

The Shire of Kondinin recognises the need for sound risk management practice throughout its organisation and has formally adopted Council Policy in this regard. Many risks are out of the control of the local government such as severe flooding, cyclones, terrorism, a major war invasion, local government reform/amalgamation, etc. however in most cases, their effect can be effectively managed and damage minimised through counter disaster / risk management planning. Those risks under the local government's control can, through sound risk management planning and practices by management, be mitigated or at least the likelihood of the risk occurring reduced.

This document, entitled Shire of Kondinin's Risk Management Plan incorporates a **Review of Risk Management, Internal Control and Legislative Compliance.** It has been prepared by the Chief Executive Officer of the Shire of Kondinin in accordance with Regulation 17 of the Local Government Audit Regulations 1996. This review identifies risks and legislative compliance affecting the Shire of Kondinin in appropriate areas and rates their likelihood of occurrence. This report is to be reviewed annually, when it is to be updated as appropriate, taking into account changing circumstances affecting the Shire of Kondinin. The reviewed report shall be presented to the Council's Audit Committee for review/adoption and the Audit Committees recommendation to Council for its formal adoption.

RISK MANAGEMENT

The Shire of Kondinin's administration, through the adoption of internal controls practiced where appropriate on a day to day basis, is required to mitigate risk affecting the local government including ensuring that legislative compliance is adhered to. The prime responsibility of ensuring that this is carried out and is achieved rests with the local government's Chief Executive Officer, in accordance with the Local Government Act, 1995 and Local Government Audit Regulations, 1996 (Regulation 17). The local government also appoints external auditors to ensure that the administration and operation of the local government is carried out in a fully compliant, transparent and well managed manner encompassing integrity, honesty and trustworthiness.

Risk Management extents to include all areas that may adversely affect the operations of the local government.

AUSTRALIAN STANDARD AS/NZS ISO 31000:2009 – RISK MANAGEMENT

(See Appendix 1)

SHIRE OF KONDININ RISK MANAGEMENT MATRIX

Identified risks will be categorised according to their **level of impact** on the organisation as follows:

- High 🟥
- Moderate 🟧
- Low impact 🟨

Identified risks will also be categorised according to their **likelihood of occurrence** as follows:

- High 🟥
- Moderate 🟧
- Low 🟨

Identified risks will also be categorised according to the **adequacy of internal controls** to mitigate the risk as follows:

- High (Inadequate) 🟥
- Moderate 🟧
- Low (Adequate) 🟨

ROLES & RESPONSIBILITIES

Council

- Appoint an Audit Committee pursuant to the Local Government Act, 1995.
- Adopt the local government's Shire of Kondinin's Risk Management Plan.
- Appoint External Auditors to audit the Shire's financial statements annually.

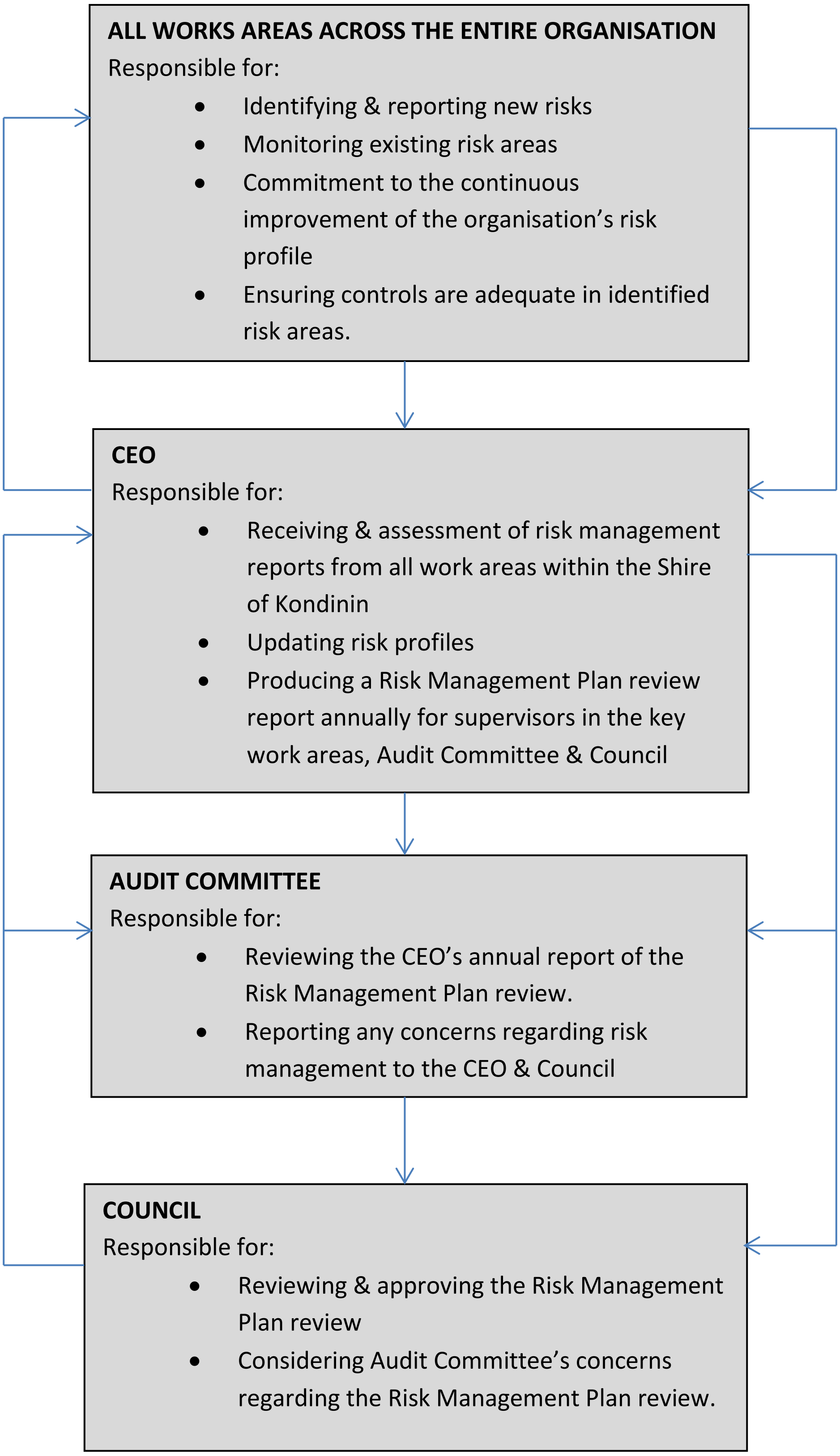
Audit Committee

- Provides corporate governance support to Council.
- Oversees external audits and reports to Council any matters concerning the external audit.
- Reports to Council any risk management concerns the Committee may have.

CEO / Management Team

- Liaises with Council in respect of risk management.
- Reviews the Risk Management Plan and reports to Council findings.
- Appoints Internal Auditors pursuant to the Local Government Audit regulations
- Promotes a culture within the organisation that works towards the reduction of risk.

RISK MANAGEMENT REPORTING FLOW CHART



ALL WORKS AREAS ACROSS THE ENTIRE ORGANISATION

Responsible for:

- Identifying & reporting new risks
- Monitoring existing risk areas
- Commitment to the continuous improvement of the organisation's risk profile
- Ensuring controls are adequate in identified risk areas.

CEO

Responsible for:

- Receiving & assessment of risk management reports from all work areas within the Shire of Kondinin
- Updating risk profiles
- Producing a Risk Management Plan review report annually for supervisors in the key work areas, Audit Committee & Council

AUDIT COMMITTEE

Responsible for:

- Reviewing the CEO's annual report of the Risk Management Plan review.
- Reporting any concerns regarding risk management to the CEO & Council

COUNCIL

Responsible for:

- Reviewing & approving the Risk Management Plan review
- Considering Audit Committee's concerns regarding the Risk Management Plan review.

IDENTIFIED RISK AREAS

Risk areas assessed under this report include:

1. General

1.1 Damage to assets through natural causes such as flood, cyclone and fire as well as terrorism & vandalism.

1.2 Theft of assets including plant, equipment, administration records, computer/IT functionality and data integrity.

1.3 Asset Management – operator skill level, staff training, maintaining quality plant & equipment through regular changeover, adequacy of building maintenance.

1.4 Security of buildings including Shire administration and depot buildings.

1.5 Provision of Medical Doctor and Hospital Services.

1.6 Disruption to Council operations through electricity cuts, flood and fire.

1.7 Adequacy of Emergency Management Services (volunteer fire control, volunteer emergency services & volunteer ambulance services)

1.8 Adverse effects to the local government community through forced reform/ amalgamation.

2. Administration

2.1 Fraud, corruption and misconduct by employees for financial gain, etc. Adequacy of Delegations Register, Financial Payments procedure (two to sign/authorise all payments), bank reconciliations, Purchase Order process.

2.2 External theft and fraud – adequacy of Shire buildings/assets (Shire depot & office) security.

2.3 Accuracy of financial management and reporting including adherence to budget

2.4 Adequacy of Records Management – Adequacy of the local government's hard copy and electronic filing record system.

2.5 Project Management - Project over-expenditure particularly in respect of major Council projects including road construction & building/infrastructure construction, knowledge of contractor terms & conditions, lack of communication & consultation, cost blowouts & achieving quality project supervision.

2.6 Human Resource Management – Risks associated with employee injury claims, sexual harassment, bullying, stress claims, etc.

2.7 Adequacy and Integrity of computer/IT system – Hardware & Software.

2.8 IT/Computer System Failure caused through software/hardware failure, virus/hacking, electricity supply failure, adequacy of backup facilities.

2.9 Potential non-compliance with legislation, regulations and standards and local government policies

2.10 Legal Litigation and Claims

2.11 Significant Business Risks

2.12 Occupational Health & Safety Risks

2.13 Adequacy of local government practices and processes to manage insurable risks and ensure the adequacy of insurance cover.

2.14 Complaints management

2.15 Business Disruption through flood, storms, cyclones, fire, earthquake, terrorism, health epidemic, electricity outage, loss of key staff, etc.

2.16 HR/People Management – Adequacy of employee training, employee performance reviews, leadership, internal communications, workforce planning & employee morale.

3. Internal Control

3.1 Effectiveness of the local government's internal control system with management and the internal and external auditors

3.2 Effectiveness of the local government's external auditors to identify fraud, corruption, legislative non-compliance and substandard financial management.

3.3 Shire of Kondinin's Procurement Framework – probity and transparency of policies and procedures/processes and whether these are being applied. Adequacy of delegations register, tender process, quotation process, e-Quotes WALGA, purchase orders and purchasing policy.

3.4 Adequacy of Contractor & Supplier Management.

4. Elected Members

4.1 Compliance with declaration of pecuniary interest by elected members of the local government.

4.2 Undue influence of elected members in respect of the local government's operations/ projects for personal financial gain.

4.3 Non-compliance with the local government's Code of Conduct adversely affecting the ability of management to manage.

5. Legislative Compliance

5.1 Monitoring compliance with legislation and regulations by administration and the local government's Audit Committee.

5.2 Review of the annual Compliance Report by the Audit Committee and reporting to Council the results of that review.

5.3 The effectiveness of the local government's management to ensure compliance with legislation and regulations.

5.4 The effectiveness of management to identify significant adverse financial trends or events affecting the local government's financial sustainability and management's efficient and accurate reporting of such information to Council.

5.5 The effectiveness of the local government's compliance frameworks dealing with relevant external legislation and regulatory requirements.

ASSESSMENT OF IDENTIFIED RISK AREAS

1. General

1.1 **Damage to assets through natural causes such as flood, cyclone and fire as well as terrorism & vandalism.**

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟧	🟨

Comment: Local VES & Fire Brigades provide excellent coverage.

1.2 Theft of assets including plant, equipment, administration records, computer/IT functionality and data integrity.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟧	🟨

Comment: History dictates that this is a low risk area.

1.3 Asset Management – operator skill level, staff training, maintaining quality plant & equipment through regular changeover, adequacy of building & road maintenance.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟨	🟨	🟨

Comment: Asset management is considered a low risk area.

1.4 Security of buildings including Shire administration and depot buildings.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟥	🟧

Comment: Security at the Shire depot requires improving with occasions occurring when access is available when no one is in attendance making theft possible.

1.5 Provision of Medical Doctor and Hospital Services.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟥	🟧

Comment: Lack of medical Doctor services is a likely risk that administration and Council are continually monitoring and endeavouring to mitigate

1.6 Disruption to Council operations through electricity cuts, flood and fire.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟨

Comment: Local VES & Fire Brigades provide excellent coverage.

1.7 Adequacy of Emergency Management Services (volunteer fire control, volunteer emergency services & volunteer ambulance services)

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟨	🟨

Comment: Local VES & Fire Brigades provide excellent coverage.

1.8 Adverse effects to the local government community through forced reform/amalgamation.

Comment: A forced unacceptable and unwise local government reform/amalgamation is considered to have a high risk factor resulting in the breakdown of the currently very strong community spirit & current local government support to its community.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟧	🟥

2. Administration

2.1 Fraud, corruption and misconduct by employees for financial gain, etc. Adequacy of Delegations Register, Financial Payments procedure (two to sign/authorise all payments), bank reconciliations, Purchase Order Process.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟧	🟨

Comment: It is considered that strong internal controls are in place to largely mitigate these risks. Senior staff receiving financial gain from contracts/tenders awarded is considered a risk area with the occurrence likelihood considered low.

2.2 External Theft and Fraud

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟧	🟧

Comment: Theft from the Shire depot caused by lack of security and IT related theft are considered risk areas.

2.3 Accuracy of financial management and reporting including adherence to budget

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟨	🟨

Comment: Due to the Shire possessing qualified and experienced accounting staff, internal control is considered adequate and risk level low.

2.4 Adequacy of Records Management – Adequacy of the local government's hard copy and electronic filing record system.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟥

Comment: Electronic records management is considered deficient with investigations currently being made regarding obtaining and implementing suitable IT software to remedy this.

2.5 Project Management - Project over-expenditure particularly in respect of major Council projects including road construction & building/infrastructure construction, knowledge of contractor terms & conditions, lack of communication & consultation, cost blowouts & achieving quality project supervision.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟧	🟨

Comment: It is considered that internal controls in this area are effective in minimising risk.

2.6 Human Resource Management – Risks associated with employee injury claims, sexual harassment, bullying, stress claims, etc.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟧	🟨

Comment: It is considered that internal controls in this area are effective in minimising risk.

2.7 Adequacy and Integrity of Computer/IT system – Hardware & Software

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟧	🟧

Comment: A hardware upgrade is considered required within two years.

2.8 IT/Computer System Failure caused through software/hardware failure, virus/hacking, electricity supply failure, adequacy of backup facilities.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟧	🟥

Comment: Testing of the computer/IT back-up system to ensure its efficiency is required.

2.9 Potential non-compliance with legislation, regulations and standards and local government policies

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟨

Comment: Internal control is considered adequate and risk level low.

2.10 Legal Litigation and Claims

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟧	🟨

Comment: Internal control is considered adequate and risk level low.

2.11 Significant Business Risks

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟨	🟨	🟨

Comment: Internal control is considered adequate and risk level low.

2.12 Occupational Health & Safety Risks

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟧	🟨

Comment: A satisfactory independent OH&S audit was conducted earlier this year.

2.13 Adequacy of local government practices and processes to manage insurable risks and ensure the adequacy of insurance cover.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟨	🟨	🟨

Comment: Comment: Internal control is considered adequate and risk level low.

2.14 Complaints Management

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟨	🟧	🟨

Comment: A complaints register exists & complaints managed.

2.15 Business Disruption through flood, storms, cyclones, fire, earthquake, terrorism, health epidemic, electricity outage, loss of key staff, etc.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟧	🟨

Comment: Flood, storms and fire are the most common risk factors likely to have a high level of impact, internal control of countering such disasters is considered adequate as well as in respect of loss of key staff.

2.16 HR/People Management – Adequacy of employee training, employee performance reviews, leadership, internal communications, workforce planning & employee morale.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟨

Comment: Internal control is considered adequate and risk level low.

3. Internal Control

3.1 Effectiveness of the local government's internal control system with management and the internal and external auditors

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟨	🟨	🟨

Comment: Internal control is considered adequate and risk level low.

3.2 Effectiveness of the local government's external auditors to identify fraud, corruption, legislative non-compliance and substandard financial management.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟨

Comment: Internal control is considered adequate and risk level low.

3.3 Shire of Kondinin's Procurement Framework – probity and transparency of policies and procedures/processes and whether these are being applied. Adequacy of delegations register, tender process, quotation process, e-Quotes WALGA, purchase orders and purchasing policy.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟨

Comment: Internal control is considered adequate and risk level low.

3.4 Adequacy of Contractor & Supplier Management.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟧	🟨

Comment: Internal control is considered adequate and risk level low.

4. Elected Members

4.1 Compliance with declaration of pecuniary interest by elected members of the local government.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟨

Comment: Internal control is considered adequate and risk level low.

4.2 Undue influence of elected members in respect of the local government's operations/ projects for personal financial gain.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟨

Comment: Internal control is considered adequate and risk level low.

4.3 Non-compliance with the local government's Code of Conduct adversely affecting the ability of management to manage.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟨	🟨

Comment: Adequate Councillor training and internal control by the Shire President as well as the demonstrated actions of Councillors make this a low risk area for this LGA.

5. Legislative Compliance

5.1 **Monitoring compliance with legislation and regulations by administration and the local government's Audit Committee/Council.**

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟨

Comment: Internal control through meeting agenda reporting is considered adequate and risk level low.

5.2 Review of the annual Compliance Report by the Audit Committee and reporting to Council the results of that review.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟨

Comment: Internal control is considered adequate and risk level low.

5.3 The effectiveness of the local government's management to ensure compliance with legislation and regulations.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟨

Comment: Internal control is considered adequate and risk level low.

5.4 The effectiveness of management to identify significant adverse financial trends or events affecting the local government's financial sustainability and management's efficient and accurate reporting of such information to Council.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟥	🟨	🟨

Comment: Internal control through qualified accounting staff's accurate reporting is considered adequate and risk level low.

5.5 The effectiveness of the local government's compliance frameworks dealing with relevant external legislation and regulatory requirements.

Level of Impact	Occurrence Likelihood	Internal Control Adequacy
🟧	🟨	🟨

Comment: Internal control through qualified staff (Town Planner, EHO, Building Surveyor, Ranger, etc.) is considered adequate and risk level low.

COUNCIL POLICY – RISK MANAGEMENT

The following forms part of the Council's Policy Manual:

4.1 ADMINISTRATION GENERAL

4.1.17 RISK MANAGEMENT

In accordance with Local Government Audit Regulations, 1996 (Regulation 17) and Australian Standards AS/NZS ISO 31000:2009, it is Shire of Kondinin Policy to achieve compliance and best practice in the management of risks affecting the Shire of Kondinin and all persons associated with the Shire.

The Shire of Kondinin encourages the CEO and all employees to work towards the mitigation, or at least reduction, of risks affecting the Shire of Kondinin.

The Shire's CEO has prepared a Review of Risk Management, Internal Control and Legislative Compliance, which document was adopted by Council at its December, 2014 ordinary Council meeting. This document is to be reviewed annually by the Shire's management team (including input invited from all Shire employees) and findings reviewed by the CEO and reported to the Council's Audit Committee for its consideration and report to Council, with a view to achieving continuous improvement of the risk profile of the Shire of Kondinin.

SUMMARY

The assessment of the above risks has been undertaken by Mia Dohnt, Chief Executive Officer of the Shire of Kondinin in consultation with senior administration staff.

This document shall be reviewed by supervisors of the Shire of Kondinin's key work areas, with input invited from all employees, with the objective of achieving on-going continuous improvement (lowering of risk) of the Shire of Kondinin's risk profile. A review shall be conducted annually with the first review scheduled to be undertaken in November, 2015. Such review shall be facilitated by the CEO and recommended changes to the document presented to the Council's Audit Committee for its review and recommended adoption of amendments by Council.

This Review of Risk Management, Internal Control and Legislative Compliance (including Council Policy relating to Risk Management), was adopted by the Council of the Shire of Kondinin at its meeting held on 17th December, 2014.

Mia Dohnt
Chief Executive Officer
Shire of Kondinin
2nd October 2019

APPENDIX 1

AUSTRALIAN STANDARD AS/NZS ISO 31000:2009 – RISK MANAGEMENT

The following is an extract from AS/NZS ISO 3100:2009:

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees.

Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is "risk".

All activities of an organization involve risk. Organizations manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. This International Standard describes this systematic and logical process in detail.

While all organizations manage risk to some degree, this International Standard establishes a number of principles that need to be satisfied to make risk management effective. This International Standard recommends that organizations develop, implement and continuously improve a framework whose *purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.*

Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this International Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. Therefore, a key feature of this International Standard is the inclusion of "establishing the context" as an activity at the start of this generic risk management process. Establishing the context will capture the objectives of the organization, the environment in which it pursues those objectives, its stakeholders and the diversity of risk criteria – all of which will help reveal and assess the nature and complexity of its risks.

The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in this International Standard are shown in Figure 1 below.

When implemented and maintained in accordance with this International Standard, the management of risk enables an organization to, for example:

- *— increase the likelihood of achieving objectives;*
- *— encourage proactive management;*
- *— be aware of the need to identify and treat risk throughout the organization;*
- *— improve the identification of opportunities and threats;*
- *— comply with relevant legal and regulatory requirements and international norms;*
- *— improve mandatory and voluntary reporting;*
- *— improve governance;*
- *— improve stakeholder confidence and trust;*
- *— establish a reliable basis for decision making and planning;*
- *— improve controls;*
- *— effectively allocate and use resources for risk treatment;*
- *— improve operational effectiveness and efficiency;*
- *— enhance health & safety performance, as well as environmental protection;*
- *— improve loss prevention and incident management;*
- *— minimize losses;*
- *— improve organizational learning; and*
- *— improve organizational resilience.*

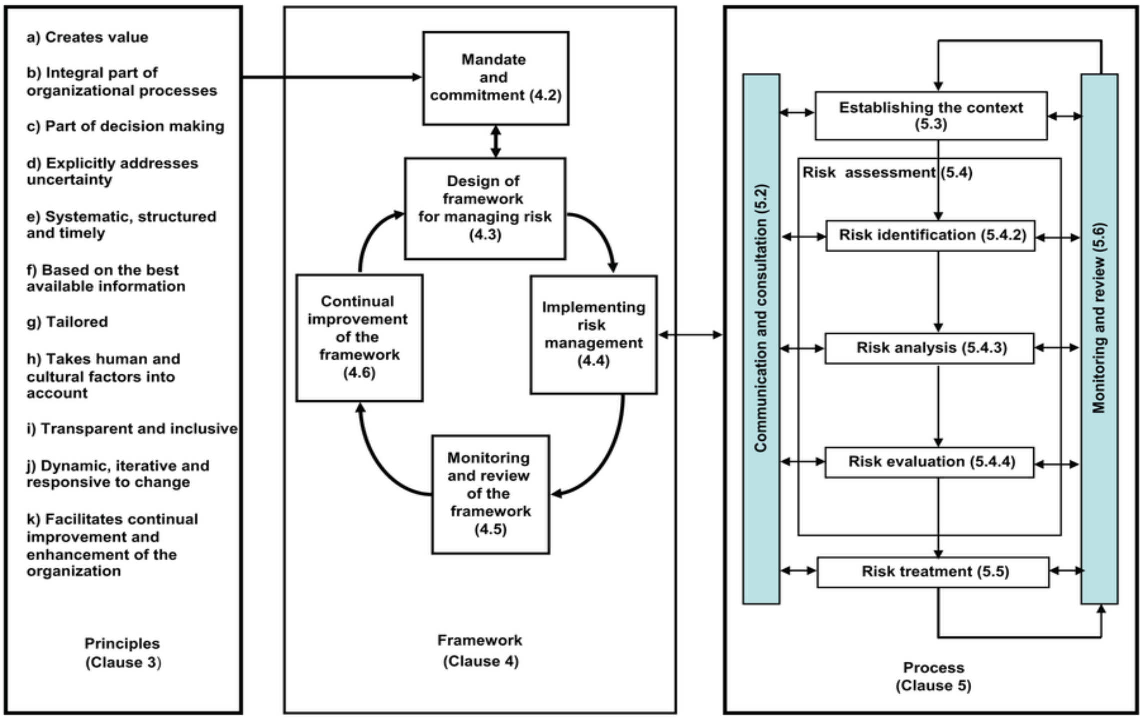
This International Standard is intended to meet the needs of a wide range of stakeholders, including:

- *a) those responsible for developing risk management policy within their organization;*
- *b) those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;*
- *c) those who need to evaluate an organization's effectiveness in managing risk; and*
- *d) developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed within the specific context of these documents.*

The current management practices and processes of many organizations include components of risk management, and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. In such cases, an organization can decide to carry out a critical review of its existing practices and processes in the light of this International Standard.

In this International Standard, the expressions "risk management" and "managing risk" are both used. In general terms, "risk management" refers to the architecture (principles, framework and process) for managing risks effectively, while "managing risk" refers to applying that architecture to particular risks.

Figure 1 — Relationships between the risk management principles, framework and process



a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Principles (Clause 3)
Mandate and commitment (4.2)
Design of framework for managing risk (4.3)
Implementing risk management (4.4)
Monitoring and review of the framework (4.5)
Continual improvement of the framework (4.6)
Framework (Clause 4)
Communication and consultation (5.2)
Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Monitoring and review (5.6)
Process (Clause 5)

1 Scope

This International Standard provides principles and generic guidelines on risk management.

This International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.

NOTE For convenience, all the different users of this International Standard are referred to by the general term "organization".

This International Standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

This International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that this International Standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

This International Standard is not intended for the purpose of certification.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
risk
effect of uncertainty on objectives
Note 1 to entry: An effect is a deviation from the expected — positive and/or negative.
Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
Note 3 to entry: Risk is often characterized by reference to potential ***events*** *(2.17) and* ***consequences*** *(2.18), or a combination of these.*
Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated ***likelihood*** *(2.19) of occurrence.*
Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.
[SOURCE: ISO Guide 73:2009, definition 1.1]
2.2
risk management
coordinated activities to direct and control an organization with regard to ***risk*** *(2.1)*
[SOURCE: ISO Guide 73:2009, definition 2.1]
2.3
risk management framework
set of components that provide the foundations and organizational arrangements for designing, implementing, ***monitoring*** *(2.28), reviewing and continually improving* ***risk management*** *(2.2) throughout the organization*
Note 1 to entry: The foundations include the policy, objectives, mandate and commitment to manage ***risk*** *(2.1).*
Note 2 to entry: The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.
Note 3 to entry: The risk management framework is embedded within the organization's overall strategic and operational policies and practices.
[SOURCE: ISO Guide 73:2009, definition 2.1.1]
2.4
risk management policy
statement of the overall intentions and direction of an organization related to ***risk management*** *(2.2)*
[SOURCE: ISO Guide 73:2009, definition 2.1.2]
2.5
risk attitude
organization's approach to assess and eventually pursue, retain, take or turn away from ***risk*** *(2.1)*
[SOURCE: ISO Guide 73:2009, definition 3.7.1.1]
2.6
risk management plan
scheme within the ***risk management framework*** *(2.3) specifying the approach, the management components and resources to be applied to the management of* ***risk*** *(2.1)*

Note 1 to entry: Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.
Note 2 to entry: The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.
[SOURCE: ISO Guide 73:2009, definition 2.1.3]

2.7
risk owner
*person or entity with the accountability and authority to manage a **risk** (2.1)*
[SOURCE: ISO Guide 73:2009, definition 3.5.1.5]

2.8
risk management process
*systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, **monitoring** (2.28) and reviewing **risk** (2.1)*
[SOURCE: ISO Guide 73:2009, definition 3.1]

2.9
establishing the context
*defining the external and internal parameters to be taken into account when managing risk, and setting the scope and **risk criteria** (2.22) for the **risk management policy** (2.4)*
[SOURCE: ISO Guide 73:2009, definition 3.3.1]

2.10
external context
external environment in which the organization seeks to achieve its objectives
Note 1 to entry: External context can include:

- *— the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;*
- *— key drivers and trends having impact on the objectives of the organization; and*
- *— relationships with, and perceptions and values of external **stakeholders** (2.13).*

[SOURCE: ISO Guide 73:2009, definition 3.3.1.1]

2.11
internal context
internal environment in which the organization seeks to achieve its objectives
Note 1 to entry: Internal context can include:

- *— governance, organizational structure, roles and accountabilities;*
- *— policies, objectives, and the strategies that are in place to achieve them;*
- *— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);*
- *— information systems, information flows and decision-making processes (both formal and informal);*
- *— relationships with, and perceptions and values of, internal stakeholders;*
- *— the organization's culture;*
- *— standards, guidelines and models adopted by the organization; and*
- *— form and extent of contractual relationships.*

[SOURCE: ISO Guide 73:2009, definition 3.3.1.2]

2.12
communication and consultation

continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with ***stakeholders*** *(2.13) regarding the management of* ***risk*** *(2.1)*
Note 1 to entry: The information can relate to the existence, nature, form, ***likelihood*** *(2.19), significance, evaluation, acceptability and treatment of the management of risk.*
Note 2 to entry: Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

- *— a process which impacts on a decision through influence rather than power; and*
- *— an input to decision making, not joint decision making.*

[SOURCE: ISO Guide 73:2009, definition 3.2.1]
2.13
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
Note 1 to entry: A decision maker can be a stakeholder.
[SOURCE: ISO Guide 73:2009, definition 3.2.1.1]
2.14
risk assessment
overall process of ***risk identification*** *(2.15),* ***risk analysis*** *(2.21) and* ***risk evaluation*** *(2.24)*
[SOURCE: ISO Guide 73:2009, definition 3.4.1]
2.15
risk identification
process of finding, recognizing and describing ***risks*** *(2.1)*
Note 1 to entry: Risk identification involves the identification of ***risk sources*** *(2.16),* ***events*** *(2.17), their causes and their potential* ***consequences*** *(2.18).*
Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and ***stakeholder's*** *(2.13) needs.*
[SOURCE: ISO Guide 73:2009, definition 3.5.1]
2.16
risk source
element which alone or in combination has the intrinsic potential to give rise to ***risk*** *(2.1)*
Note 1 to entry: A risk source can be tangible or intangible.
[SOURCE: ISO Guide 73:2009, definition 3.5.1.2]
2.17
event
occurrence or change of a particular set of circumstances
Note 1 to entry: An event can be one or more occurrences, and can have several causes.
Note 2 to entry: An event can consist of something not happening.
Note 3 to entry: An event can sometimes be referred to as an “incident” or “accident”.
Note 4 to entry: An event without ***consequences*** *(2.18) can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.*
[SOURCE: ISO Guide 73:2009, definition 3.5.1.3]
2.18
consequence
outcome of an ***event*** *(2.17) affecting objectives*
Note 1 to entry: An event can lead to a range of consequences.
Note 2 to entry: A consequence can be certain or uncertain and can have positive or negative effects on objectives.
Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 4 to entry: Initial consequences can escalate through knock-on effects.

[SOURCE: ISO Guide 73:2009, definition 3.6.1.3]

2.19

likelihood

chance of something happening

Note 1 to entry: In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

[SOURCE: ISO Guide 73:2009, definition 3.6.1.1]

2.20

risk profile

description of any set of ***risks*** *(2.1)*

Note 1 to entry: The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

[SOURCE: ISO Guide 73:2009, definition 3.8.2.5]

2.21

risk analysis

process to comprehend the nature of ***risk*** *(2.1) and to determine the* ***level of risk*** *(2.23)*

Note 1 to entry: Risk analysis provides the basis for ***risk evaluation*** *(2.24) and decisions about* ***risk treatment*** *(2.25).*

Note 2 to entry: Risk analysis includes risk estimation.

[SOURCE: ISO Guide 73:2009, definition 3.6.1]

2.22

risk criteria

terms of reference against which the significance of a ***risk*** *(2.1) is evaluated*

Note 1 to entry: Risk criteria are based on organizational objectives, and ***external*** *(2.10) and* ***internal context*** *(2.11).*

Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other requirements.

[SOURCE: ISO Guide 73:2009, definition 3.3.1.3]

2.23

level of risk

magnitude of a ***risk*** *(2.1) or combination of risks, expressed in terms of the combination of* ***consequences*** *(2.18) and their* ***likelihood*** *(2.19)*

[SOURCE: ISO Guide 73:2009, definition 3.6.1.8]

2.24

risk evaluation

process of comparing the results of ***risk analysis*** *(2.21) with* ***risk criteria*** *(2.22) to determine whether the* ***risk*** *(2.1) and/or its magnitude is acceptable or tolerable*

Note 1 to entry: Risk evaluation assists in the decision about ***risk treatment*** *(2.25).*

[SOURCE: ISO Guide 73:2009, definition 3.7.1]

2.25

risk treatment

process to modify ***risk*** *(2.1)*

Note 1 to entry: Risk treatment can involve:

- *— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;*
- *— taking or increasing risk in order to pursue an opportunity;*
- *— removing the **risk source** (2.16);*
- *— changing the **likelihood** (2.19);*
- *— changing the **consequences** (2.18);*
- *— sharing the risk with another party or parties (including contracts and risk financing); and*
- *— retaining the risk by informed decision.*

Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".
Note 3 to entry: Risk treatment can create new risks or modify existing risks.
[SOURCE: ISO Guide 73:2009, definition 3.8.1]

2.26
control
*measure that is modifying **risk** (2.1)*
Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.
Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.
[SOURCE: ISO Guide 73:2009, definition 3.8.1.1]

2.27
residual risk
***risk** (2.1) remaining after **risk treatment** (2.25)*
Note 1 to entry: Residual risk can contain unidentified risk.
Note 2 to entry: Residual risk can also be known as "retained risk".
[SOURCE: ISO Guide 73:2009, definition 3.8.1.6]

2.28
monitoring
continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected
*Note 1 to entry: Monitoring can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk** (2.1) or **control** (2.26).*
[SOURCE: ISO Guide 73:2009, definition 3.8.2.1]

2.29
review
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
*Note 1 to entry: Review can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk** (2.1) or **control** (2.26).*
[SOURCE: ISO Guide 73:2009, definition 3.8.2.2]