ENTERPRISE RISK MANAGEMENT

A GUIDE TO NAVIGATING RISKS AND UNCERTAINTY

@SurreyPlaceON

SURREY PLACE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

"Risk is now defined as the "effect of uncertainty on objectives", which focuses on the effect of incomplete knowledge of events or circumstances on an organization's decision-making."

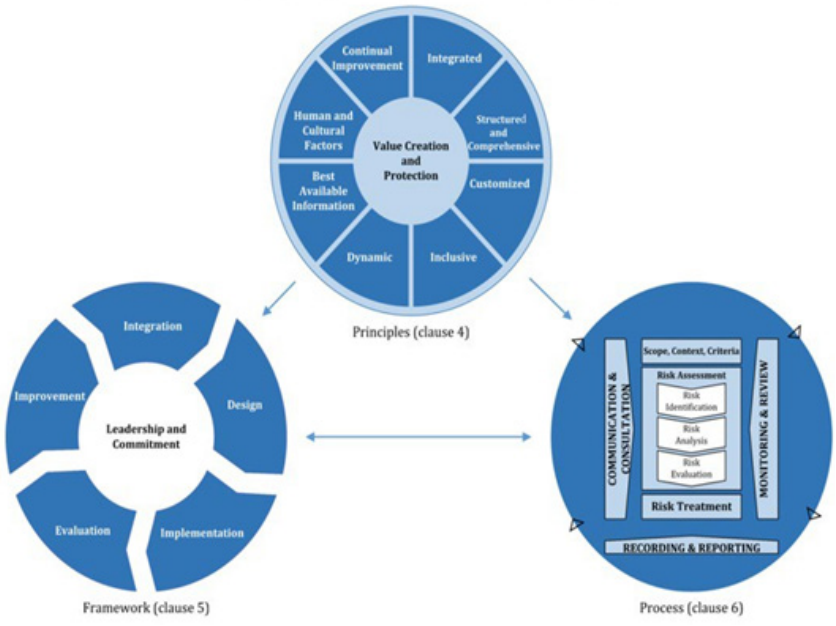
The new definition entails a paradigm shift from the traditional understanding and dealing with risks towards a more adaptable and iterative mitigation framework. With the ever-changing landscape in serving the IDD population, Risk Management is a valuable tool to help us think through what might happen as we position ourselves to harness the present and embrace the future.

In order to fully leverage the guidance of ISO 31000 Risk Management Guideline, we have adapted and tailored the standard to fit our organization's objectives. The content of this document is organized around the PRINCIPLES, FRAMEWORK and PROCESS, to guide the user through the steps of risk communication, consultation, identification, mitigation, reporting, monitoring and review.

The two other principles in the 2009 version of the ISO 31000 that are aligned to our practices are also adapted in our Guide, such as "Risk Management is part of our decision-making," and "Risk Management explicitly addresses uncertainty." These two principles represent our strengths and they are the cornerstone for all the changes in how we will be managing risks.

This is a living document and follows the iterative model of the standard. It will not remain static but will be progressively elaborated so we can be agile and nimble in responding to risks. Using ISO 31000 can help us increase the likelihood of achieving our objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment. Risk Management along with the other strategies and operational framework we developed will create the necessary conditions for us to be always true to our Mission as we navigate to changes, risks, and uncertainties.

Figure 1 — Principles, framework and process



1. INTRODUCTION

WHAT IS RISK MANAGEMENT?

Risk is the effect of uncertainty on objectives with a likelihood and frequency that something will occur. Risk is expressed in terms of consequences or impact (How bad will an event be if it happens?) and likelihood (How likely is it that the event will happen?).

As the outcomes of operational, clinical, andbusiness activities can be uncertain, they are said to have some element of risk. In the health context, risks can contribute to strategic failures, operational failures, failures in quality and safety systems, financial failures, major environmental or public health incidents, deficiencies or ineffective equipment or failures in regulatory compliance.

Risk management is an integral part of good management practice that should be embedded within all business processes. It involves identifying the types of risk exposure within an organization, measuring those potential risks and proposing means to mitigate them. While it is impossible to remove all risk, it is important to understand our organizational risks and manage and identify the level of risk we are willing to accept in the overall context of effective operation and service provision.

Risk management is essential to good management practice and effective corporate governance and ensures decisions are made with enough information about risks and opportunities.

"Risk management is an integral part of good management practice that should be embedded within all business processes."

BENEFITS OF RISK MANAGEMENT

Strategy planning

- Establishing a clear link between objectives, risks and selected strategic initiatives.
- Aligning project participants to organisational priorities.
- Supporting decision making and efficient resource allocation.

Risk reporting

- Avenue for continuously communicating the "real risks".
- Opportunity for a pragmatic risk management policy and process documentation.

Formalizing risk response

- Developing formal action plans and risk measures for risks falling outside the acceptable tolerance levels.
- Identifying risk champions responsible for the overall implementation and monitoring of risk mitigation plans.
- Bringing focus to future risk-related initiatives (internal audit, project risk management, business continuity planning, etc.).

Risk culture and ownership

- Increasing risk culture and ownership at all levels of the organisation thus enhancing the organisation's ability to understand, identify and proactively manage risks.
- Improving cross-functional risk identification and cross-departmental communication.

Table 1 - Adapted from Deloitte, Benefits of Enterprise Risk Management

2. LEVELS OF RESPONSIBILITY

There are three levels of responsibility with respect to risk management, as depicted in the figure below. At the apex lies the responsibility for risk governance, including strategic guidance and risk oversight, which rests with the Board of Directors. In the middle lies the responsibility for risk infrastructure and management, including designing, implementing and maintaining an effective risk program, led by executive management. At the base lies the responsibility for risk ownership, including identifying, measuring, monitoring and reporting on specific risks, led by the business units and functions.

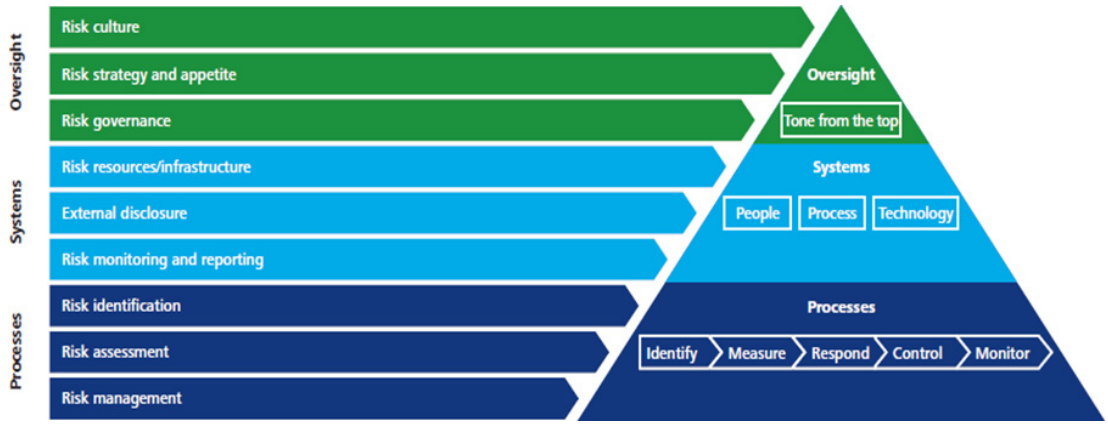


Figure 2: Deloitte Risk Management Model

Boards and management use a top-down approach to understand risk at a strategic level, while risk owners in the business units and functions use a bottom-up approach to identify and monitor specific risks, escalate concerns and generate the risk-related data to inform leadership's strategic view.

Risk Governance	**Board of Directors (and the Audit Committee)** • Foster a risk Intelligent culture • Approve risk appetite • Ratify key components of the Enterprise Risk Management (ERM) programme • Discuss enterprise risks with executive management			
Risk Infrastructure and Management	**Executive management:** • Define the risk appetite • Evaluate proposed strategies against risk appetite • Provide timely risk-related information	**Enterprise risk group:** • Aggregate risk information • Identify and assess enterprise risks • Monitor risks and risk response plans	**Internal Audit:** • Provide assurance on effectiveness of the ERM programme, and the controls and risk response plans for significant risks	**Risk Management:** • Create a common risk framework • Provide direction on applying framework • Implement and manage technology systems • Provide guidance and training
Risk Ownership	**Business units:** • Take intelligent risks • Identify and assess risks • Respond to risks • Monitor risks and report to enterprise risk group		**Support functions:** • Provide guidance/support to the enterprise risk group and business units	

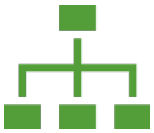
Figure 3: Deloitte Risk Management Model, showing top down and bottom up approaches

3. PRINCIPLES

Our risk management approach and processes are based on the following principles adapted from ISO 31000:2009 and 31000:2018.

a. **Risk management creates and protects value** – Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, service quality, project management, efficiency in operations, governance, and reputation.

b. **Risk management is an integral part of organizational processes** - Risk management is an integral part of all organizational activities. Risk management is not a stand-alone activity that is separate from main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of organizational processes, including strategic planning and all project and change management processes.



c. **Risk management is part of decision-making** – Risk management helps decision-makers make informed choices, prioritize actions and distinguish among alternative courses of action.

d. **Risk management explicitly addresses uncertainty** – Risk management explicitly takes account of uncertainty, and how it can be addressed.

e. **Risk management is systematic, structured and timely** – A systematic, timely, structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

f. **Risk management is based on the best available information** – The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts, and expert judgment. However, decision makers should inform themselves of, and should consider, any limitations of the data or modeling used or the possibility of divergence among experts.

g. **Risk management is tailored** – Risk management is aligned with the organization's external and internal context and risk profile.

h. **Risk management takes human and cultural factors into account** – Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.

i. **Risk management is transparent and inclusive** – Appropriate and timely involvement of stakeholders and, decision makers at all levels of the organization, ensures that risk management remains relevant and up to date. Involvement also allows stakeholders to be properly represented and to have their views considered un determining risk criteria.

j. **Risk management is dynamic, iterative and responsive to change** – Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place new risks emerge, some change and others disappear.

k. **Risk management facilitated continual improvement of the organization** – Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.

4. FRAMEWORK

GENERAL

The purpose of the risk management framework is to assist the organization in integrating risk management into significant activities and functions. The effectiveness of risk management will depend on its integration into governance of the organization including decision-making. This requires support from stakeholders, particularly top management. Risk management will be embedded within daily operations, from strategy and policy formulation through business and clinical planning, general management and operational processes. It will also be applied where Surrey Place works in partnership with other organizations to ensure that partnership risks are identified and managed appropriately.

LEADERSHIP and COMMITMENT

Surrey Place's risk management governance and culture are founded on our vision, mission, values, objectives, strategies and policies. The Board and Senior Management are the bodies mainly responsible to ensure that the risk management is integrated into all organizational activities. At a high level the following are the expectations from our leaders:

Figure 4- ISO 31000:2018 Framework

- Customizing and implementing all components of the framework.
- Issuing a policy that established a risk management approach, plan or course of action
- Ensuring that the necessary resources are allocated to managing risk
- Assigning authority, responsibility and accountability at appropriate levels within the organization

This helps Surrey Place to:

- Align risk management with its objectives, strategy and culture
- Recognize and address all obligations, as well as its voluntary commitments
- Establish the amount and types of risk that may or may not be taken to guide the development of risk criteria, ensuring that they are communicated across the organization

- Communicate the value of risk management to the organization and its stakeholder
- Promote systematic monitoring of risks
- Ensure that the risk management framework remains appropriate to the context of the organization

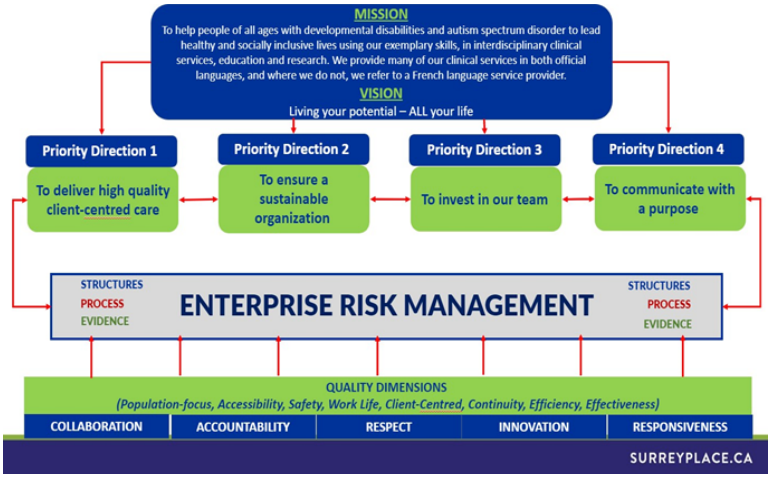
Senior management is accountable for managing risk while oversight bodies are accountable for overseeing risk management. Oversight bodies are expected or required to:

- Ensure that risks are adequately considered when setting the organization's objectives;
- Understand the risks facing the organization in pursuit of its objectives;
- Ensure that systems to manage such risks are implemented and operating effectively;
- Ensure that such risks are appropriate in the context of the organization's objectives;
- Ensure that information about such risks and their management is properly communicated.

INTEGRATION

Risk is managed in every part of the organization's structure. Everyone in the organization has responsibility for managing risk. Governance guides the course, its external and internal relationships, and the rules, processes and practices needed to achieve its purpose.

Management structures translate governance direction into strategy and associated objectives required to achieve desired levels of sustainable performance and long-term viability. Determining risk management accountability and oversight roles within an organization are integral parts of our governance.



Integrating risk management into Surrey Place is a dynamic and iterative process considering our needs and culture. Risk management is part of and not separate from the organizational purpose, governance, leadership and commitment, strategy, objectives, and operations.

Figure 6, below is an example of an integrated approach to managing risk:

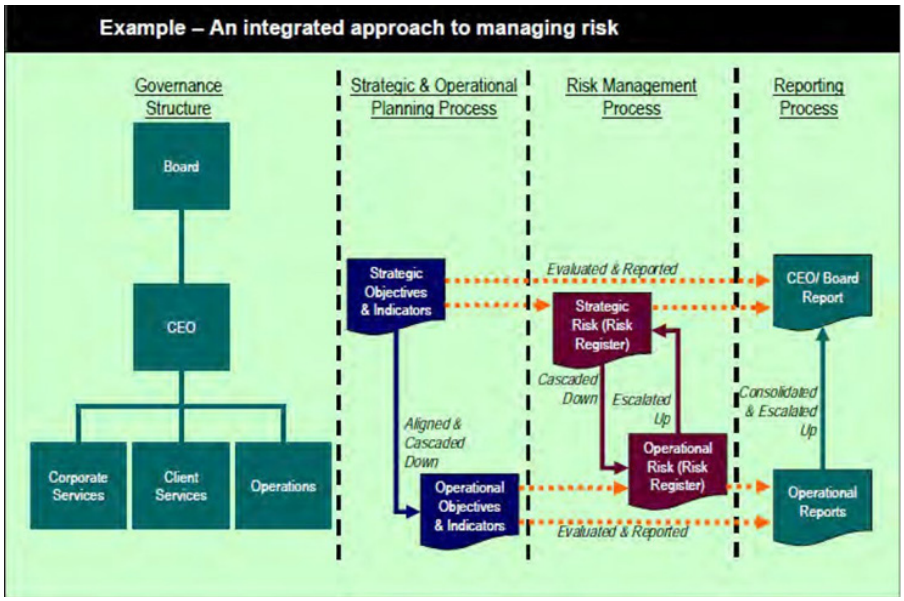


Figure 6 – Integral Approach to Risk Management

Based on Surrey Place's governance structure, and strategic and operational planning process, strategic objectives and indicators are determined at the organizational-level and cascaded down as operational objectives and indicators into various units like Corporate Services, Clinical Programs, and Operations. Strategic risks are linked to the achievement of the Surrey Place's strategic objectives and indicators. Likewise, operational risks are linked to the achievement of operational objectives and indicators.

There are objective criteria in the risk management policy for:

- Escalating operational, new or emerging risks bottom-up from operations to management and/or Board
- Cascading down strategic risk for operational/departmental/program manager's attention

Surrey Place's risk register include both strategic and operational risks.

Regular operational reports include report on the progress of operational risk treatment plans and any potential new operational risk. Operational reports are consolidated upwards whereby the nature and volume of risk information required to be reported at various organizational levels (including the Board level) and from various locations (satellite offices/partner sites) are determined.

DESIGN

Understanding the organization and its context

External Context

- The social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors whether international, national, regional, local
- Who are the key drivers? What are the trends that affect the objectives of the organization?
- Who are the external stakeholders? How is our relationship with them? What are their perceptions, values, needs and expectations?
- How is our contractual relationship? What are the commitments that need to be fulfilled?
- How complex is our network its dependencies?

SurreyPlace

Internal Context

- the vision, mission, values
- governance structure, organizational structure, roles and accountabilities;
- strategy, objectives and policies
- the organization's culture
- Are we meeting the standards, guidelines, and models that we have adopted as an organization?
- What are our capabilities, in terms of resources and knowledge? (capital, time, people, intellectual property, processes, systems and technologies)
- What type of data do we collect? What type of data can we collect? How is our information system? How is the flow of information in our organization?
- How is our relationship with our internal stakeholders? Do we take into account their perceptions and values?
- How is our contractual relationship? What are the commitments that need to be fulfilled?
- What are the interdependencies and interconnections within the organization?

Figure 7 – shows the interplay of internal and external context

Manifesting risk management commitment

Our top Management and oversight bodies continually articulate their commitment to risk management through our policies and ensuring that different tables discuss and report risks and mitigation strategies. This commitment is further manifested by:

- reiterating the organization's purpose for managing risk ad links to its objectives and other policies in different tables;
- reinforcing the need to integrate risk management into the overall culture
- leading the integration of risk management into core business activities and decision-making;
- defining responsibilities and accountabilities
- providing the necessary resources available;
- dealing with conflicting objectives;
- measuring and reporting within the organization' performance indicators;
- continuous review and improvement

The risk management commitment is communicated within the organization and to stakeholders through meetings and discussion in different tables.

Allocating resources

Our top management and oversight bodies ensured that appropriate resources are allocated for risk management that include, but are not limited to:

- people, skills, experience and competence
- organization's processes, methods, and tools to be used for managing risk;
- documenting processes and procedures;
- information and knowledge management systems;
- professional development and training needs.
- The findings on Risks, Quality and Safety reports serve as inputs to the organization's budget allocation.

GENERIC DUTIES AND RESPONSIBILITIES

Main Duties	Board of Directors	Executive Team	Clinical Directors/ Department Heads	Other Managers	All Staff
Strategy & Policy	• Determine SP vision, mission, values • Set corporate strategy • Provide leadership	• Develop and oversee the implementation of strategic plans • Develop and communicate corporate objectives • Proactively anticipate risk • Provide leadership and guidance to employees, business partners and stakeholders	• Develop and implement clinical strategy • Alignment of program objectives to Surrey Place strategy	• Alignment of team/personal objectives to Surrey Place strategy	• Deliver personal objectives • Abide by Surrey Place values and behaviours
Organize	• Establish an effective risk management system • Establish and keep under review the Board's appetite for taking risk • Focus on material risk and proactive anticipation of future risk	• Develop and apply risk management process • Accept and allocate ownership for risk • Share ownership for cross-enterprise risk	• Apply Risk Management Process • Accept and allocate ownership for risk • Proactively anticipate risk • Provide leadership and guidance	• Apply Risk Management Process • Accept and allocate ownership for risk • Proactively anticipate risk • Provide leadership and guidance	• Follow Risk anagement Process • Accept ownership for risk
Plan & Control	• Decide what opportunities, present or future, the Board wants to pursue and what risks it is willing to take in developing the opportunities selected, routinely, • Robustly and regularly scan the horizon for emergent opportunities and threats by anticipating future risks • Decide whether or not a risk can be accepted • Simultaneously drive the business forward whilst making decisions which keep risk under prudent control	• Design, apply and monitor the operation of controls to ensure the achievement of objectives and promote organizational success • Ensure failure does not disable – contingencies are in place and tested for all reasonably foreseeable situations • Allocate, structure and prioritize resources within and across divisions or directorates so that risk is managed in accordance with the Board's risk appetite	• Design and apply controls to manage risk in line with the Board's appetite for taking risk • Prepare risk management mitigation plans • Ensure adequate emergency preparedness and contingencies for foreseeable disruptive events. • Manage resources to optimum effect • Develop policies, guidelines, procedures and standards to govern the management of program risks.	• Design and apply controls to manage risk in line with the Board's appetite for taking risk • Remain alert to risk • Manage resources to optimum effect • Develop and implement risk management plan	• Undertake and keep up to date with mandatory training and other relevant training • Follow policies, clinical standards and relevant procedures • Act on lessons for learning

Main Duties	Board of Directors	Executive Team	Clinical Directors/ Department Heads	Other Managers	All Staff
Monitor	• Keep under review material risk exposures that are not accepted by the Board at each formal meeting	• Challenge, support, supervise and hold colleagues to account for performance and continuous improvement	• Monitor the operation of controls and address identified gaps in control	• Supervise the work of others to ensure controls are applied correctly	• Report concerns, adverse events or failures to contain risk adequately
Audit	• Determine Audit priorities using a risk- based approach • Take account of reports from the Audit Committee	• Determine Audit Priorities using a risk- based approach • Assist internal audit where required and ensure recommendations are acted upon by relevant colleagues • Account for control of risk to the Audit Committee where required	• Assist Internal Audit where required and ensure recommendations are acted upon by relevant colleagues • Account for control of risk to the Audit Committee where required • Undertake appropriate inspection/checks of controls for safety critical procedures	• Cooperate fully an assist internal audit • Challenge recommendations if they are not agreed • Develop and implement changes in practice within the timescales agreed • Report when concluded	• Cooperate with internal audit and act on their findings • Carry out instructions based on agreed audit recommendations
Review	• Effectively hold those responsible for managing risk to account for performance and continuous improvement. • Take decisions	• Report to the Board all material risks and significant gaps in control	• Report to the Board all material risks and significant gaps in control		

Table 2 – shows how risk management duties and responsibilities will be shared across the organization

Establishing communication and consultation

Currently the approved and more effective approach to communication is through participation in different meetings/discussion where feedback is gathered right away from the targeted audience. These feedback shape decisions and influence activities. At each step of the risk management process, information is delivered in accordance with internal policy, confidentiality, resect to individual's private date, and integrity of sensitive information is maintained. Information is be presented to key stakeholders in a timely, accurate, and factual way.

IMPLEMENTATION

Successful implementation of the Risk Mangement Framework requires engagement and awareness of stakeholders. This enables Surrey Place to explicitly address uncertainty in decision-makingm while also ensuring that any new or subsequent uncertainty can be taken into account as it arises.

The current implementation plan ensures that the risk management process is connected not only to the organization's mission, vision, values and strategic directions but also to part of our Quality Improvement Plan, Clinical Programs, and Operational departments goals and objectives and policies.

As a result of a document review, the table below shows how risk management is referenced in Surrey Place documents:

Human Resources/Staff Safety

Title of Policy/Procedures	Reference Surrey Place Documents	Risk Management Scope
1. Employee Incident and Accident Investigation reporting	• Organization Manual	• Risk identification/Analysis/ Control/Prevention
2. Organizational Health and Safety Policy for Clients and Staff	• Clinical/Organization Manual	• Risk Control/Prevention
3. Occupational Health and Safety	• Clinical/Organization Manual	• Risk Control/Prevention
4. Trip & Falls Prevention	• Organization Manual	• Risk Control/Prevention
5. Health & Safety Information for Visitors and Contractors	• Organization Manual	• Risk Control/Prevention
6. Ergonomic Policy	• Organization Manual	• Risk Control/Prevention
7. WHMIS Policy	• Organization Manual	• Risk Control/Prevention
8. Workplace Inspection	• Organization Manual	• Risk identification/Analysis/ Control/Prevention

Clinical Risks

Title of Policy/Procedures	Reference Surrey Place Documents	Risk Management Scope
9. MCSS Serious Occurrence Reporting	• Clinical Manual	• Risk identification/Risk Analysis
10. MCSS Enhanced Serious Occurrence Reporting	• Clinical Manual	• Risk identification/Risk Analysis
11. Client Incident Reporting	• Clinical Manual	• Risk Identification
12. Abuse and Sensitive Case Reporting	• Clinical Manual	• Risk Identification
13. Reporting and Disclosure of Adverse Events	• Clinical Manual	• Risk Identification
14. Consent to Treatment	• Clinical Manual	• Risk Identification
15. Abuse Policy: MARC (PACT Training) Protecting our client's guidelines for agencies handling allegations of abuse	• Clinical Manual	• Risk Identification
16. Suicide Policy	• Clinical Manual	• Risk Identification
17. Infection Control	• Clinical/Organization Manual	• Risk Control & Prevention Risk Identification

Non-Clinical/Administrative Risk

Title of Policy/Procedures	Reference Surrey Place Documents	Risk Management Scope
18. Emergency Preparedness	• Handbook/Agency Manual	• Risk Control/Prevention
19. Safety Administration Team Guidelines	• Organization Manual	• Risk Control/Prevention
20. Business Continuity Plan	• Organization Manual	• Risk Control/Prevention
21. Pandemic Plan	• Organization Manual	• Risk Control/Prevention

Non-Clinical/Administrative Risk

Title of Policy/Procedures	Reference Surrey Place Documents	Risk Management Scope
22. Purchasing Policy	• Organization Manual	• Risk Control/Prevention
23. Cash Disbursement Policy	• Organization Manual	• Risk Control/Prevention
24. HIROC Insurance Coverage		• Risk Claims Management
25. Annual Risk Self-Assessment Financial Audit		• Risk Identification
26. Annual Financial audit		• Risk Assessment/Analysis
27. MCSS/MCYS Risk Assessment Tools		• Risk Assessment/Analysis
28. Broader Public Sector Policy		

EVALUATION

In order to evaluate the effectiveness of the risk management framework, Surrey Place through the Quality & Performance and Research & Evaluation Departments will:

- Periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behavior;
- Determine whether it remains suitable to support achieving the objectives of the organization.

Communication is a two-way system, feedback from stakeholders is important during the Evaluation Stage.

IMPROVEMENT

Adapting

Surrey Place will continually monitor and adapt risk management framework to address external and internal changes. In doing so, the organization can improve its value.

Continually improving

Surrey Place will continually improve the suitability, adequacy and effectiveness of the risk management framework and the way risk management process is integrated.

As relevant gaps or improvement opportunities are identified, the organization will develop plans and tasks and assign them to those

accountable for implementation. Once implemented, these improvements should contribute to the enhancement of risk management.

5. PROCESS

GENERAL

The risk management process involves the systematic application of policies, procedures and practices to activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk. The process is illustrated in Figure 4, below:

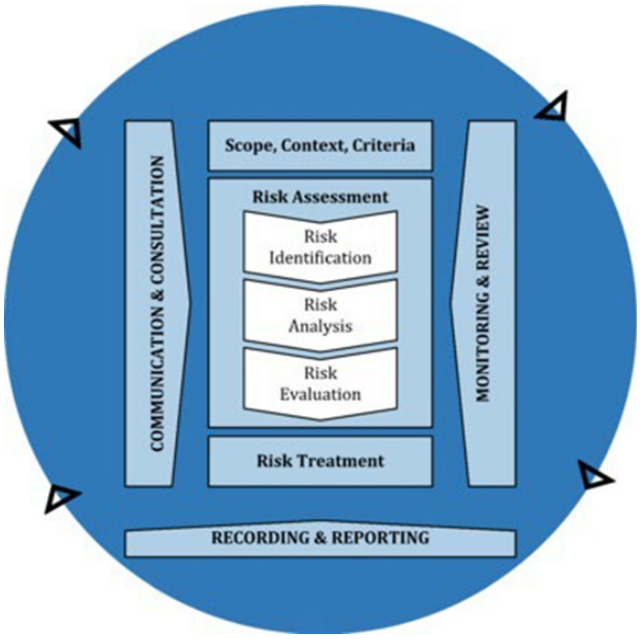


Figure 8- Risk Management Process from ISO 31000:2018

Although the risk management process is often presented as sequential, in practice it is iterative. It considers the dynamic and variable nature of human behavior and culture throughout the risk management process.

The risk management process is an integral part of management and decision making and integrated into the structure, process, and outcomes of the organization and applied at the strategic, program and project levels.

COMMUNICATION AND CONSULTATION

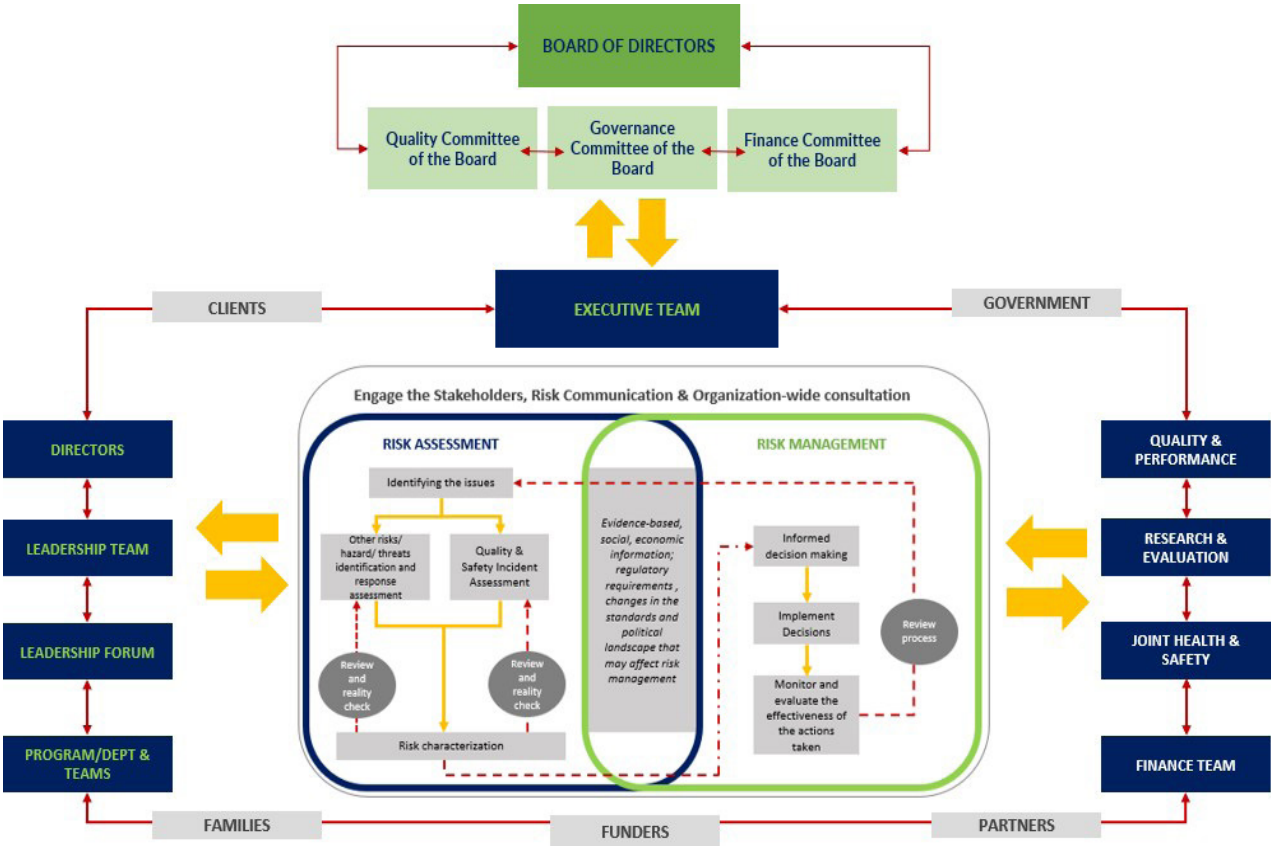


Figure 9 – Risk Communication and Consultation, adapted from enHealth.au, shows risk stakeholder engagement, communication and consultation are overarching components. This was tweaked further to highlight Surrey Place's risk communication cycle.

The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making. Close coordination between the two should facilitate factual, timely, relevant accurate and understandable exchange of information, considering the confidentiality and integrity of information as well as the privacy rights of individuals.

As shown in the figure above, communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process.

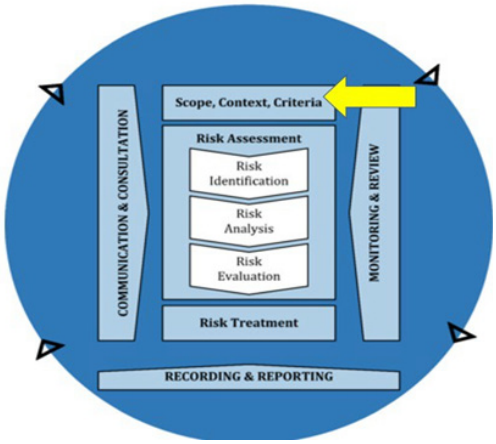
Communication and consultation are continual or iterative processes undertaken to provide, share or obtain information and to engage stakeholders about the management of risk. They are vital aspects of good risk management and should be used in each step of the risk management process. A consultative approach to the risk process will:

- Help establish the risk context appropriately
- Help ensure that the interests of stakeholders are understood and considered
- Help ensure that risks are adequately identified and defined
- Ensure a common understanding across the organization of the risks and strategies to address them
- Bring different areas of expertise together for analyzing risks
- Help ensure that different views are appropriately considered when defining risk criteria and in evaluating risks
- Secure endorsement and support for a treatment plan.
- Enhance appropriate change management during the risk management process

SCOPE, CONTEXT AND CRITERIA

Defining the Scope

In applying risk management across the organization, a well credentialed risk management frameworks need to be applied for all aspects of clients/families and clinicians' journey, strategic, operational, program, project and other activities. Such an approach provides, wherever possible, a transparent risk management approach more likely to have the wide support of stakeholders.



Surrey has adapted the ISO 31000:2018 Risk Management Standard. This handbook does not attempt to rewrite the standard but instead applies this to the context of services provision for IDD population in a community-based setting in a very practical way. The handbook outlines the most common risks and how these will be identified, treated, and assessed. Finally, this document also emphasizes the importance of communication, both internally and externally, throughout the risk assessment and management process.

In coming up the approach, the following were considered:

Types of services provided, and population served

Objectives and decisions that need to be made

Outcomes expected from the steps to be taken in the process

Time, allocation, specific inclusions and exclusions

Appropriate risk assessment tools and techniques

Resources required, responsibilities and records to be kept

Relationships with partners, processes and activities

Establishing the context

To establish the context, it is necessary to consider the strategic, organizational and risk management context in which risks will be managed. This means considering both the internal and external environment.

First consider the following three contexts for the organization:

STRATEGIC	Consider the relationship between the organization and its environment including reputational risk; identify the organization's strengths, weaknesses, opportunities and threats, consider elements that might support or impair the organization's ability to successfully manage risks.
ORGANIZATIONAL	Consider the organization and its capabilities, including goals and objectives, and the strategies in place to achieve them; align risk management with the organization's Service Agreement or business plans.
RISK MANAGEMENT	Consider the goals, objectives, strategies, scope and parameters of the risk management process, including the benefits, costs, and opportunities of risk management activities and the required resources

Questions that may assist in establishing the context include:

- What policy, program, process or activity?
- What are the KPIs?
- Who are the stakeholders?
- What are the major outcomes expected?
- What are the significant factors in the organization that have an impact on this area?
- What were the issues identified by previous reviews?
- What is the best way of restructuring risk identification?
- What risk criteria should be established?
- What are the cost and revenue considerations?

Risk Criteria and Categories

Surrey Place has specified the amount and type of risk that it may or may not take, relative to objectives. It has also defined the criteria to evaluate the significance of risk and to support decision-making processes. The risk criteria are aligned with the risk management framework and customized to the specific purpose and scope of the activity under consideration. The risk criteria reflect the organization's values, objectives and resources consistent with policies about risk management. The criteria are defined taking into consideration Surrey Place's obligations and the views of stakeholders.

The risk criteria established at the beginning of the risk assessment process are dynamic and will continually be reviewed and amended as necessary.

RISK CATEGORIES	SUB-CATEGORIES	DESCRIPTIONS
STRATEGIC RISK Potential events or circumstances that affect or are created by Surrey Place's strategic vision, priorities and goals. These circumstances may impact Surrey Place positively or negatively	**Reputation**	Activities or circumstances that impact Surrey Place's image or the long-term trust placed in us by stakeholders, partners, and community as leader. This may occur as a result of factors such as performance, strategy execution, or an activity, action or stance taken by Surrey Place and/or individuals aligned with Surrey Place.
	Research	Activities or circumstances that impact our research and performance.
	Innovation, Growth, and Partnerships, and Quality Outcomes	Activities or circumstances that impact innovation, growth and partnerships, and quality such as: • Collaborating with external partners • Strategic and competitive positioning • Educational offerings • Contractual agreements • Compliance to ROPs, standards

RISK CATEGORIES	SUB-CATEGORIES	DESCRIPTIONS
OPERATIONAL/ SERVICE DELIVERY RISK Activities carried out or circumstances relating to the day-to-day business of Surrey Place. They may be associated with structure, systems, people, services or processes. Managing operational risk protects value by avoiding adverse impacts. It also created value by optimizing positive outcomes.	**Business Disruption and System Failure**	Activities or circumstances that impact the continuity of business systems and operations, such as access to enterprise level critical systems or information
	Physical Assets	Activities or circumstances that impact our physical assets, such as facilities, buildings and infrastructure, such as: • Natural events • Security • Procurement and Utilization • Maintenance
	People/ Human Resources	Activities or circumstances that impact our people, such as: • Attraction, recruitment and retention • Managing, motivating and developing our people • Organizational culture
	Fraud (Internal/ External	Activities or circumstances that impact our integrity, such as: • Unethical behaviours • Corruption • Theft • Embezzlement • Money Laundering • Bribery • Extortion
	Information Technology/Cyber Security	Activities or circumstances that impact our technology and cyber security, such as: • Adequate systems and processes that protect critical and sensitive data • System crashing, hacking • Security breach • Adequate IT resources, software, etc.
	Health, Safety and Wellbeing	Activities or circumstances that impact the health, safety and well-being of our staff, clients, students, volunteers, visitors, and contractors, such as: • Maintaining a safe, healthy environment • Providing resources to support mental health • A strong safety culture • Maintenance of physical buildings and facilities

RISK CATEGORIES	SUB-CATEGORIES	DESCRIPTIONS
FINANCIAL RISK	**Not Applicable**	Activities carried out, or circumstances related to physical assets or financial resources, such as government support, funding from approved proposals, paid services, budget, accounting, reporting and disclosure, including internal control requirements, investments, capital and cash management, insurance, audit, financial investment decisions, etc.
LEGAL, COMPLIANCE & REGULATORY RISK	**Not Applicable**	Activities carried out, or circumstances related to compliance with laws and regulations. Conversely, activities or circumstances that do not comply with laws and regulations result in adverse impacts such as: fines, reputational damage, material financial loss, sanctions, penalties, stakeholder risk, loss or liability, criminal prosecution or inability to enforce contracts, etc.
CLINICAL SERVICES & CLIENT SAFETY	**Not Applicable**	Clinical KPI in Service Agreement; Clinical pathways and variance analysis; Clinical Quality Improvement and Clinical Practice Improvement; Transition to another program/service; Client safety including IPAC, medication safety, response to complaints an concerns about clinicians and near miss or incidents trends; Protection of clients (children and youth) and others who are unable to care for themselves while accessing services in Surrey Place

RISK ASSESSMENT

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risk assessment is conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary.

Risk identification

The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving its objectives. Relevant, appropriate and up-to- date information is important in identifying risks.

Surrey Place can use a range of techniques for identifying uncertainties that may affect one or more objectives. The following factors are taken into consideration when identifying risks:

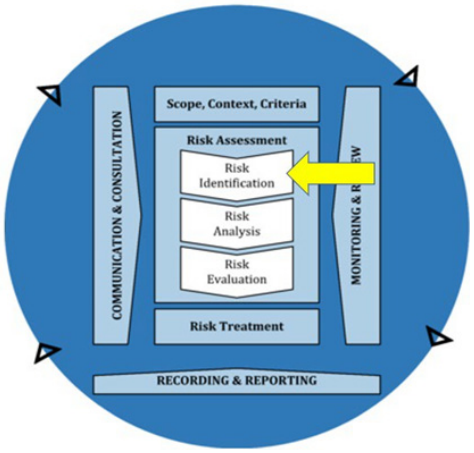


Figure 11 – ISO 31000:2018, Risk Management Process highlighting Risk Identification

• Tangible and intangible sources of risk	• The nature and value of assets and resources
• Causes and events	• Consequences and their impact on objectives
• Threats and opportunities	• Limitations of knowledge and reliability of information
• Vulnerabilities and capabilities	• Time-related factors
• Changes in the external and internal context	• Biases assumptions and beliefs of those involved
• Indicators of emerging risks	

*"Identifying risks involves asking: **What** can happen? and **How** can it happen?"*

Another way is using the following questions from HIROC to help identify significant risks:

- Is there the potential for significant impact on client care and/or safety?
- Is there the potential for significant impact on strategic objectives?
- Are there internal or emerging trends in healthcare
- that could result in exposure?
- Is there the potential for significant impact on financials?
- Does it require complex mitigation efforts?
- Are you working to prevent reoccurrence?
- Other

Identifying risks involves asking: “What can happen? And “How can it happen? To determine what can happen, it is necessary to compile a comprehensive list of events that might affect the organization, including sources of risk and areas affected.

The aim is to identify all risks regardless of whether they are within the control of the organization. The process needs to be systematic and structured, to ensure all potential risks have been identified and considered. The identification of risk can be by an individual or through a structured group process as described below:

Risk Identification Group	Examples
Structured risk and opportunity identification process	Department/Unit planning process; Risk workshops; Risk profiling; SWOT analysis; brainstorming; analysis of systems or scenarios
Risk identification through normal organization activities	Team meetings; Managers forum; Briefings; Informal ad hoc meetings; Routine date collection; Stakeholder feedback
Assessment against standards	Clinical quality reviews and audits; internal and external audits; accreditation reviews and other external reviews; Observation; JHSC safety rounds; Professional judgment
Incident or complaint	Adverse events and incident reporting; Patient complaints; Ombudsman
Internal investigation processes	Root cause analysis conduct investigations

Questions that may assist in identifying risks:

- What are we trying to achieve?
- What are our KPIs or performance criteria?
- What is going to stop us from achieving our KPIs or performance?
- What could help us to achieve it and how?
- What is in our way of getting there and why?
- How likely - what impact?
- What must be done?
- How much will/ may it cost?
- When should it be done?
- How quickly do we need to respond to prevent/reduce the impact if it does go wrong/ realize the opportunities?

- Who is the Risk Owner? Who is accountable for mitigation?
- What could go wrong? How it could go wrong
- What opportunities exist and how can they be realized?
- What resources do we already have to enable our actions to succeed?
- If required, can we obtain additional resources?
- Who else (internal/external stakeholders) needs to know or be involved?

Once risk is identified the risk needs to be described concisely, setting out what the risk is, what it is affecting, and how it impacts the objective/s. This description is important as it is where the risk story is told. It must make a reader understand the impact the risk has on the objectives. It should stand on its own and be able to be understood by those not necessarily familiar with the background detail. This in turn ensures a common understanding across different operational and management levels as to the nature and consequences of the risks.

Risk Analysis

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

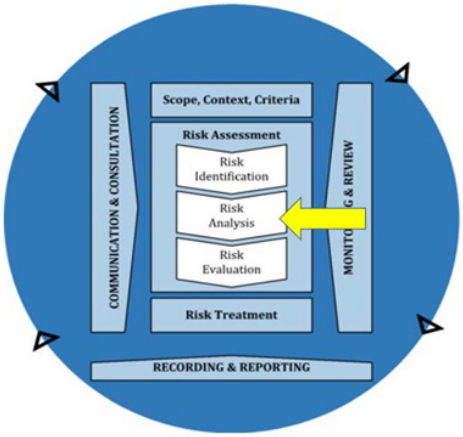


Figure 12 – ISO 31000:2018, Risk Management Process highlighting Risk Analysis

The risk analysis may be influenced by any divergence of opinions, biases, perceptions of risk and judgments.

Additional influences are the quality of information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed. These influences should be considered, documented and communicated to decision makers.

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made and the options involve different types and levels of risk.

A risk map (see figure 13), sometimes called a heat map is one of the most used methods to depict the largest risks facing an organization. It is usually visually appealing, and easy to understand and describe. It typically consists of two axes: vertical axis showing the potential impact of the risk and the horizontal axis showing estimated likelihood of the risk occurring – both usually measured on a scale of 1 (very low) to 5 (very high).

Figure 13 – Surrey Place's Heat Map adapted from HIROC

		Impact				
Likelihood		1 Very Low	2 Low	3 Medium	4 High	5 Very High
Very High	5	5	10	15	20	25
High	4	4	8	12	16	20
Medium	3	3	6	9	12	15
Low	2	2	4	6	8	10
Very Low	1	1	2	3	4	5

Risk Level:

1, 2, 3, 4	Low
5, 6, 8, 9, 10	Medium
12, 15, 16	High
20, 25	Very high

Questions that may assist when using the matrix:

- What are the potential adverse (threats) consequences of each risk if thy occur?
- What is the potential likelihood (probability) or frequency of the risks happening?
- What current controls exist to prevent, detect or correct the consequences or likelihood of the risk?

Risk Evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to:

- do nothing further;
- consider risk treatment options;
- undertake further analysis to better understand the risk
- maintain existing controls;
- reconsider objectives

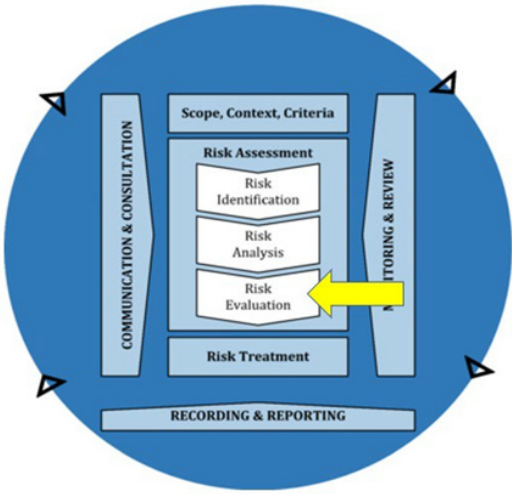


Figure 14 – ISO 31000:2018, Risk Management Process highlighting Risk Evaluation

Decisions should consider the wider context and the actual and perceived consequences to external and internal stakeholders. The outcome of the risk evaluation should be recorded, communicated and then validated at appropriate levels of the organization.

When the risk has been rated, the risk level needs to be compared with Surrey Place's acceptable level of risk or risk tolerance.

When the risk has been rated, the risk level needs to be compared with Surrey Place's acceptable level of risk or risk tolerance.

Evaluating risks involve comparing the level of risk determined in the previous step against pre-determined criteria, to decide if a level of risk is acceptable as is (referred to as "within the tolerance level"), or

action is needed to mitigate the risk (i.e. "it needs to be treated").

This required risk tolerance, which simply means the risk owners review the risk information in their responsibility to ensure the information, assessment and actions are reasonable and whether the risk is within the tolerance level.

A range of issues arise in determining at what point to classify a risk as acceptable. Appetite for taking on a particular risk will vary from one manager or clinician to another: a risk that is acceptable to one person may be unacceptable to someone else. There is also likely to be different perspectives of risk at different levels of management from team to department to executive level.

Some key issues to consider:

- A decision MUST be taken whether to accept or reject the risk, and if the latter to identify controls;
- Failure to make decision means the risk has been accepted by default or controls;
- A risk owner may decide to accept the risk within their delegation of authority.
- Organizations should nevertheless have processes in place for review and oversight of risk evaluation to ensure consistency across the organization and consideration and acceptance of tolerance levels/ evaluation at Chief Executive / Board level.

RISK TREATMENT

Risk treatment involves identifying the most appropriate actions or treatments to modify risks that are at an unacceptable level.

It controls risk by developing a treatment addressing the underlying causes and assesses how effective the treatment is. If the projected/residual risk remains unacceptable, generate an alternative treatment.

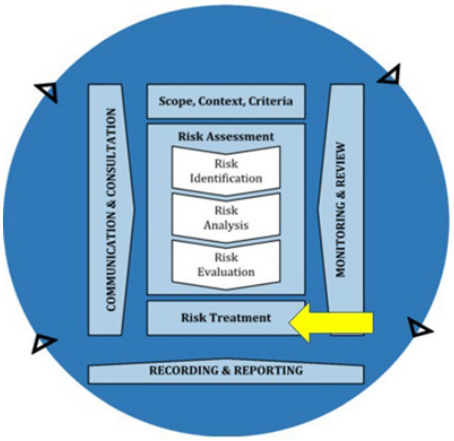


Figure 14 – ISO 31000:2018, Risk Management Process highlighting Risk Treatment

Risk treatment should be developed by, or under the direction of, a risk owner, preferable with the support of a team.

Review the risk assessment – ***Analyzing Risks***, as part of deciding risk treatment options, as well as the existing controls, to decide if they require modification as well as considering "new" treatments.

The aim is to create a balance between minimizing the risk and creating potential benefits or opportunities. For example, if a very high risk can be addressed within existing or minimal resource allocations, then treating that risk should be a priority.

Options to consider include:

Strategies to change the likelihood: implement strategies to change the likelihood of the risk occurring, either to reduce the chance of negative outcomes or increase the chance of positive outcomes.

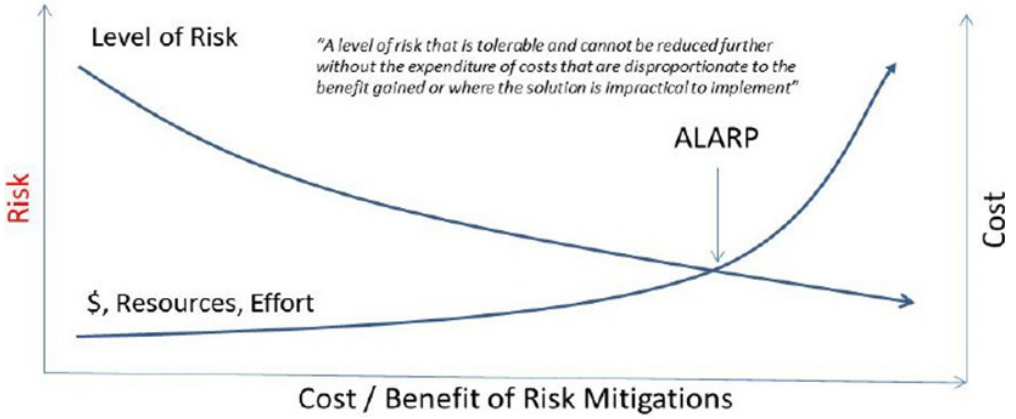
- Strategies to change the consequence: implement strategies to reduce the extent or size of negative outcomes or increase the magnitude of positive outcomes.
- Taking the opportunity: consider strategies that can also exploit potential benefits while mitigating threats
- Sharing the risk: Share or transfer the risk to other parties. Contracting arrangements or other arrangements with a third party can be a good option to reduce exposure to financial, asset or other risk. The risks that may arise from a third-party arrangement will however also need to be assessed and addressed.
- Accepting or tolerating the risk based on informed decision: This will be appropriate where the remaining risk levels are insufficient to justify potential treatment options or where it is not possible or cost-effective to treat the projected/ residual risk.
- Avoiding the risk: Is it possible to avoid risk, for instance, by not proceeding with an activity or part of the activity that could generate the risk?

Once treatments are in place, the risk rating is reviewed, and a revised current rusk rating recorded.

ALARP

When considering the right risk treatment or control the concept of "As Low As Reasonably Practicable (or ALARP) should be considered. ALARP is the point where the risk is negligible, or at least at a level where it can be managed by routine procedures.

ALARP is the level of risk that is tolerable and cannot be reduced further without expenditure of resources, time and effort being disproportionate to benefit gained or where the solution is impractical to implement.



Risk owners should consider establishing a risk tolerance table for the organization, using the ALARP model as basis.

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances.

Options for treating risk may involve one or more of the following:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing the risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk (e.g. through contracts, buying insurance);
- retaining the risk by informed decision.

Justification for risk treatment is broader than solely economic considerations and should consider all the organization's obligations, voluntary commitments and stakeholder views. The selection of risk treatment options should be made in accordance with the organization's objectives, risk criteria and available resources.

When selecting risk treatment options, the organization should consider the values, perceptions and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

When selecting risk treatment options, the organization should consider the values, perceptions and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

Risk treatments, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.

Risk treatment can also introduce new risks that need to be managed.

If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review.

Decision makers and other stakeholders should be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

Preparing and implementing risk treatment plans

The purpose of risk treatment plans is to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored. The treatment plan should clearly identify the order in which risk treatment should be implemented.

Treatment plans should be integrated into the management plans and processes of the organization, in consultation with appropriate stakeholders.

The information provided in the treatment plan should include:

- the rationale for selection of the treatment options, including the expected benefits to be gained;
- those who are accountable and responsible for approving and implementing the plan;
- the proposed actions;
- the resources required, including contingencies;
- the performance measures;
- the constraints;
- the required reporting and monitoring;
- when actions are expected to be undertaken and completed.

MONITORING AND REVIEW

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined

Monitoring and review should take place in all stages of the process. Monitoring and review include planning, gathering and analyzing information, recording results and providing feedback.

The results of monitoring and review should be incorporated throughout the organization's performance management, measurement and reporting activities.

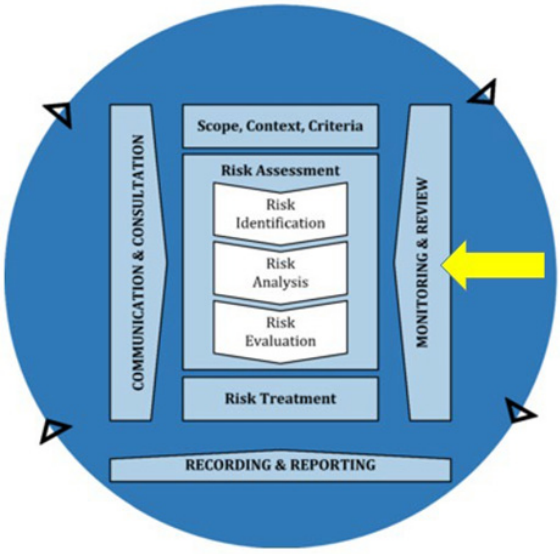


Figure 15 – ISO 31000:2018, Risk Management Process highlighting Monitoring & Review

Regular and careful monitoring is essential to ensure the effectiveness of any risk treatment. An integral step in the risk management process that enables organizations to proactively identify changes on the risk profile and adjust the organizational response as required. It also enables an organization to understand the effectiveness (impacts, benefits and costs) of implementing risk management strategies.

Risk priorities and risk management plans need to be continually monitored and reviewed. This ensures that:

- the overall management plans remain relevant and in the changing service provision and government environment
- The risk treatment plans remain appropriate and effective
- The risk ratings and exposure remain current
- New risks are identified and added, including appropriate controls and treatments
- Existing risks that have been fully addressed are closed or removed the Risk Register, with an appropriate record of the outcomes.

Questions that may assist in a risk review:

- Are the additional controls effective in minimizing the risks?
- Are the additional controls comparatively efficient in minimizing the risks?
- Do the performance indicators address the key elements for the additional controls?
- Can further improvements be made?

RECORDING AND REPORTING

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aims to:

- communicate risk management activities and outcomes across the organization;
- provide information for decision-making;
- improve risk management activities;
- assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

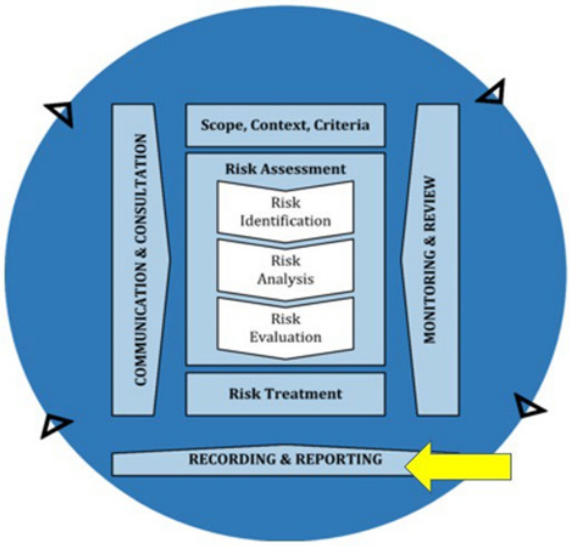


Figure 1 6– ISO 31000:2018, Risk Management Process highlighting Recording & Reporting

Decisions concerning the creation, retention and handling of documented information should consider, but not be limited to their use, information sensitivity and the external and internal context.

Reporting is an integral part of the organization's governance and should enhance the quality of dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities. Factors to consider for reporting include, but are not limited to:

- differing stakeholders and their specific information needs and requirements;
- cost, frequency and timeliness of reporting;
- method of reporting;
- relevance of information to organizational objectives and decision-making

Integrating Risk Management into the Reporting Framework

Integrate and embed risk management into the reporting framework by developing a standardized reporting format that includes the following:

- performance and variance reporting – reporting on the achievement of objectives and adherence to budgets
- reporting on new and/or emerging risk, including changes and updates to the risk register
- status report of agreed risk treatment plans

Monthly operational reports will have information on the achievement of operational objectives and updated to the operational risk register. These operational reports will be consolidated at the CEO/ Board level. Board reports would include information on the achievement of strategic objectives and updates to the strategic risk register.

Surrey Place's Risk Register captures the following information:

SURREY PLACE RISK REGISTER
ID
Department
Date Raised
Risk Type
Risk Statement
Risk Level
Risk Impact
Risk Severity
Mitigating Strategy/Action Plan
Complete Date
Contingency Plan/Action
Progress on Action
Status
Notes

6. GLOSSARY

Risk management will operate under a common language. Adopting standard risk management terms and definitions set out in the Risk Management Guideline, ISO 31000:2018 will improve consistency and avoid confusion. Common terms may include:

Control	Measure that maintains and/or modifies risk; include, but are not limited to any process, policy, device, practice or other conditions and/or actions which maintain and/or modify risk.
Consequence	Outcome of an event affecting objectives; A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.
Exposure	Extent to which the organization is subject to an event
Event	Occurrence or change of a particular set of circumstances
Hazard	Anything that has potential for harm
Incident	Event in which a loss occurred or could have occurred regardless of severity
Inherent risk	Exposure arising from a specific risk before any intervention to manage it
Level of risk	Overall magnitude of a risk.
Likelihood	Chance of something happening
Near Miss	Operational failure that did not result in a loss or give rise to an inadvertent gain.
Residual Risk	Current risk. The risk remaining after risk treatment
Risk	Effect on uncertainty on objectives
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk
Risk assessment	Overall process of risk identification, analysis, and evaluation
Risk Management	Coordinated activities to direct and control an organization with regard to risk
Risk owner	Person or entity with the specific accountability and authority for managing the risk and any associated risk treatments
Risk register	A record of information about identified risks
Stakeholder	Person or organization that can affect, be affected by or perceive themselves to be affected by a decision or activity

7. REFERENCED DOCUMENTS

- Risk Management Guide, ISO 31000:2008
- Risk Management Guide, ISO 31000: 2019
- Enterprise Risk Management, COSO. 2004
- (n.a.). Risk Management - Enterprise-Wide Risk Management Policy and Framework – NSW Health. October 2015. Retrieved on December 26, 2020 from https://www1.health.nsw.gov.au/pds/ActivePDSDocuments/PD2015_043.pdf
- NHS Foundation Trust. Southern Health. Risk Management Strategy and Policy. (December 2018). Retrieved on December 26, 2020) from file:///C:/Users/cecile.recto/Downloads/Risk%20Management%20Strategy%20and%20P olicy%20V6%20(1).pdf
- NHS Foundation Trust. Great Western Hospital. Risk Management Strategy. (September 2020). Retrieved on December 26, 2020) from https://www.gwh.nhs.uk/media/327815/risk-management-strategy.pdf
- Government of Australia. Department of Tourism and Environment. Risk Assessment and Management. (May 2008). Retrieved on December 27, 2020) from https://www.im4dc.org/wp-content/uploads/2014/01/Risk-assessment-and- management.pdf
- Deloitte Risk Advisory. Enterprise Risk Management: A Risk Intelligent Approach. (August 2015). Retrieved on December 28, 2020 from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-erm-a- risk-intelligent-approach.pdf
- Deloitte. Take the Right Step: 9 Principles for Building the Risk Intelligent Enterprise (n.d.). Retrieved on December 28, 2020 from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/Board%20of%20Dire ctors/in-gc-putting-risk-in-the-comfort-zone-nine-principles-for-risk-intelligent- enterprises-noexp.pdf
- Deloitte. Extended Enterprise Risk Management: Driving Enterprise Through Third Party Eco-systems (n.d.).Retrieved on December 28, 2020 from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-extended- enterprise-risk-management.pdf
- Deloitte. Enterprise Risk Assessment: What are your risks and how do you plan to address them. Retrieved on December 28, 2020 from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-extended- enterprise-risk-management.pdf
- Byatt, Gareth. (2018). What benefits can I get from ISO 31000:2018? The Knowledge. Strategic Risk Asia Pacific. Retrieved on December 30, 2020 from https://www.strategicrisk-asiapacific.com/the-knowledge/what-benefits-can-i-get-from- iso-310002018-/1427391.article
- Brady, Ann. (2017). The new arsenal of risk management. ISO News. Retrieved on

December 30, 2020 from https://www.iso.org/news/ref2239.html

- Griffith University. (2018). Enterprise Risk Management Policies. Retrieved on December 27, 2020 from https://policies.griffith.edu.au/
- VMIA. Risk Management for Community Based Organizations. Retrieved on December 26, 2020 from www.vmia.vic.gov.au
- Berry, Tim. (2010). North Simcoe Muskoka LHIN. Enterprise Risk Management Framework. Retrieved on December 26, 2020 from http://nsmlhin.on
- Williams, Carol (2017). Guide to developing an enterprise risk management program. Retrieved on December 29, 2020 from http://www.erminsightsbycarol.com/
- NHS Foundation Trust. Black Country Partnership. (March 2019). Clinical Risk Management