Risk Management Plan

Spokane Regional Health District

January 2024 - December 2026

DRAFT December 2023

Table of Contents

1. Introduction

Risk Management is a structured, district-wide approach to identifying, assessing, monitoring, and responding to risks, and their related opportunities, within Spokane Regional Health District's (SRHD) risk tolerance, to provide reasonable assurance of success in fulfilling SRHD's mission and strategic plan. Risk Management is integrated into SRHD's existing governance, decision-making and planning and budgeting processes.

While traditional risk assessment focuses on loss or damage and minimizing those risks with loss prevention and insurance measures, Enterprise Risk Management focuses on risks at all levels. This is because Enterprise Risk Management helps to proactively identify and control threats and vulnerabilities that could impact the organization negatively.

The Risk Management framework is a set of components that provides resources, structure, and reporting for managing risks at SRHD. The framework aligns with International Organization for Standardization ISO 31000 Risk Management Principles and Guidelines.

2. Commitment

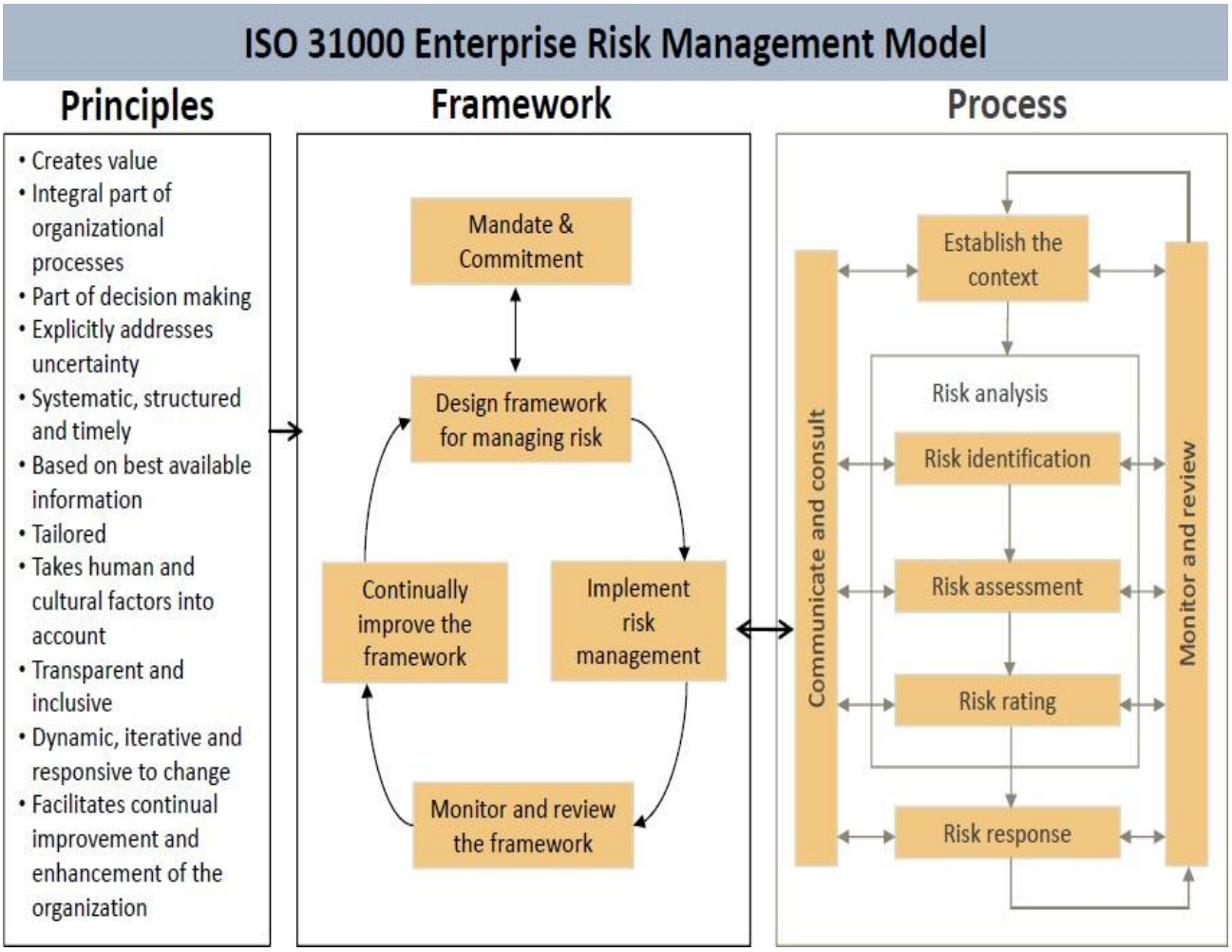
SRHD's Administrative Officer, Deputy Administrative Officer, Health Officer, Controller, SRHD Board of Health, and Executive Leadership are committed to fostering an environment that will encourage risk-informed decision-making within SRHD's culture and practices. SRHD's Executive Leadership will incorporate Risk Management into its governance, decision making, planning, and budgeting processes as set out in this framework.

3. Risk Managements, Concepts and Principles

Risk Managements and Concepts

(See: Appendix A –Risk Management Process Overview)

Risk Management is a structured, district-wide approach to identifying, assessing, monitoring, and responding to risks, and their related opportunities, within SRHD's risk tolerance, to provide reasonable assurance of success in fulfilling SRHD's mission and strategic plan.



Risk
(See: Appendix B – Examples of Spokane Regional Health District Risks)

Refers to the effect of **uncertainty** on SRHD's ability to successfully accomplish its mission and strategic plan, including the ability to successfully accomplish division strategic objectives in support of SRHD's objectives. Simply stated, they are the things that keep SRHD from achieving its objectives.

Local Health Jurisdictions face internal and external factors and influences that make it uncertain whether, when and the extent to which, they will achieve or exceed their objectives. The effect that this uncertainty has on SRHD's objectives is a **risk**.

Opportunity
Taking risks can afford opportunities. SRHD's willingness to assume risk will help deter Risk Management in the opportunities it is willing to pursue to accomplish its mission and strategic plan. At the operational level, leadership must manage the risk of uncertainty to increase the likelihood of an opportunity's success.

Risk Context
The risk context is the strategic plan or emerging, strategic initiatives of the SRHD BOH, Administrative Officer or Divisions where Risk Management is being applied.

Risk Identification
Risk identification is the process of finding, recognizing, and describing high-level risks (internal and external factors or influences) that may impact SRHD's ability to successfully accomplish its mission and strategic plan, or division or unit strategic objectives, in support of SRHD's objectives. The level of understanding of the risk at this point may be low.

Include the following points when writing risk identification statements for the matrix:

- Describe the obstacle, challenge, event, harm, financial loss, or compliance violation that is being addressed.
- Use plain language, rather than citing a specific compliance rule or regulation, for example.
- Be specific enough for assessment and rating, the next step in the Risk Management process.

Example: *SPACE LIMITATIONS: Inadequate space inventory and/or inefficient use of existing space will negatively impact SRHD's ability to accommodate its planned growth.*

Risk Assessment
Risk assessment is an evaluative process that creates an understanding of the identified risk to Risk Management where it falls within SRHD's risk tolerance. It includes an analysis of the risk's potential impact on the following areas:

- **Strategy:** How the risk may affect high-level goals aligned with and supporting SRHD's mission and strategic plan, or division strategic objectives in support of SRHD's objectives.
- **Operations:** How the risk may affect the effectiveness and efficiency of SRHD's operational and management processes, including performance and accountability goals. Safety is an operational risk.
- **Finances:** How the risk may affect SRHD's ability to effectively manage and control the potential loss of financial resources and physical assets.
- **Compliance:** How the risk may affect compliance with relevant external laws and regulations and internally imposed policies and procedures.

- **Reputation:** How the risk may affect the assets that form SRHD's image and reputation with internal and external stakeholders. Although reputation is an important asset of SRHD, it may not be under SRHD's control and only partially mitigated.

Risk assessment also includes a rating of the risks' potential likelihood and impact on SRHD's mission and strategic plan, and prioritization. See the following section on Risk Rating and Prioritization.

Risk Rating and Prioritization

(See: Appendix C – Risk Matrix and Heat Map)

Identified risks are rated using the risk matrix and heat map on a two-dimensional scale considering both the **likelihood** of the risk occurring and the **impact** on SRHD if the risk event should occur. This will also assist in the prioritization of the risks. Using a five-point scale, each risk is rated considering the following and then **prioritized** based on the results:

- **Risk Rating:**

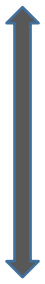
Risk Likelihood		
	Scale	**Definition**
5	**Certain**	Expected to occur in most circumstances (e.g., at least once per year)
4	**Likely**	Will occur (e.g., at least once per 3 years)
3	**Possible**	May occur at some time (e.g., at least once per 5 years)
2	**Unlikely**	Could occur at some time (e.g., at least once per 10 years)
1	**Remote**	Will only occur in exceptional circumstances (e.g., less than once per 10 years)
Risk Impact		
	Scale	**Definition**
5	**Severe**	Core mission or strategic plan impaired to the extent that achievement unlikely, operationally disabling, extremely high reputational impact (nation)
4	**Serious**	Operations must shift significantly to adjust to conditions created by consequences of risk-related incident or control failure, seriously degrades the achievement of mission or strategic plan, high reputational impact (region)
3	**Significant**	Operational changes are necessary to adjust to conditions created by consequences of risk-related incident or control failure, will degrade the achievement of mission or strategic plan, moderate reputational impact (local)
2	**Moderate**	Consequences of risk-related incident or control failure are tangible, but operations remain intact and maintain status quo, may or may not degrade the achievement of mission or strategic plan, low reputational impact (SRHD)
1	**Low**	Operations are unaffected, but risk awareness and monitoring are appropriate, little, or no reputational impact

- **Risk Prioritization:**

Prioritization is based on the likelihood of the risk occurring and the impact on SRHD if the risk event should occur, and where that falls on the heat map.

		Impact				
		1. Low	2. Moderate	3. Significant	4. Serious	5. Severe
Likelihood	5. Certain					
	4. Likely					
	3. Possible					
	2. Unlikely					
	1. Remote					

Highest Likelihood Highest Impact



Lowest Likelihood Lowest Impact

Priority
Very High
High
Medium
Low

- **Very High** – *These are the risks that the Administrative Officer, SRHD Board of Health, and Executive Leadership need to know about.* High-level, district-wide risks whose likelihood and impact will seriously threaten 1) SRHD's ability to successfully accomplish its mission and strategic plan, and/or 2) SRHD's reputation. These risks will be monitored at the SRHD Board of Health and Executive Leadership levels.
- **High** – High-level, district-wide risks whose likelihood and impact may threaten. SRHD's ability to successfully accomplish its mission and strategic plan, and/or 2) SRHD's reputation. These risks will be monitored at either the SRHD Board of Health, Executive Leadership and/or Program Leadership level, depending on their scope and nature.
- **Medium –** These risks whose likelihood and impact will or may threaten a division's functional areas and its ability to successfully accomplish its strategic objectives. These risks may also include unit-level risks identified by multiple functional areas across a division. These risks are managed without formal monitoring by the SRHD Board of Health or Executive Leadership, thus monitored at the Division level.
- **Low** - Risks that have little or no impact on SRHD's ability to successfully accomplish its mission and strategic plan. These risks are managed and monitored in the normal course of division business.

Risk Tolerance
Refers to the amount of risk, on a broad level, that SRHD is willing to take on in pursuit of its mission and strategic plan.

For example, an SRHD team may have a **low risk tolerance** related to threats to the health, safety and well-being of its community, damage or loss to its property, unreasonable potential for financial uncertainty and loss, non-compliance with internal and external compliance mandates, and compromising its reputation. While considering the foregoing, the same SRHD team may have a **higher risk tolerance** as it pursues activities, programs or services related to its mission and strategic plan.

Risk Response
Management's coordination of human, operational, capital, technological, financial, and other resources to ensure the selected action is effectively carried out to manage the risk within SRHD's risk tolerance. Elements of a risk response may be incorporated into strategic planning and budgeting processes.

Risk responses include:

- **Avoidance:** Exiting the activity, program or service that gives rise to the risk.
- **Mitigation:** Strategies and methods used to reduce the risk, including, but not limited to, control and management actions that reduce the risk's impact on strategic objectives, operations, finances, compliance, and reputation.
- **Acceptance:** No response is taken to affect the risk, other than monitor it.

Risk Profile
(See: Appendix C – Risk Matrix and Heat Map)

A risk profile includes the spreadsheet summary, or risk matrix and heat map, and corresponding Risk Management plans (if applicable) of the high-level, prioritized risks of the district or division. It would include risks that could challenge the achievement of SRHD's mission and strategic plan or division strategic objectives in support of SRHD's objectives. It is developed through use of the Risk Management process and assigns Risk Owners (and Co-Owners) and Risk Monitors.

Risk Management Plan
(See: Appendix D –Risk Management Plan Form)

A written management plan may be created for **Very High** and **High** rated strategic risks that require increased attention for management and monitoring purposes.

SCOT Assessment
A tool commonly used by SRHD stakeholders in a strategic planning setting that identifies and assesses the Strengths, Challenges, Opportunities and Threats (SCOT) of the district or a division, SRHD Deputy Administrative Officer, or department. Strengths and Challenges are internal factors while Opportunities and Threats are external.

Principles

Risk Management (ISO 31000 amended for SRHD): Creates and protects value.
Risk Management contributes to the demonstrable achievement of objectives and improvement of SRHD performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product and service quality, project management, efficiency in operations, governance, and reputation.

Is an integral part of SRHD's processes.
Risk Management is not a stand-alone activity that is separate from the main activities and processes of SRHD. Risk Management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

Is part of decision making.
Risk Management helps SRHD decision makers make informed choices, prioritize actions, and distinguish among alternative courses of action.

Explicitly addresses uncertainty.
Risk Management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

Is systematic, structured, and timely.
A systematic, timely and structured approach to Risk Management by SRHD contributes to efficiency and consistent, comparable, and reliable results.

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.

Is tailored.
Risk Management is aligned with SRHD's existing leadership and management processes.

Takes human and cultural factors into account.
Risk Management recognizes the capabilities, perceptions and intentions of external and internal influences that can facilitate or hinder achievement of SRHD's objectives.

Is transparent, as appropriate, and inclusive.
Appropriate and timely involvement of stakeholders and decision makers at all levels of SRHD ensures that Risk Management remains relevant and up to date. Involvement also allows stakeholders to be represented and to have their views considered in Risk Management risk criteria.

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.

Facilitates continual improvement of the organization.
SRHD should develop and implement strategies to improve its Risk Management maturity alongside all other aspects of development.

Risk Management (SRHD's additions): Is tied to strategy.
Risks are tied to SRHD's mission and strategic plan.

Is part of governance.
Risk Management is part of, and not separate from, SRHD's governance, decision-making and planning and budgeting processes. Leadership that is responsible for achieving strategic objectives will find that risk is an unavoidable part of the decision-making process and that risk-taking should be informed and intentional.

Is simple and pragmatic.
Care should be taken to not overcomplicate the application of Risk Management to the point of stifling the decision-making processes managed by SRHD BOH and ELT. Only consider a manageable number of **Very High** and **High** rated risks that are tied to strategic objectives.

Leverages existing processes.
Risk Management should leverage existing risk identification and assessment processes, like Strengths, Challenges, Opportunities and Threats (SCOT) processes, planning and budgeting processes, and similar practices.

4. Roles, Responsibilities and Reporting

(See: Appendix E –Risk Management Flow Chart)

SRHD Board of Health
The SRHD Board of Health, as part of its normal governance activities, engages in candid conversations at the strategic level with the Administrative Officer, Health Officer, Deputy Administrative Officer, and SRHD Controller to fulfill their shared responsibility of ensuring SRHD's risks are appropriately managed and documented as SRHD pursues its mission and strategic plan.

Finance, Audit and Risk Management of the SRHD Board of Health
The Administrative Officer assists the full Board in fulfilling its responsibility for oversight of the identification, assessment, monitoring, and response to risks, in fulfillment of SRHD's mission and strategic plan. The Risk Management Officer provides strategic oversight of matters related to the integration of Risk Management into existing decision-making, strategic planning, and budgeting processes. The Risk Manager Officer duties do not replace or duplicate established responsibilities and delegations for SRHD leadership and management.

Executive Leadership
Executive Leadership includes the Administrative Officer, Health Officer, Deputy Administrative Officer, and Directors. In consultation with the SRHD Board of Health and the Risk Management Officer, they will:

- **Establish Tone:**
  - Establish "tone from the top" and commit to implementing Risk Management at SRHD.
- **Prioritize Risks:**
  - Prioritize the division's risks within the risk profile, considering recommendations from the SRHD Risk Management Committee.

- Select and recommend **Very High** or **High** rated risks for monitoring that are tied to SRHD's mission and strategic plan.
- Select **Very High** or **High** rated risks of special interest and present to Executive Leadership for their monitoring as well.

- **Assign Risk Ownership:**
  - Establish clarity regarding ownership of and responsibility for identified risks and direct Risk Owners (and Co-Owners) to develop and implement response plans and provide progress reports. SRHD Leadership staff may also be a Risk Owner.
  - Ask Risk Owners (and Co-Owners) to create a written Risk Management plan for **Very High** and **High** risks requiring increased attention for management and monitoring purposes, and provide copies as requested to the Risk Management Committee.

- **Provide Annual Risk Management Report:**
  - Develop and provide a Risk Management Report to the Risk Management Committee, with Risk Management Committee assistance, on an annual basis with interim updates at each regular meeting, or as requested.

- **Oversee and Monitor Risks:**
  - Oversee and monitor management strategies for risks within and across their respective areas.

Risk Management Committee

The Risk Management Committee is provided administrative support by Risk, Compliance and Policy Services (RCPS). The committee will:

- **Manage Framework:**
  - Maintain and monitor the performance of the Risk Management framework, recommend changes and updates to Executive Leadership, and then make approved revisions for its continued success.
  - Provide tools for Division and Program Leadership to assist with implementing the Risk Management framework in their areas, including risk matrix, heat map and related forms.
  - Review training programs for Executive Leadership and Risk Owners (and Co-Owners).
  - Provide consultation and support to Division and Program Leadership as those areas implement the Risk Management framework. However, the committee does not have substantive responsibility for managing risks within these areas.
  - Monitor and report on the division's Risk Management effort for Executive Leadership on an ongoing basis.

- **Create and Maintain Division Risk Profile:**
  - Collect and organize division risk profiles for creation and maintenance of the division risk profile.
  - Prioritize the division risk profile based on division **Very High** and **High** rated risks while considering SRHD's mission and strategic plan and deliver to Executive Leadership for further prioritization and oversight.
  - Reconcile division risk profiles with final risk profile and return to respective Division and Program Leadership, identifying those risks that will be monitored by the Risk Management Committee, Executive Leadership and/or Program Leadership.

- **Create Annual Risk Management Report:**
    - Develop the annual Risk Management Report on behalf of Executive Leadership for presentation to the Risk Management Committee, with interim updates at each regular meeting, or as requested.

Committee membership includes:

- Deputy Administrative Officer
- Controller
- Human Resources Director
- Public Information Director
- Information Technology Manager
- HIPAA & Records Manager
- Facilities Manager

Division Leadership

Division Leadership includes the Administrative Officer, Health Officer, Deputy Administrative Officer, Division Director of Community Health, Division Director of Disease Prevention and Response, Division Director of Environmental Public Health, Division Director of Treatment Services, Human Resources Director, and Division Director of Public Information & Government Affairs. Using each area's existing leadership structures by adding Risk Management responsibilities to their normal management responsibilities, these leaders will:

- **Integrate Risk Management:**
    - Support the Risk Management framework.
    - Ensure that risks are identified, assessed, monitored, and responded to within their division or areas of responsibility.
    - Oversee the integration of Risk Management into the division or area governance, decision-making, and planning and budgeting processes.
    - Engage all Risk Owners (and Co-Owners) in the Risk Management process that may be directly impacted by it.
    - Create a "safe" and open environment for which candid discussions can occur during the Risk Management process.
    - Leverage the division's existing and related risk processes, like SCOT Assessments.
    - Reinforce "tone from the top." Promote Risk Management within the division culture and practices.

- **Create and Maintain Division Risk Profile:**
    - Create and maintain a division risk profile and provide copies as requested to the Risk Management Committee.
    - Ensure identified risks are tied to division strategic objectives, in support of SRHD's mission and strategic plan.
    - Prioritize risks based on the Risk Management framework's risk rating methodology.

- **Consider Potential Risk Owners:**
    - Risk ownership may be within one division or shared across division lines for district-wide risks, depending on the scope and nature of the risk. Collaboration between divisions may be necessary.
    - As part of their Executive Leadership responsibilities, Division Leadership will assign ownership of and responsibility for identified risks to Risk Owners (and Co-Owners), so

it may be helpful to consider potential Risk Owners (and Co- Owners) as division risk profiles are being developed.

Risk Owners (and Co-Owners)

Risk Owners may be Division Leadership, and/or those reporting to Division Leadership, including Leadership Team and subject matter experts, depending on the scope and nature of the risk. Risk ownership may be shared with Risk Co-Owners, and the functional aspects of risk ownership may be assigned to appropriate leadership or staff. However, substantive responsibility for managing the risks rests with the Risk Owners.

Risk Owners will:

- **Engage in Risk Management:**
  - Engage in the Risk Management process where risks are identified, assessed, responded to, and monitored.
  - Integrate Risk Management into the Risk Owner's governance, decision-making and planning and budgeting processes.
  - Engage and support:
    - Risk Co-Owners for which they share management of risks; and
    - Appropriate leadership or staff who may be assigned functional aspects of risk ownership.
  - Promote Risk Management within the Risk Owner's area.

- **Manage Risks:**
  - Develop and implement risk response plans for identified risks and provide progress reports to Division Leadership.
  - Elevate **Very High** or **High** rated risks to the attention of Division Leadership.
  - Create a written Risk Management plan for **Very High** and **High** risks requiring increased attention for management and monitoring purposes, or as requested by Division Leadership.
  - Assist Executive Leadership with the annual Risk Management Report presentation to the Risk Management Committee, and with interim updates at each regular meeting, or as requested.

- **Manage Other Risks**
  - In addition to risks, there are other risks that should be identified, assessed, monitored, and responded to as part of the Risk Owner's normal course of responsibility. The Risk Management framework can be used at the "local" level for such purposes as well. See Appendix A –Risk Management Process Overview.

- **Seek Consultation**
  - Proactively engage SRHD resources in consultation (e.g., Environmental Health and Safety, Public Safety, Risk Management, Compliance Management, Legal Counsel, SRHD Communications, Human Resources, Attorney General's Office, Washington State Auditor's Office, Internal Audit, Policy and Rules Development, Information Technology, etc.) to assist with the Risk Management effort. SRHD resources have no substantive responsibility for managing risks within the Risk Owner's area but serve as consultants and advisors.

Internal Audit
Internal Audit provides an ongoing independent assurance function which evaluates.
SRHD's activities to assist the SRHD Board of Health, the Board's Finance, Audit and Risk Management Committee, and Executive Leadership in the discharge of their oversight and management responsibilities, which includes the Risk Management effort.

An Internal Audit will support the Risk Management process by identifying and evaluating risks, providing advice regarding management's responses to those risks (but not make decisions about or implement those responses), and evaluating the Risk Management process itself from the perspective of Internal Audit.

5. Implementation

(See: Appendix F –Risk Management Implementation Plan Timeline)
The key elements of implementing the Risk Management framework include the following:

Implementation of the Risk Management Plan

- **Training**
  - The Risk Management team will develop an online HRIS training tool in partnership with Human Resources and a SharePoint site, and in-person training for ELT, Leadership Team, and the SRHD Deputy Administrative Officer.

- **Risk Owners (and Co-Owners) - SRHD Deputy Administrative Officer and Divisional Unit Risk Profiles and Management Plans**
  - The SRHD Deputy Administrative Officer and each divisional unit will create and maintain a risk profile that summarizes and prioritizes risks that may impact their respective area and division. (See the Risk Management Checklist)

- **Division Leadership - Administrative Officers' Risk Profiles and Management Plans**
  - The SRHD Deputy Administrative Officer and divisional directors' risk profiles will be summarized into division risk profiles prioritizing risks that may impact their division and SRHD.

- **Risk Management Committee**
  - The Risk Management Committee compiles division risk profiles into a draft risk profile, including appropriate written Risk Management plans, and submits to Executive Leadership. The Risk Management Committee drafts a preliminary Risk Management Report.

- **Executive Leadership – Division Risk Profile and Management Plans**
  - The Executive Leadership reviews and prioritizes the risk profile and management plans, assigns Risk Owners (and Co-Owners), and approves the Risk Management Report.
  - Risk owners and Co-Owners will create Written Risk Management plans for **Very High** and **High** rated strategic risks that require increased attention for management and monitoring purposes.

- **Risk Management Report**
  - The Risk Management Report to the SRHD Board of Health is presented by the Deputy Administrative Officer.

Integration of Risk Management into Existing Management Processes
This involves the integration of Risk Management response plans by Division and Program Leadership and Risk Owners (and Co-Owners) into existing governance, decision-making, and planning/budgeting processes, and vice versa.

Application of Risk Management Emerging, Strategic Initiatives
This involves the application of Risk Management Division Leadership and Risk Owners (and Co-Owners) as part of assessing and implementing new, strategic initiatives, thereby improving their chance for success.

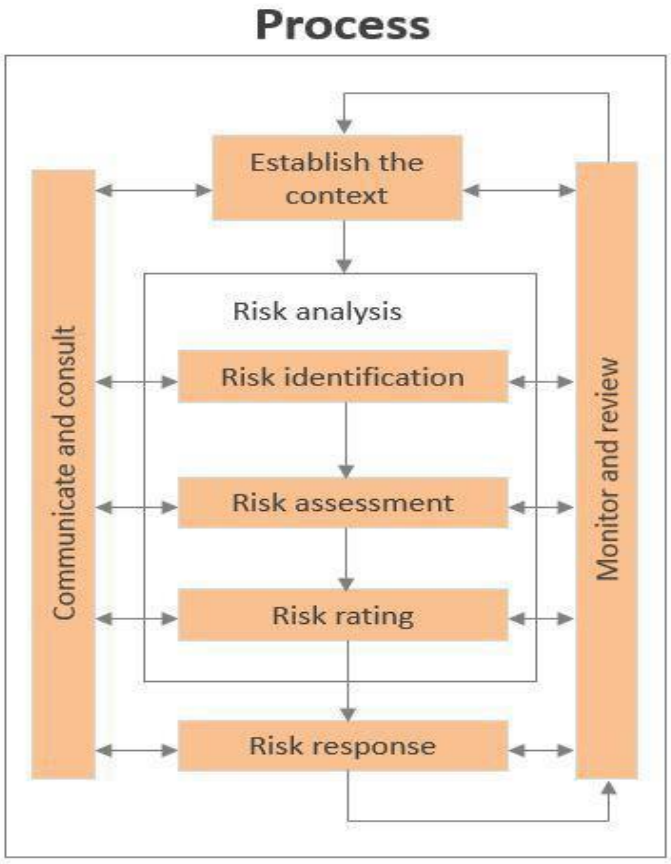
Monitoring
The intent of monitoring is to track the performance of the Risk Management framework itself and the management of risks by the division that have been identified within the Risk Management process.

- **Performance of Risk Management Framework**
    - The Risk Management Committee monitors the performance of the Risk Management framework. The Risk Management framework will be continuously improved through feedback from SRHD stakeholders to ensure that SRHD's Risk Management approach is helpful, valuable, and effective.
- **Risk Management Framework Use by Management**
  The use of the Risk Management framework will be evaluated based on the following:
    - Actionable response plans have been developed and successfully implemented by Risk Owners (and Co-Owners) for each risk identified under their Risk Management processes.
    - Downward movement on the risk rating scale and heat map based on the ongoing implementation of risk response plans.
    - Documentation of the review of risks within routine and strategic SRHD management functions.
    - Risk Management framework training was established and made available for SRHD stakeholders.

Appendix A: Risk Management Process

INTRODUCTION

The Risk Management process can be applied to high-level risks that may impact SRHD's ability to successfully accomplish its mission and strategic plan or that may impact division or unit strategic objectives supporting SRHD's objectives. The process can be an integral part of an area's management, embedded in the area's culture and practices, and tailored and scaled to the area's activities. The process comprises the activities described below:



PROCESS

Step 1: Establish the Context
Contexts are the strategic objectives and emerging, strategic initiatives of an area, or those parts of an area where the Risk Management process is being applied.

Step 2: Risk Identification
Risk identification is the process of finding, recognizing, and describing high-level **risks** (internal and external factors or influences) that may impact SRHD's ability to successfully accomplish its mission and strategic plan or division/program strategic objectives which support SRHD BOH and ELT objectives. The level of understanding of the risk at this point may be low. They can also be viewed as things that create **uncertainty** about the area's ability to achieve its strategic objectives or do it effectively.

Step 3: Risk Assessment
Risk assessment is an evaluative activity with Risk Management that creates an understanding of the identified risk and where it falls within an area's risk tolerance (usually aligned with SRHD's risk tolerance). It includes an analysis of the risk's potential impact on **strategy, operations, finances, compliance,** and **reputation**. It leads to decisions on whether a risk needs a response and on the most appropriate response strategies and methods.

Step 4: Risk Rating
Risks are rated using a risk matrix and heat map (see Appendix C – Risk Matrix and Heat Map) on a two- dimensional scale considering both the **likelihood** of the risk occurring and the **impact** on an area if the risk event should occur. This also assists in the **prioritization** of risks.

Step 5: Risk Response
Risk response will be one of the following - **avoidance**, **mitigation,** or **acceptance**. Risks that are mitigated are controlled or managed to keep them within an area's risk tolerance, which will necessitate the coordination of human, operational, capital, technological, financial, and other resources for accomplishment. Elements of a risk response may be incorporated into strategic planning and budgeting processes.

Ongoing: Monitor and Review
An area's monitoring and review processes should encompass all aspects of the Risk Management process for the purposes of ensuring the effectiveness of risk response plans, learning lessons from successes and failures, detecting changes in the original context, and identifying emerging risks.

Ongoing: Communicate and Consult
Communication and consultation with external and internal stakeholders and resources should take place during all stages of the Risk Management process. To assist in the process, it is helpful to engage internal resources for consultation, such as:

- Environmental Health and Safety
- Emergency Preparedness and Response
- Risk Management Process
- Compliance Plan and Management
- SRHD Communications
- Human Resources
- Assistant Attorney General
- Internal and External Audit
- Policy and Procedure Development
- Information Technology

Appendix B: Examples of SRHD Risks

Human Element - Operations
Leadership/Governance
Human Resources
Client Facing Services
Human Element - Staff
Daily work assignments
Identification
Restricted access
Personal items
Unusual behavior
Staff health
Human Element - Public
Visitors (Non-Employees)
HIPAA - Physical Safeguards
Office Access
Office Workstations and Remote/Mobile Device Access
Emergency/Contingency Plans
HIPAA - Technical Safeguards
Workstation Security and Encryption
Remote and Mobile Access
Clinic and or Client Testing Areas
HIPAA - Administrative Safeguards
Office Training and Awareness
Reporting of Incidents
Vendor Contracts and Agreements
IT - Systems
Access to computer systems
SRHD Campus Buildings
Physical Security
Storage and use of flammable, poisonous, and toxic chemicals
Surfaces/Stairs
Human Element - Safety
First Aid
Emergency, Health, and Safety Information
Fire Emergency/Prevention

Appendix C - Risk Matrix Heat Map (PAGE 1)

Risk Matrix

DRAFT 6-1-18

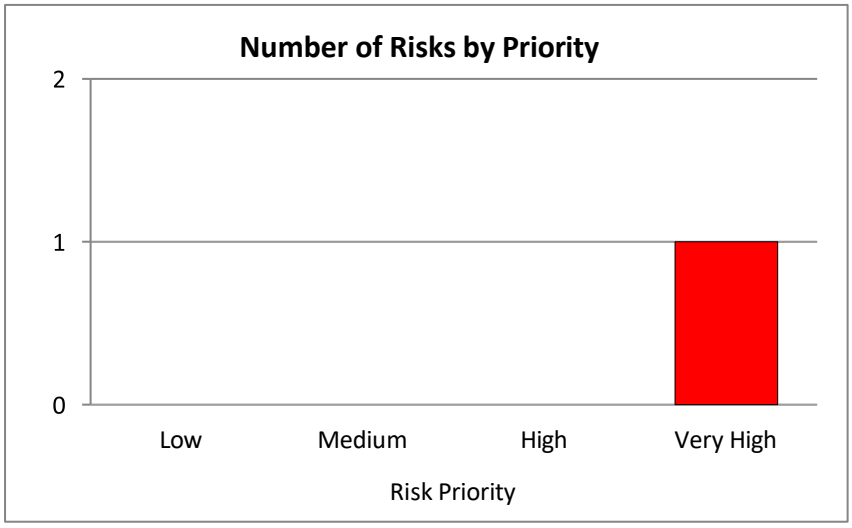
						Heat Map		
Risk #	Identification	Assessment & Rating	Response	Owner(s)	Monitor(s)	Likelihood	Impact	Priority
1	SPACE LIMITATIONS: Inadequate space inventory and/or inefficient use of existing space will negatively impact SRHD's ability to accommodate its planned growth.	The current space is mostly sufficient to meet current staff work. However, SRHD's strategic objective is to increase staff retention. Current space inventory and utilization must be reconsidered for this growth.	MITIGATE Hire a consultant to analyze existing space inventories and utilization, and potential space deficits based on SRHD's strategic objectives. Develop a space plan and budget based on the consultant's report and begin the necessary steps to address the risk.	Administrative Officer, ELT, and Controller	Administrative Officer, Deputy Administrative Officer and Controller for Business and Financial Affairs	5. Certain	4. Serious	***Very High***
2								
3								
4								
5								
6								
7								
8								
9								
10								

Appendix C -Risk Matrix Heat Map
PAGE 2)

Risk Heat Map

		Impact					
		1. Low	2. Moderate	3. Significant	4. Serious	5. Severe	Totals
Likelihood	5. Certain	0	0	0	1	0	1
	4. Likely	0	0	0	0	0	0
	3. Possible	0	0	0	0	0	0
	2. Unlikely	0	0	0	0	0	0
	1. Remote	0	0	0	0	0	0
	Totals	0	0	0	1	0	1

		Number of Risks by Priority
Risk Priority	Low	0
	Medium	0
	High	0
	Very High	1
		1



Appendix D: Risk Management Plan Form

Click or tap to enter a date.

INSERT TITLE

SUMMARY

IDENTIFICATION

Identification of Risk:

Click here to enter text.

Risk Statement:

Click here to enter text.

Opportunity Statement:

Click here to enter text.

ASSESSMENT & RATING

Rating: Likelihood: Dropdown

List Impact: Dropdown

List Priority: Dropdown

List

		Impact				
		1. Low	2. Moderate	3. Significant	4. Serious	5. Severe
Likelihood	5. Certain					
	4. Likely					
	3. Possible					
	2. Unlikely					
	1. Remote					

Summary of potential impact on:

Strategy:

Click here to enter text.

Operations:

Click here to enter text.

Finances:

Click here to enter text.

Compliance:

Click here to enter text.

Reputation:

Click here to enter text.

RESPONSE

Risk Response: Dropdown List

Risk Response Plan:

Click here to enter text.

Action Plan(s)	**Status**

OWNERS & MONITORS

Risk Owner: Click here to enter text.

Risk Co-Owner(s): Click here to enter text.

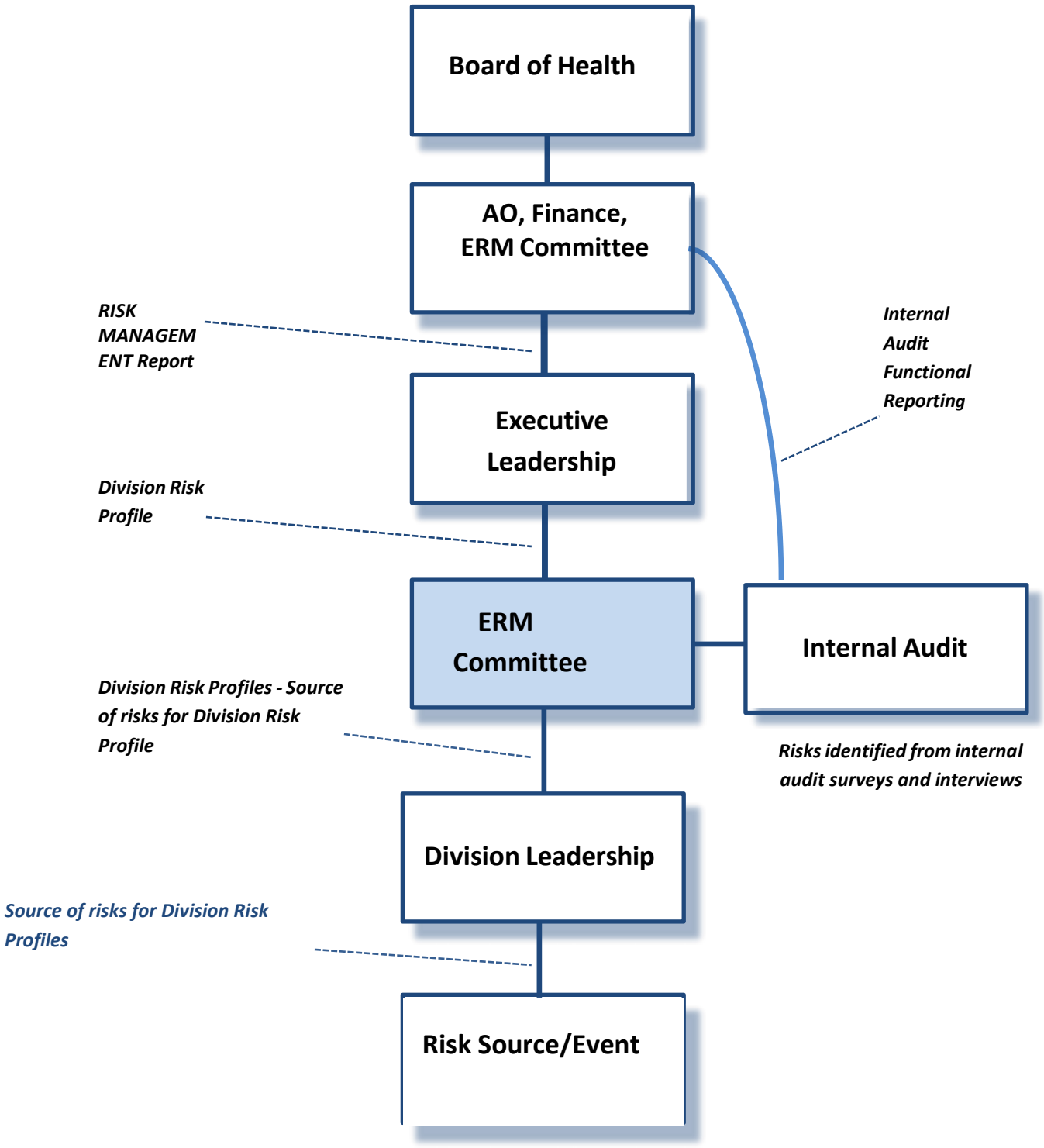
Risk Monitor(s):

☐ BOH, Finance, Audit and Risk Management Committee

☐ Executive Leadership

☐ Program Leadership

Appendix E - Risk Management Flow Chart



Risk Tables

These tables should be read and applied in conjunction with the SRHD Risk Management Plan which includes the procedure and process for risk identification.

Table 1: Consequence Rating - Identify the worst, realistic, primary consequence(s) should an incident occur. Pick the best fit on the 1-5 scale. It is not necessary to address each category.

Consequence Rating		1	2	3	4	5
Categories	**Code**	**Insignificant**	**Minor**	**Moderate**	**Major**	**Severe**
Health impact on Clients	**HP**	Increased level of care (minimal). No increase in length of relationship.	Increased level of care (minimal).	Increased level of care (moderate).	Increased level of care (significant	Death
Health impact on Employees or others	**HS**	First aid or equivalent only. Incident report completed with no notification to insurance providers	Routine medical attention required. Up to 1 week incapacity/time lost. No long-term disability approved. Temporary accommodation may be recommended. Incident report completed	Increased level of medical attention required. 1 week to 1 month incapacity/time lost. No long-term disability may be approved, or temporary accommodation may be recommended. Incident report completed.	Severe health crisis and/or injuries. Prolonged incapacity or absence for more than 1 month with time loss. Long-term disability approved. Incident report completed	Death or permanent total disability.
Critical services interruption	**CS**	No material disruption to dependent work.	Short-term temporary suspension of work. Backlog cleared in day. No public impact.	Medium-term temporary suspension of work. Backlog requires extended work, overtime, or additional resources to clear. Manageable impact.	Prolonged suspension of work. Additional resources, budget and/or management assistance required. Performance criteria compromised.	Indeterminate prolonged suspension of work. Impact not manageable. Non-performance. Other providers appointed.
Performance to budget (over or underspend)	**PB**	< 1% temporary variance	1% to 2% temporary variance	> 2% to 5% temporary variance	> 5% to 10% variance not recoverable within the budget year	> 10% variance not recoverable within the budget year, or being unable to pay staff, creditors or finance critical services
Economic loss	**FL**	Less than $5,000	$5,000 to less than $100,000	$100,000 to less than $3M	$3M to less than $20M	$20M or more
Organizational objectives or outcomes	**OO**	Minor impact.	Inconvenient delays.	Material delays. Marginal under achievement of target performance.	Significant delays. Performance significantly under target.	Non-achievement of objective / outcome. Total performance failure.
Reputation and image damage	**RI**	Non-headline exposure. Not at fault. Settled quickly. No impact.	Non-headline exposure. Clear fault. Settled quickly by Departmental response. Negligible impact.	Repeated non-headline exposure. Slow resolution. Ministerial enquiry/briefing. Qualified Accreditation.	Headline profile. Repeated exposure. At fault or unresolved complexities impacting public or key groups. Ministerial involvement. High priority recommendation to preserve. Accreditation.	Maximum multiple high-level exposure. Ministerial censure. Direct intervention. Loss of credibility and public / key stakeholder support. Accreditation withdrawn.
KPI variation	**PI**	< 2% variation	2% to < 5% variation	5% to < 15% variation	15% to < 30% variation	≥ 30% variation

Consequence Rating		1	2	3	4	5
Categories	**Code**	**Insignificant**	**Minor**	**Moderate**	**Major**	**Severe**
Non- compliance	**NC**	Innocent procedural breach. Evidence of good faith by degree of care/diligence. Minor impact.	Breach, objection/complaint lodged. Minor harm with investigation. Evidence of good faith arguable.	Negligent breach. Lack of good faith evident. Performance review initiated. Material harm caused. Misconduct established.	Deliberate breach or gross negligence. Significant harm. Formal investigation. Disciplinary action. Ministerial involvement. Serious misconduct.	Serious and willful breach. Criminal negligence or act. Litigation or prosecution with significant penalty. Dismissal. Ministerial censure. Criminal misconduct.
Environmental impact	**EN**	Negligible impact. Spontaneous recovery by natural processes. No disruption to access or exposure.	Low level impact. Quick recovery with minimal intervention. Minimal disruption to access or exposure.	Moderate impact. Medium level intervention indicated to bring about recovery. Short to medium-term restriction of access or exposure.	Prominent level but recoverable, unacceptable damage or contamination of a significant resource or area of the environment. Significant intervention. Permanent cessation of harmful activity. Long-term suspended access, presence, or use of resources.	Extensive, very long-term, or permanent, significant, unacceptable damage to or contamination of a significant resource or area of the environment. Very long-term or permanent denial of access or exposure.
Project deliverables	**PD**	≤ 1% variation to deliverables	> 1% to 5% variation to deliverables	> 5% to 10% variation to deliverables	> 10% to 20% variation to deliverables	> 20% variation to deliverables
Project budget	**PU**	≤ 1% over budget	> 1% to 5% over budget	> 5% to 10% over budget	> 10% to 20% over budget	> 20% over budget
Project time delay	**PT**	≤ 5% delay	> 5% to 10% delay	> 10% to 25% delay	> 25% to 100% delay	> 100% delay

Table 2: Likelihood Rating – Assess the likelihood of the incident occurring and having the consequence(s) assessed above. Pick the best fit on the 1-5 scale below.

Likelihood Rating		Client Facing	Operational	
Level	**Descriptor**	**Per Separations/ Occasions of Service Code "C" (Client)**	**% Chance during life of project or fiscal year for budget risk Code "%" (% Chance)**	**Time Scale for ongoing non-project activities or exposures Code "T" (Time)**
1	**Rare**	1 in 100,000 or more	≤ 5%	Once in more than 10 years
2	**Unlikely**	1 in 10,000	> 5% to 30%	Once in 5 to 10 years
3	**Possible**	1 in 1,000	> 30% to 60%	Once in 3 to 5 years
4	**Likely**	1 in 100	> 60% to 90%	Once in 1 to 3 years
5	**Very Likely**	1 or more in 10	> 90%	More than once a year

Table 3: Risk Level Matrix – *Apply the matrix to determine the risk rating.*

Risk Level Matrix		Likelihood				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Very Likely
Consequence	5 Severe	Medium	High	High	Extreme	Extreme
	4 Major	Low	Medium	High	High	Extreme
	3 Moderate	Low	Medium	Medium	High	High
	2 Minor	Low	Low	Medium	Medium	High
	1 Insignificant	Low	Low	Low	Low	Medium

Aggregate Control Assessment, Risk Acceptance/Tolerance Criteria and Specific Risk Criteria

Table 4: Aggregate Control Assessment - *Assess the overall controls managing the risk.*

Level	Description
Excellent	Comprehensive effective controls are fully in place to manage the risk. Regular monitoring, review and/or testing is undertaken. There is limited value in improving the controls.
Satisfactory	Sufficiently effective controls are in place to manage the risk. Periodic monitoring, review and/or testing is undertaken. Some minor improvements to the controls should be considered.
Marginal	Controls are only partially effective and/or partially in place to manage the risk. Some limited monitoring, review and/or testing is undertaken. Improvement opportunities to controls should be implemented.
Weak	Controls are either non-existent, not in place or not effective to manage the risk. No or limited monitoring, review and/or testing is undertaken. There is significant value in corrective and/or improvement actions.

Table 5: Risk Acceptance/Tolerance Criteria – Decisions regarding risk acceptance and further treatment should be made with reference to the risk acceptance/tolerance criteria below, the specific risk criteria (Table 6) and local requirements including risk appetite and cost benefit analysis. Acceptance of High and Extreme risks is not permitted unless approved by **at least an ELT member.** If the risk is not acceptable, risk treatment may include avoiding the risk, improving controls, and sharing or transferring the risk.

Risk Rating	Risk Acceptance/Tolerance Criteria
Low	• Risk is acceptable. • The Aggregate Control Assessment should be Satisfactory.
Medium	• Risk is tolerable. • The Aggregate Control Assessment should be Satisfactory and reviewed frequently.
High	• Risk is intolerable. • The Aggregate Control Assessment should be at least Satisfactory and improved to Excellent as soon as is practicable and monitored. • At least a Tier 2 officer must make acceptance decision.
Extreme	• Risk is intolerable. • The Aggregate Control Assessment should be improved to Excellent immediately and closely monitored. • At least a Tier 2 officer must make acceptance decision.

Table 6: Specific Risk Criteria –included to guide risk decision making.

Category	Description
Harm to Clients	• The client or their representative for this purpose determines acceptability of clinical risk from their perspective in the health care offered to them. (See Informed Consent and related processes). • There is “zero tolerance” for the risk of sentinel events occurring.
Harm to Workforce	• There is “zero tolerance” for workplace violence.
Harm to the Public	• Any foreseeable risk of injury to others or loss or damage to their property must be reduced to be the standard expected in law and provide proper discharge of any duty of care owed.
Budget Management	• There is no acceptable level of risk for budget over-runs
Compliance	• There is “zero tolerance” of any material risk of breach of legislative, regulatory, or other Government requirements.