

Enterprise Risk Management (ERM) Policy (2.16)

Policy:	Risk Management Policy	Effective Date: June, 2025
Last Review Date:		Next Review Date: June, 2028
Review Frequency:	Every 3 years	Related Supporting Documents: Council Charter

Purpose

To fulfill its mission of public protection, this policy outlines the principles and processes the CRNS Council employs to manage risks related to planning, performance management, and operations. This includes integrating risk management principles into decision-making, core activities and business processes.

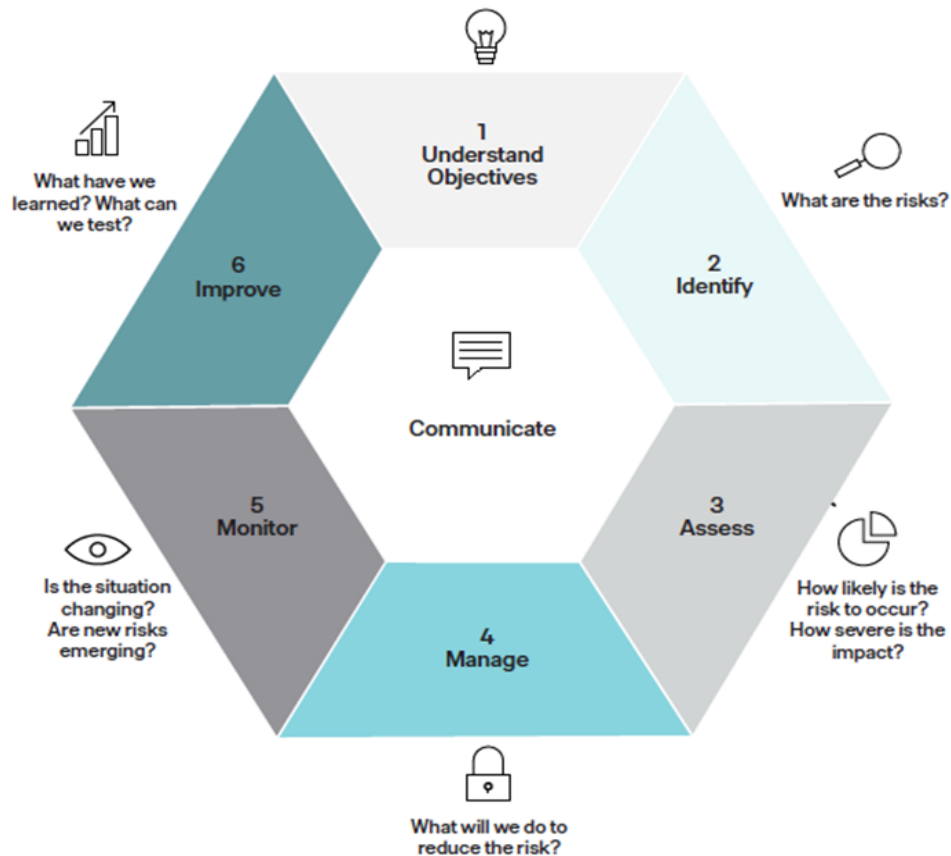
The CRNS Council uses a continuous, proactive process to identify, assess, manage, monitor, and communicate risk to make better-informed decisions to improve the probability of achieving its mandate, strategic goals and operational objectives.

Policy Statement

The CRNS Council is committed to making risk-informed decisions. It achieves this by applying a consistent approach to managing risks and leveraging opportunities. This approach includes:

1. **Identifying** risk which CRNS defines as “The effect of uncertainty on objectives “(or “any situation that may negatively affect achieving objectives resulting in danger, harm, or loss”). See CRNS Risk Categories (Appendix A)
2. **Analyzing** (assessing) the likelihood and impact of each risk. The use of common likelihood and impact descriptors in the CRNS Risk Matrix (see Appendix B) ensures a standardized approach to risk assessment across the organization
3. **Mitigating** (managing) risk that exceeds the CRNS’s Risk Appetite by creating strategies/controls to reduce unacceptable risks
4. **Monitoring** risk through regular review and updates to the CRNS Enterprise Risk Registry used to record and report enterprise risks

How the CRNS Manages Risk



For the CRNS Council to effectively fulfill its risk management commitment, the following principles must be adhered to:

- a. Integrated – Risk management is integrated into all CRNS activities.
- b. Structured and comprehensive – A structured and comprehensive approach to risk management contributes to consistent and comparable results.
- c. Customized – The risk management processes are customized and proportionate to the CRNS's external and internal context related to its objectives.
- d. Inclusive – Appropriate and timely involvement of stakeholders enables their knowledge, views, and perceptions to be considered. This results in improved awareness and informed risk management.

- e. Dynamic – Risks can emerge, change, or disappear as the external and internal context changes. Risk management anticipates, detects, acknowledges, and responds to those changes and events in an appropriate and timely manner.
- f. Best available information – The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear, and available to relevant partners.
- g. Human and cultural factors – Human behavior and culture significantly influence all aspects of risk management at each level and stage.
- h. Continual improvement – Risk management is continually improved through learning and experience.

Definitions

Risk – The effect of uncertainty on objectives (ISO31000:2018)

Risk management - coordinated activities to direct and control an organization concerning risk

Risk Appetite - the amount and type of risk that an individual or organization is willing to accept

Risk Impact: The severity of the outcomes (consequences) if the risk occurs

Likelihood: What is the likelihood (probability) the risk will happen?

Risk Appetite, Response and Escalation

CRNS Council accepts that there will always be an element of risk when pursuing its strategic objectives. It has determined, and will continuously assess, the nature and extent of the risks that the organization is exposed to and is willing to take (its risk appetite) to achieve its strategic objectives and ensure that planning and decision-making reflect this assessment. Risk tolerance reflects the boundaries within which the leadership team is willing to allow the organization's day-to-day risk profile to fluctuate while executing strategic objectives in accordance with the agreed risk appetite, in other words, the residual risk. The Council has set specific limits (risk ratings) for the levels of risk that the organization can tolerate. In setting these, risk factors in both the external and internal business environments have been considered.

Risk Appetite Statement:

The CRNS Council must deliver on its strategic objectives. This is dependent upon its relationships with its registrants, the public and strategic partners, as well as the security of its assets.

The CRNS Council has an appetite for risks created in continuous improvement and challenging the status quo to protect the public through the regulation of Registered Nurses and Nurse Practitioners.

The CRNS Council will not tolerate risks that exceed low risk levels in any of its risk categories. When risks that exceed tolerance are identified, the CRNS takes action to reduce them to acceptable levels.

Risk	Appetite Level	Response
Extreme	Unacceptable, no tolerance	For new risks, immediate mitigation action is required. Inform Council immediately
High	Unacceptable	For new risks, mitigation action should be developed and implemented as soon as possible. Inform Council within 7 days
Moderate	Unacceptable	The risk must be regularly monitored to ensure that any change in circumstances is detected and acted upon appropriately. Report to Council at established reporting cycle.
Low	Acceptable	This level of risk can be accepted. The risk must be regularly monitored to ensure that any change in circumstances is detected and acted upon appropriately.

Monitoring and Review

The progress of action taken to manage risk must be monitored through regular checks and reassessments.

The CRNS monitors its Enterprise Risks through biannual review of the CRNS Enterprise Risk Register.

Roles and Responsibilities

All CRNS staff responsible for the management of risk within their scope of responsibility. This includes identifying, assessing, managing, monitoring, communicating and when necessary, escalating risk.

The leadership team's role is to assign authority, responsibility and accountability for risk management at appropriate levels within their area. They are also responsible for allocating appropriate resources to manage risk effectively within their area and for monitoring progress in the management of risks. They must also respond when a risk is escalated.

The CRNS Council oversees the CRNS's management of risk.

The CRNS Executive Director leads the ERM program and provides reports to the CRNS Council at least annually.


Review

This policy will be reviewed every three years by CRNS Council

Appendix A
CRNS Risk Categories

- Safety
 - Harm
- Compliance
 - Policy
 - Regulatory
 - Legislative
 - Legal
- Human Resources
 - Engagement
 - Succession
- Infrastructure (includes IT)
 - Building Lease
 - Information Systems
 - Maintenance
- Financial
 - Costs
 - Cash Flow
 - Procurement
 - Inefficiencies
 - Contractual
- Strategic
 - Planning
 - Governance
 - Alignment
 - Leadership
 - Culture
- External Relations
 - Registrant
 - Public
 - Government
 - Partners
 - Reputation

Appendix B
RISK MATRIX

RISK HEAT MAP:			Impact				
Likelihood	The event is expected to occur in most circumstances. Greater than 80% probability	5 Almost Certain	Moderate 5	Moderate 10	High 15	Extreme 20	Extreme 25
	The event will probably occur in most circumstances. 50-80% probability	4 Likely	Low 4	Moderate 8	High 12	High 16	Extreme 20
	The event should occur at some time. 25-49% probability	3 Possible	Low 3	Moderate 6	Moderate 9	High 12	High 15
	The event could occur at sometime. 10-24% probability	2 Unlikely	Low 2	Low 4	Moderate 6	Moderate 8	High 10
	The event may occur only in exceptional circumstances. Less than 10% probability	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5
	 <p>RISK MATRIX</p>		1 Insignificant	2 Minor	3 Significant	4 Major	5 Critical
			Minimal impact on achieving the objective. Consequences are dealt with by routine operations. Within compliance requirements. Negligible monetary loss.	Minor impact on objective. The consequences threaten efficiency or effectiveness of some processes. may be a deviation from external standards. Monetary loss managed within budget.	Moderate impact on objective. The consequences would require significant changes to operations. Non-compliant with external standards. Monetary loss outside of budget. Local media interest.	Major impact on objective. Lack of compliance with external standards. The consequences threaten continued services. Major loss of credibility. Continued media interest.	Significant impact on objective. The consequences will be detrimental and may be hard to recover from. Major disruption to service. Inability to meet financial obligations. Long term media interest.