NSRDDA | Nova Scotia Regulator of Dentistry and Dental Assisting

Risk Management Policy

Policy Number: G-05.01.00	Next Review Date: 2029
Approved by: NSRDDA Board	Approval Date: October 10, 2025

1. Purpose

This policy outlines the risk management framework for the NSRDDA, ensuring that risks are proactively identified, assessed, managed, and monitored in alignment with the NSRDDA's mandate to regulate the profession in the public interest.

2. Scope

This policy applies to all Board members, volunteer members of Statutory Committees or staff involved in NSRDDA operations, Board and committee functions, and staff activities. It encompasses governance, regulatory, operational, reputational, financial, legal, and strategic risk.

3. Policy Statement

The NSRDDA recognizes that effective risk management is essential to fulfilling its public interest mandate. As a small regulatory body with limited resources, it is vital that potential threats and opportunities are identified early, assessed thoroughly, and addressed proportionately.

The NSRDDA will take a structured approach to risk management that:

- Promotes consistent and informed decision-making
- Supports the integrity and effectiveness of its regulatory responsibilities, including registration, investigations, and discipline
- Enhances the organization's ability to anticipate and respond to changes in its environment
- Safeguards the public trust, financial sustainability, and reputation of the NSRDDA
- Fosters a culture of accountability and continuous improvement among the Board, staff and Statutory Committees.

4. Roles and Responsibilities

The **Board** approves the Risk Management Policy and ensures appropriate oversight. It reviews strategic risk reports and adopts a risk-informed governance approach.

The **Registrar** implements the risk management framework, reports key risks to the Board and oversees organizational risk management practices.

Staff identify risks in daily operations, report notable risks to the Registrar and meet quarterly to discuss risk trends.

Statutory Committees consider risk impacts when making regulatory decisions and refer emerging risks to the Registrar or the Board.

5. Risk Categories and Risk Appetite

Category of Risk	Description	Risk Appetite
Strategic	Risks related to failure to adapt to changing conditions or external factors over which the NSRDDA has no control – e.g. risks related to changes in government and/or government policy, changes in laws or regulations, social changes/movements, economic conditions, geopolitical situations, and the overall credibility of regulated health professions	• Moderate – innovation and growth welcomed with informed decision-making
Operational	Risks related to day-to-day business processes, systems, and tools, i.e. how the work is done. Examples include IT system failure, process breakdowns, document loss, delays and failure to follow procedures.	• Moderate – minor disruptions may be tolerated if plans are in place • No tolerance for non-compliance with safety practices
People and Leadership	Risks related to the capacity, wellbeing and leadership effectiveness of the people engaged in the work of the organization. For a small organization, the departure or absence of a single individual may have a significant operational impact.	• Low tolerance for risks that compromise ethical leadership, legal compliance or fiduciary responsibility • Moderate tolerance for risk related to staff development, cross-training, and delegation in order to build resilience and flexibility
Emergency	Risks relating to unforeseen and sudden events that interfere with NSRDDA's operations including, but not limited to, pandemics, extreme weather, natural disasters, accidents, floods, fire, failure of utilities, ineffective crisis response and preparedness, and ineffective business continuity planning	• Low – the NSRDDA seeks to ensure basic continuity of operations during disruptive events and maintains basic emergency plans, backups, and preparedness to ensure essential functions continue

Reputation	Risks related to a loss of reputation and goodwill, negative media or social media, negative public perceptions of the efficiency or quality of our operations, failure to adhere to our values and ethics, loss of reputation as a good employer	• Low – reputation is critical to public trust
Legal/ Compliance	Risks related to failure to meet legal or regulatory obligations, including but not limited to fines and other regulatory penalties for such matters as failure to comply with our governing legislation and regulations, remit payroll deductions, violations of privacy laws, human rights and employment standards legislation, occupational health and workplace safety legislation, and contractual obligations	• Very low – strict compliance with legal and regulatory frameworks is expected
Information Technology	Risks related to cybersecurity, ongoing relevance of technology infrastructure and assets, ineffective disaster recovery and back-ups, availability of IT expertise, privacy and data security, or system failture	• Low – strong controls required to protect sensitive data
Financial	Risks relating to budgeting, fraud, theft, rising costs, inadequate insurance, and major financial decisions	• Low to moderate – prudent financial management expected; small variances tolerable • No tolerance for fraud or theft
Governance	Risks related to ineffective oversight and poor decision-making by the Board and Statutory Committees due to lack of skills, competencies, training and leadership continuity	• Low – Board and Statutory Committee functioning are critical to the organization's success

6. Risk Capacity and Tolerance

The NSRDDA has limited capacity to absorb high-impact risks due to its small size, limited financial reserves, and public interest mandate.

The NSRDDA has low to moderate tolerance for most risks. It tolerates low-level operational or strategic risks where benefits outweigh consequences but has zero or very low tolerance for risks to its regulatory integrity, compliance, reputation or public trust.

7. Risk Management Process

Given the small size of the organization, risk monitoring and reporting must be both practical and embedded in routine operations. The following approach ensures proportional, time, and accountable risk management:

A. Risk Identification and Monitoring by Staff

- Each staff member is responsible for being alert to risks within their operational areas (e.g. registration, investigations, finance, IT, or communications).
- Staff will use a shared risk log (e.g., in Excel or a cloud-based platform like SharePoint or OneDrive) to note any:
  - New risks,
  - Changes in the severity or likelihood of know risks, or
  - Control failures or near-miss events.
- The Registrar will act as the central point of coordination for the risk log and will provide guidance on risk definitions, escalation thresholds, and documentation standards.

B. Quarterly Risk Review Meeting

- The full **staff team** will meet **quarterly** to:
  - Review the shared risk log
  - Discuss emerging or evolving risks
  - Evaluate whether current mitigations are sufficient, and
  - Assign follow-up actions where necessary.
- The meeting may be brief but must be documented (e.g., with brief notes or an update to the log).

C. Escalation and Reporting

- **Urgent risks** (e.g., a breach of data, a regulatory failure, or a serious reputational issue) must be reported immediately to the Registrar, who will notify the Board Chair as appropriate.
- The Registrar will summarize all material risks, along with staff input, in a **semi-annual report to the Board**, highlighting:
  - Top current risks
  - Any significant changes
  - Mitigation activities, and
  - Requests for strategic input or support.
- For issues relevant to **Statutory Committees**, the Registrar will report relevant risks in the regular committee materials or as part of briefing notes.

8. Risk Reporting

A shared Risk Register (risk log) is maintained and updated by staff and overseen by the Registrar. The Registrar reports semi-annually to the Board on key and emerging risks. Urgent or significant risks are reported to the Board Chair between meetings, if needed. The Risk Register includes risk category, description, likelihood, impact, current mitigation, and responsible person.

9. Monitoring and Policy Review

The Registrar is responsible for monitoring implementation of this policy. The policy will be reviewed in accordance with the Board's policy review cycle, or sooner if needed due to organizational or environmental changes.

10. Accountability

The Registrar is accountable for ensuring compliance with this policy.