

Version Number	Description of Changes	Effective Date
1	Initial release	2020-10-21
2	Comprehensive revision	2026-09-30

Purpose

To ensure that the Hawkesbury and District General Hospital (HGH) maintains an effective, integrated, and continuously improving risk management program that identifies, assesses, prioritizes, mitigates, and monitors the key strategic risks facing the organization, and that the Board of Directors is kept informed of those risks in a timely manner so that it can exercise meaningful oversight. This policy establishes the executive limitations within which the CEO must operate with respect to risk management.

Scope

This policy applies to the identification, assessment, mitigation, monitoring, and reporting of strategic and organization-wide risks across all HGH programs, services, and functions — including clinical, operational, financial, human-resources, information and cyber security, emergency-preparedness, regulatory, and reputational risk. It is the umbrella risk policy for the Executive Limitations series and is to be read together with the risk-specific limitations set out in:

- Policy 3.1 – Financial Planning / Budgeting
- Policy 3.2 – Financial Condition and Operational Performance
- Policy 3.5 – Protection of Assets and Prioritization of Disbursements (including cybersecurity and business continuity)
- Policy 3.12 – Quality of Medical Care
- Policy 2.1 – Delegation to the CEO.

Monitoring: Annually (May), through the HGH Risk Management Monitoring Report presented to the Finance and Planning Committee and the Scorecard presented to the Quality Committee. This report also carries the annual cybersecurity attestation required under Policy 3.5.17. Escalation of high-severity or high-likelihood risks occurs as they arise, in accordance with 3.15.4.

Guiding Principles

3.15.0 The HGH Board of Directors is committed to ensuring that an effective and integrated risk management program is in place to identify, assess and manage key risks to the organization.

3.15.0.1 Board Accountability for Risk Oversight: The Board retains accountability for overseeing the organization's risks; management is accountable for identifying, assessing, and managing them, and for reporting to the Board, through the Finance and Planning Committee, so that the Board can exercise that oversight.

3.15.0.2 Risk Appetite and Tolerance: The level of risk the organization is prepared to accept in pursuing its strategic objectives is established with the Board, which sets the tone for acceptable risk through its delegation, approvals, and oversight.

3.15.0.3 Integrated, Proactive, and Continuous: Risks are managed from an organization-wide, aggregate perspective in a continuous, proactive, and systematic manner, rather than in isolated silos.

	Board of Directors Policy	V.2	Page 2/5
3.15 Risk Management Executive Limitations			

Definitions

Integrated Risk Management: A continuous, proactive, systematic approach to identifying, assessing, prioritizing, acting on and reporting strategic risks from an organizational-wide, aggregate perspective.

Risk: The possibility of loss or harm; described in terms of likelihood of occurrence and the associated impact should it occur. The terms '*risk*' and '*hazard*' are not interchangeable: a hazard is a source of potential damage or harm (e.g. water on the floor), while a risk is the potential that harm will occur if exposure to the hazard occurs (e.g. visitor fall).

Risk Appetite and Risk Tolerance: The amount and type of risk the organization is willing to accept in pursuit of its strategic objectives (appetite), and the acceptable variation around that level for a given risk (tolerance), as established with the Board.

Risk Escalation: The prompt reporting of a risk to the Board, in accordance with criteria established with the Board, based on its likelihood, severity of impact, or the adequacy of existing controls.

Risk Register: The maintained record of the organization's identified strategic and enterprise risks, including their assessed likelihood and impact, assigned most-responsible person, existing controls, mitigation strategies, and status.

Strategic Risks: Risks that pose major threats to achieving the organization's vision and strategic objectives related to patient care and human resources; finances, leadership, information management, facilities, regulations, external relations, teaching, research and reputational risk.

Procedure

Accordingly, the CEO:

- 3.15.1** Shall not fail to develop a comprehensive integrated risk management program for identifying, assessing, managing and monitoring key strategic risks to the organization and prioritize risk probability and impact, drawing on input from the Board, leadership, and management.
- 3.15.2** Shall not fail to identify controls/mitigation strategies to manage the top risks facing the organization.
- 3.15.3** Shall not fail to proceed to a complete revision of all interpretations of Board Executive Limitation policies over a four-year cycle.
- 3.15.4** Shall not fail to keep the Board informed of organizational risks in a timely manner, including the prompt escalation of risks that meet the criteria established with the Board — whether by likelihood of occurrence, severity of impact, or inadequacy of existing controls — together with the associated mitigation and response plans. Escalation shall not be deferred to the annual monitoring cycle.
- 3.15.5** Shall not fail to maintain a current risk register of the organization's strategic and enterprise risks, updated at least bi-annually, identifying for each risk its assessed likelihood and impact, its most-responsible person, and its mitigation strategies, and to review it with the Board at least annually.
- 3.15.6** Shall not manage clinical, operational, financial, human-resources, information and cyber, emergency-preparedness, regulatory, and reputational risks in isolation from one another, and shall not fail to integrate them into a single organization-wide view of risk for the Board, while ensuring that risks falling within the mandate of another standing committee are also reported to that committee.
- 3.15.7** Shall not fail to ensure that risk identification and assessment consider harms arising from racism and discrimination, and any disproportionate impacts on Indigenous peoples, Francophone communities, and equity-deserving communities.

References

- ❖ **Public Hospitals Act, R.S.O. 1990, c. P.40, and Regulation 965** (*Hospital Management — critical incident reporting*)
- ❖ **Excellent Care for All Act, 2010, S.O. 2010, c. 14**
- ❖ **Connecting Care Act, 2019, S.O. 2019, c. 5** (*Hospital Service Accountability Agreement*)
- ❖ **Personal Health Information Protection Act, 2004 (PHIPA), S.O. 2004, c. 3, Sched. A**
- ❖ **Occupational Health and Safety Act, R.S.O. 1990, c. O.1**
- ❖ **HGH Corporate By-laws (June 26, 2024)**
- ❖ **HGH Risk Management Framework**
- ❖ **HGH Risk Register (HIROC Risk Evaluation Tool)**
- ❖ **HIROC Risk Assessment Checklist (RAC) Program**
- ❖ **HGH Risk Management Monitoring Report and Scorecard**
- ❖ **HGH Emergency and Disaster Management Corporate Policy; HGH Cyber Security Incident Response Plan**
- ❖ **Guide to Good Governance (OHA) – 4th Edition – Chapter 3** (*Risk Management; risk tolerance and risk appetite; information systems and cyber-attack oversight; Monitoring Quality Risk Management*)
- ❖ **Accreditation Canada – Governance Standards (HSO A1001:2022) – Standard 3.1.9** (*governing body kept informed of organizational risks in a timely manner — High Priority*), 3.1.10 (*business continuity*), 3.4.4, Sections 5–6 (*cultural safety*)
- ❖ **Policy 1.5 – Board Committee Principles and Structure** (*Finance and Planning Committee*)
- ❖ **Policy 2.1 – Delegation to the CEO**
- ❖ **Policy 2.3 – CEO Monitoring**
- ❖ **Policy 3.1 – Financial Planning / Budgeting**
- ❖ **Policy 3.2 – Financial Condition and Operational Performance**
- ❖ **Policy 3.5 – Protection of Assets and Prioritization of Disbursements and Policy 3.5.17 – cybersecurity attestation** (*delivered through this report*).
- ❖ **Policy 3.12 – Quality of Medical Care**
- ❖ **HGH Strategic Plan 2025–2029**

Appendix A – Risk Escalation Protocol

Board-approved criteria for the timely escalation of organizational risks under Limitation 3.15.4

Purpose: This appendix sets out WHICH risks are escalated to the Board, HOW, and HOW QUICKLY, as required by Executive Limitation 3.15.4. Escalation under this protocol is in addition to, and never deferred to, the annual Risk Management Monitoring Report presented to the Finance and Planning Committee each May.

1. Escalation tiers

Tier	Escalation criteria	Route and timing	Evidence
TIER 1 Immediate	Risk or event that is occurring or imminent AND could materially disrupt clinical services, patient safety, financial viability, legal/regulatory standing, or public trust. Includes any risk scored in the HIROC register as high likelihood AND high impact where existing controls have failed or are inadequate.	The CEO notifies the Board Chair within 24 hours (verbally or in writing) and, where circumstances warrant, the Chair of the Finance and Planning Committee. The Board Chair determines whether a special meeting of the Board is required or whether written follow-up with the Board will suffice.	Written notice + Board/Committee minutes
TIER 2 Next meeting	Significant change in a registered risk — a material increase in likelihood or impact, a control failure without immediate service disruption, or a new risk warranting addition to the register.	Reported by the CEO to the Finance and Planning Committee at its NEXT SCHEDULED MEETING, with the mitigation and response plan.	Committee agenda item + minutes
TIER 3 Annual cycle	All other registered strategic and enterprise risks, including status of mitigation plans and register updates.	Reported through the annual Risk Management Monitoring Report and Scorecard (May) and the bi-annual risk register update.	Annual monitoring report

2. Illustrative Tier 1 triggers (not exhaustive)

Risk domain	Examples
Cybersecurity / privacy	Ransomware or successful intrusion; sustained outage of a clinical system; privacy breach requiring notification to the Information and Privacy Commissioner of Ontario.
Patient safety / quality	A critical incident as defined under the Public Hospitals Act; a cluster of serious adverse events; a coroner's or College investigation into hospital care.
Clinical service continuity	Imminent or actual closure, diversion, or suspension of an essential service (e.g. Emergency, Obstetrics) for reasons of staffing, equipment, or infrastructure.
Financial	Projected material deviation from a balanced budget; breach or imminent breach of the 1.5 current-ratio floor (Policies 3.1 / 3.2); loss or material reduction of funding.
Regulatory / legal	Order, directive, or investigation by the Ministry of Health, Ontario Health, or a regulatory body; litigation or claim with material financial or reputational exposure.
Emergency / infrastructure	Activation of a hospital-wide emergency code with sustained operational impact; failure of critical infrastructure (power, water, HVAC, building envelope).
Workforce / reputation	Loss or imminent loss of a critical clinical group; labour disruption; a workforce safety event with serious harm; any of the above carrying significant media, community, or political exposure.

3. Minimum content of an escalation notice

- What has occurred or is anticipated, and when it was identified.
- Assessed likelihood and impact, and the corresponding entry in the HGH Risk Register (if registered).
- Which controls failed, were inadequate, or were absent.
- Immediate actions taken, the mitigation and response plan, and the most-responsible person.

	Board of Directors Policy	V.2	Page 5/5
	3.15 Risk Management Executive Limitations		

- Regulatory, legal, funding, or disclosure obligations triggered, and any external reporting made.
- What the Board is being asked to do: note, direct, or decide.

4. Recording, follow-up and review

- Every Tier 1 and Tier 2 escalation is recorded in the Board or Committee minutes and carried into the next annual monitoring report, which confirms resolution or continued mitigation.
- Escalated risks are added to or updated in the HGH Risk Register at the next bi-annual update, or immediately where the risk is material.
- This protocol is reviewed by the Finance and Planning Committee at least every two years, or following any Tier 1 escalation that reveals a gap in these criteria.