21 Questions

Guidance for healthcare boards on what they should ask senior leaders about risk.

Drawing on strong ethical and evidence-based principles, HIROC, in collaboration with subscribers, has developed guiding questions to help boards of healthcare organizations carry out a critical governance function – the oversight of key organizational risks.

Strategic context

1 What are the organization's vision and strategic objectives and do they reflect the core mandate of delivering high quality, safe care?

Board education

2 How does the board get the knowledge and experience necessary to oversee risk management in a healthcare organization?

Risk culture

3 What is the board doing to encourage speaking up across the organization about potential risks and unsafe practices?

Risk management program

4 What is the organization's policy/ plan/framework for identifying, assessing and managing key risks?

5 How do senior leaders demonstrate ownership for key risks?

Key risks (patients & staff)

6 What are the most significant risks related to care?

7 What are the themes/trends arising from patient complaints?

8 What are the most significant risks related to human resources?

Key risks (other)

9 What are the most significant risks related to finances?

10 What are the most significant risks related to leadership?

11 What are the most significant risks related to external relations?

12 What are the most significant risks related to information management/ technology?

13 What are the most significant risks related to facilities/infrastructure?

14 What are the most significant risks related to regulatory compliance?

15 What are other significant risks (e.g. research, education)?

Risk management

16 How are decisions made on additional controls or actions required to manage key risks?

Risk prioritization

17 How do senior leaders determine top organizational risks and which risks to report to the board?

Risk reporting

18 What records are kept for key risks and how do these roll-up into regular, effective reports for management and the board?

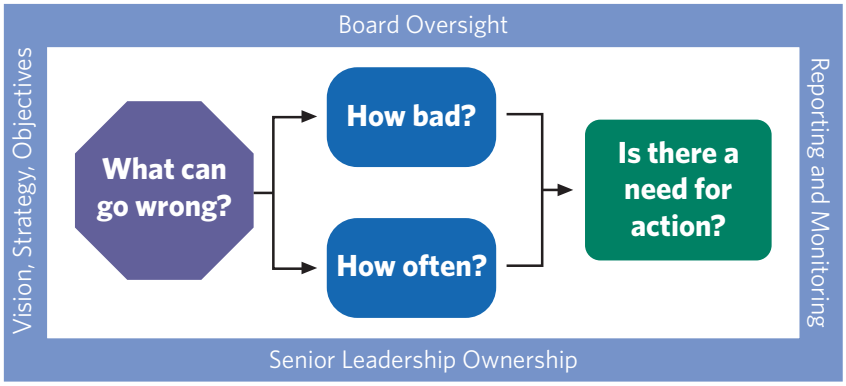
Crisis response

19 How does the organization plan for, respond to and learn from crises?

Assurance and evaluation

20 How is the board assured that controls for key risks are working?

21 How is the organization's risk management program evaluated?



A simplified risk management framework

21 Questions

Guidance for healthcare boards on what they should ask senior leaders about risk.

HIROC

Questions and Recommended Practices

Strategic context

1 What are the organization's vision and strategic objectives and do they reflect the core mandate of delivering high quality, safe care?

- ☑ Ensure the organization's vision, mission, values and strategic objectives reflect the core business of healthcare including patient care and ensuring patient safety.
- ☑ Use the organization's risk management knowledge and reports to inform strategic planning activities and annual operational planning.

Board education

2 How does the board get the knowledge and experience necessary to oversee risk management in a healthcare organization?

- ☑ Incorporate training on healthcare risk management in board orientation and through regular board education sessions.
- ☑ Ensure generative discussion at least once a year on healthcare risk management and emerging trends.
- ☑ Identify a select number of board members to be 'risk champions'.

Risk culture

3 What is the board doing to encourage speaking up across the organization about potential risks and unsafe practices?

- ☑ Understand the principles of "high reliability organizations" and create an environment to enable: preoccupation with failure, sensitivity to operations, deference to expertise, resilience, and reluctance to simplify interpretations.
- ☑ Communicate expectations to senior leaders that they openly discuss risk issues and concerns with the board.
- ☑ Ensure senior leaders foster psychological safety throughout the organization and that staff feel comfortable raising concerns related to risks and unsafe practices.
- ☑ Measure staff comfort level in speaking up through safety culture surveys.

Risk management program

4 What is the organization's policy/plan/framework for identifying, assessing and managing key risks?

- ☑ Develop and implement a risk management policy that operationalizes a simplified approach to integrated risk management.
- ☑ Ensure a board sub-committee (e.g. finance or quality) has ownership for the risk management program.
- ☑ Ensure adequate resources to coordinate organizational risk management efforts.

5 How do senior leaders demonstrate ownership for key risks?

- ☑ Ensure every key risk has an accountable senior leader assigned to it.
- ☑ Ensure the senior leader accountable for a risk is the one to speak to that risk at board meetings.

Key risks (patients & staff)

6	What are the most significant risks related to care?	☑ Receive regular reports related to patient harm and "never events" (including types, frequency and severity). ☑ Ask probing questions regarding steps being taken to reduce patient harm. ☑ Ensure risks related to care have prominence on the organization's risk register report.
7	What are the themes/trends arising from patient complaints?	☑ Incorporate trends from patient complaints into the organization's risk identification process. ☑ Ensure the board receives regular reports on patient complaints and experience.
8	What are the most significant risks related to human resources?	☑ Incorporate trends from staff incidents, engagement and culture surveys into the organization's risk identification process. ☑ Ensure the board receives regular reports on staff safety and engagement. ☑ Ensure an effective process for credentialing of independent health professionals (e.g. physicians).

Key risks (other)

9	What are the most significant risks related to finances?	☑ Ensure requirements are met in relation to a balanced budget. ☑ Incorporate trends from internal/external audits into the organization's risk identification process. ☑ Ask probing questions regarding steps being taken to reduce financial risk (e.g. contracts, fraud, funding).
10	What are the most significant risks related to leadership?	☑ Monitor common leadership related risks (e.g. leadership succession, culture, change management, strategic projects). ☑ Regularly review the organization's policies to prevent conflicts of interest and ethical breaches.
11	What are the most significant risks related to external relations?	☑ Incorporate data from community complaints, media relations (including social), and fundraising issues into your risk identification process. ☑ Regularly review reports on government and community engagement.
12	What are the most significant risks related to information management/ technology?	☑ Incorporate trends from information and technology-related incidents into your risk identification process. ☑ Ensure there are plans to monitor and manage cybersecurity.
13	What are the most significant risks related to facilities/ infrastructure?	☑ Incorporate trends from facility-related issues into the risk identification process. ☑ Ensure there are plans to monitor and manage facility-related risks.
14	What are the most significant risks related to regulatory compliance?	☑ Maintain an inventory of appropriate legislation and regulations that includes periodic assessment of compliance and plans to address significant gaps. ☑ Ensure a robust policy and framework for management of privacy.
15	What are other significant risks (e.g. research, education)?	☑ Ensure a robust research ethics program to review research activities.

Risk management

16 How are decisions made on additional controls or actions required to manage key risks?

- ☑ Ask probing questions regarding how key risks are managed (e.g. reduced, avoided, shared, and/or retained) and the overall adequacy of controls.
- ☑ Review insurance coverages and trends on an annual basis.

Risk prioritization

17 How do senior leaders determine top organizational risks and which risks to report to the board?

- ☑ Implement a quantitative, objective risk scoring framework for assessing relative impact and likelihood of risks.
- ☑ Ensure senior leaders periodically report on lower scoring but concerning or emerging risks.

Risk reporting

18 What records are kept for key risks and how do these roll-up into regular, effective reports for management and the board?

- ☑ Employ an easy to maintain risk register.
- ☑ Ensure regular reporting of the risk register to the board (e.g. at least semi-annually at sub-committees, annually with full board).

Crisis response

19 How does the organization plan for, respond to, and learn from crises?

- ☑ Ensure there is a crisis response plan (including a business continuity plan as appropriate) to cover a range of key risks.
- ☑ Ensure that staff are aware of their roles in a crisis and practice response plans on a regular basis.
- ☑ Ensure clarity on what crises should be reported to the board.
- ☑ Ensure a process for debriefing following every crisis.

Assurance and evaluation

20 How is the board assured that controls for key risks are working?

- ☑ Receive reports regarding serious patient/staff safety events including the implementation of recommendations.
- ☑ Establish an audit plan to ensure key controls put in place to manage key risks have been implemented.

21 How is the organization's risk management program evaluated?

- ☑ Annually assess the maturity of the risk management program.
- ☑ Annually assess effectiveness of the risk management program (e.g. compliance with the 21 questions and recommended practices).

Appendices and Resources

A. Case study

B. Sample Risk Policy & Risk Register Report

C. Core Knowledge & Other References

21 Questions

Appendix A

Case Study:

The Mid Staffordshire NHS Foundation Trust Public Enquiry

Background and Context

The Mid-Staffordshire National Health Service (NHS) Foundation Trust (Mid-Staffs) was a 500 bed, dual site acute care hospital approximately 250km north-west of London, UK. Over the course of a number of years (2005-2009), it was estimated that between 400 and 1200 patients died as a result of poor or substandard care received at Mid-Staffs. Considered one of the biggest scandals in the NHS, patients were treated in unsafe settings, often discharged inappropriately, kept in substandard or unsanitary conditions, administered pain medication late or not at all, or left in an undignified, soiled state for hours without attention from staff.

Five inquiries occurred in order to investigate the care at the hospital and the appalling conditions patients experienced. The culminating inquiry, led by Sir Robert Francis, QC, identified significant risks to patient care and a toxic work and patient safety culture within Mid-Staffs. His report also identified systemic failures within the Trust and outside the Trust that failed to properly identify problems within the hospital or allowed known problems to persist for years.

"The Trust Board was weak. It did not listen sufficiently to its patients and staff or ensure the correction of deficiencies brought to the Trust's attention."

Summary of Key Findings Related to Risk Management and Patient Safety

- Warning signs indicating problems with the quality of care and patient experience were ignored by the board and senior leadership within the organization. Many in the organization did not feel they had the ability to speak up or be heard should they have wished to express a concern related to patient care.
- The board ignored external reports, audits, and peer reviews of the performance of the organization and did not ensure proper oversight and accountability to ensure the recommendations of these reports were implemented.
- Many audits called into question the effectiveness of the organization's risk management program citing a lack of attention to organizational risks other than the achievement of financial targets or other metrics reported on the organizations scorecard; the board was not focused on or ignored improving patient quality or care.
- A perilous and negative safety culture was noted to be pervasive throughout the organization up to and including the Trust's board. Despite data indicating significant quality of care problems, those charged with quality improvement, namely the board and leadership, failed to act or appreciate the gravity of the situation, or in some cases, simply ignored the problem. It was noted that an engrained culture existed that was tolerant of poor standards, exhibited a focus on finance and targets, denial

"It (the Board) did not tackle the tolerance of poor standards and the disengagement of senior clinical staff from managerial and leadership responsibilities."

of concerns, and an isolation from practice elsewhere. The Trust's culture was also focused on self-promotion, rather than self-reflection and openness. It took false assurance from good news and rationalized or ignored bad news.

- Trust management and the board had no culture of listening to patients and there were inadequate process for dealing with complaints. This was attributed also to inattention and a lack of importance placed on complaints by management and the board.
- The board failed in its responsibility to exercise good governance and accountability practices; while focused on financial targets, the board completely abdicated its responsibility to provide oversight and effective risk management practices in areas related to patient care.

"These failures were in part due to a focus on reaching targets, achieving financial balance and seeking foundation trust status at the cost of delivering acceptable standards of care."

Key Recommendations Related to Risk Management and Patient Safety

1. Organizations must employ rigorous and robust systems to ensure that a culture or openness and commitment to safe care exists throughout the organization from the frontline to the board. For example, staff must be free to speak up, feel that they will be heard, decisions must be made with patient care being a top priority, a commitment to learn from mistakes, intolerance of poor standards, and looking inwards not outwards.
2. The board and senior leadership are the key components to promoting a positive safety culture.
3. Boards and senior leadership need to understand that they are responsible for patient safety and quality of care. As part of their overall accountability to patients, they need to monitor risks to patient care and ensure senior leadership is focusing on reducing risks to patients.
4. Board members should be trained in fundamentals of patient safety, quality improvement, and risk management.
5. Boards need to ensure as part of their risk management program, a robust assurance and compliance program to ensure that standards are being met and that the board receives accurate information on quality of care and patient safety within the organization.

"The patient voice was not heard or listened to, either by the Trust Board or local organizations which were meant to represent their interests. Complaints were made but often nothing effective was done about them."

For More Information

Inquiry Chairman's Press Statement

Full Inquiry Report

Channel 4 News (UK) video summary

21 Questions

Appendix B

Risk Management – Sample Policy

Purpose

The board of [insert organization name here] is committed to ensuring an effective and integrated risk management program is in place to identify, assess, and manage key risks to the organization.

Policy

1. The board of [insert organization name here] will oversee a comprehensive integrated risk management program for identifying, assessing, managing, and monitoring key risks to organizational objectives and prioritizes risks with high probability and impact.
2. The board will lead the organization in developing a culture that fosters physical and psychological safety throughout the organization so that staff feel comfortable raising and escalating concerns.
3. The senior leadership team is responsible for operationalizing the organization's integrated risk management program.
4. The board ensures the controls/mitigation strategies have been identified to manage the top risks facing the organization.
5. The board ensures that necessary resources available to assist those accountable and responsible for managing risk.

Definitions

- Risk – The possibility of loss or harm; described in terms of likelihood of occurrence 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).
- Strategic Risks – Risks that pose major threats to achieving the organization's vision and strategic objectives particularly related to patient care and human resources; could also include risks related to finances, leadership, information management, facilities, regulations, external relations, teaching and research.
- 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 Register – A report providing a high level summary of the strategic risks to the organization and including information related to risk owner, risk ratings, and key controls.

Oversight

The [insert board/committee name here] will be responsible for oversight of risk management at [insert organization name here].

Reporting

The corporate risk register will be presented and discussed [frequency] at the meeting of the [insert board committee name here]; and [annually/semi-annually] to the whole board.

Risk Management – Sample Risk Register Report

REF #	Risk category	Risk name	Description	Senior Lead	Controls	Gaps	Impact (current)	Likelihood (current)	Risk level (initial)	Risk level (current)	Adequacy of controls
CARE-1	Care	Access	The risk that the organization is not able to provide appropriate level or access to services. Demand > Capacity.	F. Jones	Patient and family advisory council/ patient perspective; Daily safety huddle;	Contingency plan development;	High	Medium	Very High	High	High
CARE-2	Care	Medication Errors	Risk of overdose with high alert medications.	F. Jones	Medication reconciliation (admission, transfer, discharge); Two identifier policy and audit;	Independent double check knowledge and testing;	High	High	High	High	Medium
HR-1	Human Resources	Workplace Violence	Risk of significant harm from violence against staff.	L. Peters	Violence in the workplace policy (including zero tolerance); Non-violent crisis intervention;	Crisis response drills;	Medium	Low	Medium	Medium	Medium
IT-1	IS/ Technology	Breach/ Loss of Information	Risk of a data breach (internal or external) and compromise of patient data.	J. Smith	Timely application of security patches and upgrades; Penetration tests;	Intrusion detection and notification solutions; Cyber incident management plan;	High	High	High	High	Medium
LEAD-1	Leadership	Strategic Projects	Risk of deficiencies/failures in large scale projects.	L. Clark	Clearly defined scope, plans, deliverables; Project Manager hired;	Stakeholder engagement; Insurance (building/ construction);	High	High	Very High	High	High
FIN-1	Financial	Revenue/ Funding	Risk of insufficient revenue/funding.	L. Clark	Government communication strategies; Contingency plan in place for unanticipated expenses;	Approve and monitor project enhancements;	High	Low	High	Medium	Very high

21 Questions

Appendix C

Core Knowledge & Other References

Core Knowledge:

HIROC Risk Notes – concise two page documents providing risk management information on topics that matter in healthcare

- Risk – Concepts and Misconceptions
- Risk Assessment
- Risk Identification
- Risk Management
- Integrated Risk Management (IRM/ERM)
- The Link Between Risk Management, Patient Safety, and Quality Improvement
- Patient Safety
- Just Culture
- Risk Notes: High Reliability and Resiliency, Human Error and Human Factors, Patient Engagement

HIROC Common Taxonomy of Key Risks in Healthcare Organizations

Other Risk Management References:

HIROC Risk Profiles: information on best practices for managing key risk from a shared risk management database (e.g. Care - Access, Finanical - Revenue/Funding, Human Resources - Workplace Violence/Disruptive Behaviour)

Caldwell, J. (2012). A framework for board oversight of enterprise risk. Chartered Accountants of Canada.

Chartered Professional Accountants of Canada. (2009). 20 questions directors of not-for-profit organizations should ask about risk.

Mikes A, Kaplan R. (2014). Towards a contingency theory of enterprise risk management. Harvard Business School Working Paper.

Other Patient Safety References:

Berwick D, Shojania K, et al. (2015). Free from harm: accelerating patient safety improvement fifteen years after *To Err Is Human*. National Patient Safety Foundation.

Canadian Institute for Health Information, Canadian Patient Safety Institute (2016). Measuring patient harm in Canadian hospitals.

Canadian Patient Safety Institute. (2018). A framework for establishing a patient safety culture.

Canadian Patient Safety Institute. (2015). Never events for hospital care in Canada: safer care for patients.

HIROC

HIROC is Canada's leading provider of healthcare liability insurance. As a not-for-profit, we partner with our subscribers to provide innovative insurance and risk management solutions that help them reduce risk, prevent losses and improve patient safety.

www.hiroc.com

4711 Yonge Street, Suite 1600
Toronto, ON M2N 6K8
416-733-2773
Toll Free: 1-800-465-7357

1200 Rothesay Street
Winnipeg, MB R2G 1T7
204-943-4125
Toll Free: 1-800-442-7751

PARTNERING TO CREATE THE SAFEST HEALTHCARE SYSTEM