Integrated Risk Management for Healthcare Organizations

Risk Resource Guide

October 2014

PARTNERING TO CREATE THE SAFEST HEALTHCARE SYSTEM

IRM for Healthcare Organizations

Acknowledgements
This document was prepared, in part, with the input of a HIROC subscribers in various stages of IRM implementation. Their candid reflections and advice is greatly appreciated. HIROC would also like to thank members of the IRM Steering Committee (2014) for their dedication, insights and support.

Comments
This document will be updated as new information and insights arise. We are very interested in receiving questions, suggestions and feedback regarding this work. Please direct your comments to:

Risk Management
Healthcare Insurance Reciprocal of Canada (HIROC)
4711 Yonge St. Suite 1600
Toronto, Ontario M2N 6K8

Tel: 1-800-465-7357
Email: riskmanagement@hiroc.com

Overview of Version Changes
Originally published in May, 2011, this version of the guide represents a significant revision to content.

IRM for Healthcare Organizations

Contents

IRM for Healthcare Organizations

Introduction

> Risk is an inescapable part of every decision. For most of the everyday choices people make, the risks are small. But on a corporate scale, the implications can be enormous. (Buchanan, 2006, p.34).

> Effective risk management is now the most pressing business issue of our time. (Moore, 2013, p.5).

High profile failures in the business, financial, and healthcare sectors have underscored the importance of anticipating and attending to serious organizational risks. Healthcare is complex, and many organizations manage risks independently as a patchwork of risk management activities within horizontal or vertical silos. The result is that one type of risk may receive attention and resources while another more important risk goes undetected or unacknowledged. Consequences of ineffective management of risks range from organizational underperformance to catastrophic failures that could threaten the continued existence of the organization. (Caldwell, 2012).

The systematic application of risk management across an organization has many names. The terms *integrated* risk management (IRM) and *enterprise* risk management (ERM) are seen as synonymous. IRM is used in this guide as it aligns with Accreditation Canada standards, it is used more frequently in the public sector, and it better reflects the objective of aligning and coordinating the risk management processes which are already in place in most healthcare organizations.

IRM provides a framework for understanding and prioritizing very different types of risks from across an organization; for creating a concise summary of the most significant risks; and for identifying whether further work is required to bring these risks to acceptable levels. Unfortunately progress towards effective IRM has been slow. There is a great deal of uncertainty about the best approach for use in healthcare and how risks should be identified, assessed and managed. Sometimes well-intentioned activities are undertaken in the name of IRM which, in retrospect, are frustrating and add little value. Efforts may also stall in the absence of senior leadership support or resources to carry out key coordinating functions. The end result is lost time and resources with little realized benefit.

The purpose of this guide is to synthesize published and tacit knowledge about IRM and to provide advice on the efficient and effective implementation of IRM in healthcare. This guide also provides background information on HIROC's on-line Risk Register tool, a common platform for use by HIROC subscribers to capture, collate and report information on their key organizational risks.

IRM Drivers and Benefits

A number of interrelated drivers and potential benefits provide the impetus for implementation of IRM in healthcare including:

1. Effective Governance and Accountability

> Boards must focus on looking after quality, and expect resources to fall out of that process, not the other way round. Where the NHS has failed patients on quality, too often a dysfunctional board has focused in the wrong areas and without the appropriate governance arrangements in place to improve quality for patients. (NLC, 2012, p.2).

Scandals in the financial sector have resulted in regulations dictating increased involvement of boards in managing organizational risk. In healthcare, boards are also being held to account not only for fiscal performance but for quality and safety outcomes as well. (Baker, 2012).

The Case of Mid Staffordshire (UK)

The Mid Staffordshire NHS Foundation Trust was a 500-bed, dual-site hospital about 250 km north-west of London, England. It became the centre of an international scandal, and a cautionary case study in risk governance and management, after it was determined that up to 1,200 patients died due to substandard care between 2005 and 2008 (Smith, 2010). The organization was the subject of a number of external reviews including two high-profile public inquiries chaired by Robert Francis, QC. The first inquiry, completed in February 2010, focused on what had gone wrong internally at the trust. The second inquiry, completed in February 2013, focused on the role of the wider healthcare system in preventing the events at Mid Staffs.

Francis uncovered many shortcomings in the organization and the broader system of regulation and oversight, but the greatest failure was seen to be an ineffective board that ignored the biggest risk facing the organization – the risk to patients of poor quality care.

> What brought about this awful state of affairs? 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. It did not tackle the tolerance of poor standards and the disengagement of senior clinical staff from managerial and leadership responsibilities. 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.
>
> …There was an institutional culture in which the business of the system was put ahead of the priority that should have been given to the protection of patients and the maintenance of public trust in the service. It was a culture which too often did not consider properly the impact on patients of actions being taken, and the implications for patients of concerns that were raised. (Francis, 2013, p.2).

In a review of multiple high profile catastrophes in NHS organizations, including Mid Staffs, Moore found a number of organizational similarities and shortfalls:

- Disconnect between the board and clinical teams related to the organization's purpose and objectives;
- Poor alignment between objectives and risk activities;
- Lack of recognition of high impact, low probability events;
- Insufficient board time allocated to review of risk reports and registers;
- Complex and overwhelming risk reports and registers;
- Risk management function operating in a corporate vacuum, remote from clinical teams. (Moore, 2012).

2. Organizational Performance

> An ERM maturity transition from a silo-based risk management process that lacks discipline and enterprise wide coordination to a mature ERM environment with established ERM routines and engagement from the top of the firm could create a value improvement of as much as 25%. (Farrell, 2014, p.28).

It has been suggested that there are two main benefits to implementing IRM: (1) reduction in the number of surprises (and losses) in the future; and (2) better allocation of valuable organizational resources (Fraser, 2007).

The International Organization for Standardization (ISO) 31000 guide to risk management provides a related and expanded list of potential benefits including:

- Improved identification of threats;
- Improved organizational learning;
- Minimization of losses;
- Improved controls;
- Increased likelihood of achieving objectives;
- Better decision making and planning;
- Improved loss prevention and incident management;
- Effective allocation and use of resources for risk treatment;
- Improved operational effectiveness and efficiency;
- Improved governance;
- Improved stakeholder confidence and trust;
- Compliance with relevant legal and regulatory requirements and international norms;
- Improved financial reporting. (CSA, 2011)

IRM is considered an emerging discipline and literature on its impact on organizational outcomes is inconclusive. However, a recent study shows a strong correlation between aspects of IRM maturity and improved financial performance (Farrell, 2014). In other work involving publically traded companies in the US, a statistical link has been shown between higher levels of risk management maturity and higher stock price returns and lower stock price volatility (Aon, 2013).

3. High Reliability and Resiliency

> High Reliability Organizations have a big incentive to contain the unexpected because when they fail to do so, the results can be catastrophic. Lives can be lost, but so can assets, careers, reputations, legitimacy, credibility, support, trust, and goodwill. (Weick, 2001, p.18).
>
> (Mid Staffs) was a culture which trumpeted successes and said little about failings (Francis, 2012, p.3).

A robust system for identifying, assessing and acting on key risks will help to drive an organization towards high reliability and resiliency – aspects of corporate performance not strictly related to the financial bottom line. Healthcare is a high-risk industry and healthcare organizations with their high numbers of employees, high degree of interdependence, complex technology, and extensive regulations are very complex. There is relentless public scrutiny and pressure to manage the unexpected well – to be resilient. This resiliency is dependent upon the extent to which disabling risks are anticipated, and how well the organization is able to adapt to problems as they emerge. (Moore, 2012).

Research into organizations in complex and high-risk industries (including healthcare) who experience less than their expected number of adverse events has yielded a common set of characteristics. These "highly reliable organizations" (HROs) develop and maintain organizational "mindfulness" through:

- Preoccupation with failure – acting on small signals of failure and guarding against complacency and hubris; identifying problems in their early stages when they can be addressed inexpensively and without disruption instead of waiting until they grow into larger failures;

- Reluctance to simplify interpretations – appreciating that their environments are complex, unstable, and unpredictable; positioning themselves to see as much as possible while recognizing that their understanding may be incomplete;
- Sensitivity to operations – being attentive to the front lines and the core work of the organization;
- Commitment to resilience – focusing on early reporting and communication of issues; keeping errors small before they devolve into more damaging situations;
- Deference to expertise – having established hierarchies but in times of stress seeking out and deferring to the individuals or teams with the most expertise (versus those with positional authority). (Weick, 2007).

HROs recognize and guard against the harmful effects of success specifically: complacency; inattention; and the development of tunnel vision and blind spots. In contrast, Mid Staffs had a culture which gave more weight to positive information about the organization than information that implied a cause for concern. (Francis, 2012).

> In effect, success narrows perceptions, changes attitudes, feeds confidence in a single way of doing business, breeds over confidence in the efficacy of current abilities and practices, and makes leaders and others intolerant of opposing points of view (Weick, 2007, p.52).

4. Accreditation and Government Expectations

Accreditation Canada standards for healthcare organizations outline the need for leadership teams to implement integrated risk management and for governing bodies to work with their chief executives to reduce risk (Accreditation Canada, 2013). The following table provides the specific wording of risk-related governance and leadership standards.

Table 1: Accreditation Canada Leadership Standards related to IRM

No.	Governance Standard
11	**The governing body works with the CEO to reduce risks to the organization and promote ongoing quality improvement.**
11.3	The governing body ensures that an integrated risk management approach and contingency plans are in place.
No.	**Leadership Standard**
4	**The organization's leaders plan and design the organization's services to meet the needs of the community.**
4.5	When developing the organization's vision and strategic plan, the organization's leaders assess risks and opportunities for the organization.
12	**The organization's leaders have a process to manage and mitigate risk in the organization.**
12.1	The organization's leaders use a structured process to identify and analyze actual and potential risks or challenges (includes classifying risks according to likelihood of occurrence and potential severity of impact).
12.2	The organization's leaders implement an integrated risk management approach to mitigate and manage risk.
12.3	As part of the integrated risk management approach, the organization's leaders develop contingency plans.
12.4	The organization's leaders disseminate the risk management approach and contingency plans throughout the organization.
12.5	The organization's leaders evaluate the effectiveness of the integrated risk management approach and make improvements as necessary.
12.6	As part of the integrated risk management approach, the organization's leaders follow established

	policies and procedures for selecting and negotiating contracted services.
12.7	As part of the integrated risk management approach, the organization's leaders evaluate the quality of contracted services.

IRM has been adopted by a number of provincial Ministries of Health with growing expectations for use by government funded healthcare organizations. The Treasury Board of Canada has also endorsed IRM and has published a guide and recommended approach to its implementation. (Treasury Board of Canada Secretariat, 2012).

IRM Challenges

> With such an abundance of principles, guidelines, and standards, scholars might conclude that (enterprise) risk management is a mature discipline with proven unambiguous concepts and tools that need only regulations and compliance to be put into widespread practice. We disagree. We believe that risk management approaches are largely unproven and still emerging. Apparently, so do the many practitioners who have expressed dissatisfaction with the proposed normative and regulatory ERM frameworks. (Mikes, 2014, p.3).

There are considerable challenges and costs (including opportunity costs) associated with IRM implementation and unfortunately the value of IRM has not always been realized. In a survey of large international organizations that had adopted IRM, only 26% of respondents said that IRM's influence on overall strategic planning was very significant or significant, with 64% saying it was partial or very little. When asked to identify barriers to successful IRM implementation, 40% said lack of tangible benefits; 34% - lack of skills and capability; 31% - lack of senior leadership support; and 30% - unclear ownership and responsibility for implementation. (Aon, 2010). Even in the NHS in England, a healthcare system with advanced IRM programs, it was found that there was considerable scope to improve the identification and specification of corporate risks, and to improve integration of risk management in the day-to-day running of organizations (Audit Commission, 2009).

One of the biggest barriers to successful implementation is seen to be overly complicated structures and processes.

> Why has it taken so long to get ERM up and running? There are a large number of common misconceptions about both the approach and the process that have become obstacles to successful implementation… Most of these errors of thinking or execution stem from a common source: the failure to recognize that ERM is in fact an easier, simpler, and more logical undertaking than most people realize. The result has been needless complications that have in turn bred misunderstandings and frustration among implementers and senior management, along with doubts about the contribution of ERM to the firm's major objectives. (Fraser, 2007, p.75).

IRM Models

There are a number of different models for IRM which are outlined below:

1. Committee of Sponsoring Organizations of the Treadway Commission (COSO)

COSO, a joint initiative of five accounting and financial associations, was organized in 1985 to study the causal factors leading to fraudulent financial reporting. In 2004, in response to the Sarbanes-Oxley Act

(regulation related to financial reporting and independence of external auditors in the US), they published a guide to IRM. The COSO framework is fairly prescriptive and articulates a focus on objectives related to strategy, operations, reporting, and compliance; and processes related to internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring (COSO, 2004). As one of the first IRM frameworks, COSO is widely recognized but it has also garnered significant criticism including that it is poorly written, difficult to understand, and impractical. (Rasmussen, 2007).

2. American Society of Healthcare Risk Managers (ASHRM)

The ASHRM framework is modeled after COSO and is described as a structured analytical process that focuses on identifying and eliminating the financial impact and volatility of a portfolio of risks for the stated purpose of gaining an advantage in the health care delivery marketplace. It classifies risks as either operational, financial, human, strategic, legal/regulatory, technological, or hazards. (ASHRM, 2006).

3. International Organization for Standardization (ISO) 31000 Risk Management Standards

The ISO framework was first developed in Australia and New Zealand and then adopted internationally. It is intended to be flexible and adaptable to any sector and includes the following processes: communication and consultation; establishing the context; risk identification; risk analysis; risk evaluation; risk treatment; and risk monitoring and review. (CSA, 2011).

4. National Health Service (NHS), England

The NHS has promoted robust IRM processes for many years and healthcare organizations there are required to develop, maintain, and report corporate risk registers. Guidance documents promote simplicity and focus on a duty to protect patients. The IRM process is summarized as answering four questions: what can go wrong? how bad? how often? and, is there a need for action? (NPSA, 2007). Defined risk categories include: safety of patients, staff and public; quality, complaints, audit; human resources, organizational development, staffing, competence; statutory duty, inspections; adverse publicity, reputation; business objectives, projects; finance claims; business interruption; and environmental impact. (NPSA, 2008).

5. Caldwell

This Canadian framework focusses on the board's role in IRM. It includes the following processes: establish context; identify risks; analyze consequences; analyze interconnectivities and compounding effects; re-analyze consequences; prioritize; assess risk tolerance; chose response strategy; and monitor. (Caldwell, 2012).

6. Haney

This somewhat elaborate model is the result of a doctoral study of IRM in Canadian healthcare organizations. It consists of five components: organizational risk network; IRM framework; strategic planning and decision process; implementation; and evaluation. Key elements of the IRM framework itself consist of: ethics based core principles; shared understanding, terminology and roles / accountability; complexity is not necessarily better; emphasize the importance of correctly defining the actual problem; risks are considered in a comprehensive context, considering other objectives; explicit

treatment of uncertainty and prioritized risks; the process is flexible and iterative; focus on clear evaluation and reporting of risk information; use all available evidence to understand risk; and analyze trending information. (Haney, 2013).

There is little alignment between the models particularly in how strategic and operational risks are defined. There is agreement, however on the need to focus on risks to key organizational objectives and the importance of board and senior leadership engagement.

IRM Learning and Advice

> Sometimes companies rush into the creation of resource-intensive activities for ERM without a clear vision of what is needed to give the most effective return on ERM-related investments. (Fraser, 2017, p.78).

There is no universal approach to IRM that will guarantee success and generally speaking, organizations need to adapt processes to match their particular circumstances (Mikes, 2014). Those that have led IRM implementation efforts in healthcare organizations have consistent advice – keep it simple. The following are potential strategies to help ensure that IRM efforts are as effective and efficient as possible.

1. Adopt a Simplified Approach

A simplified framework for understanding and carrying out IRM is illustrated below. Taking into account key organizational objectives, and enabled by board oversight, active executive support, and dedicated resources for coordination; all significant organizational risks are identified, assessed, managed and reported. This process continues in an iterative and ongoing manner.

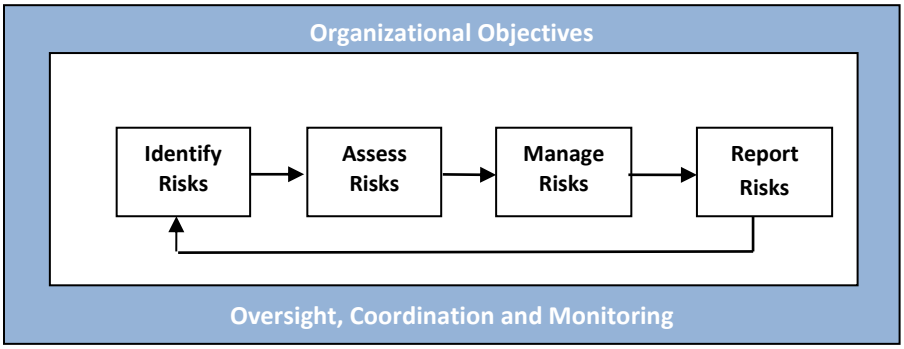

Figure 1: Simplified IRM Framework

2. Ensure Effective Oversight, Coordination and Monitoring

IRM will not succeed unless there is active and visible support from the top and dedicated resources to coordinate the program and ensure ongoing monitoring and improvement. (Fraser, 2007, Sarnie, 2010, Mikes, 2014).

Appoint an executive lead

The executive lead for IRM should default to the chief executive/executive director, but may also be the executive responsible for risk or finance. They are required to facilitate change, hold the rest of the senior leadership team to account, command the necessary resources, and be the primary conduit for IRM communications with the board.

Ensure board engagement

> In our view, boards must take a more active and direct role in risk assessment well beyond traditional oversight of typical risk management processes. In particular, risks associated with leadership and strategy are prime examples of areas where a board must assert itself more directly since management cannot be expected to objectively assess its own performance, capabilities and strategy in such areas from a risk perspective. (Caldwell, 2012, p.1).

The important role of boards in overseeing organizational risks is undisputed. Caldwell suggests that a key role for boards in this regard, is to ask challenging questions of management including:

- Does management have a robust framework and comprehensive process to assess risk?
- Does the board accept management's assessment of risk too readily even when it appears superficial?
- Are risk management processes or systems well designed such that risk is managed holistically and not in silos?
- Does the corporation have adequate systems and processes in place to monitor the effectiveness of risk management?
- Does the board and management learn from and act on instances where risk management strategies and systems have been ineffective?
- Can management adequately and objectively assess risk when it is the architect of the risk management framework?
- Does management have the openness and humility to recognize its shortcomings and the courage to recognize flawed strategy and change course? (Caldwell, 2012, p.4).

Appoint a coordinator(s)

> The effectiveness of risk management ultimately depends less on the guiding framework than on the people who set up, coordinate, and contribute to risk management processes. It is people, not frameworks, that identify, analyze, and act on risk information (Mikes, 2014, p.9).

> IRM does not create itself. It takes work and, over time, concentrated effort. Therefore, treating it like a corner of the desk project will be a sure guarantee of its untimely death, underachievement or quiet disappearance. (Graham, 2008, p.44).

Someone in the organization needs to be appointed to coordinate the IRM program. In healthcare, the manager/director responsible for risk management has typically been the designated for this. Where available, the internal auditor may also participate in this function. The coordinator(s) may also elect to put together a small implementation team, carrying out the initial round of data gathering and assessment; drawing on expertise from other parts of an organization throughout the process.

IRM coordinators require a wide range of technical and interpersonal skills (Fraser, 2007). They need to step out of their offices and develop strong links to clinical teams (Moore, 2013). They need deep field

(i.e. healthcare) expertise and self-confidence to credibly and respectfully challenge the assumptions and biases of other. (Mikes, 2014).

Top-down (to start)

Organizations are cautioned against spending a lot of time and resources trying to engage their entire workforce in IRM efforts. IRM initially, is an executive-owned, top-down exercise that requires a bird's eye view of risk. IRM can be taken deeper into the organization as the program matures. It has been suggested that in order to avoid the "fear and loathing" that may result from yet another management initiative, IRM practitioners should avoid creating unrealistic expectations about what the program will deliver (Graham, 2008).

Don't try to "overwrite" established patient and staff safety cultures

Organizations may struggle with trying to advance an IRM culture, not appreciating that much staff activity is, in effect, risk management. This is particularly so in clinical and occupational health areas although it may not be recognized as such (Audit Commission, 2009). In healthcare organizations, the cultures of patient safety and staff safety (arguably the most important aspects of healthcare risk) are already pervasive and efforts to supplant or translate these into the language of IRM should be avoided.

3. Confirm Organizational Objectives

> In those organisations subject to regulatory intervention (there was) disassociation between corporate objectives and the operational reality at service level; these trusts struggled to identify their purpose and service level objectives and thus had difficulty identifying what risks could prevent the delivery of those critical goals (Moore, 2012, p.5).

> If management identifies a risk that it feels requires managing, it needs to be clearly articulated which corporate objective(s) is threatened by such risk. If no objective can be identified, the risk may not merit attention – alternatively, the objectives may need to be restated (Fraser, 2007, p.76).

Before risk identification begins, there needs to be a clear understanding of what the organization is trying to achieve. This will help to prevent the impractical indexing of all risks within the organization. (Fraser, 2017). Organizational context is key and one of the most important steps to IRM implementation is to describe an organization's strategic objectives.

In some organizations, strategic objectives may not be explicitly stated, or stated objectives may not address significant aspects of organizational activities and risk. It may be helpful in these cases to reaffirm core operations; to provide high quality care and to ensure there are adequate resources, systems, and facilities to make this possible.

Recognize that in healthcare "operations" are often strategic

> Strategic risks are those that represent major threats to achieving the trust's strategic objectives or to its continued existence. Strategic risks will include key operational service failures. (Audit Commission, 2009, p.26).

In commercial, financially focused IRM models, strategic risks are defined as risks related to corporate growth, mergers and acquisitions (ASHRM, 2006). It is important to remember, however, that in healthcare the biggest risks relate to core operations – risks that could result in patient harm, staff

harm, and loss of resources or services. It is operational events, such as a high profile death of a patient due to an adverse event or a fraud by a key staff member, that can quickly escalate into strategic crises.

Limit the number of strategic objectives

In a review of risk management in the NHS it was determined that few trusts had a manageable number of clear strategic objectives that would enable risks to be readily identified and managed. The numbers of objectives ranged from 5 to 50 and it was suggested that this should be limited to ten or fewer. (Audit Commission, 2009).

Whether they are explicitly or implicitly stated, in all healthcare organizations there are a core set of objectives related to care, human resources, finance, leadership and governance, community engagement, community health, information systems and technology, facilities, regulatory compliance, and teaching and research (as appropriate). Appendix 1 provides a sampling of strategic objective statements from Canadian healthcare organizations related to these key areas.

4. Identify Risks (*What Can Go Wrong?*)

With key organizational objectives confirmed, the next step is to identify what can go wrong – what can put achievement of these objectives at risk? A risk is an event that could potentially happen and that has one of more causes and one or more consequences. 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). (Health Canada, 2009). Using the above example, if water is on the floor at the entrance to the hospital the risk of a visitor fall would be high, if water is in a remote storage room, the risk of visitor fall would be low.

Focus on downside versus upside risks

> If the concept of upside risk is useful and important in some circumstances, it is irrelevant and a distraction in others… The upside of risk should be dealt with only periodically, during strategic planning exercises. But when a company's strategy is in place, ERM methodologies should be focused on their main task of limiting downside risk." (Fraser, 2007, p.80).

In an effort to take the broadest view possible, some organizations turn their minds to the concepts of *upside* risks (i.e., a potential outcome that is better than expected) and *downside* risks (i.e., an event that could give rise to a loss or injury in the future) (ASHRM, 2006). This may unnecessarily complicate the IRM process. Given their overwhelming prevalence in healthcare and the industry-wide focus on patient safety, downside risks must clearly be the focus. And in order to promote organizational mindfulness and maintain a sense of urgency, risks should be described in plain language and as events or failures to be avoided.

Limit the number of risks

> Many trusts identified large numbers of principal risks for each objective; often 15 or more. This, together with a large number of strategic objectives made the assurance framework unmanageable for the board, thereby significantly reducing its effectiveness. (Audit Commission, 2009, p.27).

Comprehensive risk identification is critical, because a risk that is not identified will not be included in further analysis (CSA, 2011). On the other hand it will be difficult to operationalize a list with several

hundred or more risks. Risks included in the IRM inventory should be at a relatively high level and aggregated where possible (e.g. “hospital acquired infections” versus separate risks for different types of infections). The need for specificity may be dictated by differences in risk ownership or significant variances in mitigation strategies. The number of risks can also be limited by focusing on only the most “material” or significant ones; those that might require the attention of senior leadership.

> High risks should be defined as only those areas where the board and CEO might need to get involved if conditions warrant - that is, risks involving high impact and material probability of occurring. (Fraser, 2007, p. 79)

Finally, it must be recognized that risks are interrelated and that clear delineation between risks is not always possible; risk identification will never be “perfect”.

Don’t start from scratch

> In today’s fast evolving business environment, where the past may not always be the best predictor of the future, exclusive reliance on senior management’s intuition and experience to identify and assess risks could result in a significant loss to an organization (Aon, 2012, p.8).

In healthcare, most organizational risks are already well known. Leadership teams do not need to start from scratch, rather they can build their list of key risks starting with the wealth of information that is available from internal and external sources such as incident reports, published literature, claims, and accreditations. Common sources of internal and external risk information is included in Appendix 2.

With the input of subscribers, HIROC has developed a taxonomy of key risks in Canadian healthcare linked to key organizational objectives (separate document). This will help to ensure due diligence on the part of healthcare leaders, but will also offer the potential for standardized reporting, aggregate trend analysis, and knowledge sharing in the future.

5. Assess Risk Impacts (*How Bad?*)

As challenging as risk identification can be, risk assessment is even more so, but is essential to the prioritization process.

Articulate risk consequence domains

Understanding a risk entails understanding the losses, or consequences that could result if that risk were to be realized. In healthcare these losses include:

- Physical or psychological harm (to patients, staff, visitors, research subjects)
- Disengaged staff / physicians
- Financial loss
- Reputational loss
- Service / business interruption
- Statutory non-compliance
- Failed strategic initiatives

To promote ease of use and reliability of assessments, domains should be kept to a minimum. For example, equipment losses could have a separate domain, but it is the effects related to patient harm or service interruption that are most important. In another example, water damage from a burst pipe could be captured in a separate facility loss domain, however it is the disruption of operations (e.g. the

shutting down of a unit for clean-up and repairs) or the cost of cleanup (financial domain) that matters the most. Note that some risks may result in more than one consequence, such as the death of a patient from an adverse event that results in sustained negative publicity and ministry involvement.

Establish domain-specific, incremental definitions for the consequence scale

> Staff are sometimes asked to decide whether given risks are 'high' or 'low.' To make an informed decision, however, participants need clear definitions of what is considered 'high' versus 'low.' One of the most effective ways of quantifying and gaining agreement on risk tolerances has been to establish definitions on a five-point (or similar) scale that can be discussed and agreed to by all parties in advance (Fraser, 2007, p.76).

Organizations can take steps to make risk assessments more objective through the use of a domain specific, clearly defined consequence scale. If this cross-domain calibration is not established then financial, operational and clinical risks cannot be compared against each other and appropriately prioritized (NHS, 2008). For instance, if an organization defines 'catastrophic' as being death for the 'physical harm' domain, they would then have to define 'catastrophic' for the 'financial loss' domain as a loss that would truly be significant in terms of dollars. Recognizing, ethically, that there is no financial loss that could compare to the loss of a human life, if a proxy for cross domain equivalency is not achieved, then risk prioritization efforts would be flawed.

Appendix 3 provides an example of a domain specific, incremental definitions for the consequence scale.

Focus on residual risks

> In many cases, the concept of 'inherent risk' is impossible to measure or even define. The idea of looking at risk absent all hard controls, soft controls, or mitigations, provides little or no useful information in most cases (Fraser, 2007, p.75).

Risks are sometimes described as *inherent* – risk before taking into account controls or mitigation strategies (e.g. the risk of an adverse medication event without any controls such as unit dose systems and double-checking processes) or *residual* – risk that remains with mitigation strategies in place. Sometimes significant effort is expended by IRM practitioners in assessing inherent risks. This is a theoretical exercise with limited utility, as it is residual risk that largely drives risk management activities (Audit Commission, 2009).

Beware of cognitive biases and limitations

Human beings are prone to making errors in judgment when assessing risks. There are important psychological biases at play when people identify risks and their relative probability and importance.

> Extensive psychological and sociological studies have documented biases (such as availability, confirmation, and anchoring) that cause individuals to grossly underestimate the range of possible outcomes from risky situations; people may be aware of various risks, but they grossly underestimate the adverse consequences from their occurrence. Often, managers and employees, especially under budget and time pressure, become so inured to particular risks that they override existing controls and accept deviances and near misses as the "new normal" – a behavior referred to as the normalization of deviance. By treating red flags as false alarms rather than as early warnings of imminent danger, they incubate more vulnerability to risk events. (Mikes, 2014, p. 13).

A recent study of failure modes and affects analysis (FMEA), a proactive risk assessment process demonstrated that current approaches to quantification of risk are deeply flawed – they lack reliability (i.e. produce different results with different people) and breach mathematical properties (i.e. multiplication of ordinal numbers). The risk assessment process "is inherently subjective and the use of numerical scores gives an unwarranted impression of objectivity and precision" (Franklin, 2012). Recognition of limitations, thoughtful reflection and an agreement among team members to challenge each other's assumptions is required for effective risk assessment.

Beware of "groupthink" and defer to experts

> Organizational biases, such as "groupthink," also inhibit good thinking about risks. Groupthink arises when individuals, still in doubt about a course of action that the majority has approved, decide to keep quiet and go along. Groupthink is especially likely when the group is led by an overbearing, overconfident manager who wants to minimize conflict, delay, and challenges to his or her authority. (Mikes, 2014 p.14).

A common approach to risk assessment is to assemble a group of leaders in a room to solicit their opinions on the identity, consequence, and likelihood of risks. There is a tendency in such large settings for individuals to gravitate towards a common view of the world without appropriate push-back or demand for evidence to support the identified risks. (Graham, 2008). Treated, however, as a significant but non-definitive input into the process, this could be beneficial. Regardless of how accurate group based risks assessments may or may not be, the discussions alone could be valuable, leading to an elevated understanding of risks and clarity around the process of risk prioritization. (Aabo, 2005).

Recognize data limitations

> A possible reason for the limitations of FMEA may be that it was originally developed for use in engineering, where systems are largely deterministic and failure rates more easily quantifiable. However, in healthcare, human-based systems introduce variation, which is much harder to quantify. (Franklin, 2012, p. 610).

While every effort should be made to use the best data possible for risk assessment, "the number of incidents within an organization is usually too low to provide a basis for quantification of risk" (Pickering, 2010, p.11). Data may not be available, realistic or cost effective to obtain increasing the dependence on qualitative discourse and expert opinion. (Mikes, 2014).

6. Assess Risk Likelihoods (*How Often?*)

As with consequence, when assessing the likelihood of a risk, it is important to take into consideration the controls already in place. Likelihood is usually scored by considering the frequency of occurrence (e.g. once per month or once per year). Frequency, however, is not a useful way of scoring certain risks, especially those associated with the completion of time-limited or one-off initiatives such as a strategic project. For these kinds of risks, the score cannot be based on how often the consequence will materialize. Instead, it must be based on the probability that an initiative might fail in a given time period (NPSA, 2008).

Establish incremental definitions for the risk likelihood scale

> If risk probability assessments are faulty, the accuracy of risk prioritization will be affected, leading to a potential failure to focus on the most significant risks. This in turn could lead to selection of inappropriate responses, with attention being paid to wrongly-prioritized risks (Hillson, 2004).

As with the consequence scale, an organization should articulate specific definitions for the likelihood scale (clear descriptions of how often the adverse consequence will be realized), rather than using general descriptions and. A sample scale is included in Appendix 3.

Develop a risk matrix (but recognize its limitations)

> Risk Matrices are used to categorise and prioritise risks. However, there appears to be little scientific analysis of their value in improving risk related outcomes. (Pickering, 2010, p.15).

A risk matrix is a two-dimensional grid with consequence on one axis and likelihood on the other. The intersecting cells allows for a relative ranking of different kinds of risks, and establishes a baseline from which to measure progress and trends over time (NPSA, 2008). The figure below depicts a 5 x 5 matrix. Color coding is typically added to help visualize increasing levels of risks. Risk matrices imply a quantitative basis for risk rating however, given the inherent subjectivity of risk assessment and the compression of different types and levels of risks into wide (color coded) bands, their use may result in inappropriate over or underestimation of the relative importance of individual risks (Pickering, 2010).

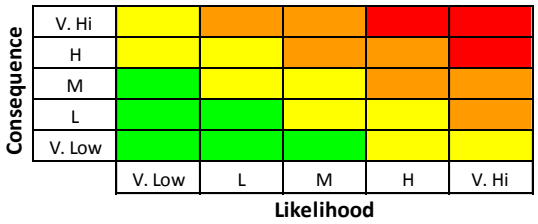

Figure 3: Risk Assessment Matrix (5 x 5)

Go with the highest combined consequence-likelihood score

Sometimes risks can be assigned different combinations of scores. For example, less serious patient falls may occur frequently, while serious falls may occur infrequently. The most conservative approach would be to use the score with the highest net rating.

Don't worry about "mapping" risks

A common step in IRM implementation is the creation of a risk map. This is the process whereby numbered risks are mapped on a risk matrix. Critical risks, deserving top priority and attention are concentrated in the upper right. Low-priority risks are those found in the lower left. For some, this is a useful exercise, but for others it is labor-intensive and frustrating. An appropriately formatted risk register (discussed below) may be easier to execute, more informative, and able to provide similar visual cues related to the most important risks.

7. Manage Risks (*Is There a Need for Action?*)

> A shift of emphasis from the risk assessment stage to the risk control stage of a hazard management process may lead to better and more timely decision making and better use of resources. (Pickering, 2010, p. 15).

Once risks at unacceptably high levels are identified, their current risk mitigation strategies should be evaluated. This could include an assessment of whether existing controls are still appropriate and if they are still appropriate, are they being consistently applied?

Treat and control risks

> Not all risks can be eliminated in an affordable way. Organizations have to carefully weigh just how much time and effort they are prepared to put into risk mitigation. (Graham, 2008, p.104).

If an informed decision is made that a specific risk is not at a tolerable level and that existing controls are not adequate, then additional or alternative mitigation plans should be developed and accountability for their implementation assigned. There are a number of risk management options, which may or may not be appropriate in a particular circumstance including:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- Removing the hazard;
- Reducing the likelihood;
- Reducing the consequence (e.g. through early warning / detection systems);
- Sharing the risk with another party or parties (e.g. contracts and insurance); and
- Retaining the risk by informed decision. (CSA, 2011).

Risk mitigation plans could include new control strategies or initiatives to improve compliance with existing controls (e.g. hand hygiene practices or ventilator associated pneumonia bundles. Organizations should look to established best practices to identify possible options, or consider implementing a quality improvement project to work towards a solution in an iterative way. Audits of mitigation strategies for high priority risks should be carried out on a periodic basis.

Allocation of resources should take into account funding constraints, opportunity costs, and tradeoffs with other risks. Leaders should give themselves permission to override subjective assessment scores to identify “top” risks and to allocate resources where they feel they will have the most impact.

Don’t worry (too much) about risk tolerance

Risk “tolerance” is a term frequently used in IRM discussions, however there is considerable confusion about the concept (Fraser, 2007). In practice, tolerance plays out in several ways: when establishing a consequence scale for risk assessment; when making informed decisions to accept (or not) the likelihood or consequence of a particular risk; and when establishing targets for key risk indicators, such as infection rates and wait times. These determinations will typically occur in meetings between risk experts/owners, and discussions around the senior management table.

8. Report Risks

The results of risk assessments need to be documented and summarized in reports to senior leadership and the board.

Develop an easy to review risk register

> Risk registers were viewed as bureaucratic, complex, overwhelming, non-value-added and difficult for boards to utilize effectively (Moore, 2012, p.13).

A risk register is a table that summarizes the results of the risk assessments. It is one of the most tangible outputs of an IRM program, providing a means to compare and evaluate very different types of risks. It is a list of all significant risks usually ranked in order of priority. Some organizations struggle with trying to include all information about a risk on their risk register, however this may make the report too lengthy and difficult to understand. It is better to capture a longitudinal record for each risk in a separate document.

Risks do not remain static, and a register is produced as an 'evergreen' document, subject to review at regular intervals and as new information about risks comes to light. It has been suggested that the frequency of review should be dictated by the "velocity of risk evolution" (Mikes, 2014).

The risk register, or excerpts from it, will form the basis for IRM reporting to senior leaders and the board. This could entail a report including one or more of the following:

- The top 5, 10, or 20 ranked risks;
- All risks above a certain threshold rating;
- Risks linked to specific strategic objectives;
- Risks requiring significant remedial action; and
- Changes made to the register between reporting cycles.

Ensure linkages between IRM and strategic planning

Once a register is populated, it becomes a valuable resource for use in setting organizational priorities and should flow into and out of an organization's strategic planning process.

Consider transparency

Organizational leaders should determine how transparent they intend to be in terms of sharing potentially sensitive risk assessments and management plans with internal and external stakeholders. They should anticipate and be prepared for intended or unintended public disclosures. In the NHS, many healthcare organizations post risk registers on their external websites.

Risk register software

Risk registers can be very elaborate and specialized software packages can be purchased to manage them but a basic spreadsheet could be sufficient to start. HIROC's Risk Register on-line application provides subscribers with a common electronic platform to capture and report risk information.

9. Program Evaluation and Improvement

> Based on results of monitoring and reviews, decisions should be made on how the risk management framework, policy and plan can be improved. These decisions should lead to improvements in the organization's management of risk and its risk management culture (CSA, 2011, p.24).

An organization's IRM program can be evaluated by assessing progress against expected benefits such as: identification of risks that would otherwise have been overlooked; improved resource allocation decisions; improved preparedness for crises; improved audit planning and assurance; and increased board and stakeholder confidence in risk monitoring and management processes. Changes in risk ratings over time can also be tracked.

Monitor program maturity

In a recent survey of over 500 large organizations, the average risk management maturity level was found to be 3 on a scale of 1-5. For the non-profit, education and healthcare sectors, the average maturity ranged was lower (2.5 to 2.75) implying even more room for development. (Aon, 2013).

The tables below outline the elements of risk maturity which can be used by healthcare organizations to assess IRM progress.

Table: RIMS Risk Maturity Levels (RIMS, 2006)

Level	Characteristics
1. Ad hoc	Implies an extremely primitive level of IRM maturity where risk management typically depends on the actions of specific individuals, with improvised procedures and poorly understood processes.
2. Initial	Risk is managed in silos, with little integration or risk aggregation. Processes typically lack discipline and rigor. Risk definitions often vary across the silos.
3. Repeatable	A risk assessment framework is generally in place with the Board of Directors being provided with risk overviews. Approaches to risk management are established and repeatable.
4. Managed	Enterprise wide risk management activities, such as monitoring, measurement, and reporting are integrated and harmonized with measures and controls established. Risk procedures are communicated and fully understood throughout the organization with the risk management principles integrated fully within the management process.
5. Leadership	Risk-based discussions are embedded to a strategic level, such as long- term planning, capital allocation, and decision making. Risk appetite and tolerances are clearly understood with alerts in place to ensure the board of directors and executive management is made aware when risk thresholds are exceeded.

Table: Aon Risk Maturity Levels (Aon, 2013)

Level	Characteristics
1. Initial / Lacking	Component and associated activities are very limited in scope and may be implemented on an ad-hoc basis to address specific risks.
2. Basic	Limited capabilities to identify, assess, manage and monitor risks.
3. Defined	Sufficient capabilities to identify, measure, manage, report and monitor major risks; policies and techniques are defined and utilized (perhaps inconsistently) across the organization.
4. Operational	Consistent ability to identify, measure, manage, report and monitor risks; consistent application of policies and techniques across the organization.
5. Advanced	Well-developed ability to identify, measure, manage and monitor risks across the organization; process is dynamic and able to adapt to changing risk and varying business cycles; explicit consideration of risk and risk management in management decisions.

Recognize IRM limitations

In healthcare, not all risks can be anticipated and events that have never happened before happen all of the time highlighting (Weick, 2007). Even if risks can be anticipated, it may not be possible to accurately predict the consequence or likelihood of these events. IRM is not a panacea for all the uncertainties facing organizations however, IRM should decrease the number of unexpected crises and increase overall capacity to manage them when they occur (Graham, 2008).

Summary

Responding to internal and external drivers, many healthcare organizations have implemented or are contemplating implementation of an IRM program to ensure the identification and management of significant organizational risks. There are many challenges associated with IRM implementation including the use of overly complicated methods and processes.

This guide has provided an overview of basic IRM concepts and advice for efficient and effective IRM implementation including:

- Adopting a simplified approach;
- Ensuring effective oversight and coordination;
- Confirming organizational objectives;
- Identifying risks;
- Assessing risks;
- Managing risks;
- Reporting risks; and,
- Evaluating and improving the program.

This guide will be updated as new information and insights arise, and as IRM experience in healthcare matures.

References

1. Aabo T, Fraser J, Simkins B. (2005). The rise and evolution of the chief risk officer: enterprise risk management at Hydro One. J App Corp Fin. 17(3):18-31.
2. Accreditation Canada. (2013). Qmentum Program: governance standards.
3. Accreditation Canada. (2013). Qmentum Program: leadership standards.
4. American Society of Healthcare Risk Management (ASHRM). (2006). Enterprise risk management part one: defining the concept, recognizing its value.
5. Aon Analytics. (2010). Global enterprise risk management survey. Aon Corporation.
6. Aon Analytics. (2012). 2012 U.S. industry report: health care. Aon Risk Solutions.
7. Aon Risk Solutions. (2013). 2013 risk maturity index report: building a robust framework and realizing value from risk management. Aon plc.
8. Aon Risk Solutions. (2013). Aon risk maturity index: insight report November, 2013. Aon plc.
9. Audit Commission. (2009). Taking it on trust: a review of how boards of NHS trusts and foundation trusts get their assurance.
10. Baker R, Denis J-L, et al. (2012). Effective governance for quality and patient safety in Canadian healthcare organizations. Canadian Health Services Research Foundation, Canadian Patient Safety Institute.
11. Buchanan L, O'Connell A. (2006). A brief history of decision making. *Harvard Business Review*. 84(1):32-41.
12. Caldwell, J. (2012). A framework for board oversight of enterprise risk. Chartered Accountants of Canada.
    Canadian healthcare leaders. Healthcare Management Forum. Fall:145-149.
13. Canadian Standards Association (CSA). (2011). Implementation guide to CAN/CSA-ISO 3100, risk management – principles and guidelines.
14. Committee of Sponsoring Organizations of the Treadway Commission. (2004). Enterprise risk management – integrated framework executive summary.
15. Farrell M, Gallagher R. (2014). The valuation implications of enterprise risk management maturity. J Risk and Insurance. Online March:1-34.
16. Francis R. (2013). Publication of the final report: press statement. The Mid Staffordshire NHS Foundation Trust Public Inquiry.
17. Franklin B, Shebl N, Barber N. (2012). Failure mode and effects analysis: too little for too much? BMJ Quality and Safety. 21(7):607-11.
18. Fraser J, Simkins B. (2007). Ten common misconceptions about enterprise risk management. J Applied Corporate Finance. 19(4):75-81.
19. Graham A. (2008). Integrated risk management implementation guide. Queens University School of Policy Studies.
20. Haney J, Church J, Cockerill R. (2013). Pursuing enterprise risk management: a local road map for
21. Health Canada. (2009). WHMIS quick facts: risk versus hazard.
22. Hillson D, Hulett D. (2004). Assessing risk probability: alternative approaches. PMI Global Congress Proceedings.
23. Mikes A, Kaplan R. (2014). Towards a contingency theory of enterprise risk management. Harvard Business School Working Paper.
24. Moore P. (2013). Countering the biggest risk of all: attempting to govern uncertainty in healthcare management. Good Governance Institute, UK.
25. National Leadership Council (NLC). (2012). The healthy NHS board: principles for good governance. NHS Leadership Academy.
26. National Patient Safety Agency (NPSA). (2007). Healthcare risk assessment made easy. NHS. UK.
27. National Patient Safety Agency (NPSA). (2008). A risk matrix for risk managers. NHS. UK.

28. Pickering A, Cowley S, (2010). Risk Matrices: implied accuracy and false assumptions. J Health and Safety Research and Practice. 2(1):9-16.
29. Rasmussen M. (2007). AS/NZ 4360 – a practical choice over COSO ERM. Forrester Research Inc.
30. Risk and Insurance Management Society, Inc. (2006). RIMS Risk Maturity Model (RMM) for enterprise risk management.
31. Sarnie R. (2010). ERM: Do you know what it means? Risk and Insurance Management Society (RIMS), Inc.
32. Smith R. (2010). NHS targets 'may have led to 1,200 deaths' in Mid-Staffordshire. Daily Telegraph, UK.
33. Treasury Board Secretariat (TBS). (2012). Integrated risk management implementation guide. Government of Canada.
34. Weick K, Sutcliffe K. (2001). Managing the unexpected: assuring high performance in an age of complexity. Jossey-Bass. Toronto.
35. Weick K, Sutcliffe K. (2007). Managing the unexpected: resilient performance in an age of uncertainty, 2nd edition. Jossey-Bass. Toronto.

Appendix 1 – Strategic Objectives

Strategic Objectives Categories and Sample Strategic Objective Statements from Canadian Healthcare Organizations

Objectives Category	Sample Strategic Objectives
Care	Deliver High Quality Care; Renewed Commitment to Quality and Safety; Reduce Wait Times; Accessible and Available Services at the Right Time; Compassionate, Respectful and Safe Care; Innovative and Evidence Based Care; Reduce Length of Stay to Meet Targeted Benchmarks; Effective Pain Management; Effective Transitions of Care; Reduce Infections; Improve Flow and Access to the Right Care
Human Resources	Provide a Safe and Engaging Work Environment of Staff and Physicians; Staff Reflect the Diverse Nature of Community; Accountable, Recognized, Respected, and Rewarded Staff; Provide a Safer and Healthier Work Environment; Enhance Physician Leadership and Accountability; Implement a Staff Wellness Program; Ensure Healthy, Engaged, Skilled and Optimized Workforce; Be the Organization of Choice for Talented People
Finances	Maintain Strong Financial Performance; Make the Best Use of Resources; Sustainability; Cost Effective and Efficient Operations; Achieve Stable Sources of Funding / Adapt to Changing Funding Models; Align Funding and Accountability to Support Goals; Develop New Sources of Revenue
Leadership/Governance	Provide Strong Leadership and Governance; Lead and Participate in Effective Partnerships; Positive Leadership That Fosters Organizational Values; Culture and System that Focuses on Learning and Collaborative Improvement Where Patient Safety is the Primary Focus for all Staff; Implement an Organization-wide Approach to Drive Performance and Transformation; Support Effective Regional Distribution of Clinical Services; Achieve Economies of Scale and Greater Integration With Our Partners; Continue to Build Organizational Capability and Capacity; Exemplify Local and Global Leadership
External Relations	Listen to the Needs of Our Community; Comprehensive Public Input; Inspire the Community to Support Patient Care and Research Programs
Information Systems and Biomedical Technology	Implement Clinical Information Systems / Electronic Tools to Improve Care and Effectiveness; Implement an Integrated and Comprehensive Business System to Improve Management of Spending; Complete the Development of the Electronic Health Record and Data Warehouse; Use Technology to Improve Quality, Safety and Continuity of Care
Facilities	Strategically Invest in Facilities; Create New Physical Space for Our Clinical Programs
Regulatory Compliance	Incorporate Performance Agreements that Reflect Strategic Directions; Achieve Exemplary Accreditation Status
Teaching	Educate Health Care Providers to Meet The Future Needs of Community; Multidisciplinary Education in Both the Academic and Workplace Environment; Provide Trainees with Exceptional Learning Experience; Become the Institution of Choice for Trainees
Research	Develop New Knowledge and Innovations; Build a Strong Academic and Research Role; Build a Strong and Sustainable Research Program
Community Health	Health Promotion and Prevention; Effective Health Education, Promotion, and Prevention Programs; Improve Health and Well Being of Community in Targeted Areas; Reduce the Incidence of Preventable Disease in Targeted Areas; Provide Quality Chronic Disease Prevention and Management Programs; Strengthen Primary Health Care; Reduce Disparities in Health Outcomes

Appendix 2 – Common Sources of Risk Information

Organizational specific and internal sources of information include:

- Critical incident reviews and recommendations;
- Incident reports;
- Morbidity and mortality reviews;
- Medical legal and property insurance claims;
- Patient/client/resident/family complaints;
- Patient/client/resident satisfaction surveys;
- Proactive risk assessments and process analysis (e.g. failure modes and effect analysis, HIROC risk assessment checklists);
- Recommendations and reports from external agencies (e.g., Accreditation Canada report, accreditations of lab and educational programs);
- Recommendations and reports from internal and external auditors;
- Key performance indicators;
- HR staffing reviews and plans; and,
- Leadership discussions (e.g., “what keeps you up at night?”).

External sources of information include:

- Product/hazard alerts, recalls;
- Medication safety bulletins;
- Legislative/legal updates;
- Coroners reports, inquests;
- Communicable diseases surveillance reports;
- Professional regulatory bodies’ communications;
- Insurance alerts, advice, and aggregate claims data;
- Global patient safety alerts (Canadian Patient Safety Institute); and,
- Benchmarking, literature.

Appendix 3 - HIROC Sample Risk Assessment Scales

Potential Impact Scale

Dimension	Very Low	Low	Medium	High	Very High
Physical/ psychological harm	• Minimal harm, no/minimal intervention or treatment • No time off work	• Minor harm or illness, minor intervention • Time off work for <3 days • Increase in LOS by 1-3 days	• Moderate harm, professional intervention • Time off work for 4-14 days • Increase in LOS by 4-15 days • Small number of patients	• Major harm leading to long-term incapacity disability • Time off work for >14 days • Increase in LOS by >15 days • Mismanagement of patient care with long-term effects	• Incident may lead to death • Multiple permanent instances of harm, irreversible health effects • Large number of patients
Disengaged staff/ physicians	• Low level of internal grievances	• Grievances occurring but not in large numbers	• Grievances show an increasing pattern • Low staff morale	• Grievances are increasing and more pervasive • Very low staff morale	• Grievances preoccupy the organization, arbitration and external review • Loss of several key staff
Financial loss	• Small loss	• 1% of budget	• 1-2% of budget	• 2-5% of budget	• >5% of budget
Reputation with stakeholders (including: community, donor, media, gov't, public, partners)	• Rumours • Potential stakeholder concern	• Local media coverage (short term) • Elements of stakeholder expectation not being met	• Local media coverage (sustained) • Short-term reduction in stakeholder confidence	• National media coverage (short-term) • Potential for political involvement • Longer-term reduction in stakeholder confidence	• National media coverage (sustained) • Political intervention • Sr. leader termination • Long-term reduction in stakeholder confidence
Service/ business interruption	• Interruption of >1 hour	• Interruption of >8 hours	• Interruption of >1 day	• Interruption of >1 week	• Permanent loss of service or facility
Compliance	• Minor non-compliance statutory duty	• Single failure to meet external standards or follow protocol • Recommendations to comply with external agency	• Repeated failures to meet external standards • Orders issued, report required by external agency	• Multiple statutory breeches /non-compliance with external standards • Prolonged inspection, significant findings • Prosecution initiated for non-compliance	• Gross failure to meet standards • Maximum fines • Criminal code violation • Impact on affiliation agreements
Business objectives/ projects	• Insignificant schedule delay	• Minor schedule delay • Small number of objectives not met	• Moderate schedule delay • Some objectives not met	• Significant schedule delay • Key objectives not met	• Initiative not implemented • Key objectives not met

Likelihood Scale

Category	Very low	Low	Medium	High	Very high
Broad descriptors	• Will probably never occur/recur	• Do not expect it to happen/recur but it is possible	• Might happen or recur occasionally	• Will probably happen/recur	• Will undoubtedly happen/recur, possibly frequently
Time-frame	• Not expected to occur for years	• Expected to occur at least annually	• Expected to occur at least monthly	• Expected to occur at least weekly	• Expect to occur at least daily
Probability	• <0.1%	• 0.1-1%	• 1-10%	• 10-50%	• >50%

Adapted from NPSA, 2008