OVERVIEW OF ISSUE
As challenging as risk identification can be, risk assessment (the determination of how bad or how often a risk may occur) is even more so, and is essential to the process of prioritizing risks. The following diagram outlines the steps in risk identification, risk assessment, and risk management. The red arrows indicate the focus of this Risk Note.

Refer to related Risk Notes for details:
• Risk – Concepts and Misconceptions, Risk Assessment, Risk Management and IRM/ERM.

THINGS TO CONSIDER
Assess risk consequence (how bad?)
• Understanding a risk entails assessment of losses, or consequences that could result if that risk were to be realized. In healthcare, 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; or failed strategic initiatives.
• It is important to adopt a domain-specific, calibrated consequence scale; e.g. ‘catastrophic’ (i.e. death) physical harm equated to ‘catastrophic’ (i.e. truly significant) financial loss.
• The image at right shows the HIROC evidence-based standardized scoring matrix for impact and likelihood.

Assess risk likelihood (how often?)
• The likelihood of the risk can be assessed 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. Instead, it must be based on the probability that an initiative might fail in a given time period (NHS, 2008). 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.
Risk Assessment

Focus on residual risks
• Risks are sometimes described as inherent – risk before taking into account existing controls or mitigation strategies (e.g. the risk of an adverse medication event without unit dose systems or double-checks) or residual – risk that remains with mitigation strategies in place (NHS, 2007).
• Sometimes significant effort is expended 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).

Don’t worry about mapping risks
• A common step in IRM implementation is the creation of a risk or heat map. This is the process whereby numbered risks are mapped on two dimensional matrix.
• An appropriately formatted risk register or list may be easier to execute, more informative, and able to provide similar visual cues related to the most important risks.

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.

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.
• 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
• 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.

Recognize data limitations
• 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).

REFERENCES