Enterprise Approach to Risk Management

Save to myBoK

by Kevin Mead

Risk management has become a key issue while patient safety makes headlines across the country. While accreditation associations already require redesign of vulnerable systems, many are looking for proactive risk assessments as well. Meanwhile, health information technology, designed to secure and speed the access of information, presents its own battery of risks through connectivity and outsourcing issues as well as the speed of change. Here, too, proactive risk assessment is necessary. To achieve this, HIM professionals need to radically re-think the definition of "risk" within HIM.

The Old View of Risk

It is relatively easy to quantify risk when taken in the narrow view. For many years, patient outcomes and events have driven the way a healthcare organization manages risk. These outcomes could be easily defined and have included incidents within the operating rooms and fall injuries. In this respect, healthcare has been very similar to other industries.

However, this reflects only a portion of the risk that exists in healthcare. Managing risk by focusing on events often means that we assess and treat the risk too late to be effective. For example, managing the risk of inappropriate information disclosure through a system monitoring access is valid, but ignores the potentially larger risk that employees may not know how to handle confidential information in a variety of situations.

What Risk Means Today

Today's risk management programs are designed with the understanding that risk exists throughout the organization and that risks in individual areas are linked. Further, total risk (also known as mission or enterprise risk) must be effectively understood and managed in order for the organization to achieve its goals. A "mission risk" model can be applied to technology and the management of information within organizations.

Under this system, all risk drives upward to mission risk. Your mission is probably already well defined within your organization, and all risks exist only in relation to the risk of failing to achieve the organization's mission. The four major groupings of risk beneath this are **customer risk, employee risk, purpose risk**, and **ethical and cultural risk**. Following is a look at each of them and how to assess your organization's readiness.

Customer Risk: This is the risk that the organization may fail to respond to customers' stated needs or that customers may not understand the organization. For example, if a healthcare provider does not understand where and how information is stored and retrieved within a system, errors might occur even though all the relevant information is available. Keep in mind that this risk refers to both healthcare consumers and all of the internal and external users of health information and systems.

Employee Risk: This is the risk that organization employees will not have received the education and training needed to operate according to the goals and objectives of the organization. While some of this risk is driven by the formal training of employees, informal efforts, such as management-to-staff communication, are also critical.

Purpose Risk: This is the risk that certain operations, though efficient, may not be the most effective for the organization's mission. For example, the organization's technology purchases should match the organization's overall mission and vision and add value to it.

Ethical and Cultural Risk: This risk addresses the possibility that your department may be operating in a way that does not uphold the ethical and cultural norms within either the organization or the environment within which it operates. While this risk is more often associated with the actions of senior management, it can be applied within HIM technology.

Many of these risks are considered strategic-level risks within the organization. To address more detailed risks related to the deployment and use of technology within the enterprise, we need to drill downward. This mirrors the way in which the organization should be operating, with the technology being driven by and responding to the strategic needs and risks of the management rather than the opposite. The tactical risks exist primarily in the areas of **process, planning**, and **governance** risk.

Process Risk: Process risk is the danger that your organization doesn't have the right technology or processes in place to support its goals and objectives. If realized, this risk would include a failure to meet agreed service levels, system unavailability, or lost or mishandled records. This risk includes the way permission is granted to access health information (including security and access control) for valid uses.

Planning Risk: This risk is part of the way management considers the future and marks proactive plans to address likely future issues. An example of risk would be organization management failing to consider future legal, regulatory, or technological developments in planning for the deployment of system changes.

Governance and Organizational Risk: Governance and organizational risk reflects the risk that your facility is not organized in a way that maximizes the effective management of technology and information.

Implementing the Program

After understanding the enterprise-wide nature of risk as well as the risks associated with technology and information, implementing a global proactive risk assessment program is the next step. Because individual risks vary based on factors such as organizational size, structural complexity, levels of regulatory oversight, employee competence, and a variety of other factors, the tool will need to be generic and related more to process than to specific assessment. The following steps model the Australian New Zealand Standard (AS/NZS) 4360 on Risk Management. While this standard does not guarantee that risks will be managed, it provides assurance that there is system in place for effective management.

Accountability: The individual accountable for risk within the organization must be identified. While many entities have a risk management officer, this individual is often concerned mainly with insurance coverage. As valuable as this is, it is important to recognize that insurance kicks in only after an event has occurred and when other risk management strategies have failed. Instead, an organization as a whole should have an individual accountable for all aspects of risk, and each functional area should also assign accountability for risk within its own responsibilities.

Establish context: Determine which activities contain risk within the organization. In HIM, this would include the storage, retrieval, and transmission of information. Not surprisingly, the very actions that create risk in your organization are also the actions necessary to fulfill the organization's mission.

Identify: At this stage, identify the negative events as a result of risk, where in the process it occurs, and what circumstances would lead to a risk actually occurring. At this point, you should also identify the personnel whose actions or inactions would lead to the risk becoming a real event.

Analyze: Assess the likelihood of risk occurring. It is critical that validated data be used rather than personal judgment. For example, the risk of an earthquake destroying your facility's data center seems remote because the facility is not located in California. However, the largest earthquake ever in the continental United States occurred in Missouri. Therefore, as you assess risk related to diverse areas such as natural disasters, system capacity, unauthorized access, and system downtime, use validated data, preferably from external sources.

Assess: In assessing the risk, a number of tools can be used. Here, we'll apply an environmental analysis to an organization's decision to move from dedicated terminal and dial-up access to records to intranet/Internet access (see page 34). The current and future environments are mapped from a variety of points of view, in this case based around customers, regulators/management, and the equipment in use. On the vertical axis the parties affected by a proposed change are mapped. On the horizontal axis, we describe the current and future status of their involvement with the system or process and determine how risk will change when the environment changes.

Because the organization is no longer responsible for the connection, meaning that a large part of service provision would be effectively outsourced, the risk profile has changed. This process is designed to ensure that as systems and processes change

within an organization, management is aware of the changes caused to risk and makes appropriate control changes in response.

Treat: Within the scope of treatment, assess the controls in place and determine if they are adequate for the documented risk. Are the controls around physical access to printed records adequate for the risk of disclosure that you have identified? If not, they will need to be changed. Risk can also be treated through insurance or through management accepting the risk and declining to treat it.

Monitor: The monitoring process is not a step in the sequence-instead, it must occur at all levels within the risk assessment process to ensure validity.

Communicate: For risk management to be effective, it must become a part of all employees' job responsibilities. As organizations focus on core competencies and required job skills, the management of risk within each employee's area needs to become an assessed and accountable function.

Document: A commitment to effective risk management is represented by documenting the risks in a facility and the steps taken to quantify, prioritize, and treat them. Additionally, it provides an indication to internal and external groups, such as regulators and auditors, of the attitude management and staff take toward risk and its management.

To operate effectively under this regime and to be truly proactive about risk, keep in mind that risk occurs because your facility provides service. It is both necessary and desirable, because only way to eliminate risk is to do nothing. Further, by understanding risks and how they link with other risks throughout the organization, a facility can move from event-based risk management to a holistic, enterprise-wide risk assessment methodology.

Reference

Swanson, Dan. "Risk Management is Fundamental to Successful Organizational Performance." *ITAudit Forum*, vol. 3 (July 1, 2000). Available at www.itaudit.org.

Kevin Mead *presents worldwide and writes on risk and control issues. He can be reached at* kmead@bellsouth.net.

Article citation:
Mead, Kevin. "An Enterprise Approach to Risk Management." *Journal of AHIMA* 72, no.9 (2001): 32,34,36.