An Integrated Nine-Step Approach to Managing Clinical Technology Risks

Tara C. Brady and George Panagiotopoulos

Adopting a formal risk management approach is crucial for a variety of reasons: Clinical technology organizations are maturing, technology is becoming more integrated and complex, and technology is increasingly relied upon in the delivery of care. As a result, healthcare technology management professionals are encouraged to make formal risk management a core competency.

This article seeks to describe how Kaiser Permanente’s Integrated Risk Management (IRM) program has addressed increasing complexity in the healthcare industry and regulatory environments. It provides an overview of the framework and process used by Kaiser Permanente to address risks in a clinical technology business unit.

A previous article detailed the step-by-step process used by Kaiser Permanente to evaluate clinical technology issues throughout the entire device life cycle, as part of a programmatic risk assessment project. It focused on how to complete a risk assessment, categorize the identified risks according to risk type and risk effect, and gauge the impact and likelihood of each potential risk.

The Kaiser Permanente Clinical Technology (KP ClinTech) program consists of four IRM objectives: 1) conduct a programmatic risk assessment to identify risks, 2) evaluate and determine level of risks, 3) establish a unified view and categorization of risks across the program, and 4) provide leadership with information necessary to approve the scope of work needed to manage clinical technology risks. The IRM model used by Kaiser Permanente can be applied to other healthcare organizations.

Importance of a Strategic Plan

After an assessment has been completed and risks have been identified, the next step is to incorporate the identified risks, risk controls, and related initiatives into a strategic plan. Risk assessment should be a routine part of every program’s strategic plan. Organizations that have not developed a strategic plan or do not have a framework currently should strongly consider developing one based on ANSI/ASSE Z690.2–2011, Risk Management—Principles and Guidelines. ISO 31000:2009 provides principles and generic guidelines on risk management. (Note: ISO 31000 is distinct from ISO 14971, which applies to the manufacture of medical devices.) Because this framework is not specific to any industry, it can be used by any public, private, or community enterprise, association, group, or individual.

One benefit of a strategic plan is its visibility. It allows the senior leadership of an organization to readily see and understand the risks and how risk management enhances the clinical technology program’s capabilities.

After completion of that first phase of the IRM process, the KP ClinTech program continued its efforts in collaboration with the National Compliance, Ethics, and Integrity...
Office and the Enterprise Shared Services Risk Management & Compliance Office, in order to begin the risk remediation process. At that stage, clinical technology leadership determined that the best way to address program risks was to incorporate all risk-related activities within the strategic plan and the program’s maturity model (described below). This enabled the business unit to move forward with remediation activities while allowing the executive sponsors to have full visibility and track progress relative to, or in alignment with, tactical initiatives specific to the strategic plan.

The strategic plan helped create a framework for risk-related initiatives, provide a single roadmap to program maturity, and drive the risk management process. Incorporating risks into the strategic plan required stratification of risks and prioritization of remediation activities.

The KP ClinTech team created a template using the framework for developing a strategic plan. The framework consists of four elements: people, process, technology, and financial. Of note, all of these steps are aimed at achieving the future state as the program grows to maturity. KP ClinTech’s strategic plan was defined simultaneously with the risk assessment. The 30 risks in the report validated and/or justified assumptions used to draft the strategic plan. The 30 risks then were mapped to the strategic plan to avoid duplication of effort and the need to manage multiple standalone initiatives.

Two factors determined the category for assigning risk: 1) the strategy area where the risk primarily fell and 2) where one should start in order to best mitigate the risk. For example, as described in Figure 1, staffing issues fall under the people element, and having one computerized maintenance and inventory management system falls under the technology element. Having an administrator to manage the system could fall under either people or technology, but it first

---

**Figure 1.** Strategic plan and risk alignment for clinical technology (CT) at Kaiser Permanente. Abbreviation used: CMMS, computerized maintenance management system.
requires creating a staffing position and then filling that role. Therefore, the risk item of not having an administrator was initially assigned to people. After that position was filled, the “people” risk was closed out and the risk was moved to the process category to ensure that the processes necessary to administer the system and manage the equipment inventory data were created. The residual risk (described in step 7) then falls back into the people category and is managed as part of staff job performance reviews.

**Nine-Step Approach to Managing Risks**

After assessing and assigning risks, the bulk of risk management work can be divided into nine steps (Figure 2).

1. **Understanding Objectives and Risk Tolerance**
   
   The process starts with understanding business objectives and bringing high-level risks to the surface. This involves an understanding of the organization's business objectives, as well as understanding those of the business unit. In this case, the business unit is clinical technology. The tasks involved in this step include identifying business objectives and what could prevent their successful achievement, recording these risks, and understanding the levels of risk appetite and risk tolerance.

   Risk appetite is the amount of risk an organization is willing to accept overall. Risk tolerance focuses on individual risks and an organization’s readiness to accept the consequences of each risk. Tolerance for risk affects the degree to which the eight additional risk management steps are performed. Past actions from leadership will inform the risk manager of the level of support that can be expected. At this stage, bringing the high-level risks to the attention of leadership, so they can be understood and addressed swiftly and strategically, is necessary. This is necessary before reaching agreement on the risk management process scope among stakeholders (e.g., clinical technology, compliance, privacy, finance, information technology [IT], risk management, and internal audit).

2. **Process Scope**
   
   Recognizing and understanding the full scope of the process is extremely important. Is it a “mega process” that is used across the entire organization or is it a subprocess that is part of a larger major process? For example, a national hazard alert and device recall process is managed by a Kaiser Permanente national department, but it could involve the KP ClinTech program, depending on the type of device being recalled. This is a mega process that involves clinical technology’s major process (i.e., how clinical technology manages medical device recalls).

   If an identified risk is part of the mega process but clinical technology has no control over that part of the larger process, then clinical technology will not be able to properly mitigate the risk. The proper owner of that process must be identified and agree to the ownership and assumption of responsibility for risk mitigation.

3. **Process Ownership**
   
   Before risks can be assessed and prioritized, determining process ownership is critical. Without a clear definition of who is responsible for what parts of the process, important tasks can be overlooked. For example, does a piece of equipment like a portable electromyograph (EMG) machine fall under clinical technology or the clinical department? If ownership of that responsibility is not defined and the portable EMG machine is subject to a recall or hazard alert, then either clinical technology or the clinical department...
could assume that the other was in charge. The result could be that neither department follows up on the recall notice. An organizational policy that clearly defines process ownership can remove this type of ambiguity. (Note: The main subject matter of this article deals with enterprise risk and falls under ISO 31000, while the manufacture of medical devices themselves falls under ISO 14971. The application of risk management for IT networks incorporating medical devices falls under ISO/IEC 80001.)

In addition, as the risk mitigation work begins, it is important to have a thorough understanding of the different phases in the life cycle of the device and to know what phase to address in the mitigation work and who is responsible for that phase. Various groups are involved across the life cycle of a device, and if a process is to be changed, the owner of that process must be involved. At Kaiser Permanente, for example, the KP ClinTech program does not own the equipment. So, when addressing a particular risk associated with an item of equipment, having conversations with the clinical business units that own and/or use the item is important.

4. Impact of IT Systems
Understanding how software applications and infrastructure contribute to the risk is an essential part of the nine-step process. A key task at this point is determining how application systems are associated with the identified risks. An example is inventory management and associated risks. The “system” that may be involved is the organization’s computerized maintenance management system (CMMS). If limited CMMS functionality creates and/or increases inventory management risks, the CMMS limitations should be highlighted to leadership so they understand that until CMMS enhancements are available, these risks will remain.

**Figure 2.** Risk management in nine steps. Abbreviations used: IT, information technology; RMU, risk management unit.
5. Assess Risks
A common process in risk management is to rank identified risks based on the projected impact of each risk and the likelihood that the negative consequences could occur. The light-green, dark-green, yellow, orange, and red colors in the familiar “heat map” correspond to risk rankings of very low, low, medium, high, and very high. The impact dimension on the heat map considers the consequences or degree of threat of disruption to the mission, strategic objectives, and operational processes. The likelihood dimension identifies the chance that the risk event will occur, taking into account current controls, processes, systems, and management practices. The combination of these two factors produces an overall risk rating that ranges from very low to very high.

Based on the risk rankings, the organization will decide which risks to address and in which order. A number of factors will affect those decisions: Is patient safety a factor? Is available funding sufficient to fix the problem? Are we in danger of jeopardizing our accreditation by delaying a response to the problem? Will we face a public relations problem (i.e., damage our brand) if we don’t address this issue?

6. Evaluate Assurance Activities
The ability for clinical technology to meet and advance its business objectives depends on a risk management balance. One side involves complying with regulations, policies, and other rules. The other side involves the ability to provide timely and affordable equipment services. Although they have been put in place for safety or other reasons, factors such as regulations, policies, and other rules can impede progress toward meeting business objectives. That inherent conflict is the reason for integrating risk management into everyday operations.

Lines of defense. To ensure that everyone is making progress toward meeting objectives while still following all the rules and avoiding the potential for risk, Kaiser Permanente uses assurance activities that have been categorized into three “lines of defense.” The activities in the lines of defense are intended to prevent occurrences such as violations of government regulations or citations during an accreditation survey, which can slow progress toward meeting business objectives.

As shown in Figure 3, Kaiser Permanente has three lines of defense. The first line of defense, operations, involves efforts by the clinical technology business unit to manage the risk associated with its day-to-day activities. In this first line of defense, risk assurance tasks include monitoring activities such as metrics, data mining, self-assessments, and quality-assurance activities. One way to manage risk on a day-to-day basis is to have a risk manager assigned to every aspect of clinical technology; however, budget limits may deem that impractical.

Another way for risk managers to work with the business unit to manage its risks is to use the second line of defense, which involves risk management units (RMUs) that are outside the clinical technology business unit. An RMU could be an independent risk department, a risk manager who is part of a quality department, or even a member of a compliance department whose primary responsibility is risk management. An RMU should check in with the first line (operations) on a periodic basis. This leverages quality-assurance methods by looking at abnormal situations and either supporting or refuting observations identified in the first line. Therefore, between the first line and the second line, any concerns would be made known to those in operations. RMUs can benefit the lines of business operations by helping to maintain risk-mitigation changes and thus ensure a continuation of the lower level of risk achieved.

At Kaiser Permanente, the risk manager is embedded with the clinical technology business unit so he/she can better understand the business operations of clinical technology on a day-to-day basis. This aspect of the second line of defense allows the risk...
manager to further help the business unit identify and manage its risk.

The fail-safe measure is the third line of defense. These are independent people—they are far removed from the daily business operations of any particular business line. They can be from outside (e.g., external auditors) or internal to (e.g., teams from internal audit services, licensing and accreditation, regulatory risk, or compliance) the organization. It is not uncommon for the third line to be brought in before a problem occurs. The third line may perform activities on its own or be invited by the business unit to perform independent activities. If the risk management process is working well, little need should exist for the third level. However, it can be beneficial to have a third party (e.g., internal audit team, external auditors) examine processes proactively.

Communication among the lines is necessary to adequately evaluate assurance activities. For example, monitoring activities by the risk management unit (second line of defense) can lead to a request for an audit (third line of defense).

7. Agreement on Action Plans or Risk Acceptance

After the risk assessment has been completed and the risks ranked based on likelihood and impact, organizational leadership must determine what risks will be mitigated and to what degree. In addition, a time frame to complete the mitigation should be agreed upon by leadership and the business line management so the goals will be completed successfully. Because some level of inherent risk will always exist, an agreement among the three lines of defense is critical to successfully manage the mitigation of risk. At Kaiser Permanente, this agreement is referred to as a Joint Plan. This is a written document describing the assurance activities that the

Figure 3. Kaiser Permanente (KP) Integrated Risk Management: lines of defense. Abbreviations used: ESS, Enterprise Shared Services; SOX, Sarbanes-Oxley Act of 2002.
business line, risk management, compliance, and internal audit teams will conduct as part of risk mitigation. A sample Joint Plan is provided in Figure 4.

The Joint Plan begins with evaluating the controls and assurance activities that should be in place to help reduce the inherent risk to the organization. After that step is complete, residual risk remains. Inherent risk is the risk that an activity would pose if no controls or other mitigating factors were in place. This can be thought of as the gross risk. Residual risk is the risk that remains after controls are taken into account. This can be thought of as the net risk.

8. Manage Risk
The most extensive part of the nine-step process is the actual management of risk. Capturing and documenting the business operations’ risk assurance information in the risk management plan is important. This will help determine future focus areas and opportunities for integration of risk mitigation within business operations.

**Strategic planning and risk alignment.**
With the framework and a process in place, the next task is to integrate these risks into the strategic plan (as described above). Figure 1 illustrates how the KP ClinTech program integrated its identified risks into initiatives. For example, after identifying and assessing risks that fall under technology, the risk assessment validated and justified the need for a single enterprise CMMS solution. That initiative addresses risks such as using multiple inventory systems and the inability to quickly pull accurate inventory data.

Identifying many of the risks that span the clinical technology life cycle is important. In the case of Kaiser Permanente, identifying those risks early and remediating them promptly allowed the organization to streamline its processes, reduce rework, and

<table>
<thead>
<tr>
<th>Business Process Area(s) and Owner(s)</th>
<th>Joint Plan Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.9 Acquire, Maintain, and Retire Clinical Technologies Owner: Carol E. Davis-Smith</td>
<td>7/1/2015</td>
</tr>
<tr>
<td>Risk Rating Date: 9/1/2014</td>
<td>Reassessment date: 12/5/15</td>
</tr>
<tr>
<td>Impact: Significant</td>
<td>Impact: Significant</td>
</tr>
<tr>
<td>Likelihood: Likely</td>
<td>Likelihood: Likely</td>
</tr>
<tr>
<td>Overall Rating: High</td>
<td>Overall rating: Very High</td>
</tr>
</tbody>
</table>

**Risk Statement**
Organization lacks a formal life cycle approach to management of medical devices, which causes life cycle phases to be managed separately and without connectivity. This leads to devices being purchased without regard for technical security capabilities, lack of planning for maintenance needs, and inconsistent disposal processes.

**Current Risk Management and Assurance Activity**
Conducted an in-depth risk analysis into each life cycle phase. Established workgroups to create processes for each life cycle phase. End product will have combined all phases so a high-level, complete life cycle process can be seen.

<table>
<thead>
<tr>
<th>1st Line of Defense Operational Activities</th>
<th>Planned Risk Assurance Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring Activities - Metrics ** Listed on the left, are examples of the types of activities.</td>
<td></td>
</tr>
<tr>
<td>Monitoring Activities - Data Mining ** In this ‘planned’ column, you simply list the actual activity you have planned.</td>
<td></td>
</tr>
<tr>
<td>Monitoring Activities - Self Testing &amp; Control Self Assessments</td>
<td></td>
</tr>
<tr>
<td>Quality Assurance Activities</td>
<td></td>
</tr>
<tr>
<td>2nd Line of Defense RMU Consulting Activities</td>
<td>Planned Risk Assurance Activities</td>
</tr>
<tr>
<td>Consultation &amp; Operations Support</td>
<td></td>
</tr>
<tr>
<td>Surveys &amp; Operational Risk Assessments</td>
<td></td>
</tr>
<tr>
<td>Monitoring Activities (Supports Ops)</td>
<td></td>
</tr>
<tr>
<td>Quality Assurance</td>
<td></td>
</tr>
<tr>
<td>3rd Line of Defense Validation Activities</td>
<td>Planned Risk Assurance Activities</td>
</tr>
<tr>
<td>Outcomes Testing</td>
<td></td>
</tr>
<tr>
<td>Audit of a Process</td>
<td></td>
</tr>
<tr>
<td>Investigations</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 4.** Sample of a Kaiser Permanente Joint Plan. Abbreviation used: RMU, risk management unit.
ultimately lower the total cost of ownership. For medical devices, the risk management process should start at the beginning of the device life cycle, which is the assessment and evaluation stage.

Having a conversation about risks with the manufacturer during the sourcing process can be advantageous. At that stage, a comparison can be made among two or more devices, potentially yielding valuable information. Early research can reveal shortcomings such as inadequate security features on one device versus a similar device.

**Governance.** For maximum success, the organization should establish governance around its risk management activities. At Kaiser Permanente, a workgroup was formed as part of the risk assessment process. This group performed the original rankings for the identified risks discussed in step 5. The workgroup evolved into a Clinical Technology IRM Advisory Committee. The committee originally consisted of more than 50 people from various areas within the organization. The size and breadth of the group fostered the synthesis of various perspectives, which was important because KP ClinTech is a horizontal business unit whose work spans the organization.

The current committee has 38 members from various lines of business, including clinical technology, risk management, compliance, privacy and security, IT, and internal audit. Ad hoc members are included depending on the risk being addressed, thereby promoting availability of subject matter expertise. In some cases, the committee may need strategic partners or those responsible for a process that clinical technology supports. One example would be product hazard alerts and recalls: Clinical technology is not responsible for the process across the enterprise, and the process is much bigger than just clinical technology.

The members of the committee have the authority to implement remediation activities in their respective areas, within the guidelines of the IRM program. Regardless of whether risk management standard ISO 31000 or ISO 14971 applies, monitoring and improvement of the risk management process and framework are required. The committee can assist in this regard by identifying gaps in the risk treatment work and by offering suggestions on how to improve the risk management process and/or framework.

The workgroup must reach consensus on action plans to address the residual risk or what amount of risk will be acceptable for the organization. Following through on action plans to manage residual risks is a long-term step that can take place over many years.

The committee meets quarterly and shares information via a collaborative software program that facilitates communication and acts as a resource bank.

**9. Reporting to Leadership**

The last step involves reporting findings to the senior leadership of the organization using tools such as dashboards and other methods to capture metrics. Communicating with the use of metrics and key performance indicators has value. Developing operational and executive dashboards can be helpful—these dashboards highlight the progress toward identifying risks and charting progress in terms of remediation.

Data can be reported to show trends and for comparison to internal benchmarks established by the governance board (described above). The data allow for discussion of clinical technology business with senior leaders using *numbers* rather than just anecdotes.

Although there is no shortage of metrics, there are no agreed-upon industry performance standards. That does not take away from the tremendous value of metrics and key performance indicators. They give important insight into any business and provide visibility that can drive changes and improve performance.

In addition, becoming a data-driven organization is key to the ongoing evolution and success of a well-run healthcare technology management program. Metrics can be used with standard business processes to transform work and drive engagement and
motivation of staff employees, managers, and executives, resulting in better customer service at a competitive cost.

Figure 5 shows an example of a dashboard that provides a high-level status report of risks that are part of Kaiser Permanente’s IRM project.

**Summary**

Risks are inherent with any project, initiative, or operational process. After identifying risks and assessing the level of attention required by each, it is important to use a risk management framework and follow a formal risk management process so that those risks can be addressed up front.

In following an IRM process—using a suitable framework and aligning identified risks with existing and planned initiatives within the strategic plan—an organization, regardless of size, will be able to meet its business objectives while mitigating risk with maximum success.

**References**


---

**Figure 5.** Sample of a Kaiser Permanente Integrated Risk Management (IRM) program. Abbreviations used: CT, clinical technology; NPSR, national product safety recall.