HIMSS System Risk Analysis Survey Report
June, 2012
Executive Summary—Overview and Analysis of Survey

Medical technology has rapidly evolved in the past 20 years and little resembles what most regulators and healthcare providers dealt with less than a generation ago when establishing many of the guidelines and regulations that are still in effect today.

Today’s medical technologies range from integrated information technology systems to complex robotics, imaging, telemedicine and micro/nano technologies. What were formerly passive technologies have largely been replaced by new systems of systems (SoS) that actively control critical physiological processes and functions.

These medical devices and systems have the potential to play a transformational role in healthcare delivery.

If fully realized, the benefits of these technologies can substantially improve the quality and timeliness of patient care while insuring that care is delivered in a safer and more cost-effective manner. However, implementation of these medical devices and systems is not without risk. New technologies also bring new challenges and vulnerabilities. If not managed well, these same technologies can financially drain healthcare organizations, create workflow nightmares and pose major risks to the care and safety of their patients.

Application of effective risk management to information technology and associated processes by healthcare providers is absolutely critical to addressing the challenges associated with these increasingly complex and integrated technologies. Application of effective risk management can identify major technology-related risks and enable organizations to focus its finite resources on real issues and realize tangible benefits.

Having recognized the importance of the application of effective risk management by healthcare providers to medical technology, the HIMSS Medical Device and Patient Safety Task Force in cooperation with the Clinical Engineering & IT Community established a project to develop a Risk Analysis Resource Guide. The Risk Analysis Resource Guide would provide healthcare providers with information they needed to establish and implement a risk management process for medical technology. To formulate an appropriate Guide, HIMSS (with cooperation of AAMI, ACCE, ASHRM) conducted a survey of healthcare organizations to determine the status of their current practices and capabilities with respect to the risk management of medical technology.

The survey conducted in spring 2012 yielded 149 responses from organizations ranging from community hospitals to academic medical centers to multi-hospital integrated delivery networks.

Key Findings

- Additional industry efforts are needed to engage owner/operators, senior management in the risk management process (RMP).
- Technology risk-management processes are far from universal with healthcare providers. Less than 60 percent of those surveyed employ a pro-active technology-related risk management process.
- Lack of consistently identified involvement on part of risk managers (RM) or other quality and/or patient safety professionals is likely the result of those professionals not being able to dedicate a substantial portion of their time to the RMP but rather having to multi-task on other professional roles.
Inconsistent application of the RMP throughout the healthcare provider community is likely due in large part to the absence of a consistent message to all stakeholders.

Technology owner/operators, IT, clinical engineering, risk management and senior management should all be involved in the RMP.

RMP should be documented in policy/procedure, meeting minutes, risk assessment findings and a mitigation plan. Sample tools and guidelines would facilitate the adoption of this practice.

Responses suggest that proper attention is most often given to systems that are clearly identified as either IT or biomedical. Some question of ownership of hybrid systems may result in their falling “through the cracks” with respect to the RMP.

Enterprise organizations may have a broader understanding of risk and the RMP as a whole, leading to better documentation and consideration of financial and operational risks as well as patient and safety risks.

All these risks (financial and operational risks as well as patient and safety risks) should be considered in the RMP. The RMP is similar for all risks and can be conducted concurrently. A broad RMP considering all risks will likely get the greatest buy-in by all stakeholders, including leadership.

Of the multiple risk elements described, most respondents from non-enterprise organizations described them as being considered independently, not linked as one might expect in a more mature RMP.

The significant lack of industry use of formal RMP guidelines suggests a need for the identification or development and subsequent promotion of such guidelines.

Manufacturers risk assessments and industry best practices should be included as major factors in the RMP.

There appear to be no common set of tools consistently used to conduct the RMP.

Leadership needs to be informed of the need for resources and the safety, clinical, financial and operational implications of not implementing an adequate RMP.

Healthcare providers need to be better informed about available references on conducting an effective technology RMP.

Goal of Survey

The goal of this survey is to obtain baseline information from healthcare providers about their application of risk management during the medical technology lifecycle (e.g., acquisition, deployment, use, modification and retirement).

Goals of the Survey:

- Determine the extent to which healthcare providers currently apply some form of risk management during the medical technology lifecycle;
- determine the nature of the risk management process for those organizations who report they have a process; and
- assess the need for additional industry guidelines that would assist all healthcare providers in the prudent application of risk management to the medical technology lifecycle.
Respondents

There were 149 respondents to the online survey. The majority of those (115 of 149) were individuals representing primary healthcare providers.

Of the 115 individuals from healthcare providers responding, community hospitals represented 37, enterprise healthcare networks represented 42 and academic medical centers represented 36.

The balance of respondents (34) were from non-healthcare providers and included representation from such diverse sources as consultants, medical device manufacturers and software developers, government and independent service organizations (ISO).

The survey and the subsequent analysis were intended and designed primarily to identify risk management practices and trends in the healthcare provider settings. Therefore, the report focuses on the results of responses from those who identified themselves as representing one of the healthcare provider categories (N=115).

Methodology

To gain a better understanding of the use of system risk analysis by healthcare organizations, HIMSS Medical Devices and Patient Safety Task Force and Clinical Engineering & IT Community, in partnership with the American Society for Healthcare Risk Management (ASHRM), conducted a web-based survey. The survey was distributed via electronic messages to HIMSS membership, CE-IT Community and ASHRM members. This survey included 15 questions, and has been completed by professionals with a variety of backgrounds (e.g., clinical, IT, administration, clinical engineering [CE]) working in a variety of positions (e.g., risk management, nursing, administration, clinical engineering, information technology).
**Specific Survey Results/Findings**

**Figure 1**

<table>
<thead>
<tr>
<th>Question 1</th>
<th>When does your organization employ a risk management process that examines risks associated with technical systems and related processes?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Response</strong></td>
<td></td>
</tr>
<tr>
<td>Prior to Acquisition</td>
<td><img src="Image" alt="Bar Chart" /></td>
</tr>
<tr>
<td>After Adverse Event</td>
<td><img src="Image" alt="Bar Chart" /></td>
</tr>
<tr>
<td>Prior to Deployment</td>
<td><img src="Image" alt="Bar Chart" /></td>
</tr>
<tr>
<td>When necessary</td>
<td><img src="Image" alt="Bar Chart" /></td>
</tr>
<tr>
<td>Never</td>
<td><img src="Image" alt="Bar Chart" /></td>
</tr>
<tr>
<td>Periodic Intervals</td>
<td><img src="Image" alt="Bar Chart" /></td>
</tr>
<tr>
<td>Don't know</td>
<td><img src="Image" alt="Bar Chart" /></td>
</tr>
</tbody>
</table>

| Findings | Twenty-four percent of respondents from all care settings reported their organizations did not employ a technology-related RMP at all and an additional 9% reported they “did not know”
Approximately 30 percent of those responding claimed they conducted a risk management process (RMP) prior to technology acquisition/deployment and after an adverse event. |
| Conclusion | Technology risk management processes are far from universal with healthcare providers. Less than 60 percent of those surveyed employ a proactive technology-related risk management process. |
**Question 2: Who "owns" this risk management process for technical systems and related processes?**

**Response:**

<table>
<thead>
<tr>
<th>Role</th>
<th>Combined</th>
<th>Community Hospital</th>
<th>Enterprise</th>
<th>Academic Medical Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE</td>
<td>35%</td>
<td>22%</td>
<td>19%</td>
<td>31%</td>
</tr>
<tr>
<td>Risk Management</td>
<td>15%</td>
<td>21%</td>
<td>16%</td>
<td>23%</td>
</tr>
<tr>
<td>ISO</td>
<td>8%</td>
<td>8%</td>
<td>9%</td>
<td>8%</td>
</tr>
<tr>
<td>System owner</td>
<td>9%</td>
<td>11%</td>
<td>5%</td>
<td>10%</td>
</tr>
<tr>
<td>Safety officer</td>
<td>5%</td>
<td>8%</td>
<td>9%</td>
<td>12%</td>
</tr>
<tr>
<td>Don't know</td>
<td>4%</td>
<td>14%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Findings**

- Fifty of the respondents to this question identified themselves as being in a clinical engineer role, and of those:
  - 50 percent (25) claimed they had some ownership of RMP.
  - 10 percent (5) claimed to have total ownership of RMP.
  - 40 percent (20) said CE plus others shared ownership of RMP.
- Twelve of the respondents to this question identified themselves as being in a risk management role, and of those:
  - 33 percent (4) claimed they had some ownership of RMP.
  - 8 percent (1) claimed to have total ownership of RMP.
  - 33 percent (4) did not know or did not respond to who had some ownership of RMP.
- Twenty-seven of the respondents to this question identified themselves as being in an IT role, and of those:
  - 63 percent (17) claimed they had some ownership of RMP.
  - 30 percent (8) claimed to have total ownership of RMP.
  - 26 percent (7) did not know or did not respond to who had some ownership of RMP.
- There is no one professional type that predominates as owner or manager of the risk management process. Of those responding, most indicated a shared responsibility.

**Conclusion**

Lack of consistently identified involvement on part of risk manager or other quality and/or patient safety professionals is likely the result of those professionals not being able to dedicate a substantial portion of their time to the RMP, but rather having to multi-task on other professional roles. Inconsistent application of the RMP throughout the healthcare provider community is likely due in large part to absence of a consistent message to all stakeholders.
Figure 3

Question 3: What stakeholders are involved in the risk management process? (check all that apply)

Response:

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Combined</th>
<th>Community Hospital</th>
<th>Enterprise</th>
<th>Academic Medical Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT</td>
<td>57%</td>
<td>57%</td>
<td>64%</td>
<td></td>
</tr>
<tr>
<td>CE</td>
<td>53%</td>
<td>57%</td>
<td>64%</td>
<td></td>
</tr>
<tr>
<td>Risk mgt</td>
<td>47%</td>
<td>46%</td>
<td>62%</td>
<td></td>
</tr>
<tr>
<td>ISO</td>
<td>14%</td>
<td>24%</td>
<td>38%</td>
<td></td>
</tr>
<tr>
<td>Sr Management</td>
<td>19%</td>
<td>38%</td>
<td>30%</td>
<td>36%</td>
</tr>
<tr>
<td>System Manufacturer</td>
<td>24%</td>
<td>30%</td>
<td>31%</td>
<td></td>
</tr>
<tr>
<td>Legal</td>
<td>0%</td>
<td>24%</td>
<td>29%</td>
<td></td>
</tr>
<tr>
<td>Facilities</td>
<td>0%</td>
<td>14%</td>
<td>26%</td>
<td>32%</td>
</tr>
<tr>
<td>System Operators</td>
<td>0%</td>
<td>14%</td>
<td>24%</td>
<td>32%</td>
</tr>
<tr>
<td>Purchasing</td>
<td>1%</td>
<td>19%</td>
<td>21%</td>
<td></td>
</tr>
<tr>
<td>Patients</td>
<td>8%</td>
<td>17%</td>
<td>3%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Findings

- Risk management, IT and clinical engineering are all reported have the highest levels of involvement in RMP (47-53%). Other professionals or stakeholders are reported to be involved 30% or less.
- Only 20 percent of respondents claimed senior management is involved and 14% claimed operators are involved.
- Some respondent comments suggest that consultants or International Standardization Organizations (ISOs) might be used more often but for a lack of financial resources.

Conclusion

At least technology owner/operators, IT, clinical engineering, risk management and senior management should all be involved in the RMP.
Question 4: How is the risk management process documented?

- Agenda/minutes.
- Policy.
- Procedures.
- Findings.
- System risk management.
- Mitigation plans.
- Designated responsibility.
- Mitigation schedules.
- Don’t know.

Response:

<table>
<thead>
<tr>
<th>Category</th>
<th>Combined</th>
<th>Community Hospital</th>
<th>Enterprise</th>
<th>Academic Medical Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agenda/Minutes</td>
<td>24%</td>
<td>19%</td>
<td>14%</td>
<td>19%</td>
</tr>
<tr>
<td>Policy</td>
<td>29%</td>
<td>24%</td>
<td>22%</td>
<td>22%</td>
</tr>
<tr>
<td>Procedures</td>
<td>36%</td>
<td>25%</td>
<td>23%</td>
<td>22%</td>
</tr>
<tr>
<td>Findings</td>
<td>36%</td>
<td>19%</td>
<td>11%</td>
<td>11%</td>
</tr>
<tr>
<td>System Risk Mgt</td>
<td>15%</td>
<td>15%</td>
<td>15%</td>
<td>14%</td>
</tr>
<tr>
<td>Mitigation Plans</td>
<td>21%</td>
<td>14%</td>
<td>8%</td>
<td>8%</td>
</tr>
<tr>
<td>Designated responsibility</td>
<td>14%</td>
<td>11%</td>
<td>5%</td>
<td>11%</td>
</tr>
<tr>
<td>Mitigation Schedules</td>
<td>10%</td>
<td>7%</td>
<td>3%</td>
<td>7%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>11%</td>
<td>7%</td>
<td>3%</td>
<td>3%</td>
</tr>
</tbody>
</table>

Findings:
- Only 17 percent of respondents claimed to document mitigation plan and less than 24 percent claimed to have documented policies/procedures, meeting minutes or report of findings. Enterprise providers are more likely to develop policies, procedures and guidelines associated with the RMP (36-38%). Community and academic hospitals report 19 percent to 24 percent have, or are in the process of developing RMP policies, procedures and/or guidelines.
- Enterprise providers were also more likely than community and academic hospitals to document RMP as mitigation plans, mitigation schedules, or designated responsibilities.

Conclusion:
RMP should be documented in policy/procedure, meeting minutes, risk assessment findings and a mitigation plan. Sample tools and guidelines would likely be beneficial.
**Figure 5**

**Question 5:** Does the risk management process address the following:
- Biomedical systems.
- IT systems.
- IT systems associated with Biomed.
- Don’t know.

**Response:**

<table>
<thead>
<tr>
<th></th>
<th>Combined</th>
<th>Community Hospital</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biomedical Systems</td>
<td>51%</td>
<td>65%</td>
<td>32%</td>
</tr>
<tr>
<td>IT Systems</td>
<td>43%</td>
<td>55%</td>
<td>25%</td>
</tr>
<tr>
<td>IT System as pertains to Med</td>
<td>7%</td>
<td>11%</td>
<td>0%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>7%</td>
<td>5%</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Findings**
- High percentages of RMP applied to individual IT systems and Biomedical systems, but RMP appears to be rarely applied to systems incorporating both information and medical technology components.

**Conclusion**
- Responses suggest that proper attention is most often given to systems that are clearly identified as either IT or biomedical. Some question of ownership of hybrid systems may result in their falling “through the cracks” with respect to the RMP.
Figure 6

**Question 6:** Does the scope of risk considered include elements of any of the following:
- Data & systems security
- Clinical risk to patient
- Physical safety of patients, visitors or staff
- Operational risks to enterprise
- Financial risk to enterprise
- Don’t know

**Response:**

<table>
<thead>
<tr>
<th>Category</th>
<th>Combined</th>
<th>Community Hospital</th>
<th>Enterprise</th>
<th>Academic Medical Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data &amp; System Security</td>
<td>49%</td>
<td>43%</td>
<td>36%</td>
<td>33%</td>
</tr>
<tr>
<td>Clinical risk to patient</td>
<td>51%</td>
<td>54%</td>
<td>47%</td>
<td>51%</td>
</tr>
<tr>
<td>Physical Safety of pt, staff, visitors</td>
<td>50%</td>
<td>62%</td>
<td>59%</td>
<td>51%</td>
</tr>
<tr>
<td>Operational risk to enterprise</td>
<td>35%</td>
<td>32%</td>
<td>40%</td>
<td>33%</td>
</tr>
<tr>
<td>Financial risk to Enterprise</td>
<td>39%</td>
<td>35%</td>
<td>40%</td>
<td>39%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>5%</td>
<td>6%</td>
<td>3%</td>
<td>8%</td>
</tr>
</tbody>
</table>

**Findings**
- Enterprise organizations were more likely to consider financial and operational risk to enterprise in RMP (~40 percent and ~60 percent) than community and academic hospitals (~32 percent and ~8 percent respectively).
- Slightly more than one third of respondents claimed their RMP addressed data & system security risks, clinical risks to patients and 28 percent claimed their RMP addressed safety risks to patients/staff/visitors. Only 17 percent overall considered operational and financial risks to organization.

**Conclusion**
Enterprise organizations may have a broader understanding of risk and the RMP as a whole, leading to better documentation and consideration of financial and operational risks, as well as patient and safety risks.

All these risks (financial and operational risks, as well as patient and safety risks) should be considered in the RMP. The RMP is similar for all risks and can be conducted concurrently. A broad RMP considering all risks will likely get the greatest buy-in by all stakeholders including leadership.
Table 7

<table>
<thead>
<tr>
<th>Question 7:</th>
<th>If scope of risk covers multiple elements, does risk management process consider these:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Individually</td>
</tr>
<tr>
<td></td>
<td>• Simultaneously</td>
</tr>
<tr>
<td></td>
<td>• Don’t know</td>
</tr>
</tbody>
</table>

**Response:**

<table>
<thead>
<tr>
<th></th>
<th>Individually</th>
<th>Simultaneously</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respondents</td>
<td>59%</td>
<td>38%</td>
<td>10%</td>
</tr>
<tr>
<td>Community</td>
<td>28%</td>
<td>24%</td>
<td>10%</td>
</tr>
<tr>
<td>Hospital</td>
<td>17%</td>
<td>17%</td>
<td>10%</td>
</tr>
<tr>
<td>Enterprise</td>
<td>16%</td>
<td>10%</td>
<td>3%</td>
</tr>
<tr>
<td>Academic</td>
<td>10%</td>
<td>10%</td>
<td>3%</td>
</tr>
</tbody>
</table>

**Findings**

- Respondents indicated that in the majority of non-enterprise organizations, the different risk categories (i.e., clinical, financial, operational) were evaluated individually.

**Conclusion**

- Of the multiple risk elements described, most respondents from non-enterprise organizations described them as being considered independently, not linked as one might expect in a more mature RMP.
Figure 8

Question 8: Have you formally defined any of the risk management elements below?
- Risk management process
- Stakeholders who participate in process
- Risk acceptance & approval process
- Risk levels with associated criteria
- Severity scores with scoring guidelines
- Probability scores with scoring guidelines

Response:

<table>
<thead>
<tr>
<th>Risk Management Element</th>
<th>Community Hospital</th>
<th>Enterprise</th>
<th>Academic Medical Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Mgt Process</td>
<td>11%</td>
<td>25%</td>
<td>43%</td>
</tr>
<tr>
<td>Stakeholders who</td>
<td>8%</td>
<td>16%</td>
<td>21%</td>
</tr>
<tr>
<td>participate in process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Acceptance &amp;</td>
<td>8%</td>
<td>16%</td>
<td>16%</td>
</tr>
<tr>
<td>approval process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Levels w/associated</td>
<td>6%</td>
<td>14%</td>
<td>29%</td>
</tr>
<tr>
<td>criteria</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severity scores w/scoring</td>
<td>11%</td>
<td>22%</td>
<td>27%</td>
</tr>
<tr>
<td>guide</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probability scores w/</td>
<td>14%</td>
<td>24%</td>
<td>18%</td>
</tr>
<tr>
<td>scoring guidelines</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Findings
- Enterprise organizations were more likely in general to have formally defined risk management elements than community or academic hospitals.
- Slightly less than one-third of all respondents reported they had a formally-defined RMP.
- Even fewer respondents formally identified stakeholders and other criteria usually described as necessary for an RMP.

Conclusion
The significant lack of industry use of formal RMP guidelines suggests a need for the identification or development and subsequent promotion of such guidelines.
Question 9: What, if any, of the following information is considered in the system risk assessment?
- System reliability & incident history
- Manufacturer information their risk management file
- System criticality (based on owner assessment)
- System utilization
- Type of data acquired/maintained
- Regulations/standards
- Industry best practices
- Policies/procedures
- Don’t know

Response:

<table>
<thead>
<tr>
<th>Category</th>
<th>Community Hospital</th>
<th>Enterprise</th>
<th>Academic Medical Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individually</td>
<td>22%</td>
<td>17%</td>
<td>26%</td>
</tr>
<tr>
<td>Simultaneously</td>
<td>31%</td>
<td>21%</td>
<td>36%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>14%</td>
<td>15%</td>
<td>12%</td>
</tr>
</tbody>
</table>

Findings: Respondents claimed that primary factors considered in RMP are technology criticality, system history/reliability, and current regulations standards.

Conclusion: Manufacturers’ risk assessments and industry best practices should be included as major factors in the RMP.
Figure 10

Question 10: Are the following tools employed in the risk management process?
- FMEA
- Risk matrix
- Risk Cause Analysis (RCA)
- Ishikawa diagrams
- Don’t know
- None of the above
- Standard checklists
- Varies by project

Response:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Community Hospital</th>
<th>Enterprise</th>
<th>Academic Medical Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMEA</td>
<td>21%</td>
<td>24%</td>
<td>22%</td>
</tr>
<tr>
<td>Risk Matrix</td>
<td>14%</td>
<td>30%</td>
<td>22%</td>
</tr>
<tr>
<td>RCA</td>
<td>8%</td>
<td>22%</td>
<td>31%</td>
</tr>
<tr>
<td>Ishikawa</td>
<td>8%</td>
<td>19%</td>
<td>35%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>2%</td>
<td>10%</td>
<td>12%</td>
</tr>
<tr>
<td>None of the Above</td>
<td>4%</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Standard Checklists</td>
<td>1%</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Varies by Project</td>
<td>1%</td>
<td>3%</td>
<td>2%</td>
</tr>
</tbody>
</table>

Findings: Root cause analysis (RCA) was the most commonly used tool among all care settings.

Conclusion: There appear to be no common set of tools consistently used to conduct the RMP.
Question 11: What is the scope of safeguards you use when mitigating identified risks?
- Administrative safeguards
- Technical safeguards
- Physical safeguards

Response: Most respondents claimed to be considering utilizing administrative, technical and physical safeguards for mitigating risks (and in roughly equal proportions)
Figure 12

<table>
<thead>
<tr>
<th>Question 12:</th>
<th>Are those responsible for healthcare technology risk management applying their RMP?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routinely to all critical medical technology systems</td>
</tr>
<tr>
<td></td>
<td>Realigning risk management processes to accommodate change in technologies</td>
</tr>
<tr>
<td></td>
<td>Give sufficient resources (i.e., staffing, financial) to conduct RMP</td>
</tr>
<tr>
<td></td>
<td>Don’t know</td>
</tr>
</tbody>
</table>

Response:

<table>
<thead>
<tr>
<th>Applying RM routinely to all critical HC tech systems</th>
<th>19%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-aligning RM processes to accommodate chg in...</td>
<td>14%</td>
</tr>
<tr>
<td>given sufficient resources (e.g., staffing, financial) to conduct...</td>
<td>10%</td>
</tr>
<tr>
<td>Don't Know</td>
<td>6%</td>
</tr>
</tbody>
</table>

Findings

- Few respondents from all care settings (10 percent) reported that their staff was given adequate resources to conduct an effective RMP.
- Only 19 percent of all respondents reported applying risk management routinely to all critical healthcare technology systems.

Conclusion

Leadership needs to be informed of the need for resources and the safety, clinical, financial and operational implications of not implementing an adequate RMP.
### Question 13:
Which of the following documents do you use as a reference or guide in the risk management process:
- ISO/IEC 60601-1:2005
- ISO/IEC 80001-1:2010
- ACCE ECRI Security Guide
- NIST
- HIMSS/NEMA HN-1 Manufacturer’s Disclosure State for Medical Device Security (MDS²)
- CSA various

### Response:

<table>
<thead>
<tr>
<th>Document</th>
<th>Combined</th>
<th>Community Hospital</th>
<th>Enterprise</th>
<th>Academic Medical Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 60601-1:2005</td>
<td>15%</td>
<td>24%</td>
<td>9%</td>
<td>11%</td>
</tr>
<tr>
<td>ISO/IEC 80001-1:2010</td>
<td>7%</td>
<td>5%</td>
<td>9%</td>
<td>10%</td>
</tr>
<tr>
<td>ACCE ECRI Security Guide</td>
<td>7%</td>
<td>5%</td>
<td>6%</td>
<td>10%</td>
</tr>
<tr>
<td>ISO/IEC 14971:2007</td>
<td>5%</td>
<td>8%</td>
<td>11%</td>
<td>11%</td>
</tr>
<tr>
<td>NIST</td>
<td>3%</td>
<td>5%</td>
<td>8%</td>
<td>17%</td>
</tr>
<tr>
<td>HIMSS/NEMA HN-1 Manufacturer’s Disclosure State for Medical Device Security (MDS²)</td>
<td>8%</td>
<td>5%</td>
<td>8%</td>
<td>11%</td>
</tr>
<tr>
<td>CSA various</td>
<td>1%</td>
<td>2%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

### Findings
- No one document stood out as a must-have reference- even the most-frequently mentioned (e.g., NIST, 80001, and ACCE ECRI) were only referenced by 15-20% of respondents.

### Conclusion
Healthcare providers need to be better informed about available references on conducting an effective technology RMP.

### Barriers to Implementation

According to the survey, some of the barriers to implementation are lack of adequate:
- Knowledge regarding nature and extent of challenge.
- Expertise (in risk management, medical and information technologies).
- Limited financial and staff resources.
Conclusion

The results of the survey indicate that a large percentage of healthcare institutions still have a considerable way to go in order to achieve a meaningful risk management program. While a sizable number of institutions do perform some level of risk management, they also state they do not have sufficient resources, which can result in the inconsistent performance of risk management activities, and often separate application of risk management techniques to IT and medical devices systems. From these observations, it is clear most healthcare institutions need assistance in moving forward to attain effective risk management programs.

Appendix A

Nomenclature

Incident.  An incident is the occurrence of any unintended event; typically an event that either resulted in an adverse outcome (i.e., having an adverse health, financial or operational impact) or potentially could have resulted in an adverse outcome.

Failure Mode Effects Analysis (FMEA)

Failure. The failure of a device/system to have its intended effect. This may occur as a condition of not meeting intended performance or safety requirements, and/or a breach of physical integrity.

Failures (or reported failures) are typically one of three types:

- **Wear-and-tear related.** The failure of device or component where the root cause is related to amount and kind of use.
- **Spontaneous related.** The failure of device or component that was tested prior to failure could not have been predicted.
- **Use or process related.** The failure (or reported failure) of a device or component where it is subsequently determined that the problem is due to physical damage or improper application (i.e., inadequate training, poorly designed processes) or some combination thereof.

Levels of Device/System Failure. The level of a system failure is defined as:

1. **Major failure:** Device/system is not operational, or device has a major safety issue.
2. **Minor failure:** Device/system is operational, but has minor defect that otherwise does not threaten operation or pose a significant safety hazard.

Probability. The probability of an event. When dealing with technology, the focus is on the probability of a major failure resulting in an adverse effect … where the probability of such a major failure may be classified as:

1. Improbable—extremely unlikely to occur in a device or system lifetime.
2. Remote—unlikely, but possible to occur in a device or system lifetime.
3) Occasional—likely to occur sometime in a device or system lifetime.
4) Probable—likely to occur several times in a device or system lifetime.

**Residual risk.** The Risk remaining after all reasonable Risk Reduction and Risk Transfer measures have been taken.

**Risk** is the expected value of a future event. A Risk may be either positive or negative and is typically rated on a scale from low to high. General usage of Risk tends to center on the negative aspects where there are human, financial or operational costs (i.e., “downside risks”) or failure to obtain some anticipated human, financial or operational benefit (i.e., “upside risk”).

**Risk Acceptance.** The Risk is accepted by the organization typically when no further Risk Reduction or Risk Transfer is possible, and the perceived benefits of proceeding outweigh the perceived cost of the Residual Risk. Depending on level of Residual Risk, acceptance may be “automatic” (e.g., for low or negligible risks) or may require authorization by a designated authority (e.g., medium or serious risks) or the organization’s senior management (e.g., high risks).

**Risk Assessment.** The process of determining the probability and severity of an identified event and assigning that event a Risk level (typically on a scale from low to high Risk). Probability and severity of an identified event are usually determined based on a history of the same (or similar) events and by individuals with an insight into the nuances of the potential probability/severity of such events.

**Risk Identification.** The process of identifying possible events. Risk Identification is generally best done by individuals who by virtue of their experience/expertise have an insight into the potential for such events.

**Risk Level.** The Risk Level is a function of (and generally proportionally related to) Probability and Severity. An increase in either Probability or Severability will increase the level of Risk.

**Risk Management** is the identification, assessment, and prioritization of risks followed by the coordinated and judicious application of resources to minimize, monitor, and control the probability and/or severity of events. Risk Management typically involves some combination of Risk Transfer, Risk Reduction and/or Risk Acceptance.

**Risk Prioritization.** The process of assigning a priority to the Reduction or Mitigation of an identified event based on the Risk Assessment (typically on a scale from low to high priority).

**Risk Reduction.** The use of Mitigation to reduce either the severity or probability of an event. Mitigation typically involves the application of some combination of administrative, technical or physical measures aimed at reducing the severity or probability of an event. Common measures include process/procedures changes, technology changes, environmental changes, education, or scheduled technical service.

**Risk Transfer.** The transfer of Risk to another entity (i.e., insurance).

**Severity.** The severity of an event. When dealing with technology, the focus is on the severity of any potential adverse effect (health, financial, and/or operational) when a major failure occurs … where the severity of such effects may be classified as:

1) Negligible—no adverse effect (health, financial, operational).
2) Marginal—reversible adverse effect (health, financial, operational).
3) Critical—permanent adverse effect (health, financial, operational).
4) Catastrophic—loss of life, total financial loss, cessation of all operations.
Risk Management Standards for Medical Devices

- ISO/IEC 60601-1: 2005 *Medical Electrical Equipment* requires manufacturers to include some information in accompanying documents if medical equipment is to be connected to an IT network
- ISO/IEC 14971:2007 *Application of risk management to medical devices*
- ISO/IEC 20000-1:2005 *IT Service Management System*
- *Information Technology Infrastructure Library (ITIL v3)*
- HIMSS/NEMA HN 1-2008 *Manufacturer’s Disclosure Statement for Medical Device Security (MDS2)*
- The Joint Commission *Sentinel Event Alert #42: Safely implementing health information and converging technologies*, December 11, 2008
  - SP 800-61: *Computer Security Incident Handling Guide*
  - DRAFT SP 800-53: *Recommended Security Controls for Federal Information Systems*
  - SP 800-55: *Security Metrics Guide for Information Technology Systems*
  - SP 800-50: *Building an Information Technology Security Awareness and Training Program*
  - SP 800-42: *Guideline on Network Security Testing*
  - SP 800-35: *Guide to Information Technology Security Services*
  - SP 800-34: *Contingency Planning Guide for Information Technology Systems*
  - SP 800-30: *Risk Management Guide for Information Technology Systems,*
Risk Analysis Tools

For integrated medical device IT networks, one standard is IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices. The goal of IEC 80001 is to apply appropriate risk management consistent with ISO 14971 to address safety, effectiveness, data and system security, and interoperability. HIMSS has developed a useful reference document for clinical institutions implementing 80001 for the first time: Integrating Medical Devices with Clinical Documentation Systems: A Quick-Start Guide Developed by the HIMSS Medical Devices Patient Safety Task Force. The following is the process flow for risk evaluation from the 80001 standard.

1 http://www.iso.org/iso/catalogue_detail.htm?csnumber=44863
2 http://www.himss.org/ASP/topics_FocusDynamic.asp?faid=295
**ISO/IEC 80001: 2010 Risk Management for Medical Devices on a Network** for characterizing the medical risk associated with a device. Risk associated with the device is a function of the severity of the probability of occurrence of harm and consequences of that harm. Residual risk is defined as the risk remaining after the application of risk control measures.

The ISO 19471:2007 model defines an exposure event as a unique failure mode for an operation, linking the hazard, sequence of events and hazardous situation as shown in Figure 2 on page 24.
Figure 2: Exposure Events in the ISO 14971:2007 Model.

The therapy based risk model also links field feedback and system modifications directly to the product risk model. This allows a better overall analysis of the product’s overall safety and risk performance.

Conversely, in the Information Technology community, risk management is usually accomplished only as it pertains to system security as a business risk. Rather than perform a holistic risk management protocol for a system, most IT organizations draw upon best practices described by ISO 20000, ("ISO/IEC 20000:2005 IT Service Management System") and/or ITIL. ITIL (IT Infrastructure Library) provides guidance for using best practices for IT service management.

Using features from these three information sources, IEC 80001-1 provides insight into the management of risks from both the medical and IT features of a system integrating the two technologies. Only by combining these concepts as addressed in the IEC 8001, can the healthcare facility ensure the key properties of an integrated medical IT network, safety for the patient and caregiver, continued efficacy of the medical device system, and security of the entire system.

**ECRI: Top 10 Health Technology Hazards For 2012**

Health IT offers many opportunities but also may pose many risks. ECRI developed a list of the top 10 risks that can be avoided.


**The Joint Commission Recommendations**
Sentinel Event Alert, Issue 42: Safely implementing health information and converging
technologies, December 11, 2008.

http://www.jointcommission.org/sentinel_event_alert_issue_42_safely_implementing_health_information_and_converging_technologies/

The Joint Commission, Sentinel Event Alert, Issue 43: Leadership committed to safety, August 27, 2009
http://www.jointcommission.org/sentinel_event_alert_issue_43_leadership_committed_to_safety/

Appendix D

References

- Grimes SL. Using 80001 to manage medical devices on the IT network. Association for the Advancement of Medical Instrumentation. IT Horizons;Fall 2011:23-6.
- Schrenker R. The case for a systems focus in healthcare. IT Horizons; 2010.
- Thompson G. The CE-IT community shifts into gear. 24x7 Magazine. Feb 2009.