How to Conduct a Risk Assessment

Risk assessments can be conducted in a number of ways. Certain common methods, such as failure mode and effects analysis, can be time consuming. By following the steps below, through a group process or by interviewing individuals, one can identify issues that should be addressed prior to implementing your health IT system.

Once the “ground rules” of conducting a risk assessment are met, the leader of the risk assessment being conducted should:

1. Gather all potential issues and system breakdowns (vulnerabilities), both electronic and person-based, through brainstorming in an interview or with a group.
2. Identify duplicate vulnerabilities.
3. Determine the source or cause of each vulnerability.
4. Prioritize the vulnerabilities based on your organization’s goals or concerns or prioritize using a scheme such as that used in failure mode and effects analysis.
5. Develop a means of solving or addressing the vulnerabilities. This can be accomplished through one or more of the following.
   a. Redesigning or refining workflows.
   b. Redesigning the software.
   c. Including findings in your health IT training program.
6. Monitor for the vulnerabilities postimplementation and make any necessary changes.