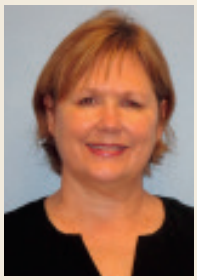
Enterprise Risk Assessments

Practical guidance for the front-line practitioner

By Debra Harrington, CISSP, CRISC, CISA

The HIPAA Security Rule requires covered entities to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity." An Enterprise Risk Assessment can help meet this requirement, and is also an important tool for your organization's leadership. A well thought-out process will put you on the path to a quality assessment.

Deb Harrington is presently a freelance writer, consultant and crusader for real risk assessments, improved controls, and better governance in healthcare. She has over 17 years' experience in IT, audit, compliance and risk management. You can reach Deb at DHarrin7882@gmail.com.



You learned you will be doing the Enterprise Risk Assessment—for the entire health system—a daunting assignment supported by executive leadership and the Board.

Assume that your manager is able to clearly articulate key performance indicators or metrics and critical assessment activities. As you prepare, ask clarifying questions and document the project charter so you and the leaders agree on the goals, roles and responsibilities, and the methodology.

It is important to have agreement on the purpose and overall objective of the Enterprise Risk Assessment. In particular, is the purpose to be compliant with regulatory mandates (HIPAA, Meaningful Use, etc.), or is it to provide leadership with better insight into the risks related to the business?

A well-considered health-system risk assessment should be broad enough to help leaders better understand the risks and opportunities presented to the enterprise.

Threats and vulnerabilities to data represent risks that are opportunities as well as challenges. It is the job of the analyst to present the risk fairly and objectively. An analyst should be able to recommend a course of action and prioritization of risk. Too often, the organization lacks an understanding of its risk profile. Gaining this understanding is often the greatest value and result of an Enterprise Risk Assessment.

So, how do you get started?

Begin with the end in mind

Here are some key starter questions:

1. Who is your key audience?
2. What do they need to know?
3. In what format do they need the information?
4. Are there other stakeholders who will need information from this effort?
5. Will they need information in different formats?

6. Do you have access to tools and utilities (like RedCap, IDEA, etc.)? Do you know how to use the tools? Do you need training or help?

7. Are there previous assessments or reports to use as templates?

8. Are others available to help?

Get agreement on the overall plan

Scope

Determining the scope is one of the most challenging aspects of the project. The CIO/CISO, who may be sponsoring the Enterprise Risk Assessment, may not have direct responsibility for ancillary information systems (e.g. lab, radiology, etc.). Yet, those areas are on the network and the CIO and CISO are responsible for the functionality and safety of the network.

Focus – Determine if the ERM will focus on information systems, applications or data. Words do matter. System access is different from data access. Entities can and do shut down access to a system like a port or firewall. An application can be on or not be on the network. Active Directory groups can manage users, devices and applications effectively.

Unfortunately, interactive data management is far more difficult. Event triggers, scripted calls, HL7 protocols, ATSM, service-oriented architectures and newer microservice architectures make data ubiquitous and accessible from an undefined number of points across the enterprise.

In many cases, the number of endpoints that access electronic protected health information can be unknown and unknowable, since the number of viewers, reports, queries, events, triggers, biomedical devices, applications and jobs is seldom inventoried. To do so is cost prohibitive.

Health systems must consider, from more holistic perspectives, the opportunities and the threats associated with the data in transit. It may make sense to map out key transmission protocols and brainstorm threat/vulnerability and risk scenarios rather than organizing by individual asset or application. The scope is ultimately a business decision, but formal documentation and approval of the scope provides legitimacy for the project.

Tip – Documenting all scoping decisions provides an audit trail and supports analysts and future decisions.

Process areas

Determine which locations, facilities, departments, business units, and practices will be included in the ERM. The 80-20 rule is recommended. Cover the major areas of the enterprise and then implement a rotational approach for ancillary and satellite areas that may be a lower or remote risk.

Most health systems have at least one electronic medical record system. Sometimes there is a separate system for the eye care area or a separate system for the pediatric area. Try to obtain several different organizational charts from various people, because the view of the enterprise depends upon where you sit.

Areas frequently overlooked in Enterprise Risk Assessments:

1. Ancillary departments: radiology, laboratory, pharmacy, cardiology, nephrology, surgery, speech/hearing, physical therapy, respiratory therapy

2. Home health services

3. Telemedicine and remote or video services

4. Research and international projects

5. Interfaces, HL7, ATSM and Service-Oriented Architecture or Event–Trigger Transmission protocols—most of which are unencrypted, clear text of patient information!

Tip – OCR recently cited UMass Medical Center for failing to include its Center for Language, Speech and Hearing as a "healthcare component" in its enterprise risk assessment.[1]

[1] www.hhs.gov/sites/default/files/umass_ra_cap.pdf

People

When agreement is reached on the areas to include, identify the key contacts and resources at each location. Some groups try to direct the assessments to only the information technology, network or systems people. You should push to include business representatives in the risk assessment discussions. Having a business viewpoint provides a different perspective.

Governance

Request a governance structure for the project. A steering committee will keep you on track and make you accountable. It will encourage support and discourage delays from areas of the organization that might not want to provide resources to the effort.

Time

Set realistic goals and timelines. If you are requesting interviews with a doctor who also has administrative responsibilities, it will take longer to schedule the interview. Try to schedule meetings in one-hour blocks. Schedule meetings with key people at least three weeks ahead.

Get approval and sponsorship

Document the scope within a project charter and have it formally approved. Find a sponsor, if possible. IT sponsorship is nice, but a medical sponsorship is crucial to a comprehensive Enterprise Risk Assessment. Departments have shadow IT or power users who support systems. These departments may not report to the CIO or to IT.

Request a project manager

Not every organization is large enough to have project management resources, but Enterprise Risk Assessment does require project management. You should use a spreadsheet or other tracking method to monitor the key activities for the Enterprise Risk Assessment, especially if there are many systems, applications and data repositories.

Develop a methodology

Adopt a framework

National Institute for Standards and Technology (NIST) 800-30 R1 (2012) provides guidance for determining the risk assessment approach, identifying threats, vulnerabilities and risk scenarios and determining the risk assessment tiers. NIST 800-53 R4, the Cyber Security Framework or ISO 27001 can be used as guidance for detailed control areas, as needed.

Adopt a tiered approach

One size does not fit all parts of the enterprise. For example, start at the top of the enterprise and use open-ended questions. Brief interviews with the C-suite and key board members will identify key risks.

Use follow-up interviews at this level sparingly. Executives expect periodic interaction with auditors about risk. Well-crafted questions usually generate productive conversations. Executives at this level view follow-up interviews as a lack of preparation.

- Draft in-depth surveys that apply these identified risks to other areas of the organization.
- Conduct surveys of leaders of divisions, business units and division leaders. Responses from the first round should drive the focus of the second round.
    - Conduct targeted interviews or assessments based on the results of the surveys for a sample or a subset of the areas, applications, systems or technologies.
    - *Tip* – Determine whether the risk should be IT/IS-focused or business-focused. Strategic mission/business objectives with an IT/IS control focus generate productive conversations.
    - Summarize the results for each division, business unit or area.
    - Each division, business unit or group should receive a list of any recommendations before they are presented to up-the-line leadership. Managers may add more detail or context, or may have simply misunderstood the requirements, especially during the Enterprise Risk Assessment.
- Conduct a different set of surveys for IT or IS specialty areas such as network support, desktop support, asset provisioning, development, etc. These areas usually support multiple parts of the organization, so it is easier to do one assessment for all areas. Sometimes these areas are unique, and will be easier to do these as interviews or as walk-through assessments.
- Managers differ on whether they require (or want) any evidence to support a risk assessment. Vulnerability reports, patch reports and scan reports are examples of evidence that supports risk assessment determinations. Access reports can also support determinations.

Tip – Request assistance from your manager, and ask for additional resources, if needed. This is not an easy task, and just tracking the activities may take a full-time person. Doing the work may take additional people. Leadership needs to be aware of the realistic effort required. Track the time to do the work in order to justify the additional FTEs.

Summarize findings in a risk register

Document reportable issues (as determined by the leaders) and maintain the status of these issues in a risk register. Unfortunately, process issues are more prevalent than technical issues. Administrative issues, such as poorly worded or missing policies or undocumented procedures are the most commonly identified. The HIPAA Security Rule requires mitigation. Management can accept, avoid or transfer risk. However, all risk decisions should be documented. Auditors will request evidence of the corrective action or management's decision regarding the risk.

Provide key findings

Create high level themes for executive leadership or for your own manager. Someone will be sure to request additional information, and it is best to plan ahead.

Conclusion

Doing an Enterprise Risk Assessment at a healthcare organization is not easy. Success will require project management, ongoing support from leadership, and communication with stakeholders. Value comes from identifying opportunities for automation and efficiency that leadership had not previously identified. **NP**

Without deviation progress is not possible.
~Frank Zappa