COSMOS
Navigate the Compliance Universe

Compliance Today - November 2019
Avoid recreating the wheel: Transparency in risk mitigation

By Gerry Blass and Jason Tahaney

Gerry Blass (gerry@complyassistant.com) is President and CEO at ComplyAssistant in Iselin, NJ. **Jason Tahaney** (jtahaney@hhsnj.org) is Director, Information Technology at Hunterdon Medical Center in Flemington, NJ.

- linkedin.com/in/gerry-blass-917a482/
- linkedin.com/in/jason-tahaney-91653618/

Did you know a typical healthcare system might perform up to 22 different types of security risk assessments each year? If the system uses a decentralized model, the assessment information is most likely gathered from a wide variety of areas—siloed, and not necessarily actionable. Although the organization is performing due diligence to adhere to the HIPAA Security Rule, is it doing its best to manage risk and resources? Probably not.

Whether or not healthcare organizations are prepared to perform a security risk assessment (SRA) each year, it is a required part of the HIPAA Security Rule[1] and should cover:

- Size, complexity, and capabilities of the covered entity;
- The covered entity's technical infrastructure, hardware, and software security capabilities;
- The probability and criticality of potential risks to electronic protected health information (ePHI); and
- The costs of security measures.

Unfortunately, healthcare organizations face immense challenges in performing security risk assessments and actually mitigating risks that are discovered, including:

- A high volume of risk areas, both inside and outside the four walls of a hospital;
- Increasing complexity of new, connected technologies;
- A siloed approach to risk assessments;
- A lack of transparency or understanding of risk across an enterprise; and
- Decentralized or unstructured risk ownership.

Because of these challenges, healthcare organizations may be spinning wheels and wasting time, energy, and money trying to make sense of the results of their annual security risk assessments. Imagine if one department discovered and mitigated a data security risk, but another department with the same or similar risk was not aware of the other department's efforts, and thus created its own risk management project. There is no need to recreate the wheel every time.

This article explores practices to make annual security risk assessments more transparent and actionable to reduce overall enterprise risk.

Manage risk across silos using a risk register

When performing SRAs, healthcare organizations typically end up with several disparate risk reports from different areas, including meaningful use, credit card processing, finance, security operations, third-party vendors, facilities management, cloud services, and both acute and nonacute care sites. Perhaps the SRAs are even performed by different teams, contributing to inconsistency in how the assessment data is gathered and reported.

With dozens of departments and corresponding assessments, you can imagine the difficulty of making truly informed decisions on how to prioritize and manage risk in ways that make the most sense for the enterprise as a whole.

With the assistance of a risk management committee, take the time to consolidate the results of each assessment into a single repository—a risk register. This risk register will be your single source of truth moving forward. Using it, you can:

- Visualize common risk across departments,
- Plan and prioritize risk mitigation, and
- Be more transparent with senior leadership.

Advantages of using a risk register

With a centralized repository of risk assessments for the enterprise, you can avoid duplication of information and reduce multiple audits that gather the same information. The risk register enables you to proactively gather data in future assessments that can be used in multiple ways.

The risk register as a single source of truth allows for easier, more transparent tracking of risk. Centralized ownership of the risk register and risk management also ensures that tasks are prioritized with the entire enterprise in mind, rather than focusing on single departments or business lines. This is especially important if and when a healthcare organization is audited by the HHS Office for Civil Rights. Rather than scrambling to pull together assessment information, evidence, and protocol documentation from disparate sources, everything is in one place, saving time and headaches.

A centralized risk register also helps healthcare organizations estimate a more comprehensive and accurate risk tolerance level. If security risk data is siloed, you may lack complete visibility into enterprise risk tolerance.

Finally, with a combined risk register, your information risk management committee or governance committee has access to a more complete picture of risk across the organization. The team can more easily prioritize around the most critical risk areas and go to senior leadership with the most pressing budget requests. Again, having a consolidated view helps reduce duplicative efforts as well as wasted time and money.

Challenges with using a risk register

Although centralized ownership is an advantage of using a risk register, there are some challenges. Consider how your organization is structured. Is it too large or fragmented to manage a single register? What about your corporate culture? Does it allow for centralized ownership across service lines? If not, it may be worthwhile to develop a federated model where a single register exists, but each department manages its own risk.

Up-front dedicated time and energy are required to consolidate your risk reports into a single register. You'll

need to plan resources accordingly. But, think of it like cleaning out your garage. Once you're done, as long as it's managed properly, you won't have to sift through scattered piles of clutter. Rather, you'll know just where to find the information you need and be able to easily access it.

Finally, be sure to involve all relevant parties in the creation of the risk register. Depending on the culture and structure of the organization, this may be a daunting task. However, your information risk management committee should enforce the governance model for the organization, and include representatives from human resources, finance, nursing, IT, compliance, privacy, legal, and ancillary practices or alternate site facilities. Ensure your committee has a senior sponsor—the chief information officer, chief medical officer, or compliance administrator.

Validate risk assessment data with field observation

Have you performed testing only to find out later—after you've put new controls in place—that your data was skewed? What about the same risk factor showing up time and again without change? Healthcare organizations can avoid rework by combining field observation with raw assessment data.

For example, email phishing attacks are one of the highest vulnerabilities in healthcare today, with goals of either gaining access to protected health information (PHI) or delivering ransomware.[2] Because of this, email security is very high on the list of healthcare IT, privacy, and security departments. Phishing exercises are common practice, testing employees' awareness and ability to recognize phishing attacks and avoid or report them. Of course, testing data is gathered on the back end—who passed, who failed, and how often. This data should then be collected in a risk register. However, does the data explain why employees pass or fail?

An organization's inclination may be to just continue, or even accelerate, testing to increase passing scores. But without personal observation, you may be wasting time and energy on that effort. Instead, field observation, one-on-one conversations, and a review of the training program will help provide context to the raw data. With that context, organizations can then create a more informed plan to improve behavior.

Consider another scenario regarding business associate agreements (BAAs) and employee access to PHI. Like phishing attacks, vulnerabilities from third-party vendors are extremely common, and contributed to 20% of healthcare data breaches in 2018, according to an industry study.[3] The study cited that more than 60% of privacy assessments found gaps in maintaining written policies and procedures to guide workforce members in managing use or disclosure of protected data.

Most BAAs include a provision to notify a hospital if an employee of the business associate is no longer employed, so the hospital can terminate access for that employee. On paper, the protocol is in place, and a security risk assessment would see this as a positive. However, what if the BAA fails to actually report, or if the hospital fails to follow through on terminating access? Without field observation and spot-checking behavior, the assessment data could fail to uncover a vulnerability.

Prepare the organization for change

Organizational change management is critical to an enterprise-wide security and risk management strategy. Change management is often an overlooked component of a foundational strategy. And healthcare organizations that do not devote sufficient effort here will likely waste significant time and resources on constant rework and re-education of staff. Organizational change management is an opportunity to not only educate staff on information security and cybersecurity, but also to instill long-term behaviors that will create a foundational culture of compliance across the enterprise.

If a healthcare organization's structure includes a formal change management committee, that group should include representation from security, IT, and compliance. Have a security representative embedded within the change management function who can assist with mitigation required from the risk register, but also look out for potential risks in other areas, such as security risk factors during mergers and acquisitions, electronic health record migrations, or the addition of new third-party vendors. Some healthcare facilities may choose to hand ownership of change management to human resources or IT. In any case, collaboration between departments is essential to make sure work is not duplicated or forgotten.

Along with preparation for change that you know will occur, it is important to understand potential risks associated with the decision not to implement a change. For example, if the organization has a documented disaster recovery plan, but chooses not to test or update it, is the organization aware of the risk?

Commit to a multiyear strategy

Again, healthcare organizations must perform security risk assessments to comply with the HIPAA Security Rule, but this does not mean you have to start from scratch every year. Using a consolidated risk register, healthcare organizations can build and modify from year to year, updating and reprioritizing based on new vulnerability findings.

Ideally, a minimum three-year strategic road map for significant changes and risk management projects will help organizations maintain steady, realistic progress. Within a three-year road map, you may split the structure into smaller, more manageable projects, such as a six-month initiative to update all operating systems throughout the enterprise. A multiyear strategy should work hand in hand with the risk register. The register becomes the backbone of the strategic direction for the enterprise and guides decision-making and budgeting.

Balance these types of long-term projects with risk mitigation tasks that are required routinely, such as phishing tests, workforce training, and cybersecurity simulations. The daily work of maintaining security is critical, and knowing the workload helps organizations plan realistically for efficient completion of long-term projects.

Takeaways

- Create a risk register to help organizations consolidate and manage risk items across the enterprise.
- Use the risk register to visualize the greatest areas of risk and avoid duplication of work.
- Balance raw assessment data with walkthroughs and observation to account for on-the-floor situations the data may skew.
- Prepare for organizational change management to maintain a culture of compliance that helps avoid future roadblocks.
- Develop a multiyear strategy and road map for risk management to streamline work across the enterprise.

1 "HIPAA security rule & risk analysis," American Medical Association, accessed September 16, 2019. https://bit.ly/2Ht04on.
2 "Protect Healthcare Data from Phishing: The Threat of Phishing Attacks on the Healthcare Industry," HIPAA Journal, https://bit.ly/2NCm18E.
3 Jessica Davis, "Third-Party Vendors Behind 20% of Healthcare Data Breaches in 2018," Health IT Security, April 15, 2019. https://bit.ly/2DoMBMn.