Compliance Today - September 2021
Rehab-focused compliance risk assessments: Identifying and mitigating your risks

By Holly J. Hester, PT, DPT, CHC, CHPC, and Yolanda G. Dockett, OTD, MJ, MOT, CHC, CHPC

Holly Hester (holly.hester@nethealth.com) is Senior Director, Strategic Client Partnerships, at Net Health in Grand Rapids, MI, and **Yolunda Dockett** (ydockett@aadermatology.com) is Chief Compliance Officer at Anne Arundel Dermatology in Linthicum Heights, MD.

- linkedin.com/in/holly-hester-50554a116/
- linkedin.com/in/yolunda-dockett-otd-mot-mjur-chc-chpc-0073a56/

The compliance risk assessment has been described as the “eighth element” of an effective corporate compliance program, emphasizing its importance above and beyond the established requirements for auditing, monitoring, and overall program assessment. An annual compliance risk assessment is essential to determine the scope of an organization’s compliance plan, to identify areas of increased risk, and to direct the overall compliance efforts of the organization.

In 2015, Deloitte defined compliance risk as “the threat posed to an organization’s financial, organizational, or reputational standing resulting from violations of laws, regulations, codes of conduct, or organizational standards of practice.”[1] Compliance risk management is the process that mitigates or reduces this risk to a level that is acceptable to company leadership or management. Risk can never be erased. It must be decreased to a level that is tolerable, and this tolerance level differs between organizations and even between specific elements of risk. For example, one organization may take a zero-tolerance approach to billing policy violations, while another company may encourage the reeducation of violators.

The compliance risk assessment helps the organization understand the full range of its risk exposure, including the likelihood that a risk event may occur, the reasons it may occur, and the potential severity of its impact. An effectively designed compliance risk assessment also helps organizations prioritize risks, map these risks to the applicable risk owners, and effectively allocate resources to risk mitigation.

Healthcare organizations should ensure each department is included in the risk assessment process. This includes rehabilitation services when it is a part of the organization’s business line. Incorporating the rehabilitation division into the risk assessment further demonstrates the presence of a comprehensive risk assessment process. Furthermore, much of an organization’s risk exposure exists within the rehabilitation services division. There is no one way to conduct a risk assessment unless a regulatory body mandates the approach, and for therapy practices and post-acute care, there is no standard or regulation.

Identifying risks

Start by reviewing previous internally identified problem areas:

- What do your internal auditing and monitoring findings tell you?
- Have you been audited or investigated by a payer or other regulatory or enforcement body?

- What are your medical review and appeal findings?
- What are your recent survey findings?
- What issues or concerns have been reported via your internal reporting process or compliance hotline?

Additionally, review data available in operational and clinical reports generated from the electronic health record (EHR) or other health information technology (IT) systems, such as utilization trends and revenue by payer, discipline, and location.

The risk identification process should also include external sources of information gathered outside of the organization:

- Applicable Office of Inspector General (OIG) Work Plan updates and audit reports;
- Corporate integrity agreements and settlement trends;
- Regulatory updates;
- Audit activity and trends from the Medicare administrative contractors and Medicare Advantage payers; and
- Current investigations and enforcement actions by the OIG, Department of Justice, and Office for Civil Rights.

Once organizational risks are identified, they should be categorized or classified into general risk areas. Some risk areas that apply to rehab services are:

- Compliance with the state practice acts for physical, occupational, and speech therapy;
- Documentation;
- Billing/coding;
- Insurance/payer regulations and medical review;
- Human resources (HR);
- Telehealth service delivery;
- Health Insurance Portability and Accountability Act (HIPAA);
- Contracts;
- Quality of care;
- Internal reporting; and
- Infection control.

Risk ranking

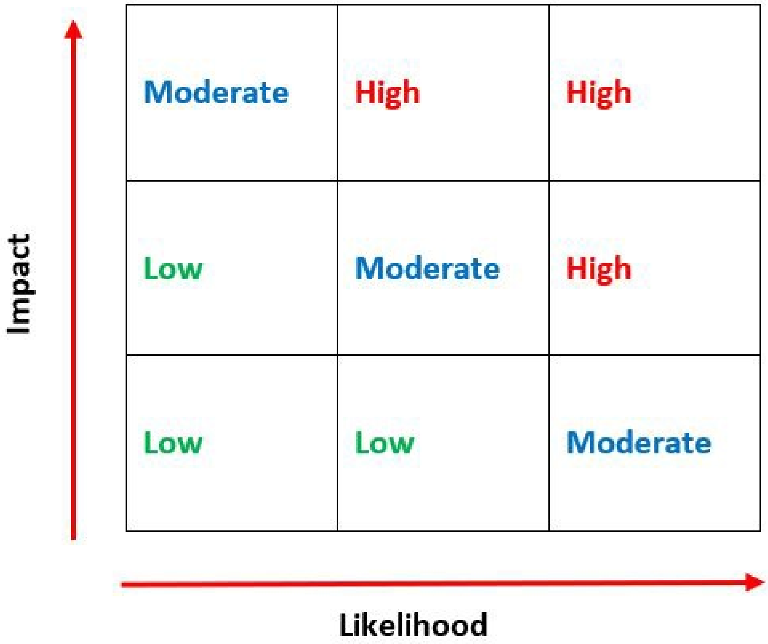
Next, categorize risks by risk type and impact, both of which will be important during the risk ranking and prioritization process: reputational, legal and compliance, and financial. Identifying the type and understanding its impact will help you obtain key stakeholder buy-in based on your organization’s risk tolerance. Sometimes risk impact can be described quantitatively based on dollars at risk. Other times, a risk's impact will be more qualitative.

Once categorized, each risk should be assessed for both the likelihood of a negative occurrence and the impact of a negative occurrence. There are different ways to assign likelihood and impact. One simple method is to use a 1–5 scale:

- Likelihood: 1 – Improbable, 2 – Remote, 3 – Occasional, 4 – Frequently, 5 – All the time
- Impact: 1 – Minimal/Negligible, 2 – Slight, 3 – Moderate, 4 – Critical/Serious, 5 – Catastrophic

Once each risk is scored on the 1–5 scale for likelihood and impact of a negative occurrence, use a grid or crosswalk with likelihood on the "x" axis and impact on the "y" axis to rank it as a low, moderate, or high-risk area.

Figure 1: Risk likelihood/impact grid



Impact

Moderate	High	High
Low	Moderate	High
Low	Low	Moderate

Likelihood

Likelihood

For example, an established therapy documentation and billing auditing and monitoring process may make the likelihood of a "negative occurrence" (i.e., incorrect billing, missing documentation, documentation that doesn't support medical necessity, or missing physician certification) relatively low—"3 – Occasional." However, if documentation and billing are not accurate, and claims come under medical review, the impact of that negative occurrence could be "4 – Critical/Serious." Crosswalk impact (4) to likelihood (3), and the risk is ranked as "high." The same ranking process is performed for each item on the risk assessment. Determining likelihood and impact may be somewhat of an art versus a clear, objective determination, but with input from key individuals in the organization (e.g., CEO, chief financial officer, legal counsel, HR), the information can be successfully used to prioritize risks and help focus the efforts of your compliance plan.

Assessing internal controls

The next step in the risk assessment process is to identify and assess the organization's internal controls. An internal control is something a company uses or implements that is intended to reduce the chance of an unwanted risk outcome. An internal control should be thought of more as a process rather than a thing. Jonathan Marks, a partner in a forensic compliance company who specializes in global and complex corporate and government investigations, defines an internal control as "a process of interlocking activities designed to support the policies and procedures," detailing the specific preventive, detective, corrective, directive, and corroborative actions required to achieve the desired process outcomes or the objective(s).[2]

To simplify, an internal control is a process that starts with established and effective policies and procedures that set up processes and systems designed to prevent, detect, and correct compliance risks in an organization.

Part of the internal control identification process is clarifying the type of internal control: preventive (controlling risk before the fact), detective (controlling risk after the fact), or directive (policy, education, and/or training process that informs what should be done). Internal controls may be a combination of types also. For example, a solid HR onboarding policy and process is both directive and preventive. It describes what should be done, and by following the processes and procedures, all of the requisite items are completed (e.g., the background check, List of Excluded Individuals/Entities database check, and I-9 form are completed, the code of conduct acknowledged, HIPAA training completed, and competency assessments are done).

Another example of a rehab-related internal control is an established documentation monitoring process. This type of control would most likely be both directive and detective. Documented policies and procedures about required documentation content and timelines along with staff education and training inform managers and staff about expectations for strong, technically and clinically solid documentation. Creating a monitoring tool or checklist that is completed monthly helps detect any issues or problems. There may be a preventive component to documentation and billing compliance if, for example, the EHR software is configured to facilitate or even require compliance with the organization's policies. EHR systems can often be configured to set required fields, schedule documentation forms (like therapist progress reports) according to payer or practice act regulations, or even to disallow continued documentation of daily notes and billing of treatment interventions if the initial plan of care is in draft and incomplete.

Each internal control should then be assessed as to its effectiveness. Is it adequate, strong, or inadequate? Consider whether the internal control has been working as intended and working consistently. Have things fallen through the cracks? Is the control outdated? Have regulations or requirements changed causing you to have to revisit the control and update a policy or retrain staff? Is your control a "hard stop" or a warning or alert that has been activated within the EHR?

Prioritizing risks

After both risks and internal controls have been identified, categorized, and ranked or assessed, each risk must be prioritized. Each organization or practice has its own risk tolerance (i.e., the level of risk that is considered acceptable). Work with leadership, the executive team, and the board to determine your organization's risk tolerance and to work through the prioritization process.

Focus on risk rank and your internal control assessment. Which risks are identified as high, and which internal controls are identified as inadequate? Understanding that even if an item is identified as high risk, if strong internal controls are in place, there may not be additional work to do. By the same token, an item identified as low risk may not have any internal controls, and therefore, would potentially move up the priority list. Consider the workload or effort required to mitigate a given risk. What do you have the time and resource to tackle? What makes the most sense to address first? The reality is most compliance professionals have limited resources—time, money, and people. Sometimes mitigating several smaller risks before tackling the one very heavy, laborintensive risk makes the most sense.

Developing a mitigation plan

Once risks are prioritized, the leadership/executive team, in conjunction with the compliance officer, should develop a plan to address each risk and to mitigate or minimize the risk to an acceptable level. It is impossible to eliminate all risk. Embrace that up front. This does not mean, however, that organizations and compliance professionals should settle for how things have always been and not push for things to change.

Residual risk is the degree of risk that remains after all controls and activities are in place. If existing risk mitigation strategies are insufficient at reducing residual risk to an acceptable level, additional measures are in order. Once the impact, likelihood, and vulnerability of the risks have been analyzed, the established controls will help you determine the most appropriate action items to include in your mitigation plan. For example:

- Should a policy and procedure be developed to address the risk? Or are revisions to current policies required?
- Is routine education and training appropriate? Should it be specific to a certain group (e.g., management)? Who is your target audience?
- Is monitoring more realistic? Will someone check the checker (e.g., audit vs. monitoring vs. education)?

Each action item should have a responsible party identified and a target completion or reassessment date set. For rehab-related risks, get rehab leadership involved in the mitigation process. The action items outlined in the mitigation plan should be specific and measurable. For example, specify a frequency for auditing, monitoring, and training. Clarify the training methods and resources to be used. Establish expected benchmarks or targets for performance, such as the percentage of medical records to review each month, the completion date for employee training, or the passing score on a competency assessment.

If rehab services are delivered by a contract rehab provider, determine whether the rehab provider has a compliance officer and an established risk assessment and mitigation plan. Partner with them to develop a collaborative plan for implementation and ongoing communication. Remember, while risks are shared, compliance remains your responsibility.

- Involve your rehab provider in your compliance committee meetings.
- Outline and review ongoing auditing and monitoring efforts.
- Understand their policies and procedures related to identified risk areas.
- Involve the provider in applicable organizational communication and training.

Review your mitigation plan routinely. Consider using quarterly compliance committee meetings as a platform to assess progress toward the targeted completion dates.

Final thoughts

Gather input from a cross-functional team. It is not up to you as the compliance professional to create and complete the entire risk assessment. And, for that matter, if you want the risk assessment to truly be comprehensive and effective, you must have input and buy-in from the team.

Build on what has already been done. There is no need to start from scratch if you don’t need to. Review past risk assessments or compliance plans as a jumping-off point for your new and improved risk assessment.

Takeaways

- Establish accountability and ownership of risk. Assign steps and items to others in the organization who have a stake in the outcome. Set expected timelines and keep people focused on the overall goal.
- Ensure the assessment is actionable and measurable and treat the assessment as a living document. Your priorities and elements will likely change throughout the year. Be prepared to be flexible and reprioritize as appropriate.
- Repeat the risk assessment at least annually. Reassess the items you identified as needing a mitigation plan. Did you complete the plan? Can the risk be reranked? Has the strength of your internal controls been improved?
- Learn from others outside of your organization. Check the Office of Inspector General Work Plan, review medical review trends, and track corporate integrity agreements and settlements applicable to your setting to gather intel into potential organizational risks.
- Use data to identify both your risk areas and your internal controls. In today's world of electronic health records, analytics platforms, and publicly available information from the Centers for Medicare & Medicaid Services, Office of Inspector General, Office for Civil Rights, and other federal and state agencies, we have access to lots of data. We need to use it to drive change.

[1] Deloitte, *Compliance risk assessments: The third ingredient in a world-class ethics and compliance program*, 2015, https://bit.ly/3jQ2JN9.
[2] Jonathan Marks, "Internal Control Defined and Some Guidance," *Board and Fraud* (blog), July 2018, https://bit.ly/3yrdEAO.