Keeping Third-Party Risk in Check

Why outsourcing business functions changes the control equation

By Warren Stippich and Kirt Seale

©iStockphoto.com/jvannice

Reliance on third parties has become a business reality in today's complex and highly competitive environment. As more healthcare organizations outsource significant and critical business functions, they are relinquishing increasing amounts of their control environment to others.

In today's data-centric business world, cloud providers, consultants, business process outsourcers, third-party transaction processors and others with whom you share sensitive or significant information are of particular concern.

Healthcare organizations that entrust outside entities with sensitive data, patient data or proprietary information need a framework for identifying, assessing and mitigating the risks involved. They will also need to ensure compliance with the multiple regulatory requirements for the healthcare sector, including HIPAA, electronic Protected Health Information (ePHI) and PCI.

Roles and responsibilities

A large portion of the responsibility for risk monitoring and control evaluation typically falls to internal audit because of its internal control mindset, risk management universe expertise, objective evaluation capabilities and ability to reach into multiple business areas across the organization.

Internal audit may drive the coordinated collection of information relating to third parties, but other functional areas—including finance, compliance, legal, procurement and operations—are critical to formulating a complete picture of third-party relationships.

Furthermore, third-party risk management should be a subset of the larger Enterprise Risk Management (ERM) program or similar initiative. The information gathered can also feed into other governance, risk and compliance efforts that include the formulation of the internal audit risk universe and annual internal audit plan.

Plan ahead

Typically, contractual protections are in place in case agreements with third parties go awry. When that does happen, it is usually too late for organizations to do much beyond trying to recoup or minimize losses. Instead, be more proactive in assessing and managing risks on the front end when relationships are established, and continue to monitor the interrelated control environment created between parties.

As organizations try to better understand the risks inherent in their dealings with outside parties, it is worth noting that exposure will vary with each relationship. The challenge is to establish a framework for risk assessment that is effective, yet flexible enough to recognize that not all risks are created equal. The expectations placed on third parties and the level of assurance needed by your organization can and should vary based on a number of factors.

Define the risk universe

No one-size-fits-all approach will work to manage third party risks, but a consistent pattern can be applied to the assessment process. As with many exercises, getting started is half the battle.

Third parties are generally defined as business partners that are not under direct business control of the organization

The challenge is to establish a framework for risk assessment that is effective, yet flexible enough to recognize that not all risks are created equal.

that engages them. These entities may include vendors, suppliers of products and services, joint venture or alliance partners, cloud providers, consultants, third-party transaction processors and business process outsourcers.

Rather than trying to do a risk assessment exercise that includes every third party in the accounts payable master file, consider excluding maintenance, repair and operations vendors, where the relationships do not usually rise to the risk level of entities that have access to sensitive data.

Some vendors should typically be subjected to a deeper third-party risk assessment:

1. Information technology hosting/co-location data center providers
2. Cloud or software-as-a-service providers
3. Outsourced financial or operational service providers such as payroll and remittance processors
4. Claims processors
5. Others that support operational activities with access to your organizations' or patients' data:
    - Courier services (e.g., medical files, cash co-pays)
    - Printing and mailing services
    - Marketing service providers
    - Telecom providers
    - Help desk or user support providers

Find third parties outside A/P

Most vendor relationships will likely surface during a thorough search of accounts payable records. An additional source of information may be your in-house legal department.

Gather any vendor information the legal department has, and develop an understanding of how contractual relationships are drawn up and approved. This information can then be crosschecked with the other data you have compiled to ensure you have identified all pertinent vendors.

Your contractual agreements should contain details useful for the risk assessment, such as a right-to-audit provision or a requirement that compliance with internal control or regulatory requirements be confirmed by an independent third party.

For organizations that take an ad-hoc approach, internal audit may also need to seek vendor information on a department-by-department basis. The goal at this stage is to identify all pertinent vendor information wherever it resides to get a complete picture of existing relationships.

At what point is a risk threshold met?

Although internal audit will perform its own evaluation of risks, it is worth noting that larger vendors or those with access to potentially sensitive patient information may have already been carefully vetted. That is not to say these entities should be ignored or written off as safe, but it acknowledges that larger vendors may have already received more scrutiny. In any case, there is still plenty of opportunity for uncontrolled risks in larger vendors and monitoring those arrangements is critical.

Define the risk threshold

A frequent early question in a risk assessment is: At what point is a risk threshold met? When your organization enters into an agreement with a third party and begins to share patient information or proprietary information, it is time to consider the risk threshold as met. Those performing the assessment may get pushback from others who believe there should be a dollar threshold that triggers risk. Think twice about this argument.

Even vendors with whom you do only a relatively small amount of business could still cost your organization millions in exposures if there is a security breach (i.e., fines, civil penalties, reputational damage, penalties for breach of ePHI, HIPAA penalties and brand erosion). It does not mean you should not use the annual service spend as a measure of the risk associated with a particular vendor. Rather, there are

Exhibit 1 – Vendor relationship organization example

Vendor name	Vendor type	Service being provided	Contractual details	Geographical considerations	Applicable regulatory req.	Primary relationship owner	Provides an audit report	Right-to-audit clause
ABC Payroll	Payroll provider	Payroll processor	Five-year agreement, approved by Legal	Payroll processed in Kansas City, Kan.	IRS, Dept. of Labor	Bob Peoples, Human Resources	Yes, SOC 1	No
IT Help	Help Desk support	IT support contractors	One-year auto-renewing contract	Local to each company site and HQ	n/a	Martin Technology, CIO	No	No
Quick Print	Printing/ mail service provider	Prints/ mails invoices/ marketing materials	Six-year agreement, approved by Legal	Local to HQ	n/a	Sally Accountant, CFO	No	No

many other factors to consider in evaluating third-party risks and they all should be considered.

Through discussions with various relationship owners within your organization, such as IT, finance, compliance, legal, procurement and operations, you can identify additional risk considerations. You can use these when you perform an initial risk ranking of the relationship. Relationship owners can help identify vendors that may present a high risk due to subjective factors such as the criticality of the relationship or the level of visibility the vendor allows into its activities.

Exhibits 1 and 2 offer examples of factors you might want to weigh and track in assessing risk. Also consider what additional factors you need to add that are unique to your organization.

Identifying and assigning a weighting to the selected risk factors/attributes for all vendor relationships gives you a good assessment of the vendors the organization is using. See Exhibit 2 as an example. This written assessment provides a basis for determining next steps because it highlights vendors that present the highest risk to your organization. These are the vendors for whom you need to plan appropriate risk mitigation techniques.

Address high-risk relationships

Although not a common occurrence, when the risk assessment identifies high-risk vendor relationships, internal auditors should consult with the relationship owner and Legal for the best way to reduce risks. It is always best to undertake a robust due-diligence process before accepting new third party business relationships.

Options may include:

- Data collection, management and monitoring, reporting and analytics
- Renegotiating contracts
- Performing site visits or audits to gain needed assurance
- Additional provider oversight or closer monitoring of vendor's performance against agreed-upon service levels

Exhibit 2 – Vendor assessment example

Vendor	Significance of data handled	Potential magnitude of loss			Frequency of interaction / degree of oversight	Cost vs. business unit income	Significance of risk		
		Financial	Reputa-tional	Opera-tional			Financial	Opera-tional	Strategic
ABC Payroll	3	1	1	5	5	4	3	5	2
IT Help	3	1	1	3	5	2	1	4	1
Quick Print	2	1	4	2	4	1	1	1	1

Three types of SOC reports[1]:

SOC 1 reports look at a service organization's system of internal control that is relevant to a user organization's control over financial reporting. SOC 1 reports are intended to be auditor-to-auditor communications, with specific content dependent on the service organization's system.

SOC 2 reports address controls at a service organization pertinent to the AICPA's Trust Services Principles of security, availability, processing integrity, confidentiality and privacy.[2] The SOC 2 report includes many of the same elements as a SOC 1 report—specifically, the independent service auditor's report, management's assertion letter, a description of the system, and a section containing the service auditor's tests of the operating effectiveness of controls and the related test results.

SOC 3 reports allow service organizations to provide user organizations and other stakeholders with a report on controls relevant to the Trust Services Principles. Unlike SOC 1 and SOC 2 reports, SOC 3 is a short-form report that can be distributed or posted on service organizations' websites as a seal.

[1] For more information on SOC, see Grant Thornton's white paper "Puzzled about Service Organization Control reports?" at www.grantthornton.com.

[2] The principles and criteria were developed by the AICPA and the Canadian Institute of Chartered Accountants. See www.aicpa.org/InterestAreas/InformationTechnology/Resources/TrustServices/Pages/Trust%20Services%20Principles%E2%80%94An%20Overview.aspx.

Your organization should be in control and comfortable with its third-party relationships. In some cases, your organization may need to consider changing to another service provider.

A closer look

An independent third-party assessment of the vendor's processes, technology, and controls used in the delivery of services is another common risk mitigation technique. A Service Organization Control (SOC 1)[1] report is commonly used to help vendors demonstrate the strength of their internal controls to current and prospective customers. For this report to be useful, it is important to know what to look for and to ensure it addresses the right controls for your organization.

Not foolproof

Having access to a SOC report can be extremely helpful when evaluating potential vendors and monitoring third-party risk on an ongoing basis. Generally, organizations that undertake an annual SOC audit to satisfy customer requirements have more sophisticated internal control structures than others.

However, the mere existence of a SOC report may not allay all of your organization's specific concerns. It is important to determine what your organization needs to have assurance on and to understand what the SOC report contains. SOC reports may provide a good baseline of control information, but they may also be too generic or superficial for your needs.

As you assess the benefits of a SOC report provided to you, consider what the report states, or does not state, relating to the following topics:

1. Handling of subservice providers through a "carve-out" vs. "inclusive" method

2. Period covered, if one is listed, and whether that aligns with your needs

3. Locations covered and those not covered within the report

4. Construction of control objectives and control activities (has something critical to your organization been left out?)

5. Bias in sampling

6. The testing approach (e.g., inquiry, observation, inspection) employed by the auditor

7. Exceptions noted by the service auditor and responses by management

Asking for a right-to-audit clause is an effective way to preserve your ability to seek additional information regarding the services provided by third-party vendors. Without having a right to audit or a SOC report to rely on, your organization may be exposed to an unacceptable level of risk.

Keep in mind that you will probably need to request the right to audit—vendors do not offer it without being asked. This underscores the importance of an ongoing program to identify and manage third-party risk.

[1] 1 Service Organization Control, SOC 1, SOC 2 and SOC 3 are proprietary service marks of the AICPA.

Conclusion

Executive management in healthcare organizations faces ongoing scrutiny and pressure from their board, external auditors and regulators to ensure robust ERM practices. Third-party relationships are a key area of concern in an era of widespread outsourcing and reliance on third parties for non-core operational services.

Healthcare organizations in particular need to have a consistent and comprehensive process for evaluating and mitigating the risks inherent in these relationships, preferably as part of the ongoing internal audit risk universe and ERM initiatives. **NP**

Warren Stippich is the National Governance, Risk and Compliance Solution Leader and the Market Leader in Grant Thornton's Chicago Business Advisory Services Group. He has over 22 years of experience working with multi-national, entrepreneurial, and high-growth public companies. Warren brings experience to the business risk consulting and internal audit services areas. You can reach him at (312) 602-8499 or Warren.Stippich@us.gt.com.

Kirt Seale specializes in IT attestation and IT security projects in Grant Thornton's Dallas office. He is responsible for delivery of IT attestation services, which include engagements focused on financial statement audits, SOC 1, SOC 2, and SOC 3 projects and IT Internal Audit services. You can reach him at (214) 561-2367 or Kirt.Seale@us.gt.com.

"I can't see your future, but I found your bank files, Social Security number and all of your company passwords."