Healthcare: **What Is a Vendor Risk Assessment?**

venminder
FOR HEALTHCARE

Healthcare: What Is a Vendor Risk Assessment?

What does it mean for a healthcare organization to perform a risk assessment on a vendor? Is it a questionnaire, review, or process?

INHERENT RISK ASSESMENT

A risk assessment begins by identifying the types and amounts of risks associated with a product or service. This first risk assessment is also referred to as an inherent risk assesment.

It includes assigning ratings that measure the identified risks' likelihood, occurrence, and severity (risk rating) and determining the level of impact your organization (or its patients) would experience if the vendor were to fail. Those impacts determine the criticality of the product or service and, therefore, the vendor.

RISK ASSESSMENT BASED ON A FRAMEWORK

Depending on the product or service type and the risk level, the next step in the process may be to require the vendor to complete a risk assessment based on a framework – like NIST 800-53 rev 5 or the CIS Controls.

For others, a risk assessment may be a review of a vendor's information security policies and related documents such as SOC reports, security certifications, business continuity/disaster recovery plans, penetration test results, vulnerability scans, and phishing tests. This part of the process is called due diligence.

These two methods are typically used in tandem to assess the risk a vendor may introduce to one's environment.

It's essential to first identify the types and amounts of risk associated in the product or service and if the vendor will be critical to your organization. This information should guide the decisions regarding the level of due diligence, contract requirements, and how you manage the vendor's risk and performance throughout the life of the engagement.

What to Include in a Risk Assessment

Does a risk assessment include compliance, cybersecurity, or many risk types?

Some think a risk assessment is compliance risk-based, while others think it's a cybersecurity function. In contrast, others consider financial, reputation, and other risks as a component.

So, what's the correct answer? All of these risks should be covered in a risk assessment.

COMPLIANCE

The assessment determines if a vendor meets regulatory and legal requirements.

CYBERSECURITY

In a cybersecurity function, a risk assessment determines a vendor's risk posture by using a control framework like NIST 800-53 rev 5 or the HITRST CSF.

PRIVACY

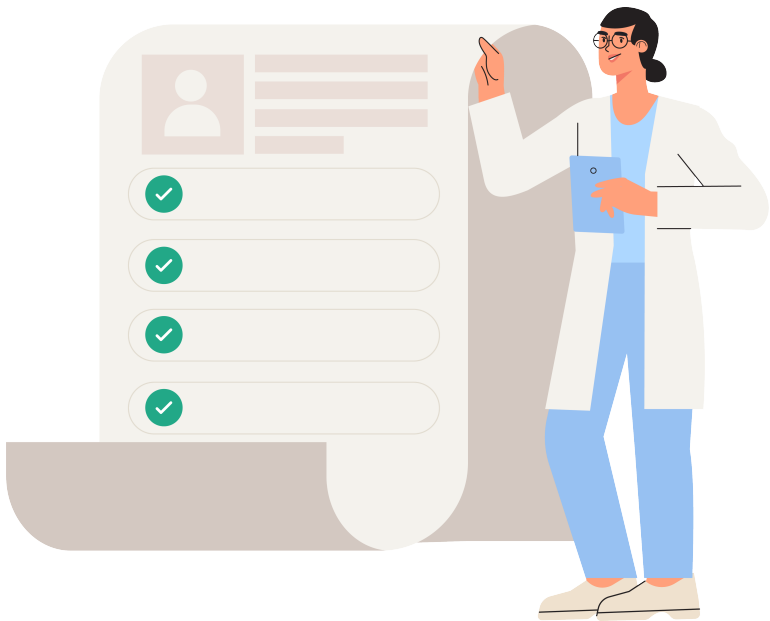
Assess how the vendor accesses, shares, or uses patient data to ensure HIPAA rules are observed.

OTHER RISKS

An assessment covers regulatory, financial, and reputation risks.

Furthermore, an organization should base its risk assessments on a cybersecurity framework, not just compliance. A cybersecurity framework will cover anything related to compliance since compliance is a subset of cybersecurity.

Healthcare organizations should also consider the financial risk of a vendor, including any potential mergers & acquisitions (M&As) that may be in process. Acquiring a vendor's products or services means entering a partnership with that company and becoming dependent on that vendor as a supplier. Confirming a vendor's financial health will ensure they can continue offering products and services throughout the contract period.



Scope of the Assessment

Does the scope of a risk assessment include a company, service, or device?

Another area in which many people have differing views of what a risk assessment is involves the scope of an assessment.

COMPANY

For some organizations, a risk assessment means that a vendor's risk posture as a company must be assessed.

For this type of risk assessment, an organization's regulatory, privacy, cybersecurity, financial, legal, and reputation practices can be reviewed or measured against a specific framework.

This should include assessing a vendor's third parties (your fourth parties), such as their cloud service provider (CSP), data centers, and offshore locations.

SERVICE

Some organizations will conduct a risk assessment of the service provided and consider how a vendor's employees will access PHI and other sensitive information while performing that service.

Services can include medical coding, lab testing, billing services, consultants, and managed service providers (MSPs). Sometimes, an organization provides the environment where a third party performs the services.

That environment could include healthcare institution-issued laptops or virtual desktop infrastructure (VDI). Or, the entire service could be performed in the vendor's environment, meaning that PHI will be accessed, transmitted, and stored in the vendor-hosted network.

In that case, the risk assessment will need to cover both the service and the vendor's security practices as a company.

DEVICE

Risk assessments may be specific to devices for some organizations. Those devices may be medical or include devices within the Internet of Things (IoT) and operational technology (OT).

Whether a device is connected to the internet or not can determine just how thorough the risk assessment needs to be. Like a service, if a medical device transmits PHI over the internet to the vendor's environment, the risk assessment should also assess the vendor's security practices as a company.

Moreover, if the device comes with a software application or mobile app that healthcare personnel access via the internet, that software should be considered a separate product or service provided by the vendor.

Understanding Inherent Risk vs Residual Risk

The term risk assessment certainly means different things to different audiences. Still, those risk assessments share a common outcome. After a risk assessment, you should be able to determine the residual risk or the risk left after all controls are considered.

Keep in mind that inherent risk is the risk naturally related to a product or service and the vendor. After those risks are identified, the process of due diligence makes it possible to discover and evaluate the vendor controls, or actions, in place to mitigate those risks. Controls help mitigate the risk by reducing the risk's likelihood, occurrence, severity, or impact. Controls are designed to either detect or prevent unwanted events. Once those vendor controls are verified, you can determine how effectively they mitigate the risks and determine the remaining risk level. The remaining risk is known as residual risk.

Once the remaining or residual risk is identified, you must decide how your organization will handle the risk.

Risk Handling Techniques - Avoid, Mitigate, Transfer, or Accept the Vendor Risk

Healthcare organizations should pay special attention to residual risk and how they handle each situation.

There are multiple risk handling techniques:

ACCEPT THE RISK	The residual risk may have been reduced to an acceptable level during mitigation, allowing a healthcare organization to accept the risk and proceed with the purchase of the product or service.
MITIGATE THE RISK	It may be necessary to go back and implement new or different controls to bring the residual risk to an acceptable level.
TRANSFER THE RISK	A healthcare organization may transfer some of that risk to a third party through contractual indemnification clauses and insurance policies. Remember, your organization is still always accountable for the risks, but you can transfer some of the financial liability.
AVOID THE RISK	If a vendor's residual risk exceeds your healthcare organization's risk tolerance, it may be wise not to purchase from that vendor.

Knowing how the term "risk assessment" can be interpreted can help healthcare organizations better understand how to assess their vendors to protect themselves and their patients.

Also, it facilitates a more relevant conversation with vendors when they're asked to provide specific documentation or additional insights into their security practices. Articulating what "risks" are being assessed ensures everyone is on the same page and speaking the same language.

Download free sample assessments of vendor controls and see how Venminder can help reduce your third-party risk management workload.

Download Now

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise, and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting, and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals, and more, are readily available in an online exchange library. The assessments enable customers to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance, and more.

venminder FOR HEALTHCARE

Manage Vendors. Mitigate Risk. **Reduce Workload.**

+1 (888) 836-6463 | venminder.com