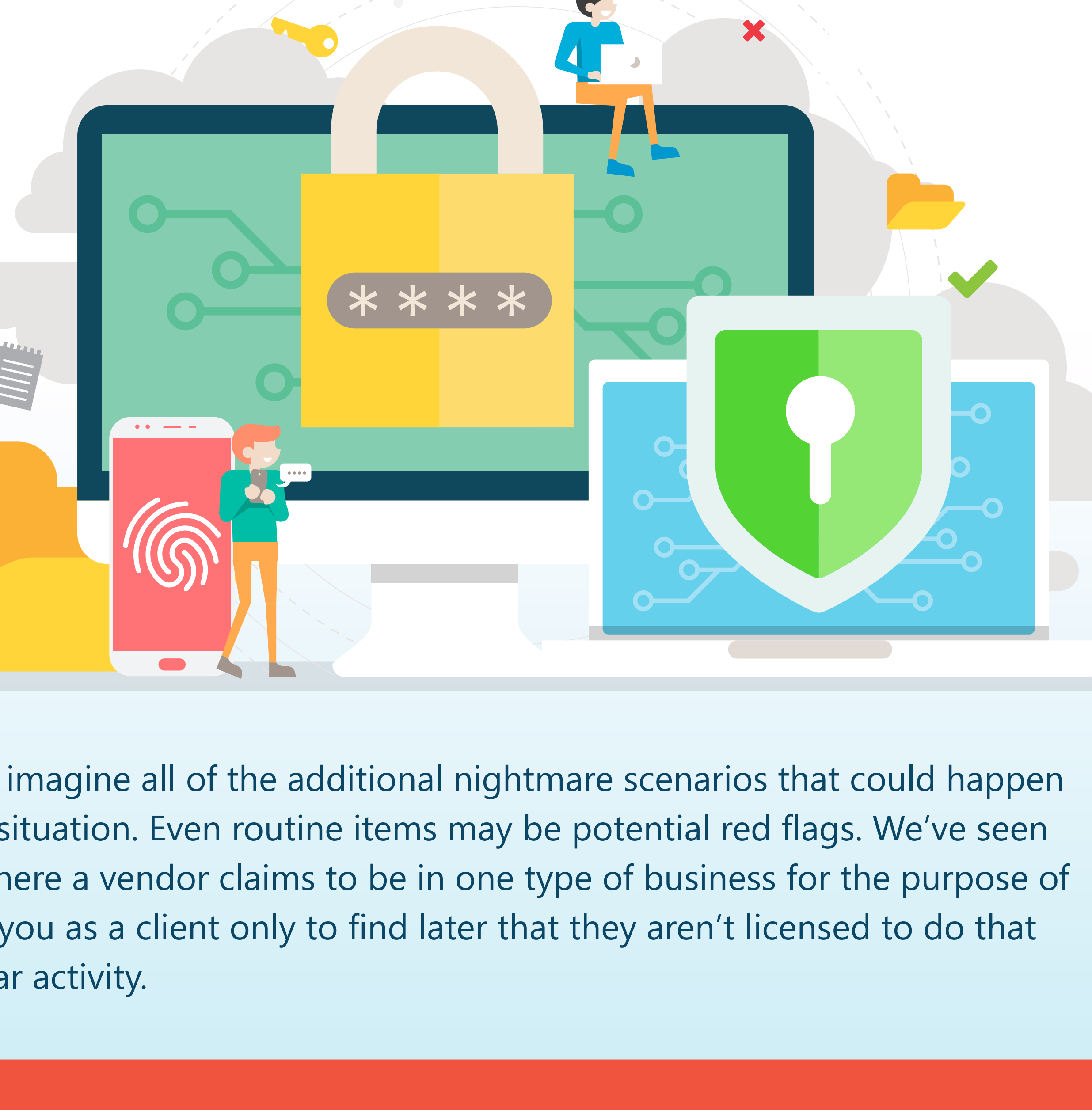
Why Vendor Due Diligence Reviews Are Not a "Check-the-Box" Activity

Due diligence is one of the most important activities in third-party risk management and what you learn can make or break a relationship. Appropriate due diligence must be tailored to match the product or service being outsourced and should be adjusted commensurate with the risk represented by the vendor relationships.

There's a natural inclination to cut corners in due diligence but doing so invites real peril – there's nothing more dangerous than finally receiving a requested piece of information, just checking it off the list and later, when there's a problem, you discover that you had an early warning sign that you simply overlooked.

Let's look at the **importance** and **what can happen** if you just "check-the-box" indicating that the vendor has the report instead of thoroughly reviewing the document:

Document	What could go wrong if you don't perform a review?
Vendor Financial Reports Understanding your vendor's financial posture and performance is an absolute must. To do this, it's important to review the annual 10-K report or statement of financial condition.	**If a company isn't performing well, it's often found that they find ways to cut cost.** One of the most common ways to cut cost is to reduce staff. Once staff is reduced, that usually means a decline in the service levels you once had and potentially affecting not only just you, but any of your customers who interact with the now underperforming third party. See the domino effect here?
Vendor SOC Reports SOC audit reports help you better understand the controls your vendor has in place and how they're performing against those controls. Not only is it a best practice, but industry guidance, such as the FFIEC IT Examination Handbook, requires the ongoing oversight.	**Simply put, you may find that there's an operational disconnect between what you want the vendor to do versus what they're actually doing.** SOC reports are an integral part of understanding what controls are in place at an organization and can help identify whether those controls offer enough assurance that breaches, unauthorized or inappropriate access and data loss are being prevented and data integrity is upheld.
Vendor Business Continuity and Disaster Recovery Plans Business continuity plans (BCP) help your organization ensure that the key products, operations and services continue to be delivered in an acceptable manner with a level of availability that's outlined in the service level agreement. Disaster recovery (DR) plans ensure that the vendor has a plan in place, should the business operations be impacted, so that resumption of normal business operations can continue as quickly as possible.	**It could be possible that while your vendor may have a BC and DR plan in place, they've never tested it, or at least not to the extent that they should.** Imagine if your core provider experienced a natural disaster like a flood or a hurricane. Do they have a plan to move their staff, computers and telecommunication connections to another ready-to-use location? And if so, do they know how quickly they can be up and running? If you answered no or not sure, it's quite possible a disaster could cause a negative ripple effect on your own operations and customer base.
Vendor Cybersecurity Policies and Procedures It's imperative that you thoroughly understand the vendor's access levels to your sensitive information, how they store it, what their incident response plan looks like and how quickly they'll notify you should a breach occur.	**You put your organization at great risk for a data breach.** If there's not a clause in the vendor's plan regarding their notification policy, then should a breach occur, they may not notify you in a timely manner. One of the worst things that can happen to an organization's reputation is finding out a breach impacted your organization after its been made public. This could lead to you not having enough time to implement your remediation plan and prepare your response prior to the questions coming in as well as loss of trust from your consumers.



You can imagine all of the additional nightmare scenarios that could happen in each situation. Even routine items may be potential red flags. We've seen cases where a vendor claims to be in one type of business for the purpose of getting you as a client only to find later that they aren't licensed to do that particular activity.

Examiners will look for documented evidence that **all steps** have been taken to adequately understand and mitigate the risk associated with outsourcing a product or service. Failing to do your proper due diligence can be a recipe for disaster.

Generally speaking, the more complex the relationship or the higher the risk, the more information you're going to need to collect and review. Remember, never take the easy way out – the practice of due diligence is the foundation of a solid risk management program and should *not* be a "check-the-box" routine.

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

Download Now

PRINTABLE VERSION

venminder

400 Ring Road, Suite 131, Elizabethtown, KY 42701 | (270) 506-5140

www.venminder.com