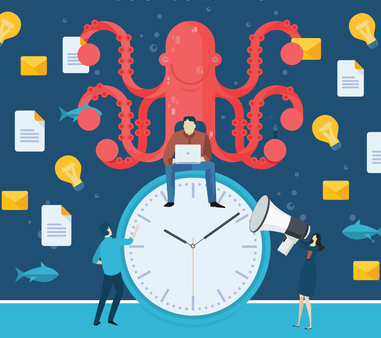
14 THIRD-PARTY RISK MYTHS YOU SHOULD DITCH



In an era where you can instantly communicate with someone on the other side of the planet and find information on virtually anything, **there's a real danger of believing wrong information**.

We see this often in third-party risk management – let's explore some common misconceptions.

	MYTH	REALITY
1	**Providing reports to the board and senior management team is all that really needs to be done.**	The board and senior management should be actively involved. It's a regulatory guidance requirement.
2	**A vendor who doesn't have access to confidential information doesn't need to be included in our inventory.**	Cybersecurity firm Darktrace made quite a splash when it announced it discovered a casino's vendor, who managed and installed fish tanks for them, installed a "fish feeding timer" hacking software to steal data.
3	**No concerns were raised in our last examination, so third-party risk management doesn't need to be a priority.**	Third-party risk management isn't just about exam time, it's a constant responsibility.
4	**The big-name vendors must be doing things well, so we can focus our time on the lower-level vendors.**	Even the largest processors have problems from time to time and all need to be actively managed.
5	**We just don't have the budget for third-party risk management, so we should stop requesting more.**	Don't stop pushing for additional resources!

6	**The most important time to perform due diligence on a vendor is during the vendor selection phase.**	Post-contract ongoing monitoring and periodically updating due diligence records are just as important to help reduce any exposure to risk.
7	**My vendor is low risk, so I don't have to do any due diligence or can cut corners.**	Due diligence should be aligned to the level of risk. You need to confirm that the vendor is a legitimate business (secretary of state website) and do a quick internet search to ensure they have a solid reputation.
8	**It's not important to actively monitor fourth-party vendors.**	If the fourth-party vendor is providing a critical product or service to your third-party vendor or has access to your confidential information, then you should analyze further.
9	**Our organization's primary regulator isn't the FDIC or OCC (or our regulators don't require third-party risk management at all), so we don't need to worry what these regulators recommend.**	Regulators are looking to one another for third-party risk management best practices, so they all do matter.
10	**Third parties only need risk assessed at the vendor level.**	There are differing levels of risk associated with different products and services. You should assess risk at the individual product/service level, especially if a vendor provides more than one.

11	**General Data Protection Regulation (GDPR) is a European regulation so a US-based organization doesn't need to worry about it.**	If your organization processes ***any*** European data, then you should be considering GDPR implications. You also need to be prepared for the California Consumer Privacy Act (CCPA) which went into effect on January 1, 2020.
12	**It's unnecessary to consider other providers because our organization has been using Vendor XYZ for years.**	Periodically look into options. There may be a competitive vendor who better aligns with your organization's strategies and needs.
13	**Right now, new consumer privacy law and regulation isn't in the works in my state, so I don't need to worry about it.**	Virginia passed the CDPA on March 2, 2021 and other states have pending legislation. Until there is federal legislation, it's likely more will follow. It's always easier to be proactive than reactive.
14	**As long as I have good due diligence on my critical vendors, auditors and regulators will be satisfied.**	Auditors and regulators examine every aspect of your program and the third-party risk management lifecycle. Ensuring risk ratings are accurate and consistent, performance monitoring, risk assessments and issue management and escalation are frequent areas of examination.

... and that's just a start!
Third-party risk management should always be a priority with an understanding of what is true and what is an industry myth.

Download free samples of control assessments and see how Venminder can help reduce your third-party risk management workload.

DOWNLOAD NOW

PRINTABLE VERSION

venminder

Manage Vendors. Mitigate Risk. Reduce Workload.

(888) 836-6463 | venminder.com