14 THIRD PARTY RISK MYTHS YOU SHOULD LEAVE BEHIND IN 2019

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	**The Consumer Financial Protection Bureau (CFPB) has gotten complacent so we don't need to work as hard at third party risk management.**	The CFPB may have re-prioritized some things but they, along with the other regulators, are still focusing on third party risk management.
2	**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.
3	**A vendor who doesn't have access to confidential information doesn't need to be included in our inventory.**	Remember, the massive Target breach was facilitated by a hacker compromising an HVAC vendor's credentials.
4	**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.
5	**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.

6	**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!
7	**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.
8	**Since "abusive" in UDAAP (Unfair, Deceptive or Abusive Acts or Practices) isn't defined, it's fine to ease up on the monitoring.**	Just because abusive isn't defined doesn't mean examiners won't expect you to have procedures around this. Check out enforcement actions at similar organizations to help you out.
9	**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, then you should analyze further.
10	**It's okay to cut corners on due diligence if the vendor is low risk.**	Cutting corners at any time can lead to unfortunate consequences.

11	**Our organization's prudential regulator is the FDIC or other body, so we don't need to worry about what the OCC recommends.**	Regulators are looking to one another for third party risk management best practices.
12	**Third parties only need risk assessed at the vendor level.**	There are differing levels of risk associated with different products and services so you should assess risk at the product/service level.
13	**General Data Protection Regulation (GDPR) is a European regulation so a US-based organization doesn't need to worry about it.**	Not necessarily. If your organization processes any European data, then you should be considering GDPR implications.
14	**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.

... 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.

PRINTABLE VERSION

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

venminder