GUARDING AGAINST UNDUE RISK FROM VENDORS

3 LINES OF DEFENSE STRATEGY

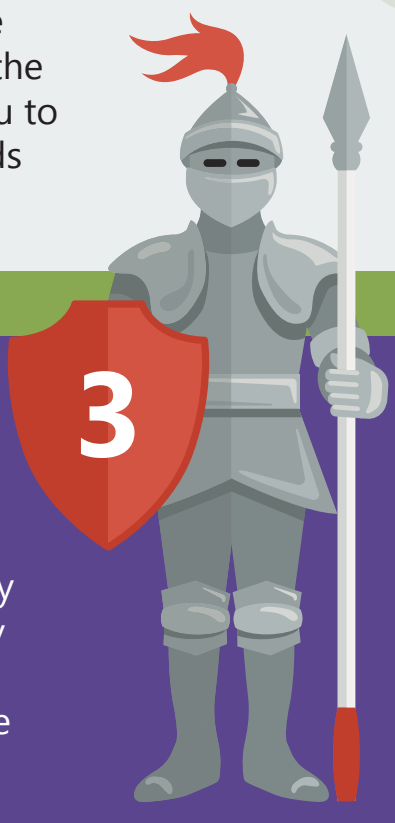
You may have heard the term **"three lines of defense"** – it has certainly been used a lot a lot since the OCC and the Committee of Sponsoring Organizations (COSO) standards made reference to the phrase in the form of guidance.

This regulation states that there are three lines of defense in an organization to guard against undue risk. We'll cover **what you need to know** to understand the strategy.

What Are Each of the Three Lines of Defense?

1st Line: The front line consists of the business owners or relationship managers who deal with the vendor daily. These are the people who are **managing the business** day to day – they need to understand what requirements they have to help comply with your vendor management practices.

2nd Line: It's the independent risk management function, such as the compliance area or the third party risk management area. For most people reading this informational piece, **this is your area of responsibility** – you need to check on the front line and be very involved but know that the third line has your back. It's up to you to develop and implement the standards and to manage the program.



3rd: It's the **independent audit function,** whether it's an internal or external audit function, but totally independent of the first two lines. They're here to make sure everything goes well and to review and advise on changes that should be made – the last backstop before things may be caught by an examiner or potentially impact the customer. But it's truly the second line that needs to do the heavy lifting in third party risk management, you should never rely on the failsafe to need to catch anything.

HOW Are They Guarding Against Undue Risk?

1. **The front line** – the business area – is said to **"own the risk"** and is responsible for managing it.
2. **The second line** is responsible for the organization's enterprise-wide risk management program along with creating a tone **from the executive level**. They must drive a comprehensive risk appetite statement and build and maintain a structure for monitoring, enforcing and reporting in support of the risk limits.
3. **The organization's third line** – the audit function – then makes sure that all of the requirements of the third party risk management program are in place and functioning, in other words, making **absolutely certain** that the appropriate steps get done in an appropriate, controlled and fully functional manner and that the controls operate as designed.

What If All Your Lines of Defense Fail?

If all of these lines of defense fail, any number of **things can go wrong** – and examination findings may actually be the least of your concerns – the more likely things are items that will cause pain long before an audit…things like:

- Lack of **effective control** over your third parties.
- New vendors being signed by the lines of business **without your involvement**.
- Failing to account for an **important risk consideration** and then the worst case scenario happening (think – data breach or a critical third party failing to do its job and you had the information that may have tipped you off right there in your possession).

4 Tips for Implementing This at Your Organization

1. Work closely with your front-line managers and **educate them well** on what they need to be responsible for when it comes to third party risk management.
2. Answer team's questions and **listen to their concerns.**
3. As the second line of defense, it's incumbent on you to make sure your program is **well-written and functioning properly.** Make sure your work matches your expectations and the regulatory guidance.
4. Rely heavily and be **fully responsive to suggestions** from your auditors and your risk management team.

Trust us, if it all falls apart, it's an ugly situation leaving your organization and customers at risk.

Download free due diligence samples and see how Venminder can help reduce your workload.

DOWNLOAD **NOW**

venminder

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

DOWNLOAD A PRINTABLE PDF