Inherent vs. Residual Vendor Risk

Determining the inherent risk and the residual risk of a third party is a key element of doing a robust risk assessment properly.

What is Inherent Risk?

Think of inherent risk as the level of risk you notice when you first walk in the door, virtually or actually.

It's about your first impression – your first glance at your vendor's financial statement, your first walk through of the call center, your first review of their compliance activities – these are, admittedly, based on limited knowledge but they should give you a good leading indicator of where the biggest risks are.

Let's say you first get a copy of their financials and they're losing money and have been losing money for quite a while – you'd likely deem that a high inherent risk. Similarly, you walk in their call center or see their call handling reports and it's evident that service levels are abysmal – you're thinking this is a high operational risk.

So, let's pause there for a second – first impressions may be lasting impressions, but they absolutely shouldn't be your last impression overall. You need to figure out what you're going to do about that risk. Perhaps there's nothing you can do – but that's rarely the case.

In the case of the financials, dig in a bit and get some ideas around what they're doing about it and perhaps set yourself to review them more frequently – discuss with management, get some additional clarity. These sort of things, along with reporting and additional information or call center monitoring, as easy examples, are **mitigating controls**. In other words, what steps you're doing to address or reduce the risks.

What is Residual Risk?

Residual vendor risk is never higher than inherent risk – if you think it is, then you likely misidentified the inherent risk. The risk when you wander on to the next vendor should never be higher than when you first got there – after mitigating controls, the remaining risk should always be equal to or perhaps less than the inherent risk level – otherwise, it's important for you to go back and determine if you misidentified the inherent risk or whether the mitigating controls are effective.

Make sure the mitigating controls are well-documented.
When mitigating controls, remember the following:

1. Include the scope, frequency and why.
2. You may want to bake those into your contractual agreement with the vendor.
3. Request the vendor deliver the controls and provide evidence.

By the time you're done with your mitigating controls, it's time to move on to other parts of the risk assessment.
Think of it as virtually leaving their building – your assessment of the remaining level of risk and the effectiveness of your controls should leave you with a residual risk.

Remember – inherent is what you first encounter; residual is where you determine you're comfortable that you've got the right controls in place. Then it's up to you to figure out how those controls work and with what frequency.

What's Next? Be certain to document it all carefully and include it in regular updates to board and senior management. After all, it's all about identifying and controlling the level of risk of doing business with a particular third party.

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