

SPIRE SEARCH PARTNERS: *ORM/ERM ROUNDTABLE* 2018

Topics:

- Embedding Risk Culture
- Strategies & Challenges in Vendor Risk



Topic 1: Embedding Risk Culture

This was the hottest topic from all those we surveyed ahead of the roundtable. The bulk of the time was used to discuss this, everyone is challenged with it in different ways. All organizations have some form of risk culture program, where the ERM/ORM heads dictate the key points but lever a 3rd party through HR to deliver the training to every single person in the organization. Specific topics include RCSA processes, Third Party Oversight, Mindful Testing, Compliance Testing and protocols around how to address a breach. Most organizations are starting to question the amount of time and money being invested in this being about 5 years into their programs and expectations are that some of this formal training will be rolled back or thinned out. Leaders in this space are concerned about how that will affect culture in the future.

Key success factors for embedding risk culture:

“Tone from the top”

- Everyone agreed, that without senior leadership (business and organizational) presence in risk culture programs they are sure to fail. HSBC will have direct reports of the CEO deliver some of the sessions.

Well-defined, separated lines of defense

- Very well defined 3 lines of defense is core to establishing risk culture, what undermines this is when the second line gets too involved with the business and ends up doing the work for them so it's important for them to not overstep their role as an advisor/challenger and start doing the work for them. Ownership needs to stay with the 1st line. Blurred lines between 1st and 2nd line undermine effectively embedding risk culture.
- This is most common in IT departments, and thus the most important place for definition and separation
- Organizations confirm that an effective governance framework is an effective tool in embedding risk culture
- One attendee firm found it effective to build risk teams in the 2nd line and then shift them into the first line to seed/establish the culture

Tying risk culture to client centric, customer first business values

- Some organizations whose culture is centered on client service tie risk culture into the business' every day client approach and find that to be an effective and natural way of embedding risk culture.

Regulatory Hammer

- Using regulatory requirements to “force” certain behaviors in the business - expectation is this will not be as strong a tool if/when regulations start to roll back

Other Interesting Points:

- Some CCPs find that they have a risk culture that is so well built into their organization's service that it can stifle innovation. They recognize the need to be more agile in their risk management to allow for new product development.
- Some banks, however, have built an internal innovation office (a dedicated product development department) to overcome this situation, which is something we are seeing develop at other firms as well.

Topic 2: Vendor Risk

Vendor risk was another major topic on all attendee's agenda. There is increasing scrutiny on the function and firms are responding but the general sense is that there are quite a few holes in the process and there is still plenty of work to do here.

Major Challenges:

- Organizations struggle with **where responsibility for third party oversight sits** within an organization, it can change throughout the vendor lifecycle. For example, it can stay with procurement or move to the first or second line once a vendor is on boarded.
- A major challenge is **getting information and insight on 4th and 5th party vendors** (the vendors supplying your vendors). Firms are responding by:
 - Ensuring it is part of contracts and SLA's
 - Using prescriptive questionnaires – very often the requested info is not furnished, firms are trying be more prescriptive as per 2017-7 exam questions
 - Trying to work more closely with the CISO organization to develop appropriate questions around IT Risk
 - Assessing/reviewing vendors on a regular basis, not just once when they are on boarded – vendor's vendors will change over time
 - Building and leveraging relationships to gain more insight - firms value a combination of questionnaires and a vendor relationship owner (VRO) who can gain additional insights through ad hoc conversation
- There is a **high dependence on internal vendor relationship owners**, challenges arise when:
 - There isn't a clear owner, ie: for Bloomberg there might be many owners that own different pieces of the whole system
 - The first line develops a close relationship with a vendor and are therefore not as stringent with their reviews

- **Common taxonomy** for board level communications - Compliance, Risk and Audit all need to use the same "language" and definitions for more effective Board and Management reporting.

Interesting Points:

- Some firms will actually send teams out to smaller/start up vendors to advise and direct them on how and what to build in terms of process, controls and governance because they don't have the time for them to figure it out on their own.
- Some firms will build out the risk assessment framework within risk or procurement and then move it to first line.
- Most firms have been hurt by not incorporating the cost of vendor oversight into the total cost of what they are getting from that vendor. They expect there are a number of vendors who would not have been engaged if they had done that.
- Many firms are using SIG documentation (from the www.ShareAssessments.org) and finding it to be increasingly valuable as more and more people are following suit.

CONTACT DETAILS

ABOUT SPIRE SEARCH PARTNERS

Launched in 2007 by two tenured financial recruiters both with financial industry experience, Spire Search Partners began as a collection of specialist teams working to provide talent across Risk, Compliance, Accounting/Finance and Quant Analytics to the financial services industry including capital markets, insurance, hedge funds and fintech firms.


In it's 10 year history the firm has placed 100s of specialized and high value professionals in both support and leadership roles with a selection of the top 20 banks, private equity funds, asset managers and insurance firms globally.

ABOUT ME

- Degrees in Economics and Finance from Gettysburg College, honors theses on Financial Market Cycles and Hedge Funds
- Early career in industry with Thomson Reuters & UBS Investment Bank in data analytics and delivery, client connectivity, client relationship management and project management
- Began recruiting in the financial services industry in 2004 with Core Financial before launching Spire in 2007
- Spent 1 year working abroad in Hong Kong and 2 years with a top global retained search boutique before rejoining Spire
- Extensive work for Global Association of Risk Professionals (GARP) as a career advisor and as a volunteer on the selection committee for Venture for America

DENNIS M. GRADY

Director of Risk Search & Market Intelligence
Spire Search Partners

 646.328.1446

 dgrady@spiresearchpartners.com

