



# **SPIRE SEARCH PARTNERS:** ***ORM Roundtable 2019***

- **Cyber**
- **Risk Appetite**
- **Third Party**
- **Project Management**
- **Regulation**
- **Reporting Structures**
- **Talent Perspective**



## Topic 1: Cyber

Cybersecurity and cyber resiliency has jumped back up to the top of the list of the Top Operational Risks and it was a priority for operational risk heads during our discussion.

- Quantification and prioritization is a major challenge
- This is one area where regulation takes a back seat to core business and risk concerns
- There are a few potential methods and vendor tools available to quantify cyber risk, but there is no “one size fits all” solution
- Ways to report on cyber to the Board and manage the Board’s expectations regarding cyber is vital and a key priority
- Board level understanding on the topic varies widely and tends to be fairly weak, however, some firms are working to improve with technology oriented members being added to their Boards
- Linking of cyber security to risk appetite is a major challenge – no one had a cut and dry answer on the most effective way, but most agreed that creating KRIs is not necessarily the solution

**Cloud Strategy** was a subtopic discussed as part of the broader cyber conversation, specifically around board level interaction.

- Boards want to understand it better, but some believe they don’t want to ask the “stupid” questions to achieve that and this is slowing the learning curve at that level
- Boards are generally engaged but in several cases are not well-informed on key topics in technology – some boards have been adding “tech-oriented” people in response to this

## Topic 2: Risk Appetite

Risk appetite emerged as a more important topic than what we had originally planned, questions around how to include cyber into the overall appetite is a formidable challenge. In my conversations with Model Risk heads, they too are struggling with this same challenge.

Attendees shared a bit about the different systems they are using/testing to overcome these challenges, including Risklens and Stroz. Most are finding them to be useful tools but all agreed that there is no silver bullet solution.

Everyone also agreed that setting up these systems and integrating them into their broader framework is requiring more time and resources than expected, specifically around setting up assumptions and other firm specific parameters.

A key concern about these tools is the way in which they measure/report data and calculations; it requires a change in viewpoint and developing an understanding of a related frame of reference. Specifically, these tools can make something very subjective look very precise by calculating and presenting data as a finite numeric measurement.

## Topic 3: Third Party Risk

Third party and vendor risk was one of two key topics in last years roundtable and is again a Risk.net top 10 Operational Risks this year.

- Some firms are moving their 2<sup>nd</sup> line Third Party Risk function into the 1<sup>st</sup> line as a BAU function, this was a strategy initially discussed in last year's round table. It will be interesting to hear what the outcome is when we meet again next year. JPM is one major firm that has it's Third Party Risk risk function in the first line as part of their sourcing organization.
- There is a growing number of different teams converging as part of the third party risk process - this is creating a need for tighter governance and better defined roles and responsibilities. Firms are seeing a decrease in overall efficiency with this trend, as well as the overall increased level of scrutiny in this area.
  - At the same time, risk assessment "fatigue" is a growing concern and a risk in it's own right – in response firms are getting focused on trying to streamline their processes
  - Generally firms are finding it cost prohibitive to outsource vendor risk assessments to a third party/consultant
  - Shared TPO platforms – efforts to build a shared platform like Truesite are off to a rocky start; with Citibank pulling out of it's involvement in Truesite and the fact that in the year since our last meeting, these efforts didn't seem to be any more established with attendees or those I surveyed. At this point PWC and Deloitte have also launched shared TPO platforms.
- Interconnectivity – a topic raised initially by firms whose business it is to provide interconnectivity between parties, highlighted the broader concern around creating connections with and plugged directly into 3<sup>rd</sup> parties. Most felt this is simply a matter of control and monitoring of people who are allowed into firewall
  - Cyber + TPO + ERM need to all be involved as a combined effort
  - The off boarding of employees and other entities is one major potential hole
  - It's critical to create an "inventory of connections"
  - The theft incident in Malaysia that leveraged SWIFT is a good case study to look at

## Topic 4: Project Management

Another topic that came to light during our conversation that had not been on the radar in the past was the project management function and its relation and affect on the broader operational risk function. A focus brought on by that of the Fed's expectations for ERM's role in project management and it's overall scrutiny of the PMO. All involved agreed that ORM/ERM needs to play a more proactive role through the project delivery lifecycle.

- Firms are working to measure the effect of major programs on the business by doing an "impact analysis" for larger, cross business projects
- Agile v waterfall: most firms seem to have Agile implemented for the risk assessment process
- The implementation of cutting edge technologies including AI & Bots raises many questions and concerns for project management teams, it's not clear if their level of understanding of the potential risks has progressed as fast as these technologies have
- All agreed that all parties need to be at the table for these conversations related project management
- Some firms are embedding ORM people into key projects teams in response to these concerns
- Several firms execute assessment of projects in the 1<sup>st</sup> line, but it was clear that outcome was best when the PMO lead in the first line has a "risk management" mentality

## Topic 5: Regulation

The regulatory landscape continues to top the agenda for Heads of ORM/ERM. Even in parts of the broader operational risk organization like Model Risk where the onset of Machine Learning and AI are a very high priority, they still agree that regulatory is #1. Everyone is feeling the pain; even as different firms are at different stages of maturity with respect to getting aligned with regulations - some are still building their programs and are well behind other's in respect to regulatory expectations.

Although there is a growing conversation about a roll back in regulation most operational risk leadership expect "more of the same" but in new ways. Specifically, a deepening of more targeted regulation and a general shift of one regulatory organizations into any space that another agency has backed away from.

- Scrutiny of cyber resilience is expected to grow, even though internally borne business risk concerns seem to be the major push there
- Tightening scrutiny is expected around data management (BCS 239)
- Insurance and market utility organizations feel more regulation is coming specifically around data; but with the Fed backing away in some areas they are already seeing other regulators (state insurance regulators) swooping in to take their place
- Overall most expect ongoing change in the regulatory landscape and an overall continued net increase in regulation

## Topic 6: Reporting Structures

We had a brief but interesting discussion around reporting structures, specifically pertaining to the CISO. Most firms have their CISO sitting in either IT or in risk and most firms have had that structure change over time. Ultimately, the discussion culminated in a view that either structure can work, but which structure works best depends on a variety of factors including cross communications, risk culture, approach, leadership's tenure in the firm, etc. So while the CISO's relationship with the ORM/ERM function is vital, actual reporting line was less important than the soft skills and relationship underlying how they communicate, interact and work together.

- In one firm where the CISO sits in IT, the CISO drives the more granular aspects and ERM has created a role specifically for oversight/interaction with the CISO & IT organization
- In several cases the CISO reports into Risk and in one of those cases the CISO was also the Head of IT
- In one firm where the CISO was reporting into Risk and is now reporting into IT, the view was that the framework was functioning better now. That, however, seemed to be tied to that CISO's tenure with the firm, healthy communications and interaction with the risk function as well as the CISO's ability to take a risk based approach

# Talent Perspective

Operational risk talent in general is in demand, but that demand is becoming more targeted, seeking out experience within specific areas of expertise from the broader ops risk spectrum. Gone are the days of transitioning professionals over from audit or operations, with sustained growth over the last few years there is a larger pool of talent to choose from that has hands on 2<sup>nd</sup> line of defense experience. That said, in certain cases there seems to be an uptick in hiring managers being open to considering first line ops risk professionals in the second line and vice versa. Where there is less flexibility is in transitioning ops risk professionals across segments of the financial services industry and across different functional focuses within those firms. As you would imagine, of most value are individuals with experience in both 1<sup>st</sup> and 2<sup>nd</sup> line from within the same type of firm and same type of function(s).

Deep knowledge of pertinent regulations also continues to be key factor for hiring managers. Equally important and in demand, yet far less common, are the leadership skills (communications, emotional intelligence, executive presence, etc) that the function seeks out to manage growing teams, increased complexities, tightening scrutiny and to face off with regulators and senior stakeholders.

## IT & Cyber Risk:

- IT risk and cyber have been driving the most demand for talent within ORM/ERM – with a variety of wide ranging requirements
- A general lack of leadership skills is the central hiring challenge in this space; most firms seek individuals with the soft skills to interface effectively with boards, regulators, functional teams etc. Even 2 levels down from a Head of ORM/ERM they want to see these skills, perhaps for succession planning or perhaps for pushing certain responsibilities down into the hierarchy as they move part of the framework into a BAU status
- Growing demand for cyber talent continues to drive up compensations faster than in other areas of ORM/ERM. Firms are also offering more flexibility and other benefits like working from home to attract the required talent.
- Other factors too, including the on-shoring of IT and operational teams to other parts of the US has added to the challenges in hiring this talent. Some “on-shore” markets have a limited talent pool, and local compensations ranges do not attract the required talent from other major markets.

## Vendor/ Third Party Risk Talent:

- This is the other specific area where I’ve seen the most demand, second only to IT and Cyber. Demand is clearly regulatory driven but has also been driven by non-banks (credit cards, insurance, asset mgmt.) building out more robust operational risk frameworks to include TPO.
- Requirements vary quite widely but in my experience hiring managers have placed a premium on direct first line experience over a general depth in 2<sup>nd</sup> line operational risk and TPO.
- Generally, there is not a deep pool of experienced talent here, we tend to find the best of it comes out of, or having spent some time in, management consulting firms. This is a common scenario in the earlier days of any area that has more recently experienced increased regulatory scrutiny.

## Project Management:

- Change management, transformational leadership and general project management skills are growing in demand. To some extent these skills are expected as part of the complete package with any ORM/ERM risk professional but with increased concern about the operational and risk impact of firm wide transformation and the increase complexity of specific projects – more hiring managers have highlighted a desire for these skills.

# 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 its 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.


The firm has been a valued partner to organizations including Goldman Sachs, Morgan Stanley, TIAA-CREF, BlueMountain Capital, KKR, MSCI/RiskMetrics and others.

## 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 in 2017
- 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](mailto:dgrady@spiresearchpartners.com)

