Third-Party Risk: A Unique Kind of Operational Risk

ARAVO

Whitepaper

Third-Party Risk
A Unique Kind of Operational Risk

The discipline of third-party risk is on a journey. Barely a twinkle in a regulator's eye a decade ago, today it's receiving intensive focus from supervisors around the globe as well as financial institutions themselves.

The impact of cyber risk and data protection issues on third-party risk management grabs a lot of the headlines. But there are a range of operational and compliance challenges that have raised red flags too – from the toll that natural disasters can take on the supply chain, to how fairly customers are treated by third parties.

As a result, supervisors are beginning to promulgate rules that require specific third-party risk management programs, and they are asking firms to create frameworks for their third-party risk programs that are aligned in philosophy and structure with their overall approach to enterprise and operational risk.

This includes creating a third-party risk appetite, incorporating third-party risk information into strategic decision-making, performing analysis, and undertaking corrective actions, as well as ensuring there is proper assurance and oversight.

The Relationship Between Risks

In response, many best-practice financial services organizations are shifting where third-party risk management "lives" in their organization. Historically, often procurement or compliance have owned this function. However, increasingly firms are either creating a stand-alone third-party risk management team within the overall enterprise risk management structure, or else they are creating a team that reports into the operational risk team. It's expected that this trend will gather pace over the next few years.

Whether the third-party risk team sits under enterprise risk or within operational risk can be a source of some debate for organizations.

Certainly, third-party risk is a form of operational risk. However, while organizations recognize that it fits within pre-existing risk management frameworks, third-party risk also has some key differences that set it apart.Below are five key differences between third-party risk and traditional operational risk, which situate third party risk as a distinct discipline:

1 As a specific type of operational risk, it's received unprecedented regulatory and legislative focus

The amount of regulation and legislation that is being promulgated about third-party risk is significant – whether it's rules targeted specifically at third-party risk or at related aspects of cyber security and data protection.

This supervisory focus will continue, in large part because the risks posed by poorly managed third-party relationships can have such systemic implications for the financial system as a whole. As a result, supervisors are asking firms to put in place measurement and management programs that, both in scope and specific requirements, go well beyond what has previously been demanded for more traditional operational risk programs. An example of this is the fast notifications of impacted clients and regulators that firms must undertake if they – or their third parties – experience a data security breach.

Traditional operational risk software solutions would struggle to capture and manage the entire cycle of activity associated with this kind of reporting, including breach detection, stakeholder activity management, and evidencing activities to the regulator.

2 Significant engagement with entities outside the core organization is required

Third-party risk – it's all in the name! Most enterprise risk and operational risk programs are inward-looking in focus, and engagement – by their very nature. The definition of operational risk – the risk of failure due to people, processes, systems, or external events – has historically looked to the interior of the organization on three of its elements. The fourth, when the definition was originally drafted, was created more with Acts of God such as fires, earthquakes, and war in mind.

This is, in large part, because operational risk was created as a discipline in an era before the significant outsourcing and third-party strategic relationships were made possible by today's IT infrastructure. Indeed, today's third-party risk management programs require significant quantities of information to be exchanged between the organization and these third parties – from on-boarding assessments to direct feeds of third-party risk, operations, and compliance data into the platform.

This data is sensitive and must be protected by levels of IT security not previously required within operational risk software solutions.

3 Third-party risk programs must be engaged with other internal stakeholders, and information types, at an intensive level

At the moment, as previously mentioned, the ownership of third-party risk management can vary by organization. Procurement, compliance, the business line, IT/infosec and a specific third-party risk team can either own the function outright or be significant stakeholders.

This varied ownership underscores the multi-faceted nature of this type of risk and the breadth of information that these stakeholders require. Procurement needs performance data, while compliance requires information about compliance processes and levels. It goes without saying that risk needs risk data.

In truth, all three data types are of interest to all stakeholders – this may sound very "GRC" but the reality is that in most other disciplines the true interaction between performance, compliance, and risk information is less urgent and less a focus for regulators. To succeed today, third-party risk programs need to be much more of a community effort – and the data must be collected and available to the community as well.

Many operational risk platforms would struggle because of the lack of flexibility of their data model to deliver on this.

4 Reporting for third-party risk can be much more complex

While it may be possible to create a solution to perform third-party risk management from a traditional operational risk tool by implementing several instances, this is a clunky approach and can particularly fall apart when it comes to reporting.

In areas of focus for third party risk, such as cyber risk and data protection, regulators are close to demanding that organizations have access to real-time information, that is acted on with immediacy. This data could be part of performance, risk, or compliance data sets – or all three – and needs to be assessed holistically to be useful.

Reporting that combines risk and performance data, or compliance and risk data, would be time-intensive to create manually. With the flexible data model of a dedicated third-party risk management solution, creating statistics based on different kinds of data is done with just a click of a button.

5 Third-party risk management needs to be integrated directly into the business workflow

Most organizations have a requirement for their third-party risk management solution to connect directly into their ERP system – whether they realize it or not!

Information needs to flow seamlessly between the two systems to maximize efficiency and avoid duplication. The third-party risk management solution also needs to be able to stop, and start, payments to third parties automatically, and flag other activities in the accounts payable system – to ensure risks are managed properly within the business line and the procurement team.

Most traditional operational risk solutions would not be capable of telling an ERP system to withhold payment.

Getting Reporting Right - Regular Third-party Scorecards

The risk appetite statement for third-party risk can then be a good starting point for creating a reporting framework. While overall reporting can and should be even broader – catering to the needs of the relationship managers in the business as well as third-party risk – a good place to start any reporting project is with putting the information elements in place that relate directly to the risk appetite statement. These data points should directly describe whether or not the organization is keeping within its stated risk appetite. For most organizations, it's a good idea to configure the third-party risk solution to report any breaches of the risk appetite immediately to all relevant stakeholders, and automatically initiate a remediation process.

However, good reporting for third-party risk can go far beyond the strict requirements of the risk appetite statement. (See below) Here, again, third-party risk professionals should consider collaborating with their operational risk and enterprise risk colleagues. These colleagues should be able to share basic information such as formatting – which can be an important detail. They can also share the kind of metrics that they follow, some of which the third-party risk team may find valuable. Even further still, there may be elements of the overall operational risk or enterprise risk framework that third-party risk may want to consider importing, such as emerging risks, loss events, and near miss reporting.

Essential Reporting

Getting a third-party risk management program off the ground is a big task – and getting the reporting right is part of that. Below are some suggestions for essential reports for the third-party risk team, which will be appropriate to share generally with the enterprise or operational risk teams, as well a senior management and the board.

Compliance completeness: Across all third-party relationships, third-party risk management teams need to be sure that compliance requirements are met on an ongoing basis – that compliance risk is being managed effectively. Reports could include:

- Compliance breaches in the reporting period by third party and by product/business line.
- Third-party relationships with the largest number of compliance breaches over the course of the relationship or within the past 12 months.
- Compliance breaches by either regulatory or organizational taxonomy type.

Performance metrics: Understanding how third-party relationships are performing relative to the contracted terms of service is an essential part of managing the overall risk of the relationship. A third party may look good from a compliance point of view, but if they don't deliver, the organization is subject to a range of risks. There is a range of performance metrics – what are the appropriate ones will depend on the nature of what product or service is being delivered. But some essential ways of looking at that kind of data include:

- Reduced performance or performance failure events by geography, business line, or product type.
- Performance events by relationship – over the past 12 months or lifetime. Depending on the nature of the relationship with the vendor, this could be at the individual entity level or across the entire breadth of relationships that exist with the third party.
- Performance events by taxonomy type – these could also be looked at over a period of time. Or, for a specific taxonomy type, by business line or geography.

Risk management indicators: These are an essential component of the reporting and should align with the way enterprise risk management or operational risk management reports are constructed. For all of the suggestions below, it's important to specifically call out cyber risk and data protection events or risks specifically or to run reports focused on those topics. Regulators will want to see that senior management and the board are aware of those issues and receive regular updates.

- Key risk indicators of third-party relationships by products, business line, or geography.
- Risks identified through assessments completed in period– understanding "red flags" raised through the assessment process by taxonomy type, relationship, or business unit can give insight into current risk trends for the business.
- Risk event loss data – this data can be served up in a number of ways, including by taxonomy type, by geography or business line. It can also be served up for a specific time period, such as for the past 12 months or over the course of a relationship. It can help the firm understand where it is losing money and how much to third-party risk events.

Intermediate Reporting

These are reports that organizations should be aspiring to implement over the next 12 months for their third-party risk teams and for sharing with their business partners, procurement, and operational risk or enterprise risk colleagues. They help provide a more in-depth view of the issues the organization is potentially facing, and can help drive more value from the third-party risk team's activities.

Recent external events – Understanding recent external events – loss events that have happened at other, similar organizations – can be a goldmine of insight. Some external loss databases operated by industry associations for financial services should have examples of third-party risk events, even if they are not labeled as such. Most operational risk teams in financial firms have membership to at least one such organization. It's worth reviewing third-party events at other organizations on a regular basis and then reviewing, at minimum, whether or not similar risks exist in the firm's own strategic third-party relationships.

Relationship review and/or control review results – these reports specifically review key strategic relationships or control frameworks on a regular basis. Reports should examine assessment results,SLA's, KRIs, KCIs, and KPIs at minimum. For relationship reviews, it's helpful to schedule these in advance of contract renewal. Other elements to consider include the potential risks from external events that other, similar relationships/organizations have experienced and potential regulatory changes that could impact the relationship.

Results by business unit, team, or individual – These reports could vary in content, depending on what interests the stakeholders. One possible report is third-party loss events by internal team, such as the team that manages the relationship from a business line perspective. Alternatives include certain key indicators, such as compliance breaches, performance levels. or even the overall residual risk of the relationship. A best practice some firms are exploring is linking these data points to compensation packages to help embed the third-party risk management culture.

Advanced Reporting

Organizations that have a well-defined third-party risk program can use the considerable amounts of information they acquire each period to produce more analytical reports, which incorporate even more operational or enterprise risk information, such as:

Relationship trends – Evaluating overall strategic third-party relationships according to two third-party categories on a grid can provide senior management and the board with insight into which relationship are working, which could potentially be expanded on, and which should be terminated. For example, viewing compliance v. performance, performance v. risk and compliance v. risk on a quadrant-style grid is possible using overall scores for these categories. Viewing multiple relationships on the same grid can also give firms a sense of the current "style" of their third-party relationships and potential areas of focus.

Near-miss events – Capturing "near miss" events can provide organizations with essential information on potential risks. Building trust with a third party, so they share this information with your team, can take time but if the goal is mutually-beneficial collaboration, the results can be very rewarding. Alternatively, "near miss" events by third party and risk type or business line could potentially be harvested from the organization's own staff, or from data feeds from the third party for certain processes or activities.

Emerging risks – Focus some reporting on capturing emerging risks. Identify potential emerging risks through workshops or assessments, and then ensure that all failure-type events are reviewed for those events to produce compliance breaches/risk events/performance failure events by emerging risk type. With strategic third parties, it may make sense to review potential emerging risks the relationship may be subject to during the annual assessment process as well.

Breakpoint analysis – Create reports that arrange third-party relationship information – such as KRIs, KPIs, and KCIs – around key "breakpoints" in the processes associated with the relationship. Relate control reporting to these processes too. This can, if done properly, create a holistic and actionable view of key elements in a third-party relationship. Such a reporting technique may be particularly suited to specific issues such as cyber risk and data security.

Conclusion

In conclusion, while best-practice financial institutions are shifting their third-party risk programs to sit within their overall enterprise or operational risk management team, it's important to be realistic about how these disciplines are similar and how they can differ in their requirements.

For example, third-party risk management has a number of very specific complexities that require a technology solution that differs from the kinds that have been traditionally used in operational or enterprise risk.

On the other hand, when it comes to creating a risk appetite statement and reporting, the level of collaboration between the business and risk teams can be an important determinant of success. As third-party risk continues to evolve as a discipline, it's likely that all the risk teams will have considerable opportunity to share and learn from each other.

ARAVO

The Definition of Better Business

Better business is built on acting with integrity. It commands better performance, delivering better efficiency, collaboration, and financial outcomes. It inspires trust. But better business is more than that – it's about lifting the ethical standard of an entire business ecosystem to build a better world.

Contact

For more information:

visit us at aravo.com

email us at info@aravo.com

call us at +1.415.835.7600 [US]