

# Meeting the Expectations of the Board

Accelerating vendor and third-party program maturity to enhance governance and oversight

# Contents

Increased Board Emphasis on Third-party Risk	1
Why Are Boards Prioritizing Third-party Risk Management?	2
Why Is Third-party Risk Such A Unique Challenge For Boards And Their Organizations?	3
What Does A Good Governance Framework Look Like?	5
What are Third-party Governance Best Practices?	6
Comprehensive governance structure	7
Clearly defined roles and responsibilities	7
Regular third party review meetings	8
Cohesion across three lines of defense	8
Third party risk appetite and thresholds well defined and understood	9
Segmentation reviewed annually	9
Issue escalation rarely needed	9
Issues resolved quickly/effectively	10
Integrated enterprise TPRM IT solutions in place	10
Third party relationship review maximized	10
Industry best practices embraced	11
Utilities and standardization	11
Enterprise view of risk, performance and compliance	11
What Can The Board Do To Help Embed Third-party Risk Governance? 1	12
Appendix 1: OCC Expectations Of The Board	13
Appendix 2: What Kind of Board and Management Reports to Consider	14

# Increased Board Emphasis on Third Party Risk

With the strategic importance of engaging third parties in today's business landscape, coupled with the level of risk that they can bring to the enterprise, it should not be surprising that third-party risk management is attracting greater focus from the C-suite and the Board of Directors.

Today, third -party relationships form a deep and far-reaching part of the strategic and operational ecosystem of any Global 2000 organization. Third parties are intrinsically linked to the success and the reputation of the business – and can include not only traditional suppliers, but also vendors, distributors, resellers, agents, partners, affiliates, contractors, managed service providers, brokers, and even intra-company groups.

According to the Institute of Collaborative Working, up to 80% of direct and indirect operating costs of a business can come from third parties, while up to 100% of revenue can come from alliance partners, franchisees, and sales agents.[1]

With third parties now becoming part of the DNA of the extended enterprise, regulators globally have made it quite clear that while organizations can outsource a task, they cannot outsource the responsibility. Increased regulatory scrutiny, however, is just a symptom of the underlying issue –the way organizations do business is evolving dramatically and rapidly. And with this, the way they manage risk and govern the extended enterprise needs to evolve quickly too.

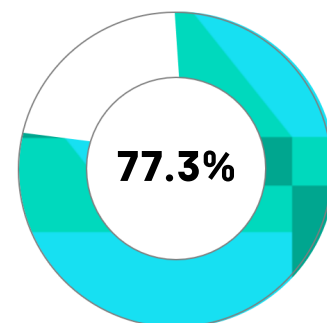
This evolution is challenging – third-party risk management is a relatively new discipline and companies are at radically different stages of maturity depending on their industry, size, and culture. From a discipline that has evolved largely from siloed and ad-hoc processes, there's a growing recognition that a more joined-up, standardized, and enterprise-wide view of risk is required.

This paper will look at why third-party risk has become so important, and explore the kinds of governance arrangements boards should put in place to ensure third-party risk, compliance, and performance is well managed across their organization.

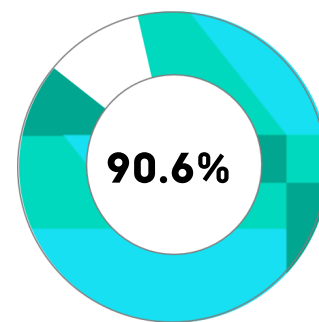
[1] Deloitte: Third Party Governance and Risk Management. Turning Risk into Opportunity.

[2] Deloitte: Overcoming the threats and uncertainty.Third Party governance and risk management (TPGRM) extended enterprise risk management global survey 2017

[3] Ibid



of boards don't have a high level of confidence in their third-party risk management processes [2]



of boards are skeptical of their third-party risk management technology's ability to deliver [3]

## Why Are Boards Prioritizing Third-party Risk Management?

Third-party risk management has shot up the list of concerns for boards of directors around the globe. For many organizations, this is a result of direct experience of a loss as a result of the activities of a third party. Third parties are a noted area of risk exposure – for instance, more than 90% of US Foreign Corrupt Practices Act (FCPA) enforcements come on the back of third-party activity, and 63% of data breaches can be tracked to third-party failures. In fact, according to research conducted by Deloitte, nearly three-quarters of companies have faced at least one third-party-related incident over the past three years. [4]

The costs are high. Deloitte has estimated that the failure by large multi-national businesses to appropriately identify and manage third parties can lead to fines and direct compensation costs or other revenue losses in the range of US\$2-50 million, while action under global legislation such as the FCPA can be far higher, touching US\$0.5 - \$1 billion. [5].

In highly regulated industries, such as financial services, this unsettling trend toward third-party culpability in risk events has led to increased supervisory focus. In particular, the US Office of the Comptroller of the Currency (OCC) issued a guidance document on managing third party risk in 2013 and updated the document in January 2017. Other regulators globally – including financial services regulators in Singapore and Hong Kong – have also issued guidance in this area. In addition, many new cyber risk-focused regulatory initiatives have a substantial third-party focus – an example is the recent New York State cyber security rules for financial services firms. As a result of this regulatory attention, boards are naturally giving third party risk more of their time and attention.

Boards have also recognized that third-party activities can drive a wide range of risks, and so have enhanced their approach to managing third parties as part of their overall enterprise-wide approach to risk management. Enterprise risks that are particularly applicable to third parties – and have boards concerned, include:

- i Strategic** – this is a key risk that is often overlooked or ignored unintentionally. It includes issues such as the robustness of the organizational planning processes and the quality and quantity of staff for key roles.
- i Cyber** – a significant number of headline-making cyber events of recent years have been the result of hackers gaining access to corporate systems via a third-party relationship, for example.
- i Info security** – again, many information security breaches happen via a third party. This area is also becoming an increasing focus of global regulation, including the EU's GDPR.
- i Business continuity plan/disaster recovery** – organizations are beginning to recognize that they do not have joint BCP/DR plans in place with strategic third parties, and so no backup if something should go wrong on either side of the relationship.
- i Compliance** – particularly in highly regulated industries, it's essential to ensure that third parties abide by all of the rules and regulations that the organization is responsible for.

[4] Deloitte: Overcoming the threats and uncertainty. Third Party governance and risk management (TPGRM) extended enterprise risk management global survey 2017

[5] Deloitte: Third Party Governance and Risk Management. Turning Risk into Opportunity.

## What the Regulators are saying

*The Board of Directors and senior management are ultimately responsible for managing activities conducted through third-party relationships as if the activity were handled within the institution."*

**Financial Institution Letter 44-2008  
"Guidance for Managing Third-Party Risk"**

*The Office of the Comptroller of the Currency (OCC) expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.*



**OCC Bulletin 2013-29**

*The financial institution's board and senior management should establish and approve risk-based policies to govern the outsourcing process. The policies should recognize the risk to the institution from outsourcing relationships and should be appropriate to the size and complexity of the institution.*

**Outsourcing technology services, Board and Management Responsibilities, FFIEC IT Examination Handbook.**

*Outsourcing does not diminish the obligations of an institution, and those of its board and senior management to comply with relevant laws and regulations in Singapore, it is thus important that an institution adopts a sound and responsive risk management framework for its outsourcing arrangements.*

**Monetary Authority of Singapore Guidelines on Outsourcing**

-  **Credit** – a very key risk if an organization has a financing arm or is a financial services firm. However, understanding the credit risks posed by third-party relationships can be important in other circumstances too.
-  **Reputational** – boards are finding this is a driver that is growing in significance. Protecting a firm's reputation via its governance responsibilities is a primary focus for most firms. With the growing incidence of third party events, boards are realizing that it is their organization's name – rather than the third party's – that often features in headlines and that this has a direct impact on shareholder value.

Boards are also beginning to understand that it's essential to have a good third party risk management program, if the organization is to have a robust enterprise risk management approach. After all, third parties form an essential part of what is the extended enterprise.

Additionally, boards are recognizing that an increased focus on third party risk just makes good business sense, given the importance third parties play in the organization's overall strategic approach. Many organizations today outsource a significant amount of their key activities to third parties – so it's prudent to have a robust risk management approach in place with these business partners.

In fact, Deloitte believe "those organizations that have a good handle on their third party business partners, can not only avoid the punitive costs and reputational damage, but stand to gain competitive advantage over their peers, out-performing them by an additional 4-5% ROE, which, in the case of Fortune 500 companies can mean additional EBITA in the range of US\$24-500 million." [6]

### Why Is Third Party Risk Such A Unique Challenge For Boards And Their Organizations?

Third party risk management can be a challenging endeavor. The larger the organization, the more important the third-party program becomes, and the more complexities are introduced. Strategically, boards – particularly at those organizations who fall within the Global 2000 – face three big challenges when it comes to their third party risk programs:



**Business scale:** Large organizations can have a range of different kinds of third parties, with different risk profiles. For example, the average number of third parties among Aravo clients is 37,000, but one client has in excess of one million to manage. Larger organizations also usually have multiple business units, geographies, and languages that programs must accommodate.



**Business complexity:** Large, global organizations are complex. Usually, there are multiple systems, multiple projects, and multiple business processes that need to be accommodated and streamlined. They may require multiple, cascading risk frameworks for different divisions, geographies, or risk types.



**Business change:** Today most organizations are subject to a significant amount of change, and their approach to third-party risk needs to be able to cope with reorganizations, mergers, expansion, and frequent regulatory change. They need a system to be agile enough to manage this change, without having to rely on expensive consulting or IT projects.

*"Those organizations that have a good handle on their third party business partners, can not only avoid the punitive costs and reputational damage, but stand to gain competitive advantage over their peers, out-performing them by an additional 4-5% ROE, which, in the case of Fortune 500 companies can mean additional EBITA in the range of US\$24-500 million."*

[6] Deloitte: Third Party Governance and Risk Management. Turning Risk into Opportunity.

Creating a governance structure that can meet these three challenges can seem fairly daunting for boards – from setting a risk appetite to ensuring information flows across the organization coherently.

Another challenge for boards arises from the way third-party risk may be managed currently in their organization. Third-party risk could potentially be owned – for the moment – by procurement, risk management, compliance, the business line, or another group entirely. Boards need to understand the strengths and weaknesses of the organization's current approach and decide ultimately who will "own" third party risk. At the same time, however, all of these important stakeholders must buy into the new governance framework going forward.

Additionally, boards often feel they are faced with the Scylla and Charybdis of governance creation. On one hand, they are wary of unleashing a burdensome governance structure on the business that does not deliver either the assurance it was intended to, nor benefits to the business itself. Perhaps board members have experience of being burned by over-inflated GRC programs in the past, or else they are worried about resources eventually being diverted from the core business challenges. They fear the program structure becoming its own "cottage industry" within the organization, self-perpetuating and even misaligned with the overall strategic goals of the organization. In short, boards worry about over-funding governance programs, and then having those programs turn into self-perpetuating monsters.

On the other hand, boards can also under-resource new governance structures, leading to exposure. Boards usually recognize instinctively what a new governance structure should do – provide the intelligence needed to make the right decisions that will keep the organization strategically on track.

However, boards often fail to take into account the time, money, and resources that will be needed to carry out this vision – or even worse, allocate resources incorrectly. A surprising number of organizations will try to "make do" with spreadsheets, documents, and other information on a shared drive, or turn to other GRC technology not designed for third-party risk - and boards wonder why they are not getting the decision-making information they require. Ironically, often cutting corners this way can actually wind up costing the organization much more – not just in the time and resources spent to create manual reports, but also in terms of the missed view into emerging risks and potential performance challenges.

In short, boards are coming to recognize the importance of properly managing third-party risk across their organizations. They are also starting to see that third-party risk presents new levels of complexity for a GRC program – and that complexity is part of the reason why a formal third-party risk governance framework is required. However, where boards are often falling down is in implementing that governance framework – and getting the investment in process, tools, and talent correctly aligned to develop the maturity of the program.

*A surprising number of organizations will try to "make do" with spreadsheets, documents, and other information on a shared drive, or turn to other GRC technology not designed for third party risk - and boards wonder why they are not getting the decision-making information they require.*

## What Does A Good Governance Framework Look Like?

More and more, organizations are opting to use their existing approach to enterprise risk management to form the backbone of their governance framework for third-party risk management. As a result, third-party risk is starting to gravitate toward the risk management teams of large organizations, particularly in financial services.

There are a range of advantages to this. First, by adapting third-party risk into the enterprise risk structure, the board can leverage existing processes and internal expertise. Second, it can usefully expand existing concepts such as "risk appetite" to third-party risk. Although the definition of third-party risk appetite is still being actively discussed within the industry, one potential definition is "the level of this type of risk a firm is willing to assume in its exposures and business activities, given its business objectives and obligations to stakeholders."

This approach is proving popular. In a recent pair of surveys conducted at two third-party risk management conferences for the financial services industry, just over half of respondents (57% in the EU and 56% in the US) said their organizations have implemented third-party risk appetites. [7]

It is still early days, however. Of those firms that are putting a third party risk appetite in place, most are in the foothills of implementation. In a global third-party risk benchmarking report, the majority of respondents (67%) expressed that their programs were in the early stages of development (initial/ad-hoc, developing/fragmented or defined). Only 5% categorized their program as optimized/agile. [8]

While embryonic, momentum does seem to be growing behind an approach to third-party risk that is embedded in the overall enterprise risk management framework. However, even here it's important to be cognizant of third-party risk's special status.

For many organizations, performance, and compliance are equally important governance areas – and parallel or integrated governance approaches to these should be included.

These approaches can often sit in silos – procurement for performance and compliance with that team. Some organizations, however, are integrating risk, performance and compliance together into one overall governance framework, and housing this information on one technology platform. In this scenario, the risk, compliance and procurement teams can collaborate to create a governance approach that is integrated and aligned to the overall organizational business strategy.

*In a global third-party risk benchmarking report, the majority of respondents (67%) expressed that their programs were in the early stages of development (initial/ad-hoc, developing/ fragmented or defined). Only 5% categorized their program as optimized/ agile. [8]*

[7] Aravo blog: Whetting the Appetite in Third Party Risk <http://blog.aravo.com/third-party-risk-appetite>

[8] Third Party Risk: A Journey Towards Maturity. Results of the 2018 'Taking the Pulse of Third Party Risk Management' Survey.



## What are Third-party Governance Best Practices?

More and more, organizations are opting to use their existing approach to enterprise risk management to form the backbone of their governance framework for third-party risk management. As a result, third-party risk is starting to gravitate toward the risk management teams of large organizations, particularly in financial services.

SYSTEM	PROGRAM	
<p><b>SHARED UTILITY (DATA) CENTRALIZED - ENTERPRISE WIDE – (TECHNOLOGY)</b></p> <p>Continuous third party risk monitoring Normalization across the industry provides benchmarking insight Predictable, low-cost of compliance per vendor Efficiencies for suppliers Due diligence follows industry best practice But centralized risk management in line with risk appetite of the individual organization</p> <p>Provides enterprise governance Provides a layer of industry governance</p> <p><b>CENTRALIZED (ENTERPRISE WIDE)</b></p> <p>Leverage custom-built or dedicated third-party solution to manage all third parties across the portfolio Improves visibility and removes duplication Cost per third party is reduced Continuous third-party risk monitoring</p> <p>Provides enterprise governance</p> <p><b>DECENTRALIZED SILOS</b></p> <p>Siloed risk management leads to duplication of activities Critical only (no long tail) Per vendor cost is high Multiple systems &amp; processes Disconnected programs Gaps augment risk (blind spots) Lack of benchmarking</p> <p>Lack of enterprise governance</p>	<p><b>Agile</b> <i>Optimized</i></p>	<p>Comprehensive governance structure with periodic meetings with board and regular governance review meetings. Third-party risk appetite and thresholds well defined and understood. Segmentation reviewed annually. Cohesion across three lines of defense. Issue escalation rarely needed and resolved quickly/effectively. Able to identify areas of improvement and measure ROI for relationship reviews and continual improvement. Industry best practices understood and embraced. Enterprise view of third-party ecosystem risk, compliance, and performance.</p>
	<p><b>Integrated</b> <i>Established</i></p>	<p>Governance model agreed at Board level. Standardized TPRM approach implemented and adopted, with documented processes. Third parties are segmented according to agreed and understood criteria. Robust performance measures are in place. Appropriate skillset and resources, with roles and responsibilities allocated. Third parties engaged and involved. Statutory/regulatory obligations met.</p>
	<p><b>Defined</b></p>	<p>TPRM program and processes are defined with roles and responsibilities agreed. A formalized approach is in place with the framework designed and control practices in place. Risk appetite not yet well defined or aligned, although inherent risk assessments are maturing.</p>
	<p><b>Fragmented</b> <i>Developing</i></p>	<p>Starting to determine a road map, with pockets of good practice emerging. Basic segmentation in place, and some standardization of on-boarding registration, and qualification. Some areas of risk management are in place (credit, ABAC, InfoSec), but are not approached in an integrated or structured way. TPRM framework agreed but not implemented, with required skill sets identified. Some basic performance management. Governance and processes not fully embedded.</p>
	<p><b>Ad-hoc</b> <i>Initial</i></p>	<p>Siloed, ad hoc practices. No TPRM framework, tools, or formal program. No third party segmentation. Lack of skills and resourcing. No defined roles and responsibilities. No governance structure or TPRM authority matrix in place.</p>



The elements that an optimized program and system could look like from a maturity perspective, include:



### Comprehensive governance structure

While having a good governance structure is essential when managing all forms of risk, it's particularly important with third-party risk because of the collaborative nature of engagement, both internally, and externally.

Internally, third-party risk usually falls within the remit of several teams, including procurement, operational/enterprise risk, compliance, and the business lines themselves. Externally, third parties are increasingly becoming strategic partners for the business, and can engage with the organization across many different points and types of engagement. The governance structure has to ensure that third parties encounter "the same" organization across all of these points, with the same policies and procedures in place.

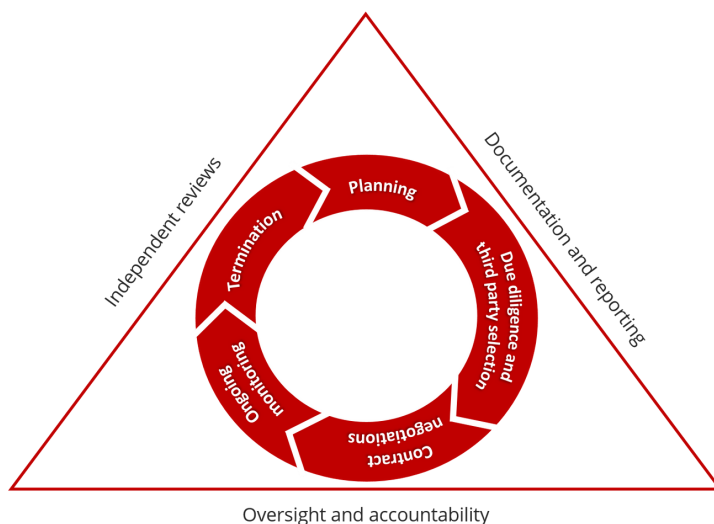
Today many boards appoint a specific director who is the point person on third-party risk. They also often put in place managing boards – by geographic region, by relationship, or by business unit. These managing boards sit within the business but have a governance role, with the main board delegating responsibilities within a more focused mandate. These subsidiary boards ensure clear communication and transparency around third party risk across the organization, helping to ensure consistency of application of policies and procedures. They also provide oversight, which can be particularly useful if there is a third party risk event, or the need to re-evaluate a relationship with a strategic third party.

*Today many boards appoint a specific director who is the point person on third-party risk. They also often put in place managing boards – by geographic region, by relationship, or by business unit. These managing boards sit within the business but have a governance role, with the main board delegating responsibilities within a more focused mandate.*



### Clearly defined roles and responsibilities

The board – or a dedicated board committee – should adopt a risk-based process that, at a minimum, establishes policies, operating standards, and procedures throughout the third-party risk management life cycle, including documentation and reporting; oversight and accountability; and independent reviews. This overall framework should be periodically reviewed and updated.



Source: OCC

Board minutes should indicate that the board reviews and approves:

- The methodology for determining critical activities
- Management's plans for using third parties involved in critical activities
- Summary of due diligence results
- Contracts with third parties involved in critical activities
- Results of management's ongoing monitoring of third parties involved in critical activities
- Results of periodic internal audit or independent third-party reviews of the organization's third party risk management processes.

The board minutes should also show that the board oversees management's efforts to remedy deterioration in performance, material issues, or changing risks identified through internal audit or independent third-party reviews.



### Regular third party review meetings

The relevant roles within the organization – including individuals from the business, subject matter experts, and third-party risk professionals – should meet on a regular basis to review third party relationships. Which relationships are reviewed should be dictated by the risk appetite and profile of the business – possibilities are to review key strategic third parties, or to review third parties by jurisdiction/geography, or by business line. More sophisticated organizations use the timely intelligence a third-party risk solution platform can provide to monitor third-party relationships for emerging risks in an ongoing fashion.

For good governance, it's essential that these meetings take place, and that they are supplemented by the key metrics and reports those attending need to understand the risks within and performance of each relationship – and its impact on the business.

Third-party scorecards can be a particularly useful tool in this context. Scorecards bring together the risk, performance, and compliance information about a third-party into a single dashboard or report. They enable the organization to understand the strengths and potential risks of the third-party relationship quickly and easily. Usually, this is accomplished by consolidating a range of information points via scoring and weighting into a series of "scores" – often red/amber/green or an alphanumeric score.

*Third-party scorecards can be a particularly useful tool in this context. Scorecards bring together the risk, performance, and compliance information about a third party into a single dashboard or report.*



### Cohesion across three lines of defense

The third-party risk management program should be embedded across all three lines of defense. All three lines of defense should be working closely together to enhance and improve the management of third party relationships – not just to better manage risks, but also to enhance performance. A natural result of this cooperation should be a steady flow of joint initiatives with stated goals as outcomes. It's important that the infrastructure the organization has in place to manage and remediate third-party risks supports this kind of collaboration.

**Third party risk appetite and thresholds well defined and understood**

An important element of third party risk governance is the application of risk appetite. Risk appetite can be defined as 'the amount and type of risk that an organization is willing to take in order to meet their strategic objectives. The COSO Enterprise Risk Framework, defines risk appetite as "the amount of risk an entity is willing to accept in pursuit of value."

In an optimized third-party risk management program, there will be a clear and shared understanding of the upper and lower thresholds of risk tolerance. Triggers should be built in to TPRM monitoring systems to alert program managers prior to thresholds being met, so that they can take and record the appropriate corrective actions.

Larger, complex organizations may have multiple, cascading risk appetites aligned to business divisions, geographies, or risk type.

The board should provide input into the risk appetite and understand and provide counsel into its development and evolution. They also need to ensure it is well communicated and understood across the organization.

*Risk appetite can be defined as "the amount and type of risk that an organization is willing to take in order to meet their strategic objectives." The COSO Enterprise Risk Framework, defines risk appetite as "the amount of risk an entity is willing to accept in pursuit of value."*

**Segmentation reviewed annually**

The third-party risk management program should review the way the organization's third-party relationships are segmented – that is, how they are classified based on the inherent risk they potentially expose the business to in light of the role of the relationship in the organization's overall business strategy. The board should be involved in this review with the third-party risk team leadership – and provide counsel of coming changes in priorities or strategies for the business or new risk concerns the board has developed.

**Issue escalation rarely needed**

The board needs to ensure that management has an effective and timely process for the escalation of significant issues to the board. These would include those events that could have a material adverse consequences to the organization and its customers, such as data breaches and the compromise of customer information. It's important that key issues or challenges are communicated to the board in a timely and accurate manner.

However, the board should also be concerned if it received too many escalations – this could be a sign that the three lines of defense are not working together harmoniously, or perhaps that key decision-makers in the organization are not receiving the risk and performance information that they need in a timely fashion. It could also be a sign that the organization does not have strong "playbooks" in place to reference in the event of a risk event or a performance failure – such as a good disaster recovery approach.



### Issues resolved quickly/effectively

A key measure of how well all three lines of defense are working together is how quickly and effectively issues are resolved. A primary enabler of effective third-party risk and performance management is that all three lines of defense are working with the same set of information – from a single source of truth. By having a single source of truth about the issues the organization is facing, it's quicker and easier for stakeholders from different functions to agree on the nature of the challenge they are facing, identify potential causes, and agree on corrective actions.

It's also important to have the right subject matter experts on staff or accessible to the organization. These are the individuals who can provide key information and insights to the business about a particular challenge.

Lastly, it's essential to have the right organizational structure, culture, and compensation plan in place – to make sure that collaborative problem-solving for third-party challenges is incentivized and “buck-passing” is actively discouraged.



### Integrated enterprise TPRM IT solutions in place

There are many ways in which third-party risk management solutions show their worth, including supporting collaboration, information gathering, and remediation management. However, reporting is where the proverbial rubber meets the road. By using a solution, management should be able to provide good quality intelligence on third-party risk to the board, including the results of ongoing monitoring of third parties involved in critical activities. When good governance is supported by a strong solution, boards should also be able to harvest information about potential emerging risks, so they are able to act on them more strategically.

Such reports can also support the review processes of internal audit or independent third parties, such as regulators by being able to evidence not just information gathering, but also the overall risk management life cycle too. This ability to evidence can save the organization valuable time and resources and also help board members to feel comfortable that their organization has the kind of transparency required by these bodies.

*When good governance is supported by a strong solution, boards should also be able to harvest information about potential emerging risks, so they are able to act on them more strategically.*



### Third-party relationship review maximized

Third-party relationship reviews should not just be an “internal” exercise – that is to say, something performed within the boundaries of the organization alone. Rather, the third party should be actively involved in the relationship review – ideally by supplying its own data about performance and risk, which can then be compared and aligned to the organization's own metrics. A good third party risk management IT solution can be configured to automatically bring these external metrics into the solution and report on them, too.

Additionally, the results of the third-party review, when ready, should be shared with the strategic/critical third party itself. Strengths and weaknesses, across risk management, compliance, and performance, should be discussed. The organization should also be ready for – and in fact actively seek – feedback from the third party about how the relationship could be improved.

By working together collaboratively to get the maximum amount of insight from a third-party review, both sides of the arrangement can ensure the relationship is in a good place for the coming period.

This also helps the buyer organization and the third-party organization drive continuous improvements.



### Industry best practices embraced

The discipline of third-party risk management is evolving rapidly. Driving this is a number of factors, including the expanded use of third parties by organizations, and a deepening understanding of how these relationships can be more thoughtfully managed. Organizations need to have the ability to actively seek out and adopt new best practices as they emerge.

It's worth noting that in some industries, it's the regulators who are driving this best practice adoption, by hard-wiring the leading strategies and tactics they discover at the firms they supervise into updated guidance. In this sense, best practices within the discipline are becoming part of the ongoing regulatory change that many industries are facing. As well, these best practices are then being transferred from one industry to another.

Organizations need to ensure they have a third-party risk governance structure in place that is flexible enough to support the change and evolution that this discipline will certainly continue to see over the remainder of the decade. This includes a technology solution that is adaptable to this – that can evolve with the organization.

*It's worth noting that in some industries, it's the regulators who are driving this best practice adoption, by hard-wiring the leading strategies and tactics they discover at the firms they supervise into updated guidance.*



### Utilities and standardization

Connected to this drive towards the adoption of industry best practice, is the growing appetite for shared services or multi-buyer/multi-supplier communities. These are sometimes called "utilities." These can add efficiency and take costs out of the business, particularly in non-competitive operational processes such as third-party data validation and due diligence.

In addition, standardized assessments are emerging, such as those delivered by Shared Assessments.

More mature programs may leverage the efficiencies and standardization that these kinds of services deliver for third-party data, in conjunction with their internal TPRM automated workflow software for risk management and reporting.










### Enterprise view of risk, performance, and compliance

Finally, optimized programs will support an enterprise view of third-party risk, performance, and compliance.

## What Can The Board Do To Help Embed Third-party Risk Governance?

For boards, the decision to implement a third-party risk management program is not a point-in-time exercise. It requires ongoing support and monitoring – both as the program is rolled out and over a longer period. To help ensure the governance program is being accepted by the organization and is delivering value, boards should:

-  Ensure the team implementing the governance program has the right resources available.
-  Ensure all those involved in third-party relationships collaborate effectively – risk, compliance, procurement, and the business, among other teams.
-  Where appropriate, incentivize third party risk management through the compensation scheme, backed up with organizational metrics.
-  Provide good training to employees involved with third-party relationships.
-  Ensure the tone from the top – the communications coming from the board – are supportive of the third-party risk program.
-  Underpin the third-party risk program with a technology platform that can serve as a single source of truth for effective collaboration, communication, and relationship management.
-  Enhance the value the third-party risk program delivers to the organization by monitoring performance and compliance metrics, as well as risk metrics.

By implementing a strong third party risk management program, boards are ensuring their organizations can deliver the value they should be creating for shareholders, while also maintaining improved relationships with those third parties and key stakeholders such as industry regulators.



## Appendix 1: OCC Expectations of the Board

### For the board, examiners will be looking toward the following:

Determine whether the board (or designated board committee) has adopted a risk-based process that, at a minimum, establishes policies, operating standards, and procedures throughout the third-party risk management life cycle, including documentation and reporting, oversight and accountability, and independent reviews. Is the process reviewed and periodically updated?

Do board minutes indicate that the board reviews and approves the following?.

- The methodology for determining critical activities
- Management's plans for using third parties involved in critical activities
- Summary of due diligence results
- Contracts with third parties involved in critical activities
- Results of management's ongoing monitoring of third parties involved in critical activities
- Results of periodic internal audit or independent third-party reviews of the bank's third-party risk management process

### For senior management, examiners will be looking toward the following:

#### Escalation

Determine whether management has an effective process to escalate significant issues or concerns to the board (e.g. events that result in material adverse consequences to the bank and its customers, including data breaches and compromise of customer information).

#### Reporting

Determine whether management provides satisfactory reports to the board regarding the following:

- Results of ongoing monitoring of third parties involved in critical activities.
- Results of internal audit or independent third-party reviews of the bank's third-party risk management process.

## Appendix 2: What Kinds of Board and Management Reports to Consider

- All third parties
- New third parties
- Critical third parties
- Third parties with breaches or incidents
- Third parties with the highest residual risk
- Operational metrics of the program
- Third parties with noted significant issues
- Third parties with the highest level of inherent risk
- Non-compliant third parties
- Third parties with control issues that are part-due
- Third parties related to an emerging risk
- Third parties about to be terminated
- Contracts with incentive compensation structures
- Presence of concentration risk related to predefined risk thresholds
- Forecasting of contract expiration
- Services with global delivery locations
- Third-party risk scorecard/profile across all applicable risk and performance domains
- Risk treatment distribution (i.e., amount accepted or remediated)
- Population of third parties based on specific criteria (i.e., business area location service)
- Identification of upcoming remediation plan due dates
- Customer/consumer-facing third parties
- Forecasting of upcoming control assessments (to be conducted in the next quarter)



© Copyright 2017 Aravo Solutions  
First Published October 2017





## 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](https://aravo.com)



email us at [info@aravo.com](mailto:info@aravo.com)



call us at +1.415.835.7600 [US]