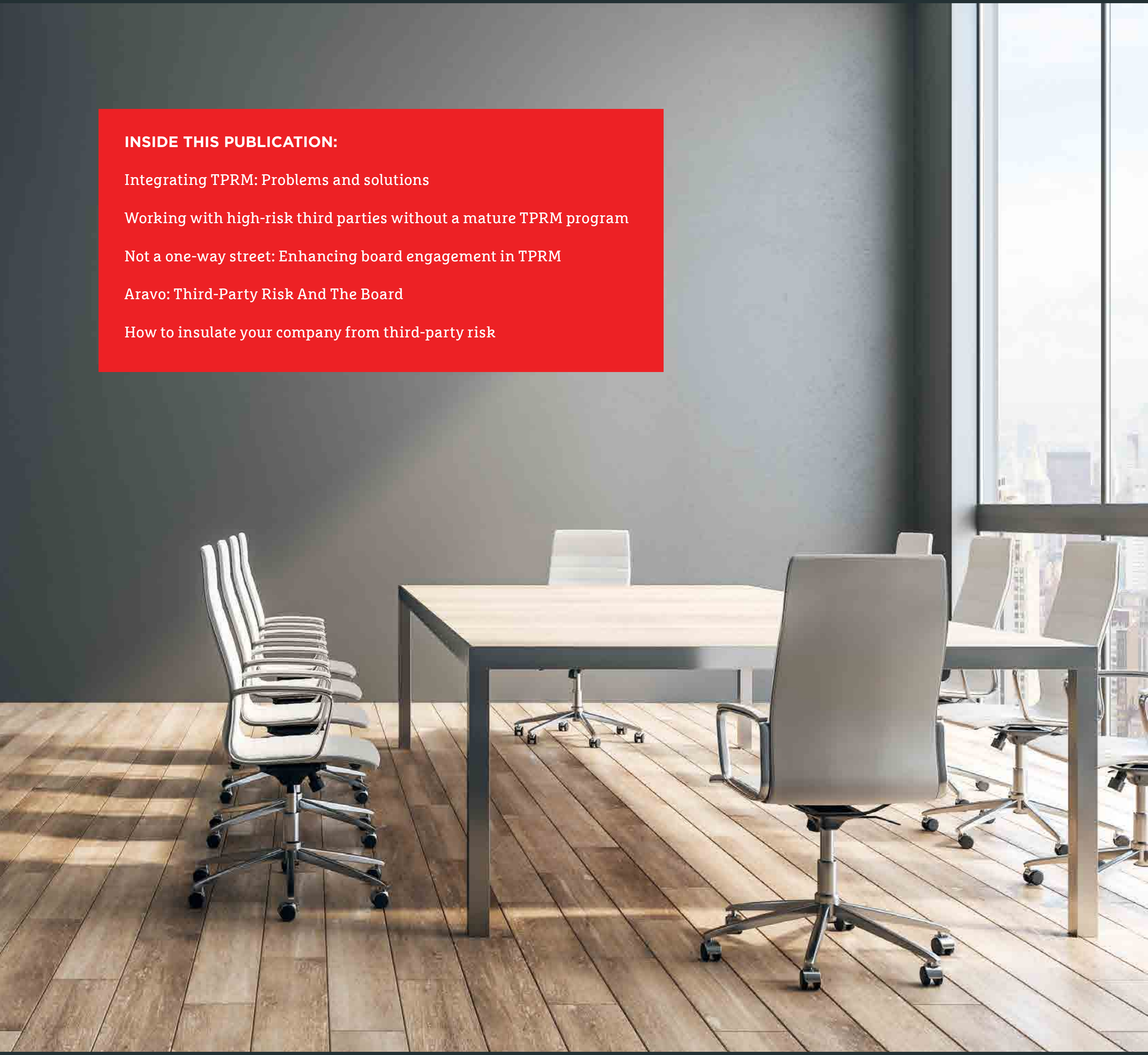
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Integrating TPRM: Problems and solutions

Working with high-risk third parties without a mature TPRM program

Not a one-way street: Enhancing board engagement in TPRM

Aravo: Third-Party Risk And The Board

How to insulate your company from third-party risk

‘Third-Party Governance & Oversight’ 2019 Survey Results

Meeting the expectations of the board

An e-Book publication sponsored by ARAVO

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and infomration service on corporate governance, risk, and compliance that features a daily email newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

ARAVO

Aravo delivers market-leading solutions for understanding, managing, and mitigating the risks posed by third-party vendors and their engagements. Using Aravo, customers maintain a single, auditable inventory of all third-party relationships and can automate risk assessments, scoring, due diligence, continuous monitoring, issue management, and corrective actions. Built on technology designed for usability, agility, and scale, Aravo supports complex custom-configured solutions used by many of the world's largest global brands as well as pre-configured applications that allow clients to stand up a best-practice program quickly and confidently. www.aravo.com

Inside this e-Book

Integrating TPRM: Problems and solutions 4

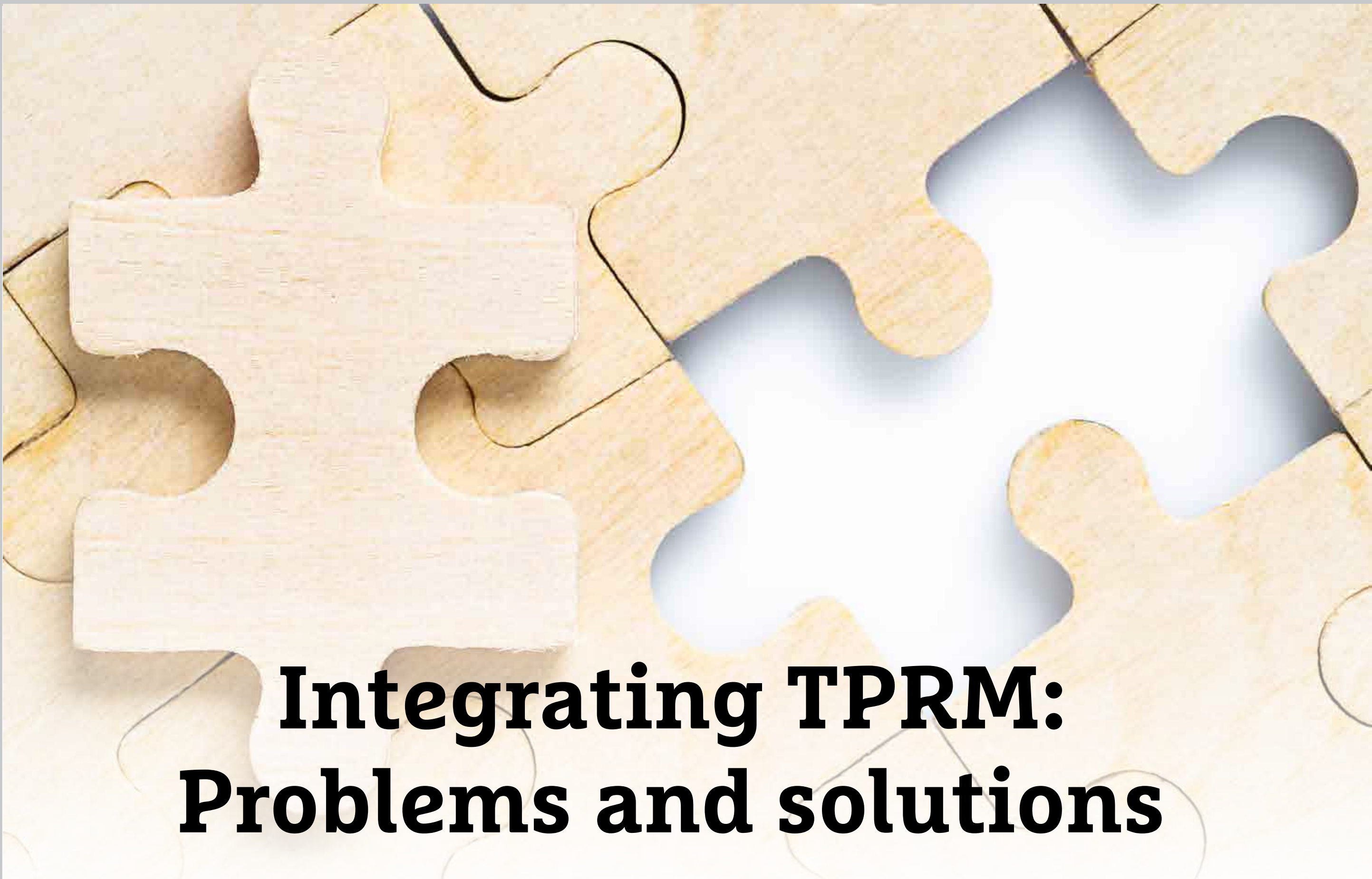
Working with high-risk third parties without a mature TPRM program 8

Not a one-way street: Enhancing board engagement in TPRM 10

More survey results 12

Aravo: Third-Party Risk And The Board 14

How to insulate your company from third-party risk 20



Integrating TPRM: Problems and solutions

The board and C-suite can't afford to be tone deaf when it comes to cultivating a culture of compliance around third parties. **Aly McDevitt** has more.

As more and more businesses expand their footprint internationally, it is increasingly critical for the C-suite, senior management, and board to pay better attention to third-party risk management.

Over two-thirds of the 169 TPRM program stakeholders polled conducted jointly by Compliance Week and Aravo engage with 100 or more third parties. A sliver (16 percent) engage with over 10,000. Almost half (46 percent) work with third parties in high risk areas of the world. And yet, half of the people who identified themselves as TPRM program owners or stakeholders perceive their programs as "evolving"—i.e., defined but unintegrated—with an additional 19 percent calling their programs "fragmented" or "ad hoc."

Our "Third-Party Governance: Meeting the Expectations of the Board" survey found the individual chiefly responsible for TPRM is most likely to be the head of compliance (22 percent), chief financial officer (14 percent), or head of risk (12 percent).

Seeing a diversity of stakeholders responsible for TPRM is a positive, encouraging an abundance of contributors to take ownership of the TPRM program's efficacy.

"Good third-party risk management can't exist in silos," says Kimberly Allan, chief marketing officer at Aravo. "Stakeholders across the enterprise include the relationship manager, compliance, procurement, IT, information security, data privacy, risk, and audit. All of these functions touch part of third-party risk management."

Then again, involving diverse stakeholders is not enough without a common framework established by the leadership team.

"You need a lot of people to come together and agree. It takes strong leadership and a buy-in to a common objective," Allan says. "This is one of the reasons tone from the top and board sponsorship is so important."

Over a quarter (27 percent) of TPRM practitioners say they report to the board infrequently on third-party matters, and another 6 percent say they literally never do. If you don't have a consistent mechanism or process for reporting to the board about third-party matters, that invariably could lead to big problems.

Challenges with board reporting

Some of the biggest challenges survey respondents cite when it comes to TPRM are resource constraints (41 percent); "no golden source of truth" on all third parties (39 percent); and a lack of standardization of processes (38 percent).

Nearly one in three survey respondents (31 percent) say it takes anywhere from one to two weeks to compile a board report on third-party issues. For some companies (18 percent), it takes over three weeks.

"If you are trying to manage third party-risks manually in spreadsheets and e-mail, or in disparate systems across the enterprise, the data will be inconsistent, structured differently, and difficult to aggregate, report on and audit," Allan says.

This checkered communication comes through in the survey results. Around 4 percent of respondents note that board reports on third-party issues are "worryingly incomplete and inaccurate." Only a fraction (17 percent) feel the information they provide to the board is wholly complete and accurate.

"That's something that boards should be taking notice of. At the end of the day, they are accountable, and they could be making decisions based on bad or incomplete data," says Allan.

As for third-party risk assessments, manual processes are highly inefficient considering the sheer volume of information being managed across multiple risk domains, particularly when working with hundreds or thousands of third parties. ("We have clients managing more than a million," remarks Allan.) Moreover, risk assessment is not a one-and-done process. Any third party's risk profile can change, so ongoing monitoring is imperative throughout the duration of the relationship.

IT solutions to fragmentation

Many companies engage in a combination of on-site reviews/assessments, Web search/background checks, screening checks, and questionnaires to collect independent data on third parties. But this flood of data can quickly become unwieldy without a centralized system of organization.

> "The board shouldn't be involved in the day-to-day business of the company. That is the CEO's job."
>
> Amii Barnard-Bahn, Managing Principal,
> Barnard-Bahn Coaching and Consulting

Fortunately, standardized assessments are gaining traction, Allan says. For instance, the Standard Information Gathering (SIG) questionnaire, developed by third-party risk membership program Shared Assessments, is a holistic tool for risk management assessments. Businesses can use it to evaluate their third parties' risk controls in the areas of cyber-security, IT, privacy, data security, and business resiliency.

Another example Allan mentions is Hellios Information, a risk management company that offers standardized qualification and accreditation systems by sector: FSQS for the financial sector; and JOSCAR for the defense, aerospace, and security sectors.

TPRM board committees

Sixty-nine percent of respondents note there is no board committee specifically dedicated to TPRM; instead, third-party issues are typically allocated to an organization's risk or audit committees.

"That is not a surprise to me, I'm afraid," says Amii Barnard-Bahn, managing principal of Barnard-Bahn Coaching and Consulting and a CW columnist. "Board committees are hard to get." She adds, however, "I would expect that in highly regulated industries, companies with primary streams of income completely reliant on third party distribution networks would want to have a committee on [TPRM]."

In the CW/Aravo survey, the small slice of practitioners who currently have a specific TPRM board committee work primarily in financial services (40 percent).

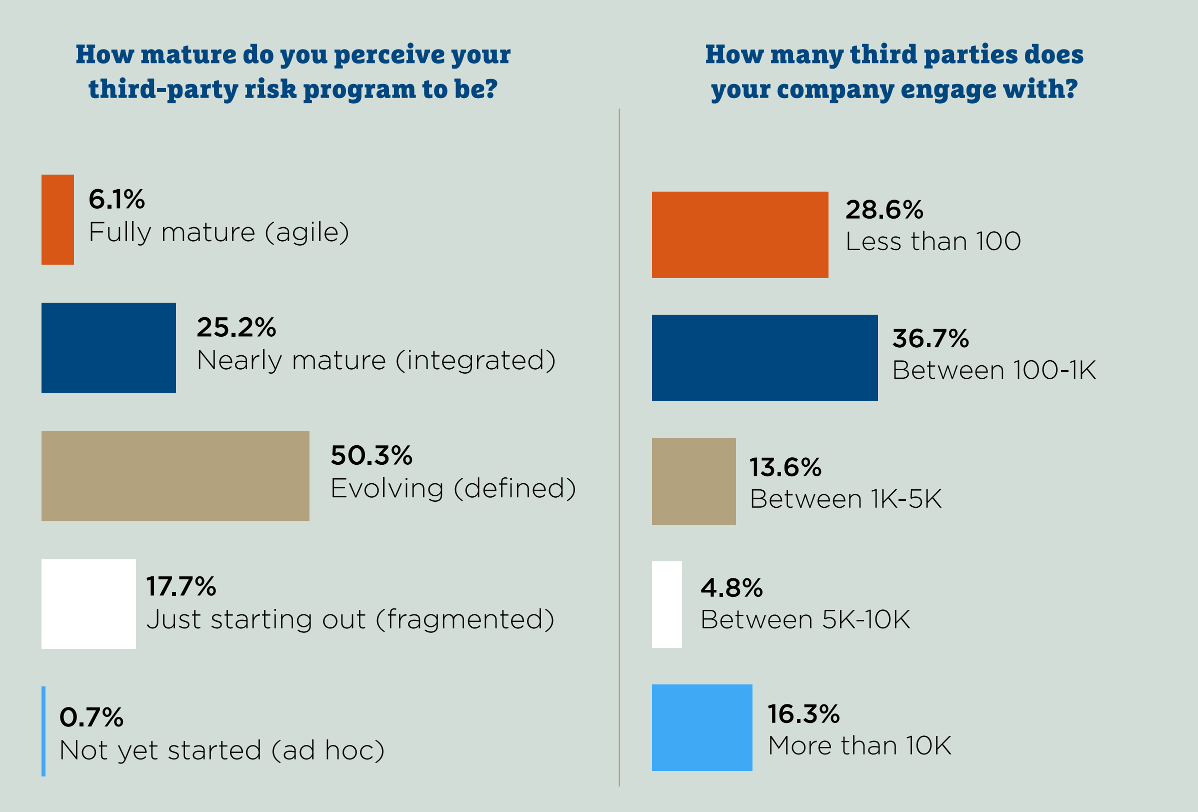
"With AI, use of blockchain, and other advances—which will increase external expectations of effective risk oversight—the velocity and the likelihood of greater risk may be a driver for boards contemplating [a TPRM committee]," predicts Barnard-Bahn.

Enhancing board engagement

The most common third-party issues to come up at board meetings, as well as the greatest concerns from the board's point of view, are cyber-security (69 percent) and data privacy (48 percent).

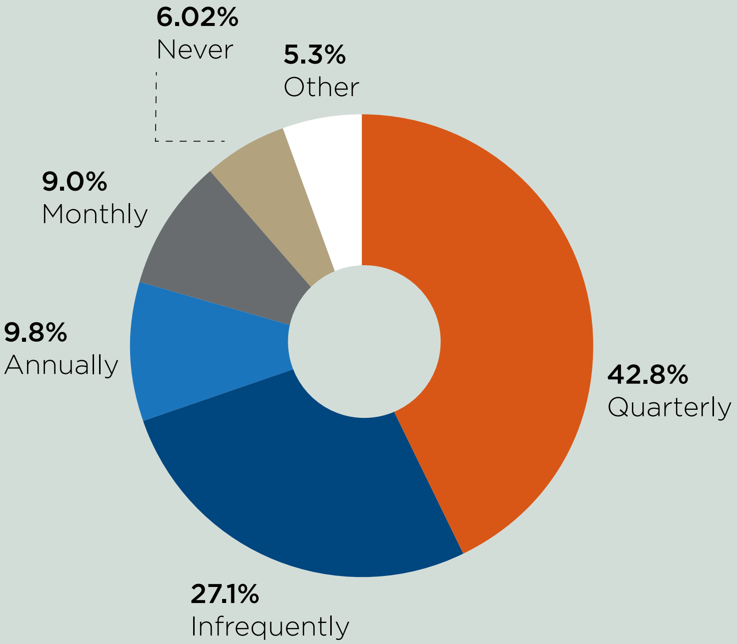
"There are two ways I've seen boards pay more attention to something," Barnard-Bahn explains. "Number one is a crisis. The second ... is when the board and company mindset is future-focused and ripe for change—such that a compliance officer can educate the board around the importance of third-party risk oversight."

Indeed, 76 percent of survey respondents say the board does not play a role in determining which third parties require enhanced due diligence. An-


How mature do you perceive your third-party risk program to be?

How many third parties does your company engage with?

How often do you report to the board on third-party matters?



other 36 percent say their board does not play a role in cutting ties with a third party at all, regardless of financial impact, reputational risk, or criminal wrongdoing.

"The board shouldn't be involved in the day-to-day business of the company," Barnard-Bahn says. "That is the CEO's job. The board's primary responsibility, when you really reduce it, is to hire and fire the CEO and hold the CEO accountable for the results. They're not supposed to get in the weeds."

As companies transition out of the evolving stage of their TPRM program's development, practitioners should consider the following action steps: Get the C-suite and senior management involved from the jump; build uniformity and cohesion around the framework and key objectives of the program; and consider using a standardized assessment to vet vendors and perform due diligence.

As for the board's role in the TPRM program development, it would be extremely beneficial, Barnard-Bahn emphasizes, if there were a board member with expertise in supply chain management to evangelize for the cause:

"If you have a former CEO on your board who had massive supply chain problems with China (for instance), they're going to know great questions to ask. That's terrific. But currently, boards are not being as intentional in seeking risk experience skills in their board recruitment and selection process as they should be. That's like a black swan event right now."

If the board isn't satisfied with the answers to those great questions, it can raise concerns to the CEO and urge the company to allocate more resources from the budget to enhance the TPRM program.

"That's how it could happen," Barnard-Bahn fin-

Working with high-risk third parties without a mature TPRM program

CW survey data shows businesses operating in sanctioned jurisdictions may lack adequate leadership and ethical business practices to mitigate risk effectively. **Aly McDevitt** has more.

Among the 40 percent of 169 respondents to a recent survey who indicated they work with third parties in high-risk areas of the world, just a fraction (3 percent, to be exact) rate their TPRM programs as fully mature. Additionally, about 20 percent of this cohort admit their firms are just starting a TPRM program.

These alarming statistics from the "Third Party Governance & Oversight: Meeting the Expectations of the Board" survey conducted by Compliance Week in partnership with Aravo might demonstrate that this group might not have the right tone at the top.

"If they didn't have ethical business practices as a core value and they felt that financial reward outweighed the potential regulatory censure," they might opt to delay implementation of a robust third-party risk management program, says Kimberley Allan, chief marketing officer at Aravo.

That approach could be a costly one, considering the average monetary sanctions imposed in Foreign Corrupt Practices Act-related actions in 2019 was $113 million to date, according to Stanford Law School's FCPA Clearinghouse.

If this cohort isn't guilty of hubris, it could be naiveté. The majority (59 percent) gauge their TPRM programs as being in an evolving stage of development. These organizations may not have a strong pulse on how to tackle the work required internally to improve their programs—or they're willfully blind to their program's deficits.

"They may feel that their TPRM program is 'good enough' or that getting an effective program in place is too hard—or they don't know where to start," says Allan.

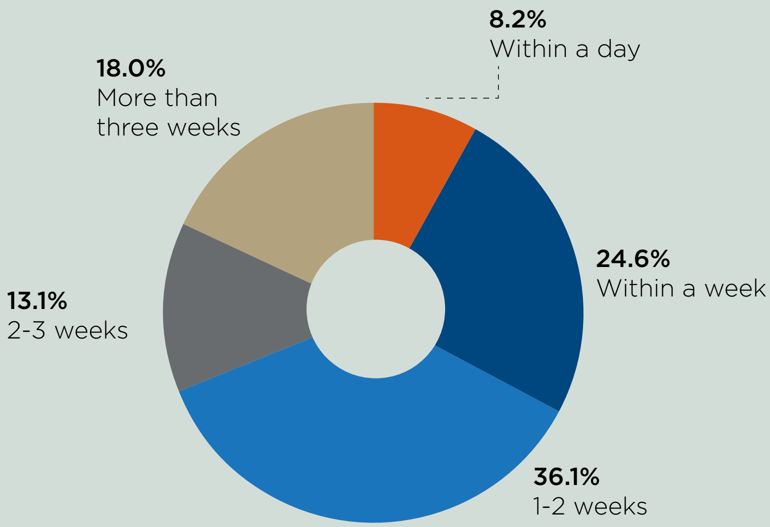
But the risks of third-party relationships don't all come with a straightforward price tag. "The financial penalties themselves don't represent the full cost to the business. Other costs include lawyers, forensic specialists, and post-settlement monitors, and then there's the impact on shareholder value associated with reputational damage of a publicly-disclosed investigation," she says.

Those pesky board reports

Performing a third-party risk assessment and compiling a board report is a laborious process at most companies. Many in this cohort we analyzed (36 percent) say it takes them one to two weeks to compile a third-party board report. And 18 percent say it takes

> "If things come up in that period between one board report and another, you still need to be able to provide reports to the board on things they need to know."
>
> Kimberley Allan, Chief Marketing Officer, Aravo

How long does it take to compile a board report on third-party issues?



over three weeks. Consider that timetable in tandem with the number of third parties a company has in its portfolio. For instance, 31 percent report engaging with over 10,000 third parties.

By necessity then, multinational enterprises (MNEs) should take a risk-based approach to each third party. Score-based ranking systems can break entities into tiers according to their risk profiles, distinguishing third parties that are relatively safe and those that require enhanced due diligence to mitigate increased risk. Entities operating in sanctioned jurisdictions internationally are prime candidates for enhanced due diligence.

The bold and the reckless

Shockingly, 13 percent note they do not report TPRM matters to the board at all.

Nearly one in two (48 percent) indicate they report third-party compliance efforts to the board when important and unexpected issues arise, but 33 percent do so strictly on that basis—which is insufficient. Quarterly reports on third-party matters are a good rule of thumb, and 44 percent abide by that. But that, too, is not enough. It should be a combination of both.

"TPRM programs must also have a sense of agility, because the regulations change, risks change, the relationships that you have with third parties change, and your business changes," warns Allan. "So, if things come up in that period between one board report and another, you still need to be able to provide reports to the board on things they need to know."

Fortunately, 92 percent have fail-safes written into some, if not all, third-party contracts. If warranted, these MNEs could easily sever a third-party relationship. But a fail-safe isn't a "get out of jail free" card. If your company gets caught up with a third party that skirts the rules, you could still be on the hook for reputational and financial damages.

Rather than stoking the fire by resting on the comfort of a fail-safe, MNEs should spend more time going through the process of enhanced due diligence in order to better anticipate and safeguard against avoidable threats. ■

Not a one-way street: Enhancing board engagement in TPRM

It's time to shine a spotlight on TPRM strategy at board meetings, experts say, as 46 percent of surveyed practitioners claim their board doesn't have a good handle on their company's third-party risks. **Aly McDevitt** has more.

Compliance Week's recently concluded third-party risk survey was designed to determine whether companies' TPRM programs are meeting the expectations of their boards of directors. What our results tell us, however, is perhaps it's the boards themselves that need to take a more active role in determining the guidelines and risk appetites for their business partners.

Nearly half (42 percent) of respondents to the "Third Party Governance & Oversight: Meeting the Expectations of the Board" survey, conducted jointly with Aravo, say their board does not set the risk appetite at their organization (and another 19 percent "don't know" whether they do). More than 1 in 3 (36 percent) report the board does not play a role in cutting ties with a third party; and a whopping 76 percent admit their board does not participate in assessing which third parties require enhanced due diligence.

"In my experience, third-party risk is underworked and underappreciated by boards," explains Amii Barnard-Bahn, managing principal of Barnard-Bahn Coaching and Consulting and a Compliance Week columnist. "Frankly, most boards don't do a great job with compliance oversight—period—and third-party risk is a subset of that, so it's unfortunately not a surprise."

Aravo CEO Michael Saracini thinks the board absolutely should be more involved in the oversight of a company's third parties.

"Research indicates that an organization's ability to effectively mitigate third-party risk is tied to greater board involvement. … There is a strong correlation between board involvement in TPRM strategy and TPRM program maturity," Saracini explained to ethicalboardroom.com. Perhaps a lack of in-depth involvement is why so few survey respondents—6 percent—identify their company's TPRM program as fully mature.

While 72 percent of respondents—which include 169 TPRM program owners, overseers, and stakeholders—report regulatory expectations for third-party management are communicated effectively to the board, there is little survey data attesting to open communication from the board. This one-way flow of information is a big missed opportunity for both sides.

The board "has the potential for better optics than anyone," says Barnard-Bahn. "The board has the power to demand the data and to ask the questions."

When asked how engaged their board is with third-party governance, 29 percent of respondents said, "infrequently engaged," and 6 percent said their board was "not at all" engaged. Clearly, there is room for improvement.

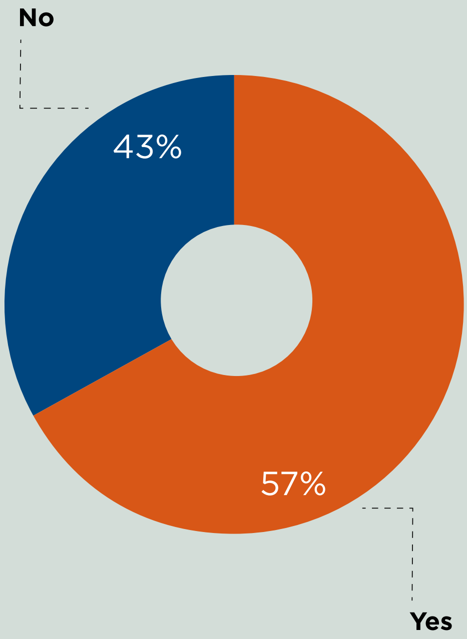
Moreover, the board does not have the luxury of disengagement. In the financial services sector, for instance, "the board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships as if the activity were handled within the institution,” says Kimberley Allan, chief marketing officer at Aravo.

“You can outsource the task, but you can’t outsource the risk.”

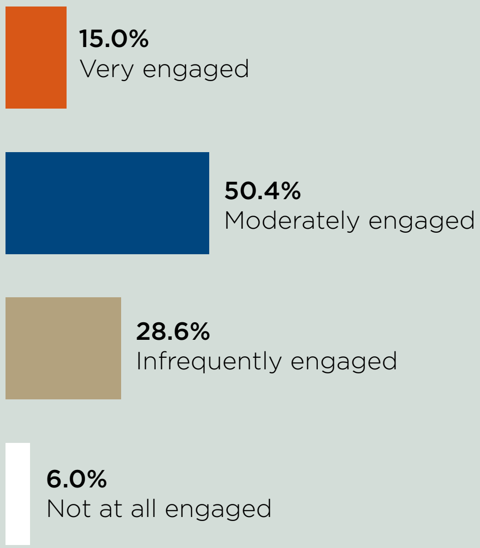
Allan identified seven clear-cut action steps a board can take to better engage and steer the organization toward a more robust TPRM program:

- 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.
- Where appropriate, incentivize third-party risk management through compensation, backed up with organizational metrics.
- Provide adequate training to employees involved with third-party relationships.
- Ensure communications coming from the board are supportive of the third-party risk program.
- Support 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. ■

Generally speaking, do you think your board has a good handle on third-party risks your company is exposed to?

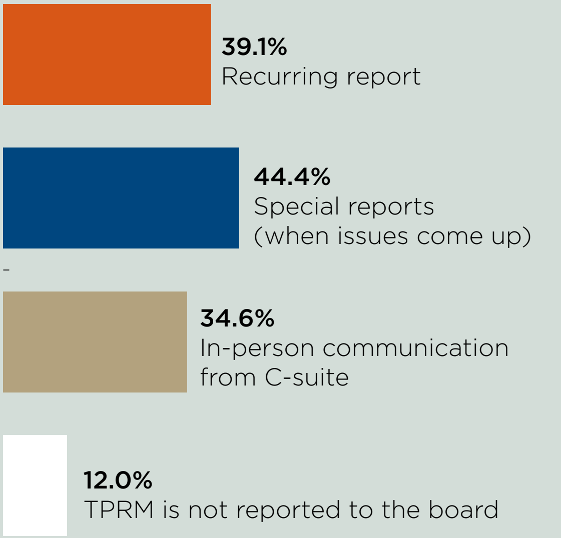


How engaged is your board with third-party governance?

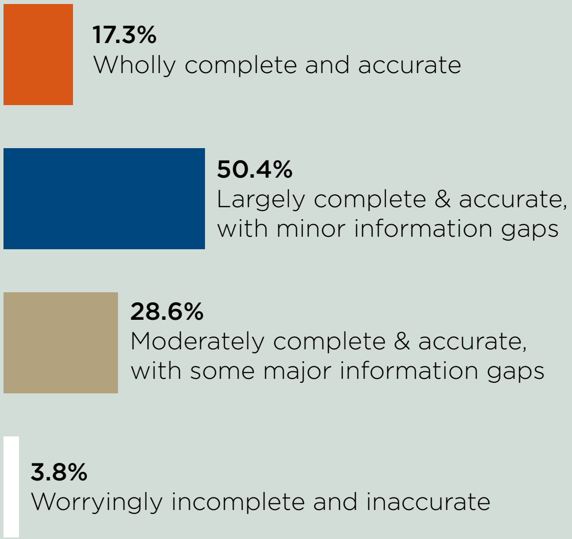


More survey results

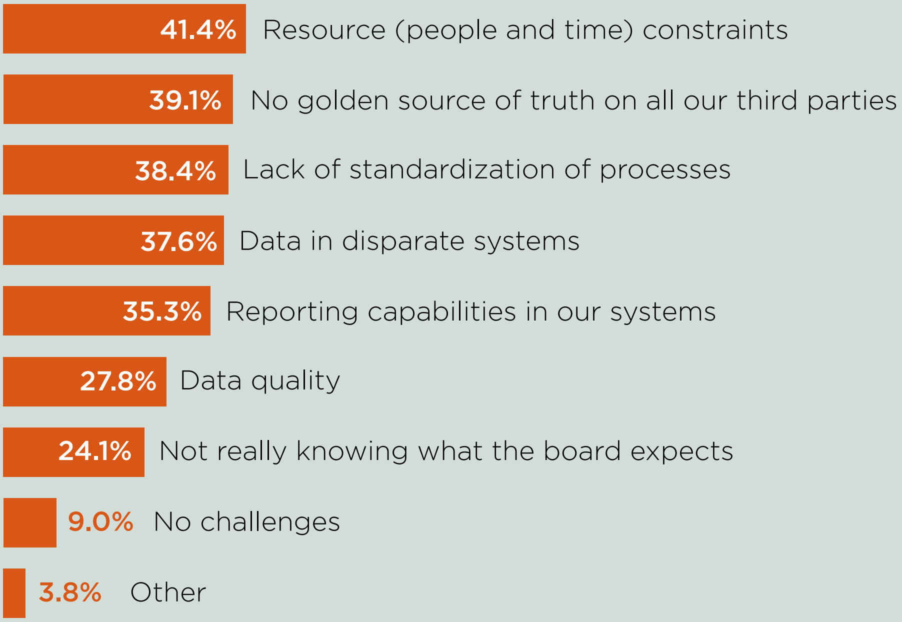
How are third-party compliance efforts reported to the board? (Check all that apply)



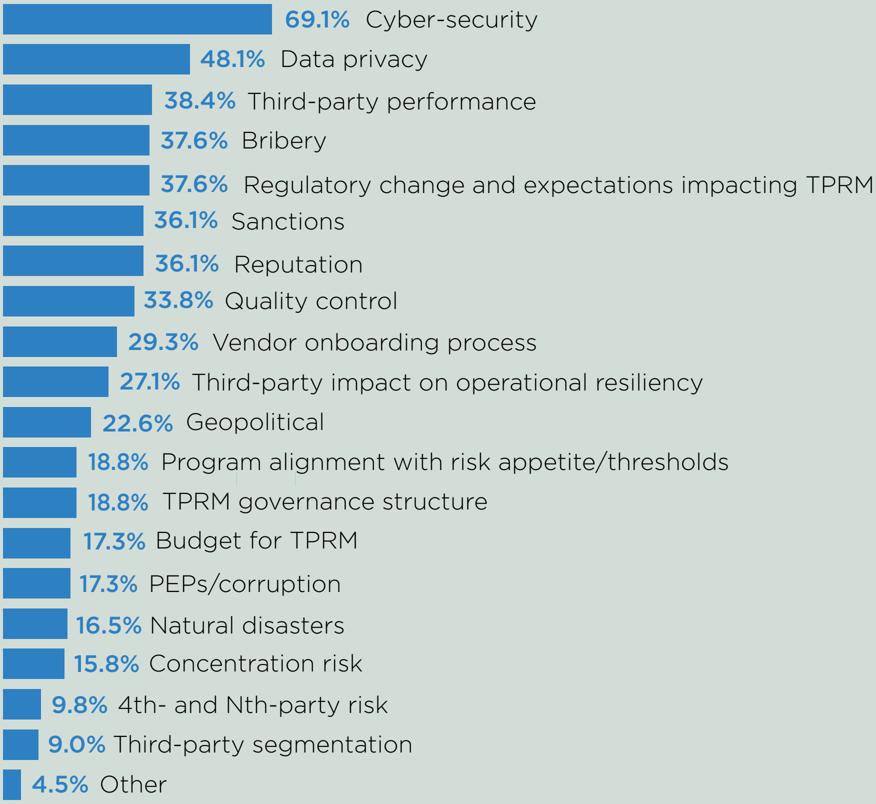
How complete and accurate would you estimate the data to be in your board reports?



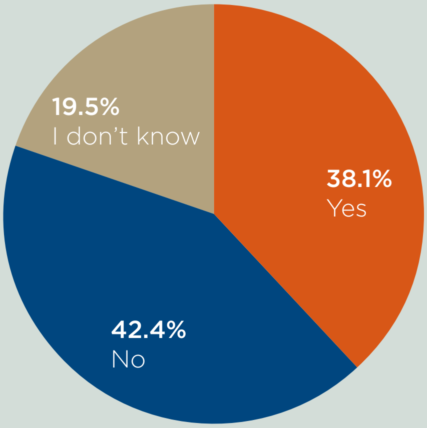
What is the biggest challenge in compiling information on your third-party risk management program for the board?



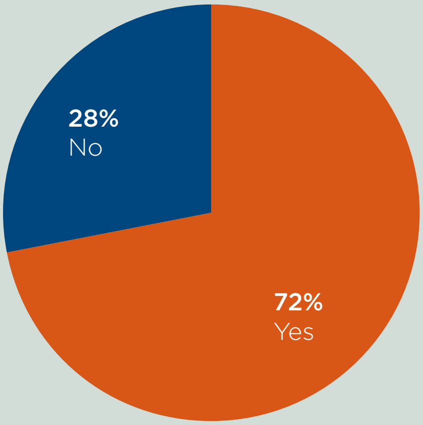
What third-party issues get brought up at the board level? (Select as many as apply)



Has your board set the risk appetite for third-party risk in your organization?



Are regulatory expectations for third-party management communicated effectively to the board?



Third-Party Risk And The Board

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] More than 70% of organizations report that they have a moderate to high dependency on third parties.[2]

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 their 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.

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.

According to a global benchmarking survey of third-party risk management professionals, 75% of respondents' organizations had experienced a third-party incident that either did or had the potential to cause business disruption or reputational damage in the previous 12 months.[3]

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 traced to third-party failures.[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]

43% of respondents did not think that their board had a good handle on third-party risks[6]

31.1% of respondents reported that it would take 2 or more weeks to compile a board report[7]

Only 17.3% of respondents believed the data in their board reporting to be complete and accurate[8]

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 guidance in January 2017. Other regulators globally have also issued guidance in this area. In addition, many new cyber risk-focused regulatory initiatives have a substantial third-party focus.

As a result of this regulatory attention, boards are naturally giving third-party risk – and its management - more of their time and attention.

Third-Party Risk Management

Third-party risk management is a process that allows management to identify, evaluate, monitor and manage the risks associated with an organization's third-parties and their contracts.

With this increased strategic and operational reliance on third-parties comes increased risk which must be identified, understood and managed. This can be a complex exercise as an organization may have many thousands of third-parties, and there are many risks that a third-party can present, including:

Reputational Risk

A risk of loss resulting from damages to an organization's reputation, in lost revenue; increased operating, capital or regulatory costs; or destruction of shareholder value.

Geopolitical Risk

A risk of loss associated with a third-party's ability to meet contractual arrangements due to political, socioeconomic and cultural factors (events, trends, developments) of a specific country or region.

Financial Risk

The risk of loss should a third-party is unable to meet the terms of the contractual arrangements or to otherwise financially perform as agreed.

Regulatory and Compliance Risk

The risk of exposure to legal penalties, financial sanctions and material loss an organization faces when it (or its third-party) fails to act in accordance with industry laws and regulations, internal policies or standards.

Cyber/Information Security Risk

The risk of financial loss, disruption, or reputational damage from a failure of information technology systems.

Concentration Risk

The risk of loss due to lack of diversification. This includes over-reliance on a single vendor as well as geographical concentration of third-parties and their subcontractors in a single place.

Strategic Risk

The risk of loss arising from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with the organization's strategic goals.

Business Continuity and Resiliency Risk

The risk of loss arising from a third-party's ability (or lack thereof) to overcome serious incidents or disasters and resume its normal operations within a reasonably short period.

Operational Risk

The risk loss arising from inadequate or failed procedures, systems or policies. Any event that disrupts business processes.

4th Party Risk

It's not just third-parties that bring risk – it extends to their third-parties and beyond. This is the risk assumed when third-parties use sub-contractors to manage part of their service or product.

Data Privacy Risk

The risk of financial loss, disruption, or reputational damage from a failure to protect personal information.

Bribery and Corruption Risk

The risk of offering, paying or receiving a bribe through an officer, employee, subsidiary, intermediary or any third-party acting on the commercial organization's behalf.

Progressive boards are recognizing that an increased focus on third-party risk makes good business sense given the importance third-parties play in the organization's overall strategic approach.

Good board oversight has an impact on the quality and maturity of third-party risk programs. A recent survey by Aravo and the Centre for Financial Professionals suggests that organizations with a high level of board oversight were more than twice as likely to report that their programs are at the highest level of maturity compared to those with boards that demonstrated only moderate oversight. Of the organizations that reported low board oversight, none of them rated their programs at the highest level of maturity. [9]

Good third-party risk management is also good business. 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, outperforming 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." [10]

But there's more to board oversight fiduciary duty. There is a bigger purpose which has far-reaching implications. Ethical boards and the 'tone from the top' that they and their C-suite deliver, are integral to ensuring that the business acts with integrity and keeps bad business practices – such as corruption, human rights abuses or environmental crime - from their wider business relationships and supply chain. Put simply, boards are not fulfilling their oversight responsibilities if they don't take measures to lead ethical business practices across the enterprise, which includes the third-party ecosystem.

What Is Best Practice For Third-Party Risk Management?

An organization with a mature, agile third party risk management strategy has immediate enterprise visibility into third-party risk at every level: an overview of the inherent risks across the third-party portfolio, a robust risk profile of each individual entity, and insight into third-party risk and performance related to specific contracts or KPIs. To achieve this level of insight and confidence, organizations can follow a few interrelated best practices:

A Federated Approach

A balance of centralized risk management responsibility with participation from business owners and relationship managers allows organizations to standardize third-party risk management policies and procedures. As a single source of truth across risk domains, a federated third-party risk system can generate insights the board needs for high-level oversight as well as be alerted to risks that might be overlooked when information is in silos.

What The Regulators Are Saying

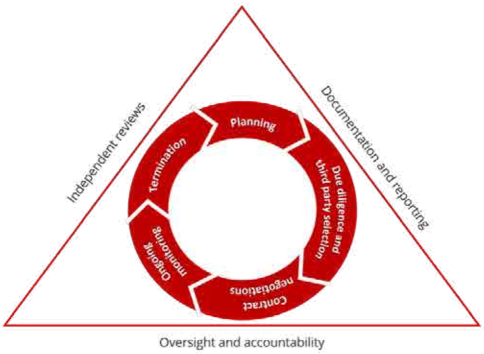
The Board of Directors and senior management are ultimately responsible for managing activities conducted through third-party relationships as if the activity were handled within the institution."
Financial Institution Letter 44-2008 "Guidance for Managing Third-Party Risk"

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

An effective third-party risk management process follows a continuous life cycle for all relationships...
OCC Bulletin 2013-29


Independent reviews
Documentation and reporting
Oversight and accountability
Planning
Due diligence and third party selection
Contract negotiations
Ongoing monitoring
Termination

Source: OCC

For instance, in a disconnected system, leaders may not realize that a third-party has relationships in multiple critical areas and underestimate the risk they present to the organization. If that third-party crossed a risk threshold (like a change of ownership that signaled a corruption risk), it's possible that not everyone would be alerted.

Management of the entire life cycle

Assessing third-party risk isn't a "one and done" exercise. Between onboarding and termination, a third-party's risk profile can change or they may fail to meet contractual obligations and have to go through a remediation process. Juggling documents and spreadsheets for ad hoc third-party risk management processes or cobbling together disconnected silos of third-party risk management practice won't provide the enterprise visibility you need to fulfill your oversight obligations. The organization would also be squandering valuable resources trying to analyze and report on data across the third-party ecosystem while increasing potential exposure to unforeseen risks.

Enterprise visibility

While the board sets the tone for creating a culture of ethical behavior and accountability, multiple people are responsible for executing, sustaining, and auditing third-party risk management policies and procedures. Most of those people also have other responsibilities as well, so it's important that they can easily and securely receive notifications and view the data they need based on their roles, whether in a high-level dashboard, detailed reporting, or by drilling down into specific records. As the centralized system of record, third-party risk management must be able to deliver an enterprise view of the data based on the user's role in the organization.

Secure agility

In addition to changes in risk profile, internal policies and regulatory requirements also change, so organizations need to be able to adapt without prolonged or complicated projects. For instance, the General Data Protection Regulation (GDPR) which came into enforcement in 2018, meant that organizations that hold or processed Personally Identifiable Information (PII) for EU citizens will have needed to evaluate their portfolio of third parties to identify which were in scope with the regulation, assess them for their compliance posture, and ensure reporting and escalation process were in place for reporting to the regulators. With new regulations always coming online, organizations can't afford to be locked in to rigid systems.

Building Effective Third-Party Risk Management Oversight

Identify your risk appetite

As part of their oversight responsibility, board members should agree on and articulate what is an acceptable risk and what isn't. Obviously, there are third-party behaviors that can't be tolerated such as clear ethical and criminal violations, but somewhere between the impossible goal of zero risk and unacceptable behavior, there is a point at which the organization is willing to accept the risk-to-value ratio.

Understanding and evolving the level of acceptable risk requires input and counsel from board members. Larger or more complex organizations may determine varying risk appetites based on factors such as geography, division, or risk type. Certain kinds of risk (such as establishing a critical third-party relationship in a country with high incidence of corruption) call for greater due diligence than others (such as warehouse janitorial services). These thresholds should be built into the third-party risk management system to trigger automatic warnings and remediation when they are exceeded.

Create and support a governance structure

Consistent policies and procedures make it possible for an organization to identify, analyze, and manage risk in a way that can be communicated both internally and externally. To oversee the execution of policies and procedures, many boards are appointing a specific director as the point-person for third-party risk. Some are also establishing managing boards in regions or business units to reinforce both the guidelines as well as the culture of ethical behavior and compliance.

Balancing centralized risk management responsibility with participation from business owners and relationship managers allows organizations to standardize third-party risk management policies and procedures without having to run a "risk business unit." By investing in technology that automates processes and empowers employees to manage risk in a federated system, organizations can impose centralized control without sacrificing overall productivity.

Clearly defined roles and responsibilities

With an overall culture of compliance, there should be clear expectations and accountability across all three lines of defense: 1. Those who own and manage risk (e.g., a business owner or relationship manager), 2. Those responsible for overseeing risk management or compliance (e.g., a risk and compliance executive), and 3. Those who validate compliance with third-party policies and procedures (e.g., internal auditors).

Review regularly

Alarmingly, a 2018 survey by Ernst & Young found that only 22% of organizations report breaches to their boards.[11] Even with the most robust system for managing and understanding third-party risk, the board needs to maintain ongoing oversight. Management should be expected to report on critical KPIs and significant changes, re-mediation/residual risk, and critical relationships that could impact the organization's financial or reputational performance.

The board should review the overall third-party risk management strategy annually to ensure that it stays current with organizational goals and the business ecosystem. While it shouldn't require a complete overhaul, factors such as a change in risk appetite, new initiatives that introduce new risk domains, and changing legislation or enforcement guidance will require adjustments to policies, procedures, and processes.

Regulatory Expectations For Board Members

Recognizing the ethical leadership role of board members, regulators are holding them accountable for poor behavior, which could lead to board shake ups and even personal liability.

Board minutes should reflect board input, review, and approval of third-party risk management strategy as well as remedial actions. Some of the things regulators expect to see included in board minutes of compliant organizations include:

- A record of attendance and participation in regular third-party review meetings
- The methodology for categorizing critical activities
- The approved plan for employing third-parties for critical activities
- Third-party contracts for critical activities
- A summary of due diligence results and ongoing monitoring of third parties involved in critical activities
- Results of periodic internal or independent third-party audits of third-party risk management processes
- Proof of oversight of management efforts to remedy deterioration in performance, material issues, or changing risks identified through internal or external audits.

Supporting With Technology

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, external independent auditors and 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.

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, the business, and 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. Be clear about what kind of information and reports you need from the organization.
- Support the 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.

Third Party Risk Management Maturity Model

SYSTEM	STAGE	PROGRAM
SHARED UTILITY (DATA) FEDERATED - ENTERPRISE WIDE – (TECHNOLOGY) 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 Federated risk management in line with risk appetite of the individual organization Provides enterprise governance Provides a layer of industry governance	**Agile** *Optimized*	Governance model is agreed at the board level and effectively communicated and supported across the organization. Third-party risk appetite and thresholds well defined and understood. Managing risk in an integrated way across multipe domains, with continuous monitoring in place. 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. Agile enough to respond to change.
	Integrated *Established*	Well defined and executed processes at the organizational level. Governance model agreed at Board level. Standardized approach implemented and adopted with documented processes. Third parties are segmented according to agreed-upon and understood criteria. Appropriate skill set and resources, with roles and responsibilities allocated. Statutory/regulatory obligations are met.
CENTRALIZED (ENTERPRISE WIDE) 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 Provides enterprise governance	**Defined**	Well defined and executed processes at the departmental level, with some efforts underway to join up processes across the organization.Roles and responsibilities agreed. A formalized approach is in place with the framework designed and control practices in place.
DECENTRALIZED SILOS Siloed risk management leads to duplication of activities Critical only (no long tail) Per-vendor cost is high Multiple systems & processes Disconnected programs Gaps augment risk (blind spots) Lack of benchmarking Lack of enterprise governance	**Fragmented** *Developing*	Starting to determine a road map, with pockets of good practice emerging. Basic segmentation in place, and some standardization of onboarding registration, and qualification. Some areas of risk management may be in place (ABAC, InfoSec), but are not approached in an integrated or structured way. Framework agreed but not implemented, with required skill sets identified. Governance and processes not fully embedded.
	Ad-hoc *Initial*	Siloed, ad hoc practices. No documented policies or procedures for third party management. No defined program or governance framework. No single inventory of third-party information. No consistent process for due-diligence. Reactive approach that addresses issues as they arise.

Increasing Maturity

Sources:

1,5,10 www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-third-party-governance-risk-management-report.pdf
2 www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-extended-enterprise-risk-management-global-survey-2019.pdf
3,9 www.aravo.com/white_papers/third-party-risk-chasing-maturity-in-a-dynamic-landscape
4 iapp.org/news/a/surprising-stats-on-third-party-vendor-risk-and-breach-likelihood
6,7,8 Third-party Governance & Oversight: Meeting the Expectations of the Board - Compliance Week, Aravo Survey 2019
11 www.ey.com/Publication/vwLUAssets/EY-transforming-your-third-party-risk-into-a-competitive-advantage/$FILE/EY-transforming-your-third-party-risk-into-a-competitive-advantage.pdf

How to insulate your company from third-party risk

As firms increasingly turn to external partners, the risks they acquire can become an internal problem. **Joe Mont** has more.

As if compliance officers don't have enough on their plates, their responsibilities frequently extend beyond the bubble of their own companies and into the ever-expanding, increasingly risky world of third parties, vendors, service providers, and supply chain partners.

As the business world diversifies and goes global, companies more and more are turning to specialized firms to fulfill complicated niche services and meet product needs. Examples include cloud services, emerging technologies, payment services, licensees, and providers of commodities, parts, and finished products.

Although vital, the extended enterprise is nonetheless ripe with escalating risk. A recent Deloitte report detailed some of the reasons why: "During the recession, we saw many organizations push more of their business out to third parties in an effort to reduce internal costs across the extended enterprise. Higher volume, of course, can mean higher risk."

There is also an increasing focus by regulators. Outsourcing doesn't allow you to export your compliance obligations, they say. Guidance issued by the Office of the Comptroller in 2013, for example, laid out its expectations regarding third-party relationships for financial institutions.

It "expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party," OCC examiners wrote. "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."

Institutions, it added, "should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships." An effective risk management process throughout the lifecycle of the relationship includes plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.

The Securities and Exchange Commission and Department of Justice have similarly issued guidance and advisories on the importance of assessing third-party risk, with the latter agency focusing on bribery and violations of the Foreign Corrupt Practices Act.

Steve Klemash, who leads the EY Center for Board Matters, says a starting point for assessing vendor risk starts, quite logically, with an inventory of the third parties partnered with a company.

"Then the assessment gets back to what is the risk appetite, how material are these third parties, and what is the likelihood that something could go wrong? How are they connected to our systems? It actually comes down to just classic business management," he says. "A lot of these organizations are extensions of the enterprise, but it's easy to kind of forget about them when you're just thinking about management and the people you're seeing, day to day, reporting to the board."

Third-party risk must be understood as just another facet of overall, ongoing risk assessments. "It's another risk in the universe," Klemash says. "[These risks] continue to grow given the nature of how businesses are creating more agility through outsourcing and a contingent workforce. You need to understand it from that perspective."

Boards, more so than ever before, need to consider whether third-party risk should fall under their purview. "If something is material, and it has a high likelihood of having a negative impact on the organization, the board is going to spend more time in that area," Klemash says. "If it's not, you're going to let management do their thing. It all depends upon materiality. The more material and significant a vendor is, then boards are more likely to go in and try to

"There needs to be a qualitative and quantitative risk assessment of the relationship. You've got to look at the inherent risk that that third party is bringing to the table and into the relationship. If you don't, you're going to wind up in a relationship where maybe you're managing issues that you should have already thought through."

Tom Grundy, Senior Director, U.S. Advisory Services, Wolters Kluwer understand the contractual terms, understand security, and what happens if something goes wrong."

Tom Grundy, senior director of Wolters Kluwer's U. S. Advisory Services, stresses the importance of managing the "entire lifecycle of the relationship."

"You've got to be able to envision that relationship when it's in place and plan for all aspects of the lifecycle," he says. "Are they a good fit in terms of strategy? Are you going to be able to achieve shared goals? There needs to be a qualitative and quantitative risk assessment of the relationship. You've got to look at the inherent risk that that third party is bringing to the table and into the relationship. If you don't, you're going to wind up in a relationship where maybe you're managing issues that you should have already thought through."

"Third-party risk is getting more complex because it bleeds into so many other areas," says Kristy Grant-Hart, founder and CEO of Spark Compliance and author of "How to be a Wildly Effective Compliance Officer."

"There can be cyber-security risk, modern slavery and supply chain risk, and reputational risks surrounding shareholder activism and social media, particularly around political statements," she says. "If you're closely involved with a company that is making political statements and choices, that can be risky as well."

The biggest challenge Grant-Hart sees is in-company compartmentalization and the "silo effect that has made it so that you really don't get the sort of joined-up due diligence that is required, particularly for big companies in this day and age."

"Moving forward, that will be the biggest push and the biggest requirements as we continue to build compliance and develop more mature systems," she says. "The lack of centralized systems is really problematic, and mergers and acquisitions make that even harder. Data doesn't work together."

Contractual language laid out at the start of a vendor relationship and during renewals can provide a framework for the relationship. The requirement for certain risk-related disclosures should be a key element of that process.

"The contract has to be very clear in establishing expectations," Grundy says. "It's a whole laundry list of things. If you look across industries, there are a lot of common elements that go into these. You've got to have a right of access to data and reporting, so that you can understand what they're doing and what they've promised to do for you. You need to have an understanding about data security standards."

A company should establish service-level agreements to set expectations, including those for a reporting cycle, Grundy says. You can, for example, set expectations for ensuring consumer complaints are handled according to the agreement.

"If you think you have a problem or even if you get the whiff of a problem you haven't confirmed yet, you have to tell us," Grant-Hart says of the preemptive language in a contract that can clarify expectations regarding data breaches, FCPA violations, and sanctions-related problems.

"You try to put the onus on the third party to tell you," she says. "That's pretty effective because then it is the obligation of the third party to proactively tell you. You can put damages clauses in there, attorney's fees, and all sorts of things that make it ugly for the third party if they don't follow through."

Contractual language can also impose audit and termination rights. "When getting audit and termination rights, really think about how they are going to work in practice," Grant-Hart says. "One of the challenges that compliance folks deal with is they need to talk to the business units. It is all well and good to have audit and termination rights, but if it is your most important supplier and it's going to take six months to get a new one, what are you going to do? Are you really going to terminate that contract right now? Do you have a backup supplier? What would that mean in terms of operations, as well as for the compliance and legal team, and prosecution risk?"

Those conundrums tie into another best practice: assessing critical suppliers as part of a risk assess-

"The lack of centralized systems is really problematic, and mergers and acquisitions make that even harder. Data doesn't work together."

Kristy Grant Hart, Founder & CEO, Spark Compliance

ment. "It is important to assess who you can really not manage without," she says.

Grant-Hart stresses the importance of internal auditors when vetting third parties.

"Internal audit is often underutilized, compared to the expense of hiring an external audit firm to go in for a two-week-or-longer assignment. Let's say that there is a requirement for training from your third party, or that they need to submit an annual attestation," she says. "That is a basic internal audit function checkbox. You can see if they're not doing a training every year, for example. If you look for the small things, you can sometimes be clued in that maybe you should look for the bigger ones as well."

A common practice is for companies to send their third-party partners periodic questionnaires and surveys that are intended to better understand their operations, commitment to regulatory compliance, and potential red flags.

Grant-Hart is not a fan of how these questionnaires are traditionally deployed. The idea is good, she says, but forms overthink and overcomplicate the process. "Most of them are far too long and make my head spin," she says.

Expect pushback from vendors, frequently along the lines that certain disclosures could compromise data privacy laws, especially when employee information comes into play.

"There are really good arguments about why due diligence complies with GDPR and why it's necessary," she says. "Then there are people who feel very differently, and we don't really have a good answer from the EU's [statute]. There definitely are divergent opinions about that."

Nevertheless, the exercise can be an informative one, Grant-Hart says, even as she urges that the questions be streamlined. It is important to ask for information about beneficial ownership, for example, although it may require an outside form to properly confirm the provided information for high-risk parties.

Grant-Hart recently published a list of potential questions on her firm's blog.

Sought-after information should include basic company background: the name of key leaders, whether any executives are current or former government officials, the percentage of ownership of each owner, and whether the company is wholly or partially state-owned.

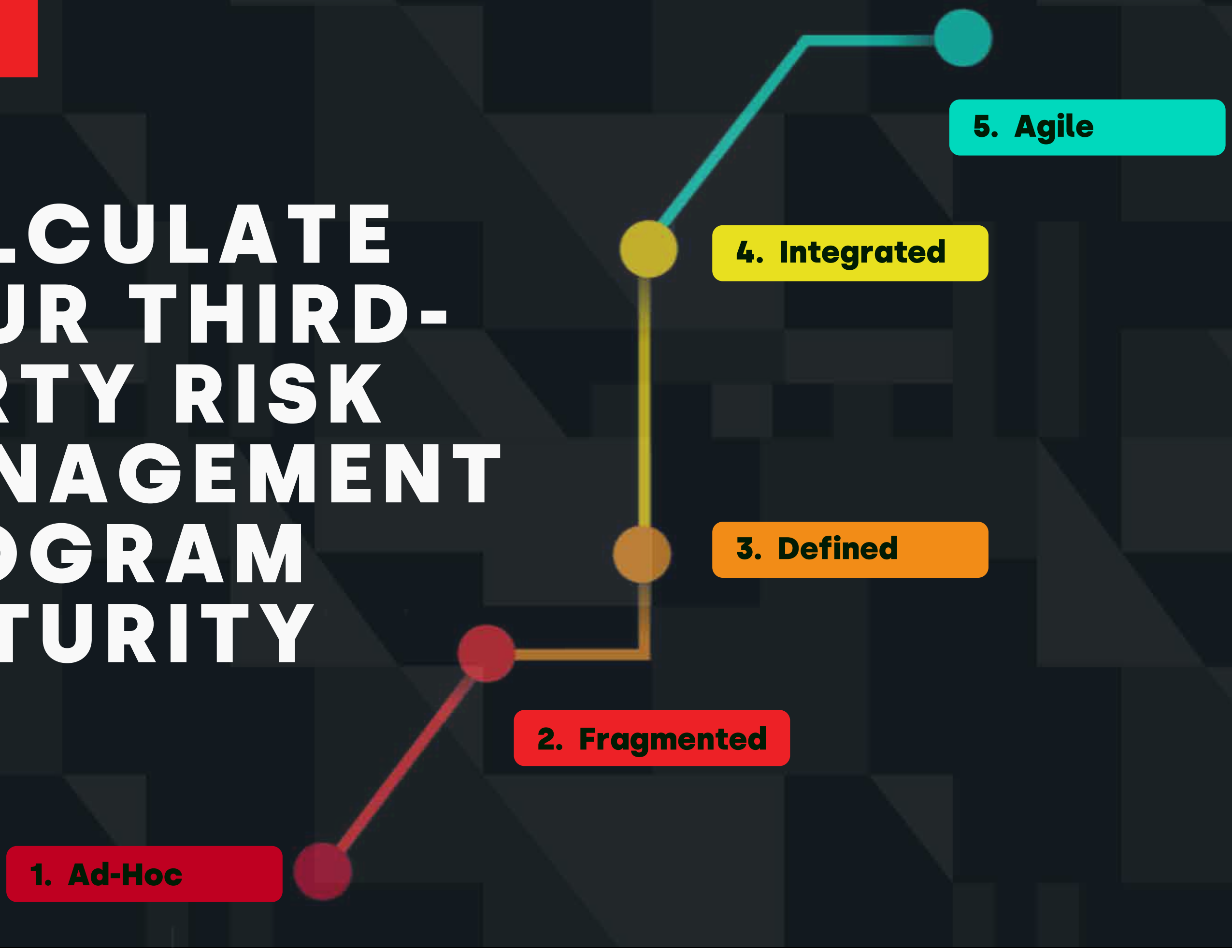
Will the third party be hiring sub-contractors? Is it going to be reimbursed for gifts, hospitality, or entertainment it gives on your behalf? Will the third party be dealing with government officials on your company's behalf?

Other questions to ask:

- Has the third party or its executives ever been convicted of a crime?
- Has anyone associated with the third party been indicted, plead guilty to, or been convicted of a crime related to bribery or corruption?
- Has the company ever been under a consent decree, corporate monitorship, deferred prosecution, or non-prosecution agreement related to bribery or other compliance-related failures?
- Has the third party been included on a sanctions list?
- Is anyone at the third party related to or in an intimate relationship with a person at your company?

A questionnaire can also assess other areas of corporate concern, such as modern slavery prevention, data privacy, information security, anti-trust, and confidentiality, Grant-Hart says. ■

CALCULATE YOUR THIRD-PARTY RISK MANAGEMENT PROGRAM MATURITY



5. Agile
4. Integrated
3. Defined
2. Fragmented
1. Ad-Hoc

Most third-party risk management programs are only six years old, or younger. Every program is on a maturity journey, from Ad-hoc through to Agile.

At what stage is yours?

In order to map your path ahead - it's important to understand where you are on your journey today. That's why Aravo, the market's leading third-party risk management solution provider, created an easy online calculator, so you can calculate the maturity of your program. And take action.

It's free, it takes only five minutes, and you'll receive a detailed, custom report detailing your stage, its charateristics, and importantly, what you should be considering to advance your program to the next stage of maturity.

Free Custom Report

Calculate now at: aravo.com/maturity-calculator