The Business Case For Better Third-Party Risk Management

The Business Case For Better Third-Party Risk Management

Achieving better business outcomes through good third-party governance

You Can't Outsource Responsibility

Third-party risk management is high on the agenda of both the C-suite and the Board of Directors. Leading organizations recognize that the Board holds ultimate responsibility for third-party risk and now often appoint a specific member charged with ownership. Consequently, engagement at the C-suite level has also never been higher.

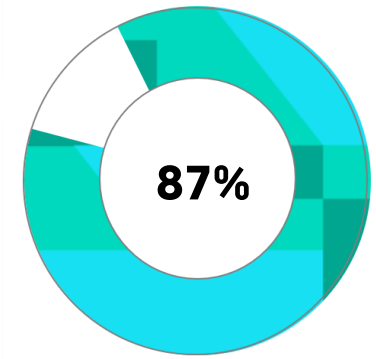
So why is there so much focus on third-party risk? Around the world, regulators have certainly helped elevate the level of attention that third party risk is receiving – with significant sanctions, fines, and the negative headlines that ensue. Regulators have made it quite clear that while organizations can outsource a task, they cannot outsource the responsibility.

Regulators are just a symptom, however, of the underlying issue – the way organizations do business is evolving dramatically and rapidly. And with this, the way they manage risk needs to evolve quickly too.

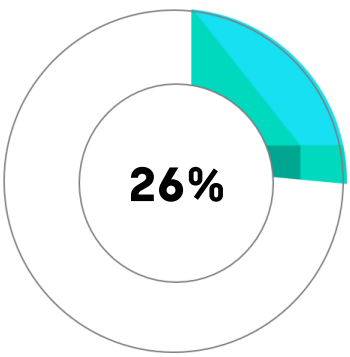
Yet management of the risks that these third parties can create for their partner organizations has often not kept pace with the rate at which the business landscape has evolved.

Some key areas in which third-party relationships can result in damaging loss events include:

- Compliance risk: The third party not complying with essential industry regulations and standards.
- Bribery and corruption risk: Employees of the third party engaging in illegal behaviors in the context, or outside the context, of a third-party relationship.
- Cyber risk: An organization's data could be at risk if a partner isn't adequately protected. Or if it does not abide by increasingly stringent data protection legislation.
- Operational risk: An organization can fail to deliver its products or services to customers if a third party has a significant operational risk issue.
- Reputational risk: Recently many organizations have found their name in the headlines, even though the loss event was caused by a third-party relationship.



of organizations faced a disruptive incident with third parties in the last 2-3 years



of organizations suffered reputational damage due to third parties

A Blinding Lack of Insight

Boards of directors together with their C-suite teams have begun to realize just how little risk information they actually have about their third-party relationships and how fragmented that information can be across even a modest-size organization.

Important data about third-party relationships can sit in a variety of siloes, including procurement systems, traditional GRC platforms, bespoke solutions created to solve a specific information need, or even email, spreadsheets, and documents.

Faced with this blinding lack of unified processes and data, senior executives are discovering that governance of third-party risk needs to evolve rapidly. Today's medium-sized organization may have thousands, or even tens of thousands, of third-party relationships. A large organization could have more than a million. The use of third-party relationships is set to increase even more over the coming decade. As a result, the management of third-party risk is now a strategic priority within many organizations' growth plans.

Building a Best-practice Approach

Given the need for a third-party risk program to meet the requirements of a dynamic organization, business cases for the development of a best-practice approach will usually address seven key benefits.

Each of these should be the outcome of a well-executed third-party risk program – the focus of which should not just be about managing risk but also embracing the opportunities that a better understanding of third-party relationships can provide.

1 Gain real time visibility of third-party risks, organization-wide, for improved decision-making.

Presently, some 65% of companies are unable to report third-party breaches to their Board. More than 60% of companies are unable to generate risk reports for 100% of their third parties. And 55% of companies are unable to generate third-party risk reports in a week or less.

Often the reason behind this poor quality of reporting is the disparate approaches most organizations have to third-party risk information. It is difficult to aggregate information about thousands of third parties that sit across multiple platforms and desktops.

Seven Key Benefits

1. Gain real time visibility of third-party risks, organization-wide, for improved decision-making.
2. Accelerate third-party due diligence, on-boarding, and regular reviews – making the organization a valued business partner.
3. Manage risk – including operational risk and internal controls – better day-to-day.
4. Minimize exposure to reputational risk, compliance risk, and regulatory risk.
5. Ensure good governance of third party programs, including full auditability.
6. Improve strategic and financial outcomes of third-party relationships.
7. Expand third-party and supply networks – and enter into new markets – with confidence.

Important data points such as:

- Third parties with the highest levels of inherent or residual risk
- Customer-/consumer-facing third parties
- Third parties related to an emerging risk
- Non-compliant third parties
- Third parties with breaches or incidents

can so easily slip through the cracks of a program that is not technologically unified.

This lack of a single version of the truth at the Board level of most organizations undermines the ability of Directors to carry out their key governance function in the area of third party risk. It can result in significant blind spots – not just for risks but also for opportunities. It impairs decision-making and can result in a lack of business agility.

Technology Should Be an Enabler

A third party risk program should be able to use technology to integrate sources of information across the business – collating and collecting data and putting it into context through good visual reporting. It should also be able to do this quickly – so that reporting is available "right now" in real time.

As a result of improved reporting, the Board, the C-suite, and the entire organization will be empowered to make more informed decisions about third-party risks – from their impact on strategy, down to day-to-day choices about individual third parties in the business.

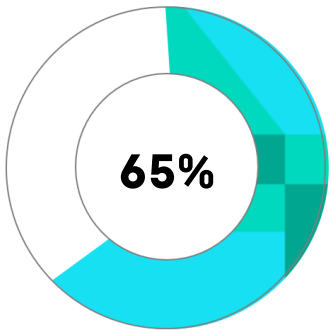
Additionally, the Board and C-suite will have dramatically improved governance of third party risk, and be able to rapidly identify issues that need resolving in the business.

Companies that develop this more mature approach to risk management, which includes the ability to manage third party risk at the enterprise level, experience clear financial business advantage. Studies have found that companies that have a mature risk framework, generated three times the level of EBITDA as those without. Investment in better risk management pays dividends.

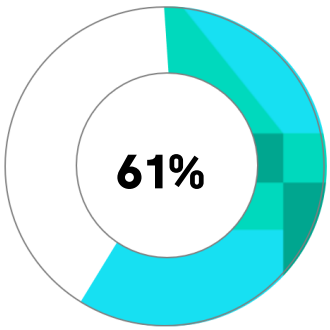
BUSINESS DRIVERS FULFILLED

Improve profitability: Better, faster decision making to drive better business performance.

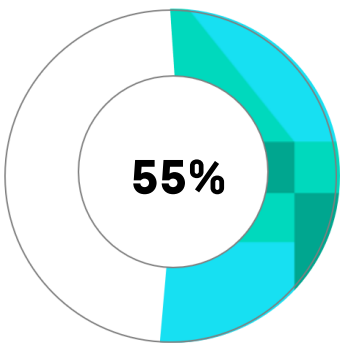
Protect business value: Protect against financial and reputational risk losses from penalties, sanctions, and negative media headlines.



of companies are unable to report third-party breaches to the board



of companies are unable to generate risk reports for 100% of their third parties



of companies are unable to generate risk reports in a week or less

2 Accelerate third party due diligence, on-boarding, and regular reviews – making the organization a valued business partner.

It's a simple fact of life – organizations that are easier to do business with get more business.

Today's world of complex compliance requirements for third-party programs can often tax even the best relationships. Bringing a new third party into the business requires organizations to:

- Identify risks within the new relationship
- Prioritize risks for assessment and management
- Conduct risk assessments
- Perform and record due diligence/EDD activities
- Ensure risk, compliance and performance requirements are incorporated into contracts
- Manage contracts, including segment expiration

Of course, the need to manage third-party risk doesn't end with a successful on-boarding. Ongoing relationships need careful management too – often these can be a significant source of unidentified issues if they are not monitored properly.

A good program should:

- Record and monitor against KPIs
- Conduct risk assessments across all risk profiles, including operational, compliance, performance, concentration, etc.
- Document and escalate issues
- Schedule third party reviews
- Provide real time risk reporting of program outcomes

Organizations that undertake these processes in a manual, ad-hoc or non-integrated way often encounter delays in on-boarding new third parties or in re-affirming existing relationships, which can damage the collaborative ecosystem that the organizations wish to build together.

Lost documentation, un-aligned processes, technology limitations, and other issues can drag out the time it takes and the resources required to complete these processes. It can also lead to compliance gaps.

Even more importantly, a non-integrated approach to these processes means that important metrics – data crucial to the third party risk governance process – is not being captured in a systematic way. And data that isn't captured cannot be reported on.

In summary, a robust approach to due diligence, on-boarding, and regular reviews should significantly enhance the collaborative ecosystem between organizations and third parties through shorter and more efficient processes that are fully compliant. Capturing and reporting on risk information obtained during these processes in a systematic way – to improve the management of risk – should become the cornerstone of a strong third-party risk program.

...a robust approach to due diligence, on-boarding, and regular reviews should significantly enhance the collaborative ecosystem between organizations and third parties through shorter and more efficient processes that are fully compliant.

BUSINESS DRIVERS FULFILLED

Reduce business costs: Reduce time and costs associated with on-boarding and monitoring.

Maintain regulatory compliance: At on-boarding and as an ongoing process.

Protect business value: Protect against financial and reputational risk losses from penalties, sanctions, and negative media headlines.

3 Manage risk – including operational risk and internal controls – better day-to-day.

Nearly nine out of ten organizations faced a disruptive incident with third parties over the past two-to-three years. More than one-quarter suffered reputational damage. This translates into significant financial impact – fines, customer reparations, and other revenue losses now stretch into billions of dollars for large multinationals that fail to manage third parties appropriately.

Share prices suffer too, with Deloitte estimating a 2.55% reduction in share value as the result of a regulatory sanction.

High priority risk areas in third party relationships include:

- Breakdown in customer service
- Breaching a regulation or law
- Suffering reputational damage
- Disruption in the supply chain
- Experiencing financial fraud or exposure
- Business failure of third party derailing delivery

The Three Lines of Defense

Managing operational risks and ensuring the correct controls are in place across the "Three Lines of Defense" in an organization requires information, collaboration, and communication. Dozens of stakeholders within an organization will be involved in managing the operational risks and controls associated with a single third party. It's nearly impossible to understand risks a third party might pose in context if information about those risks is not in a single, central source of truth.

Share prices suffer too, with Deloitte estimating a 2.55% reduction in share value as the result of a regulatory sanction.

The First Line of Defense

For example, the business – always the First Line of Defense in managing risk – may not have appropriate feedback mechanisms to guide it in the choices it makes about the third parties it works with. Even more worrying, it may not have the information it needs to understand whether a third-party relationship is a suitable solution to a particular business challenge.

Without easy access to information about operational risks and controls – information that the business can use, and therefore perceive as being "of value" – it's unlikely to engage wholeheartedly in a collaborative ecosystem around third-party risk management. Even worse, a third-party risk program that results in delays and problems with customer on-boarding, due diligence, and ongoing review can be perceived by the business as a source of operational risk in and of itself.

The Second Line of Defense

Risk and Compliance – the Second Line of Defense – face a different set of challenges. Too often risk and compliance programs that are not supported by the correct governance structure and technology platform find themselves focusing on the wrong things. For example, the effort required to collate information from a variety of incompatible systems can be a manual, spreadsheet-driven process.

Instead of analyzing and working across the Three Lines of Defense to better manage risks and controls, these two key teams wind up focusing on their own internal process – depriving the organization of the significant value these teams could be generating.

The Third Line of Defense

As for the Third Line of Defense – not having third party risk information in a format that is easily auditable by either internal or external auditors – that valued third line of defense – can lead to costly annual audits, perceptions of risk that may be skewed by the presence or absence of information, and missing the opportunity to identify key internal control needs.

It's clear that having the right approach to a third-party program in place can dramatically improve operational risk and internal control outcomes by ensuring all Three Lines of Defense have the information they need to be mindful of internal controls and act in a risk-aware way.

Having the right program and technology in place can deliver further benefits, however. It's obvious that today's organizations are constantly evolving – organizational structures can change significantly over relatively short periods of time; businesses are bought and sold; and new and unexpected risks can emerge.

Having a single source of truth across a whole third-party risk program should enable organizations to more quickly pivot their responses to these changes – helping the business to be more nimble.

Having a single source of truth across a whole third party risk program should enable organizations to more quickly pivot their responses to these changes – helping the business to be more nimble.

BUSINESS DRIVERS FULFILLED

Increase business agility: Respond to business and regulatory change quickly and efficiently.

Reduce costs: Reduce time and costs associated with program management and change.

Protect value: Potential for disruptive incidents/impact minimized through better risk management across all three lines of defense.

4 Minimize exposure to reputational risk, compliance risk and regulatory risk

Despite being an elevated source of potential compliance and legal risk, third party compliance is too often overlooked or even placed in the 'too-hard' basket. With a focus on compliance within the figurative 'four-walls' of an enterprise, companies are failing to properly consider the impact of their 'extended enterprise.'

But, under the FCPA, the EU's General Data Protection Regulation (GDPR) and other regulations, not only do organizations need to keep their own houses in order – they need to be confident in the compliance of their third parties' houses as well. Executives need to ask - into whose hands is the organization placing its brand reputation that has taken so much time and investment to build? Who has the potential to expose the enterprise to significant financial penalty? More often than not, third parties are the greatest area of risk exposure – for data security and for regulatory compliance.

Managing the Pace of Regulatory Change

Regulatory change – given the volume of new rules that are in the works, many with extraterritorial components – is also a crucial challenge for most third party risk programs. If programs are not flexible and adaptable both in their governance structure and in the underlying technology that supports them, they are doomed to come unstuck through failure to adapt quickly and correctly to new third-party risk rules.

Having the correct approach to third party risk management can help organizations ensure that the businesses they partner with are compliant with all existing rules and regulations that impact the relationship. It can also help the organization – and as a result, its partners – better adapt to changes to those rules. The end result is not just a more robust, compliant organization, but also an organization that is in a better position to avoid significant reputational risk losses from penalties, sanctions, and media headlines.

A typical financial services organization deals with an average of 182 - at times conflicting - regulatory developments on a daily basis.

Source: Thomson Reuters

BUSINESS DRIVERS FULFILLED

Protect business value: Protect against financial and reputational risk losses from penalties, sanctions, and negative media headlines.

Maintain regulatory compliance: Even as regulations change

5 Ensure good governance of third-party programs, including full auditability

Boards and the C-Suite of global organizations are lacking oversight of their third parties at the enterprise level. While there may be robust programs operating at the business unit or regional level, they are not rolling up into a single, clear view of enterprise risk.

An Increase in Personal Liability

This lack of insight comes at the same time as increased personal liability of senior executives for compliance failures. New emphasis has been placed on director and officer personal criminal liability as an enforcement priority by regulators, elevating the personal (not solely business) impact of governance shortcomings.

With a lack of unified processes and data, executives are exposed. Their biggest risk is what they don't know. All too often, there are different processes and systems for different parts of a third party's relationship with the enterprise and disconnected systems and processes for each compliance program (such as data security, anti-bribery and corruption and responsible sourcing). All these disconnects add to enterprise governance risk.

A Federated Approach to Third Party Risk is Essential

Third-party risk management needs to be a federated process, that results in a single source of truth across all third parties. This requires full third-party life cycle management, starting at data collection and including due diligence and third party selection; contracting and on-boarding; management and monitoring; and terminating and off-boarding.

But, at the same time, there's the business reality of multiple sources of data across an enterprise that exist in ERP and procure-to-pay systems that are a critical part of business operations. Enterprises need to identify a third-party risk management system that provides the flexibility to integrate with these and ingest, validate, de-duplicate, clean. and feed back critical data, all the while acting as the single source of truth for risk and compliance business processes and reporting.

> *I continue to believe that prosecuting individuals – and levying substantial criminal fines against corporations – are the best ways to capture the attention of the business community.*

Then-Assistant Attorney General for the Criminal Division, DoJ, Lanny Breuer

Audit

The ability to be able to audit the program is also a critical component of governance. When data and records are in disparate systems and desktops across the enterprise, audit becomes incredibly inefficient and resource intensive. It also speaks volumes about the overarching governance and compliance standards of the organization, raising red flags to any regulator. Best practice programs are supported by an audit ready solution for third party risk.

BUSINESS DRIVERS FULFILLED

Protect business value: Protect against financial and reputational risk losses from penalties, sanctions, and negative media headlines. Help keep executives out of jail.

Reduce costs: Reduce time and costs associated with program audits

6 Improve strategic and financial outcomes of third-party relationships

Most Boards and C-suites are now focused on how they can engage in third-party relationships from a strategic perspective – what areas of their organization they should be working with third parties on to reduce costs, reallocate resources, and improve the value that is delivered to the business.

But Boards and C-suites need to understand that a strategic decision to work with third parties for a particular area of the business doesn't end with that "yes" choice. To succeed with a third-party strategy, Boards and C-suites need to consider the governance and processes they need to put in place to ensure the risks that are associated with third party relationships are managed properly. They need to explore the investment needed to create a truly collaborative ecosystem with third parties. And they need to ensure they put the right reporting and information-sharing programs in place.

The rewards from taking such an approach are many. Two key ones are:

- Improve strategic outcomes – a robust third-party risk management program can help ensure that the objectives for the third-party strategy are actually delivered.
- Increase financial metrics – better managing risk and controls associated with third-party programs make them more likely to hit their financial targets, feeding directly into organizational profitability and shareholder value.

The ability to be able to audit the program is also a critical component of governance. When data and records are in disparate systems and desktops across the enterprise, audit becomes incredibly inefficient and resource intensive.

Good third-party risk programs help ensure that the direction the Board and C-suite set are carried out across all Three Lines of Defense, so that strategic aims are fulfilled.

BUSINESS DRIVERS FULFILLED

Grow business value: Through optimized third-party performance.

Support business resiliency: Ensure that business resiliency is factored into third-party and fourth-party relationships.

7 Expand third-party and supply networks – and enter into new markets – with confidence

Implementing or improving an organization's third party risk management program isn't just about ensuring that today's strategic goals are delivered. It's about the future, too.

One of the biggest reasons why Boards and C-suites decide not to work with third parties – and potentially increase profitability and shareholder value – is fear of the unknown risks they might encounter. This reason also accounts for decisions to not enter into new, potentially lucrative geographic or category markets.

Having a strong third-party risk management program can help provide Boards and C-suites with the information they need to make more informed, risk-aware decisions.

Businesses exist to grow, and having a strong third party risk program in place can enable Boards and C-suite teams to make decisions on new plans that involve third-party partners with confidence.

Having a strong third party risk management program can help provide Boards and C-suites with the information they need to make more informed, risk-aware decisions.

BUSINESS DRIVERS FULFILLED

Grow business value: Through optimized performance, expansion, and innovation opportunities associated with third parties.

Approaching An Enterprise Program

In reviewing the business case for third-party risk management programs, it's clear there are significant benefits for an organization that makes the investment of time and resources. Organizations looking to establish or review their approach to third-party risk should review the existing state-of-play around:

- Tone from the top: How is internal messaging about third-party risk being handled?
- Ownership: Who owns third-party risk in the organization? It is the right role?
- Information: Where does data about third-party relationships sit? Where ought it to be?
- Relationship: How does the current third-party risk management arrangements impact the collaborative ecosystem?
- Regulation: What should an organization's third parties comply with? Are they?
- Communication: How well is information about third-party risk harvested from the organization, analyzed, and reported back?
- Decision: Is information about third-party risk regularly incorporated into the strategic thinking of the Board and C-suite?

Program Rewards

Having the right building blocks in place is important. And, with a good program in place, Boards and C-suites can have more confidence when they move into a new relationship.

Third-party programs can help:

- Raise awareness of current risk issues with similar relationships
- Flag control challenges with similar relationships
- Identify regulatory frameworks that need to be implemented for a given relationship, based on industry and geography
- Help the organization perform due diligence, or enhanced due diligence, on potential third-party partners.
- Put new third-party partners through a robust on-boarding program that has a track record of success in identifying issues
- Ensure new third-party partners are re-assessed at intervals appropriate to the risk they pose
- Communicate information about the progress of the third-party partnership, emerging risks, and other information to stakeholders quickly and clearly.

OUTCOMES

Third party risk programs – done well – can add significant value to an organization over time, enabling it to execute on strategy, improve profitability, and enhance its reputation.

...in the spirit of promoting a culture of integrity, I want to leave you with the wisdom of this ancient proverb: if you desire to know a person's character, consider his friends. You can help protect your business by using caution when selecting associates and by ensuring appropriate oversight. Always make sure that you can stand proudly with the company you keep.

Deputy Attorney General Rod J. Rosenstein
Keynote Address on FCPA Enforcement Developments
Washington, DC ~ Thursday, March 7, 2019

Third-Party Risk Management Application

Aravo for Third-Party Risk Management is a software-as-a-service application that allows you to understand, manage, and mitigate the risks posed by your third-party vendors and their engagements.

With Aravo's base Third-Party Risk Management Application you can maintain a single inventory of all your third-party relationships and automate inherent risk assessments, scoring, due diligence, continuous monitoring, issue management, and corrective action processes.

Because it comes with a package of pre-defined capabilities, you can stand up a best-practice program quickly and confidently.

> To be compliant today requires a defensible record of due diligence and monitoring of third party relationships. To do this in manual processes encumbered by documents, spreadsheets, and emails is ineffective, inefficient, and certainly not agile. Manual processes also lack a robust audit trail and system of record to defend the organization.
>
> Michael Rasmussen, GRC 20/20

Key Benefits

- Achieve a single version of the truth. Delivers a standardized and centralized process for managing all your third parties and their engagements, which cuts through data and business silos.
- Drives efficiency and reduces costs. Reduces operational burden with automated processes, saving time and resource.
- Deliver confidence in your program to senior management and regulators. Real-time reporting and complete auditability mean you can demonstrate compliance to the board, senior management, auditors, and examiners.
- Mature your program faster and scale easily. Built on technology that helps you mature your program faster and supports the scale, complexity, and change dynamics associated with third-party management programs.

End-to-end third-party risk management

Engineered to automate and accelerate your best practice third party risk management program.

Centralize all your third parties, and their engagements into a single inventory

- Deliver a standardized process for the intake and scoping of new third parties and initiating new engagements
- Gather relevant documents, certifications, policies, and data
- Gain a single source of truth about vendors and their engagements

Actively manage third-party issues and remediation activity

- Identify and report issues
- Initiate action plans for remediation
- Involve cross functional teams and the third party in the issue resolution process
- Manage offboarding plans

Understand and manage the risk associated with third-parties and their engagements

- Automated inherent risk assessment
- Segment third parties by criticality and inherent risk score at the enterprise, entity, and engagement levels
- Determine the level of exposure to your organization across multiple risk domains
- Be alerted to changes in risk and compliance posture for issue management and remedial action.

Report and monitor with complete visibility across the organization

- Real-time reporting and analytics
- Reporting at the enterprise, entity, and engagement levels
- Role-based dashboards – dynamically drill into any detail
- Full audit trail across the entire third-party risk management process.

Conduct third-party inherent risk due diligence

- Automatically send scoped due diligence assessments based on engagement
- Screen and validate third-party information
- Ongoing monitoring for changes in risk profile to trigger remedial action

> Robust functionality and excellent features. Good user interface, covers all features and cost effective. I Highly recommend.

Procurement Consultant,
Healthcare Provider.
Gartner Peer Insights

> Best fit for our requirements, transparent and capability to handle greater volume of requests with ease.

Process Lead,
Financial Services Firm
Gartner Peer Insights

> Aravo's strength for me lies in its traceability and high level of automation

Social Accountability Manager, Global Manufacturing Firm
Gartner Peer Insights

> Implementation takes no time, great features and excellent functionality.

Sr. Procurement Executive
Services Industry
Gartner Peer Insights

Core capabilities to stand up your program quickly

The base third-party risk management application comes with predefined:

Standard data model for

- Third Parties
- Contacts
- Engagements
- Issues
- Corrective Actions

Standard questionnaires, templates and workflow for

- Initial Third Party Registration and Pre-Qualification
- Initiating New Engagements
- Off-boarding and Termination

Standard workflows for

- Issues and Corrective Actions
- Escalations
- Alerts
- Ongoing monitoring
- Renewals

Standard roles

- Relationship manager
- LOD 1 (Business)
- LOD 2 (Controls)
- LOD 3 (Audit)
- Third Party
- Exec Management
- BOD
- Administrator

Inherent risk scoring for

- Compliance Risk
- Operational Risk
- Strategic Risk

Integrated Financial Risk Scoring

- Based on Altman-Z Score

Workflows process visualization

- Drag-and-drop change management
- Full audit trail, including attestations

Integrated Sanctions/Restricted Party and Corruption checks

- US Consolidated Screening List
- Corruption Perception Index Risk aligned with Transparency International
- Google geolocation
- UNSPSC product standardization

Standard Reports

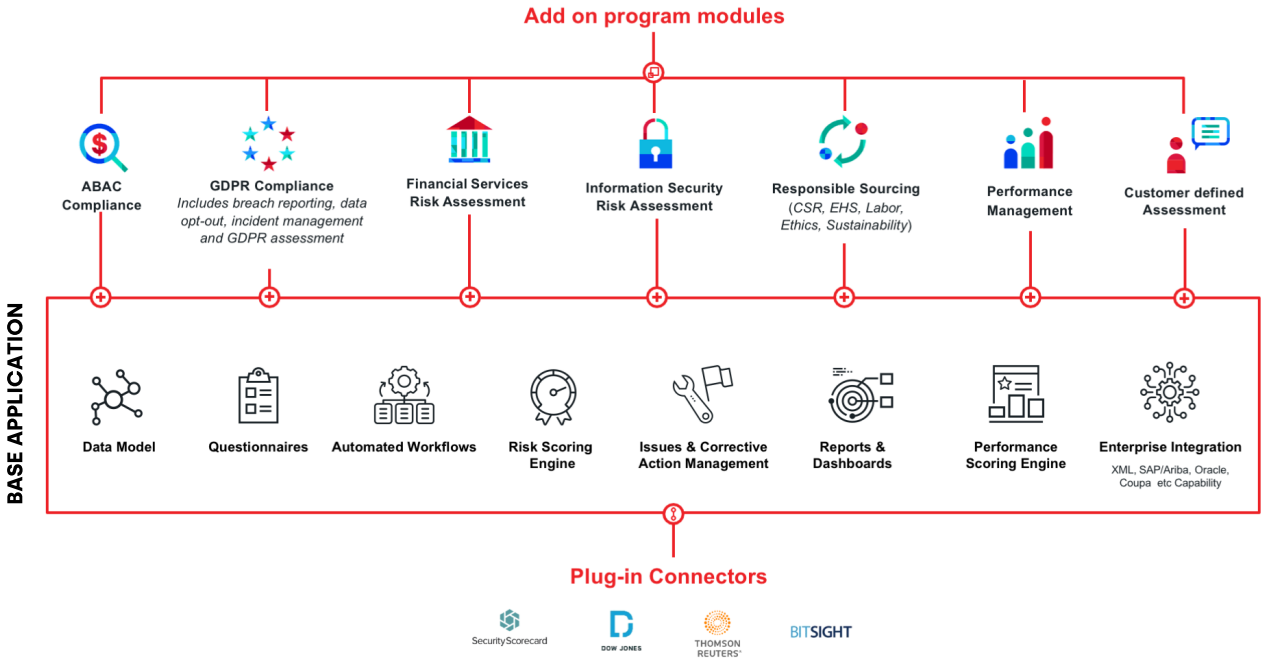
- Third Party Status Report
- Third Party Inherent Risk Report
- Third Party Engagement Status Report
- Third Party Offboarding Status Report
- Denied Third Party Report
- Third Party Termination Due Report
- Third Party Termination Due Report
- Issue Detail Report
- Corrective Action Details Report
- Third Party Compliance Risk Report
- Email Notification Status Report
- Business Process Status Report
- Active and Inactive Users with Roles Report

Standard Dashboards

- Third Party Overview
- Inherent Risk Scores
- Inherent Risk Tiers
- Compliance Risk
- Third Parties
- Tasks
- Reports
- Engagements
- Issues
- Corrective Actions
- Operational Metrics

Core capabilities to stand up your program quickly

The base third-party risk management application comes with a set of pre-predefined capabilities designed to help you stand up and accelerate your program, quickly, and extend it as required. You can add programs and/or connectors to the base application in line with your program requirements.



Future-proof your third-party governance, risk and compliance

Aravo's product suite is built on a single unified code base, which means that you have virtually limitless options when it comes to updating, modifying, or expanding your program without custom coding. The most common ways to extend your Aravo Third-Party Risk Management base application include:

Specialized risk and compliance solutions from Aravo. Pre-configured solutions for GDPR, anti-bribery/anti-corruption, and information security are built to leverage Aravo's Third Party Risk Management base application to quickly address new risk areas. They include assessments, workflows, and reporting specific to the risk domain that rolls up into the overall risk assessments.

Third-party data integrations. Many organizations leverage outside data sources to refine the results of risk models. Aravo's open architecture allows for easy integration with commonly used data providers as well as enterprise applications.

Custom-configured solutions to meet unique corporate requirements. Aravo's flexible, configurable technology architecture lets you define your own assessments, workflows, and questionnaires that can be added to the Aravo Third Party Risk Management base application. For instance, you might conduct additional screening during registration (such as health and safety), have a compliance workflow process that is unique to your organization, or want to send questionnaires to third parties to learn more about their capabilities or conduct a satisfaction survey. Aravo's experienced professional services team can help you design and configure these solutions according to industry best practices.

For more information about Aravo's base Third-Party Risk Management Application go to www.aravo.com or contact us for a demo.

+1.415.835.7600 info@aravo.com

ARAVO

The Definition of Better Business

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

Contact

For more information:

visit us at aravo.com

email us at info@aravo.com

call us at +1.415.835.7600 [US]