April 2022

360° Risk Intelligence in the Extended Enterprise

Ensuring Agility, Resiliency & Integrity in Third-Party Performance

STRATEGY***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

©2022 GRC 20/20 Research, LLC. All Rights Reserved.

No part of this publication may be reproduced, adapted, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of GRC 20/20 Research, LLC. If you are authorized to access this publication, your use of it is subject to the Usage Guidelines established in client contract.

The information contained in this publication is believed to be accurate and has been obtained from sources believed to be reliable but cannot be guaranteed and is subject to change. GRC 20/20 accepts no liability whatever for actions taken based on information that may subsequently prove to be incorrect or errors in analysis. This research contains opinions of GRC 20/20 analysts and should not be construed as statements of fact. GRC 20/20 disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. Although GRC 20/20 may include a discussion of related legal issues, GRC 20/20 does not provide legal advice or services and its research should not be construed or used as such.

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

©GRC 20/20 Research, LLC; Redistribution Rights Granted to Supply Wisdom

360° Risk Intelligence in the Extended Enterprise

Ensuring Agility, Resiliency & Integrity in Third-Party Performance

The Modern Organization is an Interconnected Web of Relationships

The structure and reality of business today has changed. Traditional brick-and-mortar business is a thing of the past: physical buildings and conventional employees no longer define the organization. Instead, the modern organization is an interconnected web of relationships, interactions, and transactions that extend far beyond traditional business boundaries. Even the smallest organization can have dozens of relationships that they depend on for goods, services, processes, and transactions. In large organizations, this can expand to tens of thousands of third-party relationships with suppliers, vendors, partners, and service providers.

With businesses increasingly relying on a complex network of third-party relationships to thrive, the governance, risk management, and compliance (GRC) of third-party relationships become even more critical. Without effective GRC, organizations will fail to manage uncertainty, avoid disruptions, act with integrity, and achieve business objectives.

In a dynamic risk environment, resiliency requires agility and the ability to navigate great uncertainty. Effectively mitigating the exposure of potentially disruptive events requires real-time and comprehensive risk intelligence with insights to both assess the current and future risk landscape and drive sagacious action.

The Inevitability of Failure: Fragmented Views of Third-Party Risk

Too often, organizations struggle to adequately govern their third-party relationships because of their reliance on outdated practices. Recent technological advances in automation, machine learning, and data science enable organizations to be more effective and do more with fewer resources, but unfortunately, too many organizations have failed to seize the opportunity to evolve beyond expensive and inefficient legacy solutions.

Failure in third-party GRC comes about when organizations rely on outdated risk practices including:

- **Silos of third-party oversight.** Silos of oversight occur when an organization allows different business functions to conduct third-party oversight without coordination, collaboration, and architecture. The risk posed by a third party for one business function may seem immaterial but is actually significant when factored into multiple risk exposures across all of the business functions relying on the same third party. Without a single pane of visibility into the risk in their

third-party relationships, silos leave the organization blind to risk exposures that are material when aggregated.

- **Limited resources to handle growing risk and regulatory concerns.** Organizations are facing a barrage of increasing regulatory requirements and an ever-expanding risk landscape. While risk functions are operating with limited budgets and human teams, they need to do more with less. In reality, truly effective continuous monitoring and mitigation of today's dynamic and ever-expanding risk landscape is beyond human capabilities alone.

- **Overreliance on manual processes.** When organizations govern third-party relationships in a maze of documents, spreadsheets, emails, and file shares, it is easy for risks to be missed amidst the extensive volume of data. In addition, when things go wrong, these manual processes neither support agility nor a robust feedback loop to improve processes going forward.

- **Limited view of risk vectors.** Organizations often over-rely on third-party financial and cyber risk management and suffer from risk exposure in domains such as compliance, operations, ESG, location and Nth parties. To fully understand the complete risk picture, an organization needs to have full-spectrum risk coverage.

- **Scattered third-party risk solutions.** When different parts of the organization use different third-party risk solutions, silos of risk data and intelligence are created that are difficult to assimilate, thus making it difficult to maintain, aggregate and provide comprehensive, accurate, and current third-party analysis. The resulting redundancies and inefficiencies make organizations less agile and impact the effectiveness of third-party risk programs.

- **Overreliance on Periodic Assessments.** For many organizations, third-party risk analysis occurs primarily during the onboarding process at the onset of the business relationship with only periodic re-assessment of risk over the length of the engagement. This approach fails to keep organizations informed in a timely manner when the risk exposure changes between assessments. Without a continuous source of real-time risk intelligence feeds, the organization lacks the ongoing situational awareness necessary for proactive risk mitigation.

- **Inadequate incident response.** How organizations respond to incidents can often dictate how quickly and adequately they mitigate risk. Most enterprises often respond to an incident today by sending a survey to all their third parties asking them if they have been impacted. This process takes time, often with low response rates and then has the added burden of how to assess and report on the responses. Most importantly, this is at a point in time and so often a wasted effort. Incidents and impact often unfold over time and the best approach is one that is real-time and continuous.

- **Negative news services can overwhelm risk teams.** Risk intelligence has the potential to overwhelm organizations. Information feeds from various sources such as legal, regulatory updates, newsletters, websites, emails, journals, blogs,

tweets, and content aggregators can drown the risk team as they struggle to monitor a growing array of regulations, legislation, corporate ratings, geopolitical risk, and enforcement actions. Risk intelligence that requires weeding through an exorbitant volume of notifications that includes noise and false positives to identify relevant risks only compounds the problem. One needs an intelligent system that can deliver accurate and actionable insights and remove the noise.

The bottom line: The modern business is dependent on third-party relationships and requires real-time and continuous awareness of its current and future risk landscape. A manual and point-in-time approach to third-party risk intelligence compounds the problem and can lead to elevated risk exposure. It is time for organizations to step back and move from legacy practices, defined by manual processes and periodic assessments, to a third-party risk intelligence architecture that includes integrated full-spectrum real-time feeds of situational awareness that impacts the extended enterprise and operations.

Delivering 360° Third-Party Risk Situational Awareness

A dynamic business environment requires the capability to actively manage risk intelligence and fluctuating risks impacting the organization and its relationships. The old paradigm of uncoordinated third-party risk management is inadequate given the volume of risk information, the pace of change, and the broader operational impact on today's business environment and operations. Organizations need to address third-party risk intelligence with an integrated strategy and an enterprise-wide information architecture that provides 360° third-party risk situational awareness. The goal is to provide actionable and relevant risk intelligence to support third-party risk governance and oversight to ensure the organization is agile, resilient, and acting with integrity in its business relationships.

Third-Party Risk Intelligence Architecture: Core Elements

Comprehensive 360° situational awareness requires a system to gather information, weed out irrelevant information, route critical information to subject matter experts (SMEs) for analysis, track accountability, and determine the potential impact on the organization. Therefore, an effective enterprise-wide third-party risk intelligence architecture includes:

- **A Comprehensive Risk Framework.** The third-party risk framework should be a hierarchical and comprehensive catalog/index of third-party risk domains with the potential to impact the organization. Third-party risk domains should be further broken into categories comprised of individual risk metrics logically grouped into related areas (e.g., ESG risk domain would include risk categories of Environmental, Social, and Governance. The Social category would include sub-category risk metrics related to diversity & inclusion, pay equality, health & safety, child labor, human rights, etc.).

- **Intelligence content aggregation.** The organization needs to identify the best sources of risk intelligence. Content feeds can come directly from various sources - regulators, law firms, consultancies, news feeds, blogs by experts, etc. - or from content aggregators. It must be mapped to the risk intelligence framework.

The most economical and efficient way to address this need is through a risk intelligence provider that leverages automation and AI to aggregate risk content while removing noise and false positives. Additionally, there can be great efficiencies and cost savings that can be realized by leveraging a single solution that can provide a comprehensive and consistent view.

- **Metrics, dashboarding & reporting.** To govern and report on the third-party risk intelligence process, the organization needs the ability to monitor metrics and reports to determine process adherence, risk/performance indicators, and risk issues and exposure. The dashboards should provide the organization with a quick view into the current risk exposure and potential emerging risks, which individuals are responsible for triage and/or impact analysis and overall risk impact on the organization.

- **Defined roles and responsibilities.** Successful risk management requires accountability: making sure the right information gets to the right person with knowledge of the risk domain and its impact on the organization. This requires the identification of SMEs for each risk category defined in the taxonomy. This can be subdivided into SMEs with particular expertise in categories, metrics, or specific jurisdictions, or who perform specific actions as part of a series of changes to address risk developments and exposure.

- **Workflow and task management.** Real-time third-party risk intelligence feeds into a risk management platform providing a system of structured accountability to manage changes based on business impact analysis. Workflow and task management route details and required actions to the appropriate SMEs for further analysis with escalation capabilities when items are past due. The process tracks accountability on who is assigned risk tasks, establish priorities, and determine appropriate course of action. Automation is leveraged to handle routine risk mitigation actions, freeing up team members to focus on only the most critical risks that require human intervention. Organizations use technology to document, communicate, report, monitor change, and facilitate business impact analysis of third-party risk developments.

Third-Party Risk Intelligence Architecture: Additional Capabilities

In addition to the core elements, the following additional capabilities provide further value to a third-party risk intelligence architecture:

- **Accountability.** A primary directive of a third-party risk intelligence architecture is to provide accountability. Accountability needs to be tracked as risk information is routed to the right SME to review and define actions. The SME should be notified when further evaluation is necessary and given a deadline based on an initial criticality ranking. The SME must be able to reroute the task if it was improperly assigned or forward it to others for input. Individuals and/or groups of SMEs must have visibility into their assignments and time frames. The built-in automatic notification and alert functionality with configurable workflows facilitate risk intelligence in the context of the organization's operations and its third-party relationships.

- **Business impact analysis.** The architecture needs to provide the functionality to identify the impact of changes in risks on the third-party business environment and its operations and then communicate to relevant areas of the organization how the development impacts them. This is conducted through a detailed business impact analysis in the platform and is facilitated by being able to tag risk areas/domains to respective business relationships, services, and operations. The overall system needs to be able to keep track of changes by assessing their impact and triggering preventive and corrective actions. Furthermore, the solution ensures that stakeholders and owners are informed, tasks related to actions are assigned, and due dates for the completion of actions/tasks are defined.

- **Mapping risks, policies, controls and more.** A critical component to evaluate is the architecture's ability to link third-party risks to assessments, policies, controls, reports, and processes. The ability to map to business lines, products, and geographies allows companies to manage a risk-based approach to third party developments and strategy. The workflow automatically alerts relevant stakeholders for necessary action and relationship changes. It also supports electronic signoffs at departmental and functional levels that roll up for executive certifications on risk exposure and acceptance. Mapping is another area where artificial intelligence/cognitive technologies are providing greater efficiency and effectiveness value for third-party risk intelligence.

- **Audit trail and system of record.** It is absolutely necessary that the risk architecture have a full audit trail to see who was assigned a task, what they did, what was noted, notes that were updated, and be able to track what was changed. This enables the organization to provide full accountability and insight into whom, how, and when risks were reviewed, measure the impact on the organization, and record what actions were recommended or taken.

- **Reporting capabilities.** The architecture is to provide full reporting and dashboard capabilities for clear visibility into the risks monitored, task assignments, overdue actions, and the identification of issues that pose the most significant risk to the organization's third-party relationships. Additionally, by linking risk intelligence to the various other aspects of the platform – including relationships, processes, objectives, policies, controls, and more – the reporting should provide an aggregated view of a risk across multiple relationships and business owners.

Third-Party Risk Intelligence Architecture: Provider Considerations

The right third-party risk information and technology architecture allows risk experts to profile risks, link with sources and content aggregators, push new developments or alerts into the application and disseminate for further review and analysis. It delivers effectiveness and efficiency, using technology for workflow, task management, and accountability documentation—allowing the organization to be agile amidst change. It enables the organization to harness internal and external information and be intelligent about third-party environments and developments globally.

In evaluating third-party risk intelligence solutions that integrate risk intelligence and technology, organizations should ask the following key questions:

- **What is the quality and speed of the risk intelligence?** Keeping up with the volume of risk data can be a challenge in today's dynamic risk environment. While some organizations hire analysts to comb through mountains of risk data, technological advancements including natural language processing, predictive analytics, machine learning, and robotic process automation can make this process more efficient, effective, and agile. Not only can a machine read it, sort it, categorize it, and link risk information much faster than humans, but it also works around the clock. After evaluating of the possibility of an in-house solution, most organizations will find that it is more practical, efficient, and economical to partner with a risk intelligence provider that leverages automation to aggregate their risk content. As the risk intelligence quality and capabilities of third-party risk intelligence providers vary greatly, careful consideration should be made when evaluating third-party risk intelligence solutions including:

- **How comprehensive is the risk intelligence?** Evaluation of solutions should consider the breadth and depth of risk coverage, supporting analysis, and actionable guidance and should identify information such as geographic area/jurisdiction, issuing source, subject, and guidance. Ideally, the guidance should give commentary on how risk alerts are effectively transformed into actionable tasks and modifications to protect the business and its extended enterprise. True 360° situational awareness requires risk intelligence across a full spectrum of risks that go beyond financial and cyber to include other risks such as ESG, compliance, operations, Nth parties, and location factors including geopolitical risks.

- **How frequent are the updates?** Today many cyber intelligence solutions are continuous and provide real-time updates, however, few solutions covering other risk domains are continuous. More advanced solutions provide full-spectrum risk intelligence that leverages automation to continuously monitor thousands of information sources for risk events and risk trends that need to be monitored closely. This capability helps ensure that third-party risk teams are up to date on new, changing, or evolving risk developments. The best solutions provide real-time alerting and update risk metrics and reports in real-time across all risk domains.

- **What is the quality of the risk intelligence?** Many solutions that leverage automation like a negative news service are plagued with a high percentage of noise and false positives forcing risk teams to commit considerable resources to risk identification. More advanced solutions will leverage cognitive technologies and artificial intelligence to cleanse the data, thus enabling risk teams to shift resources from risk identification to instead focus on critical risk mitigation efforts.

- **How strong is the solutions technology?** Most risk management solutions provide workflow and task management capabilities. The evaluation of the solution needs to go deeper to assess its ability to integrate risk intelligence feeds, conduct business impact analysis, and understand the risk impacts to

relationships and processes. As SMEs across the enterprise may not be technical gurus, an intuitive user experience is also a plus.

- **How flexible is the solution?** As no two organizations are identical in their third-party risk processes, taxonomy, regulations, structure, and responsibilities, the system must be fully configurable and flexible to fit the organization's third-party risk intelligence architecture.

Third-Party Risk Intelligence Architecture: Value

The right third-party risk information architecture allows risk experts to profile risks, link with sources and content aggregators, push new developments or alerts into the application, and disseminate for further review and analysis. It delivers efficiency, effectiveness, and agility, using technology for workflow, task management, and accountability documentation—allowing the organization to be agile amidst change. It enables the organization to harness internal and external information and be intelligent about third-party environments and developments globally in order to secure supply chains, mitigate or even avoid disruptions, and ensure resiliency.

- **Effective.** Organizations have a greater understanding of their third-party risk landscape, the impact on the organization and third parties, and the ability to be proactive in mitigating risk in a dynamic environment.

- **Efficient.** The organization optimizes human and technology resources to consistently address third-party risk and enable sustainable management of risk exposure as the business and third-party landscape change.

- **Agile.** The organization is more agile and adapts quickly to the rapid changes in its risk landscape. Greater agility provides an advantage over competitors with inefficient manual processes and a limited view of current and potential risk exposure intelligence.

GRC 20/20's Final Perspective

The constant changes in today's third-party risk translate to a growing burden on organizations in terms of the number of risk information sources they face and their scope. Many organizations do not possess the necessary third-party risk intelligence infrastructure and processes to address these changes and, consequently, find themselves at a competitive disadvantage and subject to risk exposure, regulatory scrutiny, reputational damage, business disruptions, and losses that were preventable. These organizations can greatly benefit from moving away from manual and ad hoc processes for third-party risk and toward an architecture specifically designed to manage third-party risk intelligence comprehensively and consistently. Such a system gathers and sorts relevant risk information from a variety of sources, routes critical information to subject matter experts, models and measures potential impact on the organization, and establishes personal accountability for action or inaction.

©GRC 20/20 Research, LLC; Redistribution Rights Granted to Supply Wisdom

The end goal in mature third-party risk management is agility. This is where organizations will find the greatest balance in collaborative third-party risk management and oversight. It allows for some aggregation of third-party risk intelligence relevant to individual departments, business functions, and relationship owners with a common integrated risk intelligence information architecture that aggregates and monitors risk across these areas. Third-party risk intelligence architecture delivers agility through the ability to connect, understand, analyze, and monitor risks and underlying patterns of risk in context of relationships, objectives, processes, and services within the organization and across third party relationships. Different functions participate in third-party risk intelligence with a focus on coordination and collaboration through a common core risk intelligence architecture that integrates and plays well with other systems.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com