August 2020

Value of a Third-Party Assessment

Measuring Risk Reduction in Breaches Through Assessments

VALUE***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

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.

Value of a Third-Party Assessment

Measuring Risk Reduction in Breaches Through Assessments

Managing Risk in an Interconnected Business

The Organization is a Maze of Relationships

No man is an island, entire of itself;
Every man is a piece of the continent, a part of the main.[1]

Replace the word 'man' with 'organization' and the seventeenth-century English poet John Donne is describing the modern organization. In other words, "No organization is an island unto itself, every organization is a piece of the broader whole."

Traditional brick and mortar business is a thing of the past: physical buildings and conventional employees no longer define the enterprise. The modern organization is an interconnected maze of relationships and interactions that span traditional business boundaries. Layers of relationships go beyond traditional employees to include suppliers, vendors, outsourcers, service providers, contractors, subcontractors, consultants, temporary workers, agents, brokers, intermediaries, and more. Complexity grows as these interconnected relationships, processes, and systems nest themselves in intricacy, such as deep supply chains.

In this context, organizations struggle to manage risk in their third-party relationships. Risk and compliance challenges do not stop at traditional organizational boundaries. An organization can face risk by establishing or maintaining the wrong business relationships, or by allowing good business relationships to sour because of weak risk governance and control. Third-party problems are the organization's problems and impact brand and reputation while increasing exposure to risk and compliance issues. When questions of security, privacy, business practice, ethics, safety, quality, human rights, corruption, and the environment arise, the organization is held accountable, and it must ensure that third-party partners behave appropriately.

1 *A famous line from English Poet John Donne's Devotions Upon Emergent Conditions (1624) found in the section Meditation XVII.*

Inevitable Failure in Third-Party Risk Management

Reactive, ad hoc and manual assessments of third-party relationships lead the organization to inevitable problems as they fail to actively manage risk in the context of the relationship. Failure in third-party risk management comes about when organizations have:

- **Growing risk and regulatory concerns with inadequate resources.** Organizations are facing a barrage of increasing regulatory requirements and expanding geopolitical risks around the world. The organization is encumbered with insufficient processes and resources to manage risk and requirements impacting third-party relationships.

- **Silos of third-party oversight.** Allowing different parts of the organization to go about third-party risk governance in various ways without any coordination, collaboration, or common technology architecture leads to greater risk exposure. This leads to the unfortunate situation of the organization having no end-to-end visibility of third-party relationships.

- **Documents, spreadsheets, and email-centric approaches.** When organizations assess third-party relationships in a maze of documents, spreadsheets, and emails, it buries third-party risk management in a mountain of data that is difficult to maintain, aggregate, and report on. Managing and reconciling documents requires a tremendous amount of staff time and resources to consolidate, analyze, and report on third-party risk. When things go wrong, the organization is exposed as it lacks a robust audit trail of who did what, when, how, and why.

- **Inability to Regularly Assess Critical Vendors.** Risk and compliance assessments are often only done during the on-boarding process to validate that the organization is doing business with the right companies through an initial risk assessment process. This approach fails to recognize that additional risk and compliance exposure incur over the life of the relationship.

The bottom line: Organizations need to move forward with a third-party risk assessment strategy and process that is done throughout the lifecycle of the relationship. This process should be automated with technology to avoid the inevitability of failure. However, moving forward requires a clear and compelling business case that measures the value of risk reduction in managing third-party risk and conducting assessments. As risk exposure in third-party relationships is multi-faceted, organizations are best served to build a clear and compelling business case of the value of third-party risk assessments.

Elements of Successful Third-Party Risk Management

The primary directive of a mature third-party risk management program is to reduce risk exposure in relationships and in a way that efficiently uses human capital and financial capital resources effectively to mitigate risk and deliver agility in a dynamic business environment that is continuously changing.

A strategic third-party assessment strategy with standard processes, information, and technology architecture gets to the root of the problem. Leading organizations adopt a common technology approach with shared processes to manage third-party risk in a dynamic and distributed business environment.

A resilient third-party risk assessment process delivers better business outcomes because of increased risk governance in third-party relationships, which will:

- *Lower* costs, while simultaneously scaling the program, reducing redundancy, and improving efficiencies.
- *Deliver* consistent, actionable, and accurate information.
- *Improve* decision-making and insight into risk exposure in business relationships.
- *Enable* the organization to defend itself with an agile third-party risk management program designed to mitigate risk exposure.

Organizations need to be intelligent about what processes and technologies they deploy. A proactive third-party risk assessment approach means looking to the future and mitigating risk, as opposed to putting out fires reactively. With increased exposure to regulations and scrutiny of third-party relationships, how does an organization respond? It requires that the following third-party risk management elements be in place:

- **Continuous third-party risk monitoring.** An organization must have a risk-based approach to managing third-party relationships. This includes periodic (e.g., annual) assessment of relationships. However, the risk-assessment process should also be dynamic — completed each time there is a significant business, risk, or regulatory change or event that could lead to exposure. Risk assessments should be continuous and cover exposure in specific markets, relationships, and geographies.
- **Approach third-party relationships in proportion to risk.** How an organization implements third-party controls and assessments varies on the proportion of risk it faces. If a particular business partner carries a higher risk, the organization must respond with more robust governance and controls. Proportionality of risk also applies to the size of the business — smaller organizations are not expected to have the same measures as large enterprises.
- **Set the tone at the top.** The board of directors and executives must fully support the third-party risk management program. Communication with top-

level management must be bidirectional. Management must communicate that they support third-party risk governance. At the same time, they must be well-informed about the effectiveness and strategies for third-party risk management initiatives.

- **Know who the organization does business with.** It is critical to establish a risk-monitoring framework that catalogs third-party relationships, markets, and geographies. Get a comprehensive list of vendors and establish priority categories. While every entity is evaluated, the depth and frequency can be adjusted based on relative importance to your organization. Due diligence efforts must be in place to make sure the organization is contracting with the right entities. If there is a high degree of risk in a relationship, additional preventive and detective controls to be established in response.

- **Third-party oversight.** The organization needs a group that is responsible for the oversight of risk assessment in third-party relationships. This involves a collaborative effort between information security, privacy, legal, compliance, procurement, and other business functions. This cross-functional team should have the authority to report to independent monitoring bodies, such as the audit committees of the board, to disclose issues.

- **Established policies, procedures, training, and communication.** Organizations need documented and up-to-date policies and procedures that govern third-party relationships supported by training, so team members know what is expected. This starts with a vendor/supplier code of conduct and filters down to other policies that address risks such as IT security and privacy policies in third-party relationships, as well as those that help employees affirm and attest to the policies. These requirements and processes must be clearly documented and adhered to and supported by channels of communication that enable individuals to ask questions and report misconduct.

- **Investigations.** Even in the best organization, things go wrong. Investigation processes must be in place to quickly identify potential incidents and promptly and effectively investigate and resolve issues. This includes reporting and working with outside law enforcement and authorities.

- **Third-party controls.** Organizations must keep detailed records that fairly and accurately reflect controls, transactions, and interactions with third-party relationships. This includes contracts, assessments, due diligence and verification, accounts payable, security ratings, and financial stability.

- **Teams empowered to affect positive change.** When a risk team finds an issue with a critical supplier, they need the ability to require fair and reasonable remediation from the vendor and continuous communication between the vendor and the organization. The goal is to build strong symbiotic relationships.

Measuring the Value of an Assessment

Building the Business Case of Value

Successful third-party risk assessment strategies deliver the ability to effectively mitigate risk, meet requirements, satisfy stakeholders and auditors, achieve human and financial efficiency, and meet the demands of a changing business environment. Third-party risk assessment solutions enable strong processes that utilize accurate and reliable information. This allows a better performing, less costly, and more flexible process that protects the organization from uncertainty and exposure.

GRC 20/20 measures the value of third-party risk assessments, and structures the business case to move forward with initiatives, across the elements of efficiency, effectiveness, and agility. Organizations looking to achieve third-party risk assessment value through automation will find that the value proposition in a business case needs to be:

- **Efficient.** Third-party risk assessment automation provides efficiency and savings in human and financial capital resources by reducing operational costs through automating processes, particularly those that take a lot of time consolidating and reconciling information to manage and mitigate risk and meet compliance requirements. Third-party risk assessment efficiency is achieved when there is a measurable reduction in human and financial capital resources needed to address third-party risk in the context of business operations.

- **Effective.** Third-party risk assessment automation achieves effectiveness in risk, control, compliance, security, audits, and other third-party risk processes. This delivers a greater assurance of the design and operational effectiveness of third-party assessment processes to mitigate risk, protect the integrity of the organization, and meet regulatory requirements. Third-party risk assessment effectiveness is validated when relationships are operating within the controls and policies set by the organization and provide greater reliability of information to stakeholders, auditors, and regulators.

- **Agile.** Third-party risk assessment automation delivers business agility when organizations can rapidly respond to changes in the internal business, and it's relationships, as well as the external environment (e.g., external risks, industry developments, market and economic factors, and changing laws and regulations). Third-party risk agility is achieved when organizations can identify and react quickly to issues, failures, non-compliance, and adverse events promptly so that action is taken to contain these and keep them from growing.

These three elements — efficiency, effectiveness, and agility — provide the core framework of measuring the value of an assessment and building the business case to move forward with assessment automation. Value across these elements is used to measure the quantitative and qualitative value of an assessment to achieve the overall business case of both tangible and intangible benefits. Using these three elements, the value of an assessment can be measured around:

- **Greater integrity in relationships.** The organization stands in the shoes of its relationships. Third-party issues are the organization's issues. In this day and age of greater social responsibility and accountability, the organization must do business with third parties that share the same values that it does. Third-party assessments contribute directly to the shared integrity, ethics, and values of the organization. Organizations are to look for shared values, ethics, processes, and policies enforced with their business partners.

- **Meeting requirements and avoiding penalties.** Third-party assessments enable the organization to demonstrate that it has proper due diligence procedures in place and conducts assessments to ensure that third parties meet legal, regulatory, contractual, and voluntary requirements in these relationships. This further enables the organization to demonstrate compliance, pass regulatory exams and audits, and mitigate or avoid penalties. Consider that an average HIPAA violation is $1.5 million, or an FCPA violation can be hundreds of millions to close to a billion dollars in penalties. This is a significant area of risk reduction and cost avoidance.

- **Reduction in audit issues and resolving issues.** Through third-party assessments, the organization can be preemptive in discovering and resolving control issues in third-party relationships before auditors or regulators find them. It takes time to respond to audit issues as well as resolve issues. The more organizations can assess and ensure controls and processes are in place in third parties leads to less time responding to problems in the future and less time resolving issues raised by auditors and regulators.

- **Reduction in third-party audits and inspections.** Robust and regular automated assessments can lead to a reduction in the number of onsite third-party inspections and audits being performed. With increased and accurate assessments, there is a reduced need for onsite inspections and audits of third-party relationships.

- **Enhanced contract negotiation and value.** Third-party assessments build stronger relationships that can, in turn, lead to less contract exposure, which benefits both parties in better terms, greater accountability, cost avoidance in the need to switch third parties, and an overall reduction in contract renewal costs.

- **Incident/data breach exposure reduction.** Organizations can mitigate and lower their risk exposure and costs of a data breach through regular and reliable third-party assessments. This is explored further as an example in the following section.

- **Streamlined operational costs.** With third-party assessments, organizations can ensure that everything is in place to manage uncertainty and maintain continuity of services and operations with third-party relationships. This is measured through more reliable relationships that are delivering goods and services to reliably achieve the objectives in the relationships while reducing risk exposure and uncertainty in their delivery.

- **Reputational cost avoidance.** Having the right relationships are critical. Third-party assessments ensure that the relationships in place are aligned with the organization to avoid turnover of customers, lost opportunities, an overall decline in the goodwill and value of the organization.

- **Efficiencies in internal staff time.** Automated third-party assessments lead directly to efficiencies in staff time. A recent survey done by Prevalent, one solution provider in this space, found that automation reduced the time required to manage assessments by 49%. A petroleum organization that GRC 20/20 interviewed discovered they could manage the assessments of 5,000 suppliers with one FTE that they required 6 FTEs to do in manual processes of documents, spreadsheets, and emails. The Prevalent survey also found that staff was three times more productive in doing assessments, and the number of assessments done with automation increased by 179% over what they could do with manual processes.

- **Agility and responsive processes.** Organizations find that automated assessments result in fewer items slipping through cracks. With automatic reminders and escalation, as well as validation that all questions are answered, organizations find that assessments are being completed 44% more quickly, with an average of 8.3 days of savings for assessments to be completed which leads to less exposure (Prevalent survey).

Measuring Data Breach Risk Exposure & Value of an Assessment

To achieve a third-party risk management and governance strategy requires a clear and compelling business case of value. Each of the preceding areas of value in a third-party assessment can be built out to provide both quantitative and qualitative benefits in a business case for assessment automation over manual processes. To illustrate this from one angle, the following is a model to demonstrate how third-party assessments reduce the risk exposure of a data breach.

The cost of a breach is significant. The Ponemon Institute and IBM, in their most recent Cost of a Data Breach[2] survey and report, that:

- $3.92 million is the average cost of a data breach around the world.

- In the United States, the average cost of a data breach is more than double this amount at $8.19 million.

- The highest cost by industry for a data breach is in healthcare - at an average cost globally of $6.45 million.

- The cost of a data breach in a third-party relationship is higher than the average cost of a data breach globally, at $4.29 million.

2 *https://databreachcalculator.mybluemix.net*

These costs are broken out and measured across these four areas:

1. Breach detection and escalation.
2. Customer/employee breach notification.
3. Post data breach incident response.
4. Lost business and customer trust, accounting for 36% of total breach cost.

The Ponemon/IBM report measures the longtail of a data breach impact over several years and finds:

- Two-thirds of the cost of a breach happens in the first year.
- 1/3rd of breach costs are incurred over the following second and third years.
- Breach costs do not scale down proportionately with smaller organizations. Small organizations face disproportionately higher breach costs when measured in the context of larger organizations. The probability that an organization will have a data breach over the next two years is nearly 30%. So out of every 100 organizations, there will be 30 that have a data breach in the next two years.

A critical factor in lowering data breach costs is technology automation. Consider:

- The average data breach cost with automation goes down to $2.65 million from $3.92 million.
- If you factor in the higher breach cost from a third-party data breach with this same factor for automation, the cost of a single breach could move from $4.29 million down to $2.9 million.

A robust third-party risk assessment process automated with technology not only reduces the cost and impact of a breach but also reduces the likelihood of a breach.

Formula for Calculating the Value of an Assessment

In the context of this illustration for a business case, the question is: how do you measure the value of a third-party risk assessment in the reduction of exposure to a data breach? See the illustration below, followed by the narrative explanation.

Value of Assessment Calculation

	Without Automation	With Automation
Average number of third parties	1,000	1,000
% of vendors considered higher-risk or critical	50%	50%
# of higher-risk or critical vendors	500	500
Average cost of a third-party data breach	$4,290,000	$2,900,000
Inherent likelihood of a breach in the next two years	30%	15%
Risk exposure (average cost x likelihood)	$1,287,000	$435,000
Risk exposure per vendor (risk exposure / # of higher-risk or critical vendors)	$2,574	$870
Value of Assessment (Risk reduction per vendor)	***$1704***	

For an average-sized organization, it can be assumed there are 1,000 third-party relationships. In the context of risk exposure to a data breach, there may be 50% of these (this is an assumption for this model), or 500, that are at risk of a data breach. Many are not in scope as they pose low to no risk of a data breach. Hypothetically, it is the 500 that have moderate to high risk of a data breach. Note that these are not just third parties that house, store, and work with third-party information but also those that have network access and connections that could lead to exposure.

The average cost of a data breach from the breach of a third-party is $4.29 million. Assume there is no automation at this point, and any assessments done are manual documents, spreadsheets, and emails, if done at all. With the inherent likelihood of a breach in two years at 30%, using a basic risk calculation of impact times likelihood equals risk exposure, the overall risk exposure is $1.29 million. If there are 500 vendors of moderate to high risk of a data breach exposure, in the hypothetical, this brings the overall risk exposure to $2,574 per third-party assessed.

With automation (e.g., assessments), the overall risk exposure of an average data breach moves from $4.29 million to $2.9 million. Assessments and automation impact the cost of a breach, but also affect the likelihood of a breach occurring. More assessments that address weaknesses in third-party controls means the likelihood of a breach over two years may drop from 30% to something lower. In this context, hypothetically, it will be assumed that the likelihood drops from 30% to 15% for a breach. Using the same

math of impact x likelihood equals risk exposure, we see that the overall risk exposure of automated assessments is $435,000. With the 500 vendors of moderate to high-risk exposure of a data breach, this brings the overall residual risk exposure with automated assessments down to $870 per third-party assessed.

The value of an assessment, in the context of a data breach, is then the inherent risk exposure of $2,574 minus the residual risk exposure of $870 per third-party assessed. This model measures the value of each assessment in risk reduction at $1,704 of risk savings to the organization for each third-party assessed. For every assessment conducted, this is how much risk can be taken out of the business.

This is a model, and no model is perfect. The reality is that the cost savings are more significant than this, as it is just considered one aspect of assessment and that of a data breach. The reality is that organizations also have risk exposure to a range of other risks in third parties that require assessment and automation. Given the variety of assessment areas of anyone third-party in an organization, the risk savings of an assessment can be exponentially more.

There is also value received through lower regulatory fines and penalties, reduction in onsite audits/inspections, and reduction in audit issues/findings in third parties. In the context of organizations that have to assess third parties to meet contractual and regulatory requirements (e.g., PCI DSS, HIPAA, GLBA, GDPR, CCPA), where an assessment is not an option, there are more significant savings in automation through human and financial capital savings that can go into a business model of value and justification for automation over manual processes to do the same.

GRC 20/20's Final Perspective

The organization should have a complete view of what is happening with third-party relationships in the context of assessments. Contextual awareness requires that third-party risk management have a central nervous system to capture signals found in assessments, as well as changing risks and regulations for interpretation, analysis, and holistic awareness of risk in the context of third-party relationships.

The primary directive of a mature third-party risk management program is to deliver effectiveness, efficiency, and agility to the business in managing risk across the breadth of third-party relationships. This requires a strategy that connects the enterprise, business units, processes, and information to enable transparency, discipline, and risk control of the ecosystem of third parties across the extended enterprise. Automation of assessments of third parties that pose an exposure to the organization enables the organization to buy down their overall risk exposure and deliver value to the organization.

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
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com