October 2017

SureCloud Third Party Risk Manager

Streamlining Third-Party Risk Management

SOLUTION***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.

SureCloud Third Party Risk Manager

Streamlining Third-Party Risk Management

Addressing the Exposure of Third-Party Risks

Gaining Control of the Interconnected Mesh of Relationships

Brick and mortar business is a thing of the past: physical buildings and conventional employees no longer define an organization. The modern organization is an interconnected mesh of relationships and interactions that span traditional business boundaries. Over half of an organization's 'insiders' are no longer traditional employees. Insiders now include suppliers, vendors, outsourcers, service providers, contractors, subcontractors, consultants, temporary workers, agents, brokers, dealers, intermediaries, and more. Complexity grows as these interconnected relationships, processes, and systems nest themselves in layers of subcontracting and suppliers. It is estimated that over half of IT security breaches are from a third-party relationship.

In this context, organizations struggle to adequately govern risk in third-party business relationships. Third-party problems are the organization's problems that directly impact brand, reputation, compliance, strategy, and risk to the organization. Risk and compliance challenges do not stop at traditional organizational boundaries as organizations bear the responsibility of the actions or inactions of their extended third-party relationships. An organization can face reputational and economic disaster by establishing or maintaining the wrong business relationships, or by allowing good business relationships to sour because of poor governance and risk management. When questions of business practice, ethics, safety, quality, human rights, corruption, security, and the environment arise, the organization is held accountable and it must ensure that third-parties behave appropriately.

Inevitable Failure of Silos of Third-Party Governance

Governing third-party relationships, particularly in context of risk and compliance, is like the hydra in mythology: organizations combat each head, only to find more heads springing up to threaten them. Departments are reacting to third-party management in silos and the organization fails to actively implement a coordinated strategy for third-party management across the enterprise. Organizations manage third-parties differently across different departments and functions with manual approaches involving thousands of documents, spreadsheets, and emails. Worse, they focus their efforts at the formation of a third-party relationship during the on-boarding process and fail to govern risk and compliance throughout the lifecycle of the relationship.

This fragmented approach to third-party governance brings the organization to inevitable failure. Reactive, document-centric, and manual processes cost too much and fail to actively govern, manage risk, and assure compliance throughout the lifecycle of third-party relationships. Silos leave the organization blind to the intricate exposure of risk and compliance that do not get aggregated and evaluated in context of the organization's goals, objectives, and performance expectations in the relationship.

Failure in third-party management happens when organizations have:

- **Growing risk and regulatory concerns with inadequate resources.** Organizations are facing a barrage of growing regulatory requirements and expanding geo-political risks around the world. Many target third-party relationships specifically, while others require compliance without specifically addressing the context of third-parties. Organizations are, in turn, encumbered with inadequate resources to monitor risk and regulations impacting third-party relationships and often react to similar requirements without collaborating with other departments, which increases redundancy and inefficiency.

- **Interconnected third-party risks that are not visible.** The organization's risk exposure across third-party relationships is growing increasingly interconnected. An exposure in one area may seem minor but when factored into other exposures in the same relationship (or others) the result can be significant. Organizations often lack an integrated and thorough understanding of the interconnectedness of performance, risk management, and compliance of third-parties.

- **Silos of third-party oversight.** Allowing different departments to go about third-party management without coordination, collaboration, consistent processes, information, and approach leads to inefficiency, ineffectiveness, and lack of agility. This is exacerbated when organizations fail to define responsibilities for third-party oversight and the organization breeds an anarchy approach to third-party management leading to the unfortunate situation of the organization having no end-to-end visibility and governance of third-party relationships.

- **Document, spreadsheet, and email centric approaches.** When organizations govern third-party relationships in a maze of documents, spreadsheets, and emails it is easy for things to get overlooked and buried in mountains of data that is difficult to maintain, aggregate, and report on. There is no single source of truth on the relationship and it becomes difficult, if not impossible, to get a comprehensive, accurate, and current-state analysis of a third-party. To accomplish this requires a tremendous amount of staff time and resources to consolidate information, analyze, and report on third-party information. When things go wrong, audit trails are non-existent or are easily covered up and manipulated as they lack a robust audit trail of who did what, when, how, and why.

- **Scattered and non-integrated technologies.** When different parts of the organization use different approaches for on-boarding and managing third-

parties, the organization can never see the big picture. This leads to a significant amount of redundancy and encumbers the organization when it needs to be agile.

- **Due diligence done haphazardly or only during on-boarding.** Risk and compliance issues identified through an initial due diligence process are often only analyzed during the on-boarding process to validate third-parties. This approach fails to recognize that additional risk and compliance exposure is incurred over the life of the third-party relationship and that due diligence needs to be conducted on a continual basis.

- **Inadequate processes to monitor changing relationships.** Organizations are in a constant state of flux. Governing third-party relationships is cumbersome in the context of constantly changing regulations, risks, processes, relationships, employees, processes, suppliers, strategy, and more. The organization must monitor the span of regulatory, geo-political, commodity, economic, and operational risks across the globe in context of its third-party relationships. Just as much as the organization itself is changing, each of the organization's third-parties is changing, introducing further risk exposure.

- **Third-party performance evaluations that neglect risk and compliance.** Metrics and measurements of third-parties often fail to properly encompass risk and compliance indicators. Too often metrics from service level agreements (SLAs) focus on delivery of products and services by the third-party but do not include monitoring of risks, particularly compliance and ethical considerations.

The bottom line: When the organization approaches third-party management in scattered silos that do not collaborate with each other, there is no possibility to be intelligent about third-party performance, risk management, compliance, and impact on the organization. An ad hoc approach to third-party management results in poor visibility across the organization, because there is no framework or architecture for managing third-party risk and compliance as an integrated framework. It is time for organizations to step back and define a cross-functional strategy to define and govern risk in third-party relationships that is supported and automated with information and technology.

SureCloud Third Party Risk Manager

Streamlining Third-Party Risk Management

SureCloud Third Party Risk Manager is a third-party management solution that GRC 20/20 has researched and evaluated, that is capable of managing third-party risk in organizations. SureCloud delivers a third-party management solution to identify, assess, and mitigate risk in third-party relationships across the organization. The solution can be deployed to manage specific third-party risks (e.g., information security, privacy, human rights) or can be implemented as a platform to manage the range of third-party risks across the organization. GRC 20/20 finds that the SureCloud solution enables organizations to be efficient, effective, and agile in their third-party management strategy and processes. SureCloud Third Party Risk Manager is well suited for use in organizations

of all sizes and industries that are looking for an efficient, effective, and agile approach to third-party management.

GRC 20/20's evaluation of SureCloud Third Party Risk Manager reveals that it enables the organization to:

- *Identify* and manage the range of third-parties across the organization
- *Evaluate* and monitor third-party risks across the organization
- *Prioritize* control and mitigation efforts in context of third-party risk exposure
- *Manage* the lifecycle of the third-party risk analysis process
- *Conduct* initial and ongoing assessment efforts of third-parties based on risk exposure
- *Monitor* and track individual third-party relationships as well as groups of relationships (e.g., type of relationship, type of risk, geography)
- *Provide* a system of record and audit trail to provide evidence when under legal or regulatory scrutiny

After interviewing several SureCloud Third Party Risk Manager clients, GRC 20/20 finds the following to characterize organizations that utilize Third Party Risk Manager:

- **Before SureCloud Third Party Risk Manager:** Typical clients struggled with silos of third-party management in different parts of the organization. No one had a complete view of third-party risk and compliance activities and processes, and there were significant inefficiencies, redundancies, as well as gaps. Clients typically came from manual processes using a bewildering maze of documents, spreadsheets, and emails for third-party risk management. They struggled managing hundreds to thousands of third-party management related documents, spreadsheets, and emails that became cumbersome and required significant time to manage and report on. Information was scattered and inconsistent, tasks and assessments fell through cracks, deadlines were missed, and things were going in every direction. Organizations particularly struggled with lack of assessment completion/partial completion that drove them to evaluate automated solutions to manage the process.
- **Why organizations chose SureCloud Third Party Risk Manager:** Clients chose Third Party Risk Manager as they desired a solution to automate the workflow, tasks, and overall process of third-party management across business operations and GRC functions. They particularly desired a third-party management solution with the ability to make risk monitoring active throughout the lifecycle of a third-party relationship. They particularly required a Cloud accessible solution hosted and available to the breadth of their third-parties on the Internet that was intuitive and affordable to carry out questionnaire assessments of third-parties.

- **How organizations are using SureCloud Third Party Risk Manager:** SureCloud clients are managing a range of third-party risk and compliance activities and functions within Third Party Risk Manager. They are integrating risk and compliance assessments and assurance activities to drive third-party management to be more efficient, effective, and agile. The ability to integrate the full scope of third-party risks with controls and assurance activities in one platform provides clients with 360° contextual intelligence into third-party risk.

- **Where SureCloud Third Party Risk Manager has excelled for organizations:** Organizations utilizing Third Party Risk Manager tell GRC 20/20 that the solution has excelled for them in aligning third-party strategy and objectives with risks and controls. Organizations are using it to provide an integrated view of third-party risk across procurement, operational risk, compliance, information security, and even social responsibility and sustainability. They find value in having an integrated third-party management platform with one harmonized process for all risk areas, compliance, and control of risks.

What SureCloud Third Party Risk Manager Does

GRC 20/20 has evaluated the capabilities of the Third Party Risk Manager solution and finds that it delivers an intuitive and robust third-party risk management solution to manage third-party relationships in context of today's demanding requirements. Third Party Risk Manager automates what was manual, labor-intensive tasks found in managing third-parties in a maze of documents, spreadsheets, and emails.

SureCloud Third Party Risk Manager Enables Third-Party Management

Third Party Risk Manager effectively and efficiently enables an organization's third-party risk management strategy by providing a platform to manage risk in the lifecycle of third-party relationships. Third Party Risk Manager automates:

- **Ongoing risk management processes.** Third Party Risk Manager manages the periodic interactions, assessments, tasks, communications, and attestations that happen during onboarding as well as throughout the lifecycle of the relationship. This includes:

  - ***Policies.*** Third Party Risk Manager directs the regular periodic communication and reminders to third-parties about code of conduct and related policies they need to follow.

  - ***Attestation.*** Providing accountability, Third Party Risk Manager manages the gathering of periodic attestations by third-parties to their behavior and conformance to policies and contractual requirements.

  - ***Self-assessments.*** The Third Party Risk Manager solution is used to send surveys and self-assessments to third-parties for them to assess themselves and communicate back to the organization.

- *Reporting and system of record.* Third Party Risk Manager provides a detailed evidence trail of all communications, attestations, and interactions with third-parties on aspects of the relationship and in that context of performance, risk, and compliance.

- **Monitoring processes.** Third Party Risk Manager enables the management and automation of the array of tasks needed to continuously monitor third-party risk in the organization. These include:

  - *Risk monitoring.* Third Party Risk Manager provides integrated risk monitoring processes to identify and evaluate potential risks relevant to each third-party relationship throughout their lifecycle in the organization.

  - *Compliance monitoring.* Third Party Risk Manager manages the processes in place to monitor relationships for ongoing conformance to compliance requirements.

  - *Issue reporting & resolution.* Even the most successful business relationships encounter issues. Third Party Risk Manager automates the process for capturing and resolving issues that arise in third-party relationships. Issue reporting processes may be internal and done by employees and management, by the third-parties themselves, or through external sources such as customer complaints.

  - *Audit & inspections.* Organizations utilize Third Party Risk Manager to manage audits and inspections of third-parties as the organization systematically exercises the right to audit clauses and do onsite inspections of third-party premises and facilities.

Foundational Capabilities in SureCloud Third Party Risk Manager

While Third Party Risk Manager can manage a range of third-party risk management processes, it can also be used for specific third-party risk and compliance purposes. Specific capabilities Third Party Risk Manager delivers that enable organizations in third-party risk management, no matter the scope of their third-party strategy, are:

- **Third-party register.** Third Party Risk Manager provides a centralized location to register and document all of the organization's third-party relationships as well as the risk associated with each relationship.

- **Questionnaires, self-assessments, and surveys.** Third Party Risk Manager delivers a full range of survey capabilities to gather information from internal stakeholders and third-parties with embedded instructions and validations to help ensure completeness and accuracy. This can be a one-time self-assessment or a periodic automated self-assessment. The solution provides pre-defined question templates that can easily be modified to meet an organization's specific requirements.

- **Inspections and audits.** Third Party Risk Manager allows for the management and documentation of on-site inspections and audits when organizations choose to exercise right to audit clauses. This includes the ability to scope and manage the array of third-party audits being conducted.

- **Issue and remediation management.** Third Party Risk Manager provides issue remediation and management capabilities to document, record, and manage issues, incidents, and cases that arise in context of third-party relationships.

- **Configurability.** Third Party Risk Manager is designed to be highly agile and adaptable to the unique requirements of organizations. The solution can evolve to accommodate the dynamic nature of third-party risk and compliance as well as changing business requirements.

- **Risk Analytics.** Third Party Risk Manager delivers contextual risk analytics of third-parties that is intelligent through the triangulation of collected information and initiates workflow due diligence for resolution and clarification with third-parties when red flags occur. The solution enables organizations to provide a standardized objective calculation of risk a third-party presents to determine whether to move forward with a new relationship, review an existing relationship, or terminate a relationship immediately.

- **Notifications.** Third Party Risk Manager provides notification through email templates to notify stakeholders and third-parties of programs and expectations with embedded links to online questionnaires and tasks.

- **Workflow and task management.** Third Party Risk Manager provides a full range of capabilities to flexibly build workflow and tasks. This includes the ability for follow-up action management, tasks, workflows, alerts on pending tasks that are soon due, and escalation of missed tasks.

Benefits of SureCloud Third Party Risk Manager

Organizations are most likely to move to the Third Party Risk Manager platform because they found that their manual document centric approaches took too many resources to administer, only addressed specific areas of third-party management, and found things slipping through the cracks because of the continuous barrage of change.

Specific benefits organizations can expect from implementing the Third Party Risk Manager solution are:

- *Reduction in time* spent managing third-parties. One organization found they were spending 25% of their time on administrative tasks required by manual processes before they moved to Third Party Risk Manager.

- *Agile risk and compliance reporting* of third-parties and their status.

- *Improved decision-making* on third-parties through accurate risk and compliance information.
- *Elimination of time and inefficiency* in managing documents, spreadsheets, and emails for third-party risk management.
- *Data integrity* with Third Party Risk Manager being the system of record for all third-party risk and compliance information.
- *Reduction in errors* by allowing third-parties to enter their own data directly into the system instead of emailing documents and information to the organization that were incomplete or incorrectly entered.
- *Significant efficiencies in time through automation* of workflow and tasks as well as reporting. Specifically, the time it took to build reports from hundreds to thousands of documents and spreadsheets now is just a matter of seconds.
- *Collaboration and synergies* by providing a single platform with consistent interface to manage third-party information and interactions across departments instead of different departments doing similar things in different formats and processes.
- *Consistency and accuracy of information* as all internal stakeholders and third-parties must conform to consistent processes and information collection. A single solution with a uniformed and integrated process and information architecture.
- *Accountability with full audit trails* of who did what and when; this particularly has delivered value in less things slipping through the cracks.
- *Notifications of tasks* completed results in less frustration because things were not filled out and had to be sent back to a third-party.
- *Greater visibility into third-party risks* as all information is stored in one common data architecture, which provides a single source of truth which is more accurate and readily available.

Considerations in Context of SureCloud Third Party Risk Manager

Every solution has its strengths and weaknesses, and may not be the ideal fit for all organizations in all situations. While GRC 20/20 has identified many positive attributes of SureCloud Third Party Risk Manager to enable organizations in the consistent management and monitoring of third-party relationships — readers should not see this as a complete and unquestionable endorsement of SureCloud or Third Party Risk Manager.

Overall, organizations should have a high degree of satisfaction with their use and implementation of Third Party Risk Manager. The solutions adaptability and ease of use is a benefit to organizations. The solution is agile by allowing their distributed internal stakeholders to get what they need while providing consistency across functions involved

in third-party management. Clients report that SureCloud is easy to work with and is responsive to serve their clients. Though clients do report that they would like stronger platform documentation/guides, as well as a dedicated mobile and tablet application.

GRC 20/20 finds that Third Party Risk Manager provides value in managing risk in third-party risk across departments and functions. As many organizations respond to growing regulatory requirements in third-party relationships and risk exposure they often enter a fire-fighting reactive mode to deploy a solution for specific purposes where the need for automation has been the greatest given regulatory and audit pressures upon the organization. GRC 20/20 finds that organizations will find greatest value in implementing Third Party Risk Manager to enable an enterprise third-party risk management strategy, but will also find value in deploying Third Party Risk Manager for specific third-party risk and compliance scenarios. An existing Third Party Risk Manager implementation can be expanded to include third-party risk management or implemented specifically for third-party risk management then expanded to broader GRC purposes across 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