June 2019

Third Party GRC Maturity Model

A New Paradigm in Governing Third Party Relationships

STRATEGY**PERSPECTIVE**

Governance, Risk Management & Compliance Insight

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.

Third Party GRC Maturity Model

A New Paradigm in Governing Third Party Relationships

Third Party GRC in an Interconnected Business

The Organization is an Interconnected 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 organization. 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 govern third party relationships. Risk and compliance challenges do not stop at organizational boundaries. An organization can face reputation and economic disaster by establishing or maintaining the wrong business relationships, or by allowing good business relationships to sour because of weak governance of the relationship. Third party problems are the organization's problems and directly impact the brand, as well as reputation, while increasing exposure to risk and compliance matters. 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 party partners behave appropriately.

Inevitable Failure of Silos of Third Party Governance

Fragmented governance of third party relationships through disconnected silos leads the organization to inevitable failure. Reactive, document-centric, and manual processes fail to actively govern relationships and manage risk and compliance in the context of the third party relationship and broader organizational objectives and values. Silos leave

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

the organization blind to intricate relationships of risk and compliance exposures that fail to get aggregated and evaluated in context of the overall relationship and its goals, objectives, and performance.

Failure in third party governance comes about 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. The organization is encumbered with inadequate resources to monitor risk and regulations impacting third party relationships; different parts of the organization end up finger pointing, thinking others are doing this. Or the opposite happens: different parts of the organization react to the same development without collaborating which increases redundancy and inefficiency.

- **Interconnected third party risks that are not connected.** The organization's risk exposure across third party relationships is becoming increasingly interconnected. A risk in one area may seem minor, but when factored into other risk exposures in the same relationship can become significant. The organization lacks a complete record or understanding of the scope of third parties that are material to the organization.

- **Silos of third party oversight.** Inefficiency and potential risk exposure increase when different parts of the organization are allowed to go about third party governance without any coordination, collaboration, and architecture. If the organization also fails to define responsibilities for third party oversight, the impact is exacerbated. As a result, the organization faced the unfortunate situation of having no end-to-end visibility of third-party relationships.

- **Document and email centric approaches.** When organizations govern third party relationships in a maze of documents, spreadsheets, emails, and file shares, it is easy for things to get overlooked. Silos of third party management can become 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 to impossible to get a comprehensive, accurate, and current analysis of a third party. To accomplish this requires a tremendous amount of staff time and resources to consolidate, analyze, and report on third party information. When things go wrong, document trails 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 legacy GRC technologies.** When different parts of the organization use legacy internal GRC solutions and processes for onboarding third parties, monitoring risk and compliance, and managing the relationships, the organization is often limited in capabilities and depth in the governance of third party relationships. This leads to a significant amount of redundancy and inefficiency. It impacts effectiveness while encumbering the organization when it needs to be agile.

- **Processes focused on onboarding only.** Risk and compliance issues are often only analyzed during the on-boarding process to validate the organization is doing business with the right companies through an initial due diligence process. This approach fails to recognize that additional risk and compliance exposure is incurred over the life of the third party relationship.

- **Inadequate processes to manage change.** Governing third party relationships is cumbersome in the context of constantly changing regulations, relationships, employees, processes, suppliers, strategy, and more. Organizations are in a constant state of flux. The organization has to 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 party relationships are changing, introducing further risk exposure.

- **Third party performance evaluations that neglect risk and compliance.** Metrics and measurements of third parties often fail to fully analyze and monitor risk and compliance exposures. Often, metrics are focused on third party delivery of products and services, but do not include monitoring risks such as compliance and ethical considerations.

Managing third party activities in disconnected silos leads the organization to inevitable failure. Without a coordinated third party governance strategy the organization and its various departments never see the big picture. Consequently, they fail to put third party governance in the context of business strategy, objectives, and performance, resulting in complexity, redundancy, and failure. The organization is not thinking about how processes can be designed to meet a range of third party needs. An ad hoc approach to third party management results in poor visibility across the organization, because there is no framework or architecture for managing risk and compliance as an integrated part of business. When the organization approaches third party governance in scattered silos that do not collaborate with each other, there is no possibility to be intelligent about third party performance, risk management, and compliance while understanding its impact on the organization.

The bottom line: A haphazard department- and document-centric approach for third party governance, risk management, and compliance {GRC) compounds the problem and does not solve it. It is time for organizations to step back and mature their third party GRC approaches with a cross-functional and coordinated strategy and team to define and govern third party relationships. Organizations need to mature their third party GRC with an integrated strategy, process, and architecture to manage the ecosystem of third party relationships with real-time information about third party performance, risk, and compliance, as well as how it impacts the organization.

Third Party GRC Maturity Model

A New Paradigm in Governing Third Party Relationships

The primary directive of a mature third party GRC management program is to deliver effectiveness, efficiency, and agility to the business in managing the breadth of third party relationships in context of performance, risk, and compliance. This requires a strategy that connects the enterprise, business units, processes, transactions, and information to enable transparency, discipline, and control of the ecosystem of third parties across the extended enterprise. In the end, third party management is more than compliance and more than risk, but is also more than procurement. Using the definition for GRC[2] – governance, risk management and compliance – third party GRC is a "capability to reliably achieve objectives [GOVERNANCE], while addressing uncertainty [RISK MANAGEMENT], and act with integrity [COMPLIANCE]" in the organization's third party relationships.

> 3rd party management is a capability that enables an organization to:
>
> G) reliably achieve objectives
>
> R) while addressing uncertainty and
>
> C) act with integrity
>
> in and across its 3rd party relationships.
>
> SOURCE: Adapated from the OCEG GRC Capability Model

Lacking an integrated view of third party GRC results in business processes, partners, employees, and systems that behave like leaves blowing in the wind. A targeted third party GRC strategy with common processes, information, and technology gets to the root of the problem. Leading organizations adopt a common framework, architecture, and shared processes to manage third party risk and compliance, increase efficiencies, and be agile in response to the needs of a dynamic and distributed business environment. Mature third party GRC delivers better business outcomes because of stronger governance, which will:

- Lower costs, reduce redundancy, and improve efficiencies.
- Deliver consistent and accurate information.
- Improve decision-making and insight into what is happening across business relationships.
- Enable the organization to defend itself with a robust third party governance program designed to mitigate risk and ensure integrity of relationships aligned with the value and commitments of the organization.

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

[2] *This is the OCEG definition of GRC.*

- **Understand your risk.** An organization must have a risk-based approach to managing third party relationships. This includes periodic assessment (e.g., annual) of relationships. However, the risk-assessment process should also be dynamic — completed each time there is a significant business change or event that could lead to exposure. Risk assessments should cover exposure in certain markets, relationships, and geographies.

- **Approach third party GRC in proportion to risk.** How an organization implements compliance procedures and controls is based on the proportion of risk it faces. If a certain area of the world or a business partner carries a higher risk, the organization must respond with stronger governance and controls. Proportionality of risk also applies to the size of the business — smaller organizations may not be expected to have the same measures as large enterprises.

- **Tone at the top.** The third party governance program must be fully supported by the board of directors and executives. Communication with top-level management must be bidirectional. Management must communicate that they support the third party GRC program, set the risk appetite for the organization, and will not tolerate corruption in any form. At the same time, they must be well-informed about the effectiveness and strategies for third party GRC initiatives.

- **Know who you do business with.** It is critical to establish a risk-monitoring framework that catalogs third party relationships, markets, and geographies. Due diligence efforts must be in place to make sure the organization is contracting with ethical entities. If there is a high degree of corruption risk in a relationship, additional preventive and detective controls must be established in response. This includes knowing contractors' and third parties' beneficial owners, and conducting background checks to understand if they are susceptible to corruption and unethical conduct.[3]

- **Keep information current.** Third party due diligence and risk assessment efforts must be kept current. These are not point-in-time efforts; they need to be done on a regular basis or when the business becomes aware of conditions that point to increased risk.

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

- **Established policies and procedures.** Organizations need documented and up-to-date policies and procedures that govern third party relationships. This

[3] *Likewise, if the third party has access to the organization's clients' or employees' personally identifiable information (PII) data, the organization must be confident of the third parties' data privacy and information security practices and in their own third party risk management programs, if they subcontract. The organization needs to 'follow the data' and understand any fourth parties or n'th parties that may process or have access to it.*

starts with a vendor/supplier code of conduct, and filters down to other policies that address risks in the relationship and its activities that serve the organization. These requirements and processes must be clearly documented and adhered to.

- **Effective training and communication.** Written policies are not enough — individuals need to know what is expected of them. Organizations must implement training to educate employees and business partners. This includes getting acknowledgements from employees and business partners to affirm their understanding, and attestation of their commitment to behave according to established policies and procedures.

- **Implement communication and reporting processes.** The organization must have channels of communication where employees and third parties can get answers. This could take the form of a help line that allows an individual to ask questions, a FAQ database, or via form processing for approval on activities and requests. The organization must also have a hotline reporting system for individuals, including those within third parties, to report misconduct.

- **Assessment and monitoring.** In addition to periodic risk assessment, the organization must also have regular due diligence, assessment, and monitoring activities to ensure that policies, procedures, and controls that govern third parties are in place and working.

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

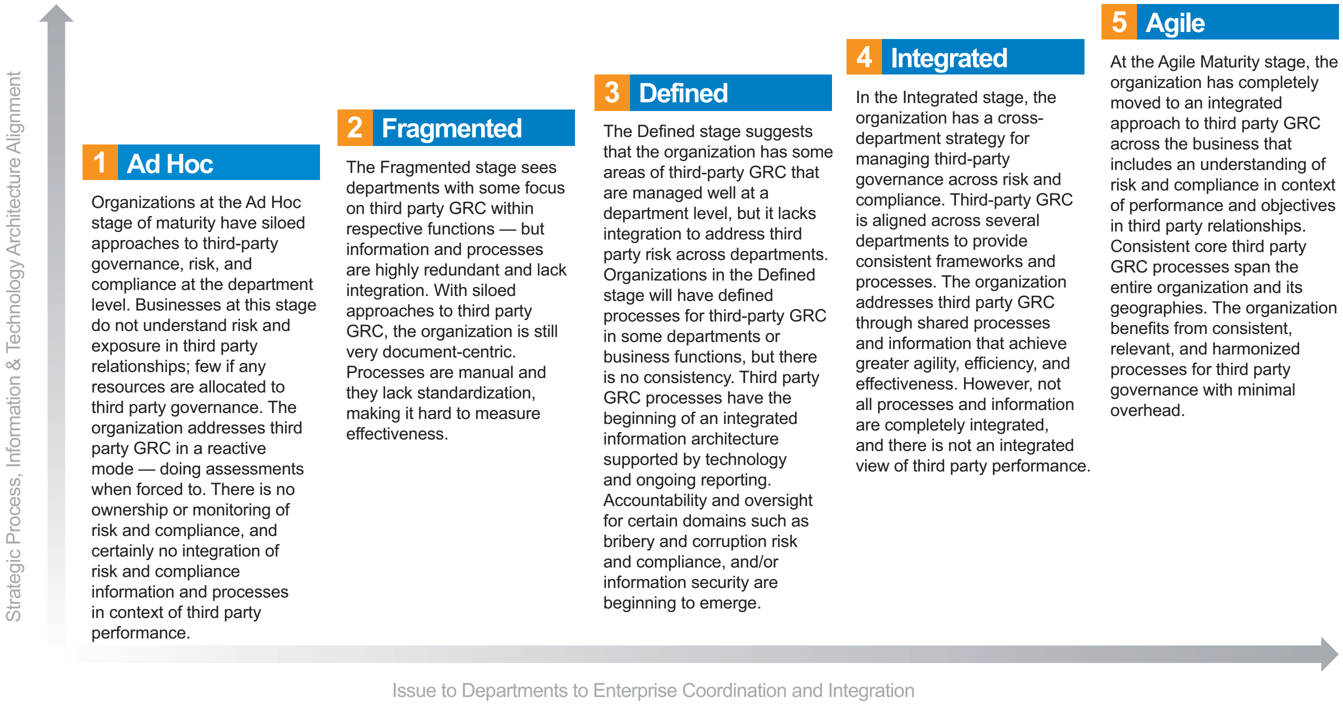
- **Third party controls.** Organizations must keep detailed records that fairly and accurately reflect transactions and interactions of third party relationships. This includes contract-pricing review, due diligence, and verification of foreign business representatives, accounts payable, financial account reconciliation, and commission payments.

- **Conduct audits and inpsections.** Every contract with a third party typically includes right to audit/inspections language. The organization should establish clear and consistent practices when and how these are conducted and follow through with them.

- **Manage business change.** The organization must monitor for changes that introduce greater risk of third party relationships. The organization must document changes in result from observations and investigations, and address deficiencies through a careful program of change management.

Five Stages of Third Party GRC Maturity

Mature third party GRC is a seamless part of governance and operations. It requires a top-down view of third party governance, led by the executives and the board, where third party risk management is part of the fabric of business - not an unattached layer of oversight. It also means bottom-up participation, where business functions identify and monitor transactions and relationships that expose the organization. GRC 20/20 has developed the Third Party GRC Maturity Model to articulate maturity in the Third Party GRC processes and provide organizations with a roadmap to support acceleration through their maturity journey. There are five stages to the model:


Strategic Process, Information & Technology Architecture Alignment
Issue to Departments to Enterprise Coordination and Integration

1 Ad Hoc

Organizations at the Ad Hoc stage of maturity have siloed approaches to third-party governance, risk, and compliance at the department level. Businesses at this stage do not understand risk and exposure in third party relationships; few if any resources are allocated to third party governance. The organization addresses third party GRC in a reactive mode — doing assessments when forced to. There is no ownership or monitoring of risk and compliance, and certainly no integration of risk and compliance information and processes in context of third party performance.

2 Fragmented

The Fragmented stage sees departments with some focus on third party GRC within respective functions — but information and processes are highly redundant and lack integration. With siloed approaches to third party GRC, the organization is still very document-centric. Processes are manual and they lack standardization, making it hard to measure effectiveness.

3 Defined

The Defined stage suggests that the organization has some areas of third-party GRC that are managed well at a department level, but it lacks integration to address third party risk across departments. Organizations in the Defined stage will have defined processes for third-party GRC in some departments or business functions, but there is no consistency. Third party GRC processes have the beginning of an integrated information architecture supported by technology and ongoing reporting. Accountability and oversight for certain domains such as bribery and corruption risk and compliance, and/or information security are beginning to emerge.

4 Integrated

In the Integrated stage, the organization has a cross-department strategy for managing third-party governance across risk and compliance. Third-party GRC is aligned across several departments to provide consistent frameworks and processes. The organization addresses third party GRC through shared processes and information that achieve greater agility, efficiency, and effectiveness. However, not all processes and information are completely integrated, and there is not an integrated view of third party performance.

5 Agile

At the Agile Maturity stage, the organization has completely moved to an integrated approach to third party GRC across the business that includes an understanding of risk and compliance in context of performance and objectives in third party relationships. Consistent core third party GRC processes span the entire organization and its geographies. The organization benefits from consistent, relevant, and harmonized processes for third party governance with minimal overhead.

1: Ad Hoc

Organizations at the Ad Hoc stage of maturity have siloed approaches to third party governance, risk and compliance at the department level. Businesses at this stage do not understand risk and exposure in third party relationships; few if any resources are allocated to third party governance. The organization addresses third party GRC in a reactive mode — doing assessments when forced to. There is no ownership or monitoring of risk and compliance, and certainly no integration of risk and compliance information and processes in context of third party performance.

Key elements that identify an organization is at the Ad Hoc stage are:

- **Blind-spots.** Businesses at this stage are subject to many blind-spots. Understanding of risk and exposure in third party relationships is vital.

- **Reactive.** The organization addresses third party risk and compliance in a reactive, firefighting mode e.g. completing assessments when forced to.

- **Lack of ownership or accountability.** No one has been appointed to take control of third party risk.

- **Lack of process.** There is no defined process or methodologies for managing third parties or the risks that they expose the organization to.

- **Under resourced.** Few resources are allocated to third party governance.

- **Manual.** With little technology support in place and a reliance on spreadsheets and email, processes fail to be consistent.

Characteristics of the Ad Hoc stage are:

- Siloed and ad hoc practices
- No third party segmentation
- Lack of skills and resourcing
- No defined roles and responsibilities
- No governance structure or third party risk management matrix in place
- No defined third party management program or risk framework
- No documented policies or procedures
- Ad hoc and reactive assessments
- Document-centric approaches
- Ad hoc, reactive approach that addresses issues as they arise
- Little to no technology in place
- No visibility, trending, or analytics
- No board or senior management sponsorship

Organizations in the Ad Hoc stage are very much in reactive mode and are likely to answer many of the following in the affirmative:

- Does third party governance, risk, and compliance lack clear owners and accountability within departments?

- Are assessments and controls put in place after the fact, when the organization realizes it is exposed or someone is insisting on them?

- Is third party risk and compliance largely undocumented, or trapped in silos of spreadsheets and documents?

- Does the organization lack any process, information, and technology architecture to support third party GRC?

- Does the department or business function have no ability to report and trend third party risk and compliance over time?

2: Fragmented

The Fragmented stage sees departments with some focus third party GRC within respective functions — but information and processes are highly redundant and lack integration. With siloed approaches to third party GRC, the organization is still very document-centric. Processes are manual and they lack standardization, making it hard to measure effectiveness.

Key elements that identify an organization is at the Fragmented stage are:

- **Pockets of good practice emerging.** Your program may have some pockets of good practice emerging but they need joining up.
- **Blind-spots.** Businesses at this stage are still subject to blind-spots, especially across the organization as so much information exists in departmental silos.
- **Inefficient.** You can all be working hard to address risk in silos, but without a full picture of risk you could duplicate a lot of efforts.
- **Disconnected.** Risk is still being addressed in a disconnected way. Disconnected across departments, disconnected across domains, and disconnected across systems. Not only is this inefficient, it means risk can be exacerbated as it is not understood and addressed across the enterprise.
- **Manual.** With little technology support in place and a reliance on spreadsheets and email, processes fail to be consistent. This can slow your progress, with little ability to audit programs and activities.
- **Hard to measure and monitor.** While some data is beginning to emerge, it's in disparate systems and incomplete.

Characteristics of the Fragmented stage are:

- Tactical siloed approach to third party governance in different departments
- Starting to determine a roadmap with pockets of good practice emerging
- Basic segmentation in place and some standardization of on-boarding registration and qualification
- Third party risk management framework agreed but not implemented
- Some basic performance data may be present in a procurement silo
- Third party governance and processes not fully embedded
- Processes are defined at the department level
- Some areas of risk management are in place (e.g., anti-bribery/corruption, information security) but are not approached in an integrated or structured way
- No integration or sharing of third party related risk and compliance information
- Reliance on fragmented technology and lots of documents
- Difficult to measure programs or determine trends

Organizations in the Fragmented stage of maturity answer many of the following questions affirmatively:

- Are third party risk and compliance activities tactical and siloed?
- Does the organization lack an integrated third party risk and compliance approach across the organization?
- Is third party risk and compliance information scattered across various documents and technology sources?

- Is it difficult and time-consuming to track and trend third party risk and compliance information and reporting?

3: Defined

The Defined stage suggests that the organization has some areas of third party GRC that are managed well at a department level, but it lacks integration to address third party risk across departments. Organizations in the Defined stage will have defined processes for third party GRC in some departments or business functions, but there is no consistency. Third party GRC processes have the beginning of an integrated information architecture supported by technology and ongoing reporting. Accountability and oversight for certain domains such as bribery and corruption risk and compliance, and/or information security are beginning to emerge.

Characteristics of the Defined stage are:

- Third party GRC program and processes are defined with roles and responsibilities at a department level
- A formalized approach is in place with the framework designed and control practices in place
- Risk appetite not yet well defined or aligned, although inherent risk assessments are maturing
- Strategic approach to governing third parties is happening at a department level
- The organization is addressing islands and areas of third party risks
- Some reporting and trending at a department level

Key elements that identify an organization is at the Defined stage are:

- **Better efficiency, but room for fine tuning.** You are beginning to gain efficiencies at the department level as you move away from document- and email-centric processes, but compiling reports across the business is likely to take time, and data is likely to be incomplete.

- **Semi-automated.** You are beginning to automate some business processes, leading to better onboarding times and other efficiencies in parts of your program.

- **Reporting is getting better.** Better reporting and monitoring at the individual level, but it is still hard to extract an enterprise-view of risk.

- **Governance and oversight is starting to develop.** There is some senior management engagement, and particular risk domains, such as anti-bribery and corruption and information security, may be benefiting from an enhanced level of oversight.

- **Better vision and transparency.** Businesses at this stage are beginning to eliminate blind-spots with a more integrated view of risk and compliance. However, the organization is still blinkered at the enterprise view of risk.

Organizations in the Defined stage answer many of the following questions affirmatively:

- Does the organization have silos of mature third party GRC processes at a department, geographic area, or business unit level?
- Do individual departments have defined third party information and technology architectures?
- Can the department or geography readily report and trend on third party risk and compliance over time?
- Have departments removed reactive document-centric approaches?
- Is there clear accountability and responsibility for third party risk and compliance at a department level?

4: Integrated

In the Integrated stage, the organization has a cross-department strategy for managing third party governance across risk and compliance. Third party GRC is aligned across several departments to provide consistent frameworks and processes. The organization addresses third party GRC through shared processes and information that achieve greater agility, efficiency, and effectiveness. However, not all processes and information are completely integrated, and there is not an integrated view of third party performance.

Key elements that identify an organization is at the Integrated stage are:

- **Good vision and transparency.** The organization benefits from an integrated view of risk and compliance, across departmental, regional, and enterprise levels. The organization is beginning to consider implications of performance in third party assessments.
- **Good efficiency.** Silos have been broken down across the organization. It is likely that the organization has seen onboarding times drop dramatically, adoption rates for third party assessments increase, and all three lines of defense operating in a single system.
- **Reporting is robust.** Reports are comprehensive and delivered to management about multiple

Characteristics of the Integrated stage are:

- Strategic approach to third party governance across departments, from a risk and compliance perspective
- Governance model agreed at board level
- Standardized third party risk management approach implemented and adopted, with documented processes
- Third parties are segmented according to agreed and understood criteria
- Robust performance measures are in place
- Appropriate skill-set and resources, with roles and responsibilities allocated
- Third parties engaged and involved
- Silos have begun to be eliminated
- Common process, technology, and information architecture across the business
- Trending and reporting across the business

categories of risk associated with third parties and their engagements. The organization is beginning to collect data about the performance of the program which can contribute to continuous improvement and ROI/value conversations.

- **Fully auditable.** The program has a system with full audit capabilities, so the organization can understand every action that has been taken in the program and whom it has been done by, when.

Organizations in the Integrated stage answer many of the following questions affirmatively:

- Does the organization have a third party GRC strategy that goes across departments?
- Does the organization have shared processes for third party GRC?
- Does the organization have a shared information and technology architecture for third party GRC?
- Can the organization report and trend on third parties across departments?
- Can the organization aggregate and understand third party risk across the business?

5: Agile

At the Agile stage, the organization has completely moved to an integrated approach to third party GRC across the business that includes an understanding of risk and compliance in context of performance and objectives in third party relationships. Consistent core third party GRC processes span the entire organization and its geographies. The organization benefits from consistent, relevant, and harmonized processes for third party governance with minimal overhead.

The Agile is where most organizations will find the greatest balance in collaborative third party governance and oversight. It allows for some department/business function autonomy where needed, but focuses on a common governance model and architecture that the various groups in third party governance participate in. The Agile stage increases the ability to connect, understand, analyze, and monitor interrelationships and underlying patterns of performance, risk, and compliance across third party relationships - as it allows different business functions to be focused on their areas while reporting into a common governance framework and architecture. Different functions participate in third party management with a focus on coordination and collaboration through a common core architecture that integrates and plays well with other systems.

Key elements that identify an organization is at the Agile stage are:

- **End-to-end visibility.** Full visibility of governance risk, compliance, and performance throughout the third party relationship lifecycle.

- **Proactive ability to identify risk, compliance, and performance issues and remediate quickly and effectively.** Engagements outside the risk appetite of the organization are not entered into, and the organization is prepared to terminate third parties who do not comply/cannot be remediated.

- **Continuous monitoring of third party risk and performance.** If defined risk thresholds are met, appropriate actions are automatically triggered. Established data and predictive analytics mean issues can be identified before they become a problem.

- **Issue management rarely needed.** When issues are detected, they are resolved quickly and effectively.

- **Organizational resilience.** The organization understands the resiliency and recovery capabilities of critical vendors -- and their fourth parties -- and have plans and playbooks in place in the event of a 'crisis event'.

- **Cohesion across three lines of defense.** Lines of business, compliance, risk, audit, and senior management are all working in a coordinated way.

- **Innovation initiatives captured.** Third party relationships can bring even more strategic advantage to the organization through the capture and execution of collaborative innovation initiatives.

- **Board and senior management led engagement.** Senior management champions the program. Periodic meetings with the board and regular governance review meetings ensure senior management is fully engaged and well informed about the governance and strategies for third party GRC.

- **Third party governance is seen as a differentiator and impacts brand.** The business recognizes the value of the program, both in terms of market differentiation through corporate integrity and well as the ROI efficiencies across the organization can bring.

Characteristics of the Agile stage are:

- Comprehensive governance structure with periodic meetings with board and regular governance review meetings
- Third party risk appetite and thresholds well defined and understood
- Third party segmentation reviewed annually
- Cohesion across three lines of defense in a third party context
- Issue escalation rarely needed and resolved quickly/effectively
- Able to identify areas of improvement and measure ROI for relationship reviews and continual improvement
- Industry best practices understood and embraced
- Enterprise view of third party ecosystem risk, compliance, and performance
- Third party governance is integrated into roles and responsibilities
- Third party governance has an integrated view of third party performance as well as risk and compliance
- Third party governance is seen as a differentiator and impacts brand
- Extensive measurement and monitoring of third party risk in the context of business strategy and objectives
- Board and senior management led engagement, senior management champions the program

- **Extensive measurement and monitoring of third party risk in the context of business strategy and objectives.** Data derived from the program fuels continuous improvements.

Organizations in the Agile Maturity stage answer many of the following questions affirmatively:

- Is there a single third party governance strategy for the entire organization that all departments participate in?
- Is third party governance understood and monitored in the context of third party performance and aligned with business strategy and planning?
- Can the organization monitor and trend third party governance and performance?
- Does the organization have mature processes, information and technology implementations to support third party governance?
- Is there regular monitoring for improvement in third party governance?

Getting to the Head of the Class

Advancing Your Organization's Third Party Governance Maturity

Organizations with third party GRC processes siloed within departments operate at the Ad Hoc, Fragmented, or Defined stage. At these stages third party GRC programs manage third party risk and compliance at the departmental level and lack an integrated view with no gain in efficiencies from shared processes.

In the Integrated and Agile maturity levels, organizations have centralized third party GRC oversight to create consistent programs around the world with a common third party GRC process, information, and technology architecture. These organizations report process efficiencies reducing human and financial capital requirements, greater agility to understand and report on third party performance, risk, and compliance, and greater effectiveness through the ability to report and analyze third party risk and compliance data. The primary difference between the Intgrated and Agile stage is the integration of third party GRC in the context of performance, objectives, and strategy in individual relationships alighed with the organization. Differences may be seen in top-down support from executive management, and when various risk and compliance functions align with strategy to collaborate and share information and processes.

Considerations for Moving From Ad Hoc and Fragmented to Defined

Departments at the Ad Hoc and Fragmented stage have siloed approaches to third party GRC at the department level. This means no integration or sharing of third party governance program and related risk and compliance information, processes, or technology. An organization that sees itself at the Ad Hoc stage should skip the Fragmented stage and plan to move to the Defined stage.

To move from Ad Hoc or Fragmented to Defined requires the department to reduce manual data integration and improve overall visibility into third party risk exposure. Organizations should consider defining third party GRC process and information architecture at the department level, and implement technology to manage multiple risk and compliance initiatives cohesively.

Considerations for Moving From Defined to Integrated

Departments at the Defined maturity stage are in a good place to lead the organization in a third party GRC strategy to the Integrated stage. They have a strategic approach to third party GRC at the department level, supported by mature third party GRC processes that can be extended to other departments.

To move from the Defined to the Integrated stage requires a common process, information, and technology approach that spans multiple departments. Organizations can leverage third party risk insight to improve planning and strategic decisions. A common governance model for third party management is used across lines of business, functions, and processes. The organization needs a common third party methodology and taxonomy. Organizations at this level report process efficiencies - reducing human and financial capital requirements, greater agility to understand and report on third parties, and greater ability to report and analyze risk and compliance data.

Considerations for Moving From Integrated to Agile

The difference between the Integrated and Agile stages is primarily one of context. At the Integrated stage the organization provides a consistent approach to managing third parties from a risk and compliance context. This is supported by an established third party GRC process, information, and technology architecture. While third party GRC is understood in the context of the business, it is still focused more on risk and compliance than performance and strategy. At the Agile stage, the organization has performance, strategy, and objectives setting the context.

Achieving the Agile stage requires third party GRC expectations set as part of the annual strategic planning processes. The organization has measured and monitored third paties in the context of business strategy, performance, and objectives. There is shared data and technology about third party risk, control, and compliance, as well as decision support, optimization, and business intelligence. The organization has integrated risk and finance data to drive performance, while mitigating third party risks and ensuring integrity across relationshps.

Fundamental Steps to Establishing Your Third Party GRC Strategy

To achieve the full benefits from an third party GRC strategy, GRC 20/20 recommends the following next steps:

- **Gain executive support and sponsorship of the third party GRC strategy.** The organization needs to work in harmony on third party GRC. Different groups doing their own thing handicap the business. Executive support is critical to align the organization.

- **Establish a dedicated cross-functional team focused on a common approach.** It is vital to dedicate a cross-functional team to oversee ongoing harmonization of third party GRC processes, integration of information, collaboration across risk and compliance functions, and execution of the third party GRC strategy. This group identifies strengths within existing functions and enables other areas to benefit from them. The goal of this team is to develop a shared framework, processes, and information.

- **Define a third party GRC framework.** Companies must document and prioritize third parties and third party risks. This includes defining who owns relationships, who owns risk, the subject matter expert for risk, and which function or process monitors third party relationships. Policies, controls, and issues must be mapped back to the third party GRC framework.

- **Develop harmonized processes.** Key to success is identification of shared processes and information for third party GRC across the enterprise. This includes identifying technology solutions to support integrated information and process architecture.

The Role of Third Party GRC Information & Technology Architecture

Third party GRC fails when information is scattered, redundant, non-reliable, and managed as a system of parts that do not integrate and work as a collective whole. The third party GRC architecture supports the overall third party strategy. With processes defined and structured, the organization can now get into the specifics of the architecture needed to support third party processes. The third party management architecture involves the structural design, data model, labeling, use, flow, processing, and reporting of third party management to support third party GRC processes.

Successful third party GRC architecture will be able to integrate information across third party management systems, ERP, procurement solutions, and third party databases. This requires a robust and adaptable information architecture that can model the complexity of third party information, transactions, interactions, relationship, cause and effect, and analysis of information that integrates and manages:

- **Master data records.** This includes data on the third party such as address, contact information, and bank/financial information.

- **Third party compliance requirements.** Listing of compliance/regulatory requirements that are part of third party relationships.

- **Third party risk and control libraries.** Risks and controls to be mapped back to third parties.

- **Policies and procedures.** The defined policies and procedures that are part of third party relationships.

- **Contracts.** The contract and all related documentation for the formation of the relationship.

- **SLAs, KPIs, and KRIs.** Documentation and monitoring of service level agreements, key performance indicators, and key risk indicators for individual relationships, as well as aggregate sets of relationships.

- **Third party intelligence databases.** The information connections to third party databases used for screening and due diligence purposes, such as sanction and watch lists, politically exposed person databases, cyber-security ratings, as well as financial performance or legal proceedings.

- **Transactions.** The data sets of transactions in the ERP environment that are payments, goods/services received, etc.

- **Forms.** The design and layout of information needed for third party forms and approvals.

The third party architecture operationalizes information and processes to support the overall third party management strategy. The right technology architecture enables the organization to effectively manage third party performance and risk across extended business relationships and facilitate the ability to document, communicate, report, and monitor the range of assessments, documents, tasks, responsibilities, and action plans.

There can and should be be a central core technology platform for third party GRC that connects the fabric of the third party GRC processes, information, and other technologies together across the organization. Many organizations see third party GRC initiatives fail when they purchase technology before understanding their process and information architecture and requirements. Organizations have the following technology architecture choices before them:

- **Documents, spreadsheets, and email.** Manual spreadsheet and document-centric processes are prone to failure, as they bury the organization in mountains of data that is difficult to maintain, aggregate, and report on - consuming valuable resources. The organization ends up spending more time in data management and reconciling, as opposed to active risk monitoring of extended business relationships.

- **Point solutions.** Implementation of a number of point solutions that are deployed and purpose built for very specific risk and regulatory issues. The challenge here is that the organization ends up maintaining a wide array of solutions that do very similar things but for different purposes. This introduces a lot of redundancy in information gathering and communications that taxes the organization and its relationships.

- **ERP and procurement solutions.** There is a range of solutions that are strong in the ERP and procurement space that have robust capabilities in contract lifecycle management, transactions, and spend analytics. However, these solutions are often weak in overall third party governance, risk management, and compliance.

- **Enterprise GRC platforms.** Many of the leading enterprise GRC platforms have third party (e.g., vendor) risk management modules. However, these solutions often have a predominant focus on risk and compliance, and do not always have the complete view of performance management of third parties. These solutions are often missing key requirements, such as third party self-registration, third party portals, and established relationships with third party data and screening providers.

- **Third party GRC platforms.** These are solutions that are built specifically for third party GRC, and often have the broadest array of built-in (versus built-out) features to support the breadth of third party GRC processes. In this context they take a balanced view of third party governance and management that includes performance of third parties, as well as risk and compliance needs. These solutions often integrate with ERP and procurement solutions to properly govern third party relationships throughout their lifecycle and can feed risk and compliance information into GRC platforms for enterprise risk and compliance reporting where needed.

The right third party GRC technology architecture choice for an organization often involves integration of several components into a core third party governance platform solution to facilitate the integration and correlation of third party information, analytics, and reporting. Organizations suffer when they take a myopic view of third party GRC technology that fails to connect all the dots, and provide context to business analytics, performance, objectives, and strategy in the real-time business operates in. Some of the core capabilities organizations should consider in a third party GRC platform are:

- **Internal integration.** Third party GRC is not a single isolated competency or technology within a company. It needs to integrate well with other technologies and competencies that already exist in the organization – procurement system, spend analytics, ERP, and GRC. So the ability to pull and push data through integration is critical.

- **External integration.** With increasing due diligence and screening requirements, organizations need to ensure that their solution integrates well with third party databases. This involves the delivery of content from knowledge/content providers through the third party technology solution to rapidly assess changing regulations, risks, industry, and geopolitical events.

- **Content, workflow, and task management.** Content should be able to be tagged so it can be properly routed to the right subject matter expert to establish workflow and tasks for review and analysis. There should be standardized formats for measuring business impact, risk, and compliance.

- **360° contextual awareness.** The organization should have a complete view of what is happening with third party relationships in context of performance, risk, and compliance. Contextual awareness requires that third party management have a central nervous system to capture signals found in processes, data, and transactions, as well as changing risks and regulations for interpretation, analysis, and holistic awareness of risk in the context of third party relationships.

Checklist to Measure & Improve Third Party GRC Maturity

The mature third party GRC program can be measured against critical elements across governance and oversight, people and engagement, process and execution, and information and technology.

Third Party Governance & Oversight

- ❑ Governance model is agreed at the board level and effectively communicated and supported across the organization
- ❑ Policies and procedure for third party GRC fully documented and consistently applied across the organization
- ❑ Third party management framework well defined
- ❑ Measurement and trending now available at an enterprise view
- ❑ Risk appetite is well defined

People & Engagement

- ❑ Clear roles and responsibilities across the organization
- ❑ Skills and resources are being applied to programs
- ❑ A dedicated team is in place and recognized as a center of excellence
- ❑ Skilled subject matter experts engaged in reviews
- ❑ Training and development is embedded
- ❑ Resource is focused on strategic value-added components of the program rather than tactical components
- ❑ Organization may be outsourcing some industry standardized activities to shared services communities

Process & Execution

- ❑ Well defined and executed processes across the organization
- ❑ There is a single version of the truth for all your third party information that is well-integrated with your other business systems
- ❑ The onboarding process is standardized and automated
- ❑ Segmentation and risk tiering is in place
- ❑ Clear view of inherent and residual risk at both the third party and engagement level
- ❑ Applying a risk-based approach that incorporates critical third parties and the long-tail
- ❑ Multiple risk categories being assessed for each third party and their engagements
- ❑ Issue management is in place, and full tracking and remediation is taking place in a single system
- ❑ Ongoing monitoring is established, with changes in risk profiles automatically triggering the appropriate actions
- ❑ Clear view and controls for fourth parties or beyond
- ❑ Managing risk through the full third party relationship lifecycle
- ❑ Performance management fully embedded in the program
- ❑ Program improvement decisions are facilitated by robust data

Information & Technology

- ❑ Leveraging third party GRC management software
- ❑ Third party portal for assessments, document collection, issue management, and collaboration
- ❑ Third parties are able to update their profiles proactively within the portal
- ❑ Supports innovation projects with strategic third parties
- ❑ Leveraging third party risk intelligence content to support automated business processes, and to support enhanced decision making

GRC 20/20's Final Perspective

The primary directive of a mature third party governance program is to deliver effectiveness, efficiency, and agility to the business in managing the breadth of third party relationships in context of performance, risk, and compliance. This requires a strategy that connects the enterprise, business units, processes, transactions, and information to enable transparency, discipline, and control of the ecosystem of third parties across the extended enterprise.

The Agile Maturity approach is where most organizations will find the greatest balance in collaborative third party governance and oversight. It allows for some department/ business function autonomy where needed, but focuses on a common governance model and technology architecture that the various groups in third party GRC utilize. A federated approach increases the ability to connect, understand, analyze, and monitor interrelationships and underlying patterns of performance, risk, and compliance across third party relationships. It allows different business functions to be focused on their areas while reporting into a common governance framework and architecture. Different functions participate in third party GRC management with a focus on coordination and collaboration through a common core 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
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com