April 2022

ProcessUnity

Delivering Value in Third-Party Risk Management

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.

ProcessUnity

Delivering Value in Third-Party Risk Management

The Third-Party Risk Management Challenge

The Modern Organization is an Interconnected Web of Relationships

Gone are the years of simplicity in operations. Exponential growth and change in risks, regulations, globalization, distributed operations, competitive velocity, technology, and business data impede third-party relationships and the business's ability to manage them.

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 company. In other words, "No organization is an island unto itself; every organization is a piece of the broader whole."

The structures and realities of business today have changed. Traditional brick-and-mortar business is outdated: physical buildings and conventional employees no longer define the organization. The modern organization is an interconnected web of relationships, interactions, and transactions 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, dealers, intermediaries, partners, and more. Complexity grows as these interconnected relationships, processes, transactions, and systems nest themselves in intricacies, such as deep supply chains and subcontracting relationships. Roaming the hallways of an organization means crossing paths with contractors, consultants, temporary workers, and

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

more. Business today relies and thrives on third-party relationships; this is the extended enterprise.

In this context, organizations struggle to govern their third-party relationships and too often manage risk and compliance in relationships in silos that fail to see the big picture of risk exposure and impact on the relationship's objectives. Risk and compliance challenges do not stop at organizational boundaries. An organization can face reputational and economic disaster by establishing or maintaining the wrong business relationships or allowing good business relationships to sour because of weak risk governance. Third-party problems are the organization's problems and directly impact the brand, and reputation, increasing exposure to risk and compliance matters. When questions of delivery, business practice, ethics, privacy, safety, quality, human rights, resiliency, corruption, security, and the environment arise, the organization is held accountable, and it must ensure that third-party partners behave appropriately.

The business's ability to achieve corporate objectives directly depends on the governance of third-party relationships and whether the organization has established the right connections and can reliably achieve objectives in the relationship. The organization's ability to manage uncertainty, risk, and resiliency in its relationships requires that its objectives, values, and risks be managed together. Corporate integrity is measured by its relationships as well. The saying, ***"Show me who your friends are, and I will tell you who you are"*** translates to business: show me who your third-party relationships are, and I will tell you who you are as an organization.

The Inevitable Failure of Silos of Third-Party Governance

The world of business is distributed, dynamic, and disrupted. It is distributed across a web of relationships. It is dynamic as business and relationships change day-by-day - processes change, employees change, relationships change, regulations change, risks change, and objectives change. The ecosystem of business relationships is complex and interconnected. Rather than a dissociated collection of processes and departments, it requires a holistic, contextual awareness of third-party GRC (governance, risk management, and compliance). Change in one area has cascading effects that impact the entire ecosystem. This interconnectedness of business is driving demand for 360° contextual awareness in the organization's third-party relationships. Organizations need to see the intricate intersection of objectives, risks, and boundaries in each relationship.

This challenge is even more significant when third-party risk management is buried in the depths of departments and operating from silos, not as an integrated discipline of decision-making that has a symbiotic relationship on performance and strategy of relationships. Fragmented risk governance of third-party relationships through disconnected department silos leads the organization to inevitable failure. Siloed information and 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 the organization blind to the intricate relationships of risk and compliance exposures that fail to get aggregated and evaluated in the overall relationship and its goals, objectives, and performance.

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 growing regulatory requirements and expanding geopolitical risks around the world. The organization is saddled with insufficient 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 complete visibility or understanding of the scope of risk in third parties that are material to the organization.

- **Silos of third-party oversight.** This is when the organization allows different parts of the organization to go about third-party risk management in different ways without any coordination, collaboration, and architecture. This is exacerbated when the organization fails to define responsibilities for third-party oversight. This leads to the unfortunate situation of the organization having no end-to-end visibility of third-party relationships.

- **Document and email-centric approaches.** When organizations govern risk in third-party relationships in a maze of documents, spreadsheets, emails, and file shares, it is easy for things to get overlooked and bury silos of third-party management in mountains of data that are difficult to maintain, aggregate, and report on. There is no single source of truth in 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 siloed 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 third-party risk technologies.** When distinct parts of the organization use legacy internal third-party risk 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, impacts effectiveness, while also encumbering the organization when it needs to be agile.

- **Processes focused on onboarding only.** Risk and compliance issues are often only analyzed during the onboarding 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 risk in 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 must monitor the span of regulatory, geopolitical, economic, and operational risks across the globe in the context of its third-party relationships. Just as much as the organization itself is changing, each of the organization's third-party relationships is 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 thoroughly. Often, metrics are focused on third-party delivery of products and services but do not include evaluating risks such as compliance, security, resiliency, and ethical considerations.

Managing third-party activities in disconnected silos leads the organization to inevitable failure. Without a coordinated third-party management strategy, the organization and its various departments never see the big picture and fail to put third-party risk management 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 risk 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 the business. When the organization approaches third-party management in scattered silos that do not collaborate, it is impossible to be intelligent about third-party performance, risk management, and compliance while understanding its impact on the organization.

The physicist, Fritjof Capra, made an insightful observation on biological ecosystems that rings true when applied to third-party management:

"The more we study the major problems of our time, the more we come to realize that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent."[2]

Capra's point is that biological ecosystems are complex, interconnected, and require a holistic understanding of the intricacy of interrelationship as an integrated whole rather than a dissociated collection of parts. Change in one segment of an ecosystem has cascading effects and impacts on the entire ecosystem.

This is true in third-party risk management. What further complicates this is the exponential effect of third-party risk on the organization. Business operates in a world of chaos. Applying chaos theory to business is like the 'butterfly effect,' in which the simple flutter of a butterfly's wings creates tiny changes in the atmosphere that ultimately

2 *Fritjof Capra, The Web of Life: A New Scientific Understanding of Living Systems (New York: Anchor Books, 1996), 3.*

impact the development and path of a hurricane. A small event cascades, develops, and influences what ends up becoming a significant event.

Dissociated data, systems, processes, and a myopic risk vision leaves the organization with fragments of the truth that fail to see the big picture of third-party performance, risk, and compliance across the enterprise and how it supports its strategy and objectives. The organization needs to have holistic visibility and situational awareness of third-party relationships across the enterprise. The complexity of business, intricacy, and interconnectedness of third-party risk data requires that the organization implement a third-party risk management strategy.

Defining Third-Party Risk Management

The primary directive of a mature third-party risk management program is to deliver effectiveness, efficiency, and agility to the business in managing the breadth of third-party relationships in 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 GRC management is more than compliance and risk and is also more than procurement.

The integrity of the organization relies on the integrity of its third-party relationships. Organizations are re-evaluating their internal core values, ethics, and standards of conduct and how this extends/is enforced across third-party relationships. This includes a focus on human rights, privacy, environmental standards, health and safety, conduct with others (e.g., customers, partners), and security in third-party relationships.

The organization must maintain operations amid uncertainty and change. This requires a holistic view of a third-party relationship's objectives and performance in the context of uncertainty and risk within those relationships. The organization must be resilient with full situational awareness of the interconnected risk environment that impacts them. Given the reliance on third-party relationships, this requires a holistic view of the governance, risk management, and compliance of each third-party relationship and how it serves and provides value to the organization.

Third-party GRC/Risk Management is a "capability to reliably achieve objectives [GOVERNANCE], while addressing uncertainty [RISK MANAGEMENT], and act with integrity [COMPLIANCE]"[3] in and across the organization's third-party relationships." This is adapted from the official GRC definition in the OCEG GRC Capability Model. Breaking this down, third-party GRC delivers:

- **Third-party governance.** It starts with integrated governance of third-party relationships and monitoring relationships across the extended enterprise to ensure they meet the objectives and purpose the relationship was established for, and thus, returning value to the organization.

3 *This definition is adapted from the OCEG GRC Capability Model that can be found at www.oceg.org.*

- **Third-party risk management.** Understanding the governance objectives of the relationship sets the context to then assess, analyze, and monitor the uncertainty and risk in the relationship. Risk, by official definition, is the effect of uncertainty on objectives. Each relationship has its objectives (or component of the relationship like a contract or service level agreement) and uncertainty needs to be managed against those objectives.

- **Third-party compliance.** Compliance aims to see that the organization acts with integrity in fulfilling its regulatory, contractual, and self-imposed obligations and values across its third-party relationships. Compliance follows through on risk treatment plans to assure that risk is being managed within limits and that controls are in place and functioning within each relationship to mitigate risk.

The bottom line: The modern business depends on, and is defined by, the governance, risk management, and compliance of third-party relationships to ensure the organization can reliably achieve objectives, manage uncertainty, and act with integrity in each of its third-party relationships. A haphazard department and document centric approach for third-party risk management compounds the problem and does not solve it. Organizations need to address 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 and how it impacts the organization. It is time for organizations to step back and implement a third-party risk management strategy supported by a third-party risk information and technology architecture that delivers value to the business. This value can be measured in efficiency, effectiveness, and agility. A third-party risk management platform saves time and money and creates an environment where the organization can measure the effectiveness and efficiencies of resources.

The Third-Party Risk Management Process

Distributed and dynamic business requires the organization to take a strategic approach to third-party risk management. Organizations need complete situational and holistic awareness of third-party risks across the third-party risk lifecycle. This is best approached through structured and accountable processes that enable an integrated information and technology architecture for third-party risk management. The goal is to manage risk across the lifecycle of a third-party relationship and risk across relationships and their impact on the organizational objectives by seeing the big picture and trends of third-party risks and their impact on overall risk and compliance exposure.

Two essential components for a mature and robust third-party risk management program are:

1. ***Structured processes*** for third-party risk management.

2. ***Integrated information and technology architecture*** for third-party risk management.

Third-party risk management processes determine the types of information needed, gathered, used, and reported. Through the integrated information and technology architecture,processes can be properly managed. The architecture defines how organizational processes, information, and technology are structured to make third-party risk management effective, efficient, and agile across the organization.

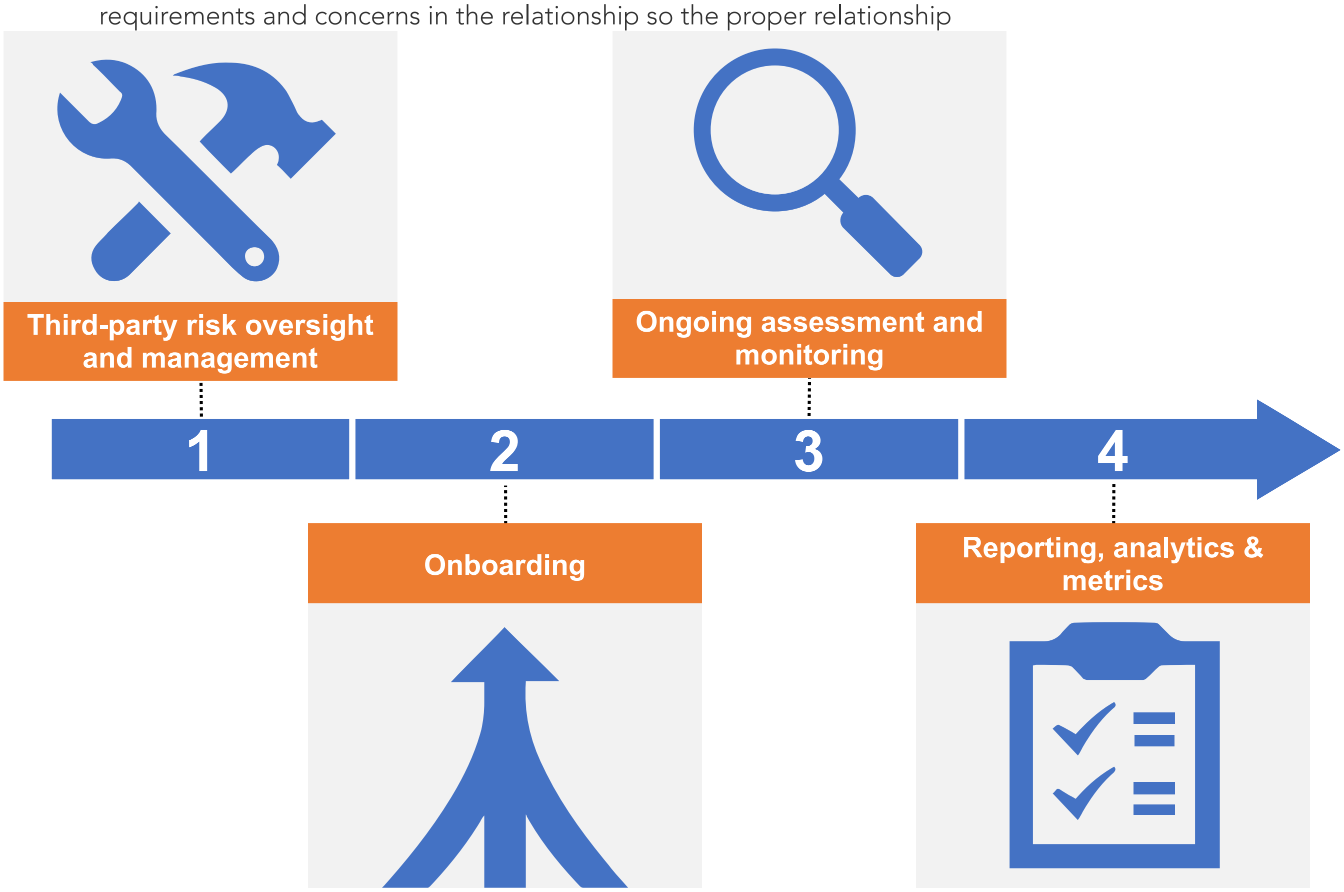
Third-Party Risk Management Process Structure

Structured processes for third-party risk management define responsibilities, workflow, tasks, how issues are reported, cases managed, and how the processes work together as an integrated whole with other organizational processes.

There are four foundational process components that organizations should have in place for third-party risk management:

1. **Third-party risk oversight and management.** This involves the ongoing planning and administration of third-party risk strategy and management as a coordinated effort. Core to this is the planning, administration, and coordination of third-party risk processes and assessments.

2. **Onboarding.** This is the collection of processes aimed at automating a standard, objective approach for identifying third parties to work with, onboarding them through the collection of third-party data, and conducting appropriate due diligence. This process identifies new third parties or existing third parties to contract with for new business purposes. This includes the details of the purpose of the relationship and includes the initial scope of performance, risk, compliance requirements and concerns in the relationship so the proper relationship



can be identified. Once a third party has been selected, the next step is the qualification and screening process to validate that the third party can meet the requirements of the relationship and does not introduce unwarranted risk and compliance exposure. The screening process will go through due diligence steps to ensure that the third-party is the right fit for the organization. Relationships, particularly high-risk ones, must be evaluated against defined criteria to determine if the relationship should be established or avoided. Upon passing initial qualification and screening, the next sets of processes are contracting and negotiation processes to come to terms and establish the relationship. When contracting and negotiation processes are complete, the organization moves into registration and onboarding. The registration process may have already started in the qualification and screening phase to gather information but concludes with setting up the third-party in the system with master data records, financial and payment information, contact information, insurance, and licensing documentation. Further steps of the onboarding process will be the communicating of code of conduct and related policies, getting attestations to these, completing associated training requirements, and conducting initial audits and inspections.

3. **Ongoing assessment and monitoring.** This state includes various processes to continuously monitor third-party relationships over their lifecycle in the organization. These activities are typically done within the organization to monitor and assess the third-party relationship on an ongoing basis. It includes the processes to monitor relationships for risk and ongoing conformance to compliance requirements. This includes ongoing due diligence and assessment processes that can monitor and screen third parties on a continuous and periodic basis.

4. **Reporting, analytics & metrics.** This is the stage of the process that provides detailed reports on both individual third parties and metrics and measurement of risk across relationships. The organization should be able to track past due tasks, benchmark third-party risks, identify where issues are and can be mitigated, and reduce compliance gaps in relationships.

Third-Party Risk Management Information & Technology Architecture

With processes defined and structured, the organization can now define the information architecture needed to support third-party risk management processes. Third-party risk management fails when information is scattered, redundant, non-reliable, and managed as a system of parts that do not integrate and work as a structured and coordinated whole. The third-party risk management information architecture involves the structural design, labeling, use, flow, processing, and reporting of information to support third-party risk management processes. This architecture supports and enables the process structure and overall third-party risk management strategy.

Successful third-party risk management information architecture will be able to integrate, manage, and report on third-party risks across the organization. This requires a robust and adaptable information architecture that can model the complexity of information, transactions, interactions, relationships, cause and effect, and analysis of information that integrates and manages with a range of business systems and data.

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

There can and should be a central core technology platform for third-party risk management that connects the fabric of the processes and information together across the organization. Many organizations see third-party risk management initiatives fail when they purchase technology before understanding their process and information requirements. The "best" systems are the ones that are highly configurable to a client's situation and can be adapted to the company's processes and technical architecture. The system should not run the business; the business should run the system. Organizations have the following technology architecture choices before them:

- **Documents, spreadsheets, and email.** Manual spreadsheet and document-centric processes are prone to failure. 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, instead of active risk monitoring of extended business relationships.

- **Point solutions.** The implementation of several 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 an array of disconnected solutions that do very similar things but for different purposes. This introduces a lot of redundancies in information gathering and communications that tax the organization and its relationships. They typically focus on one, possibly more, areas of third-party risk.

- **ERP (Enterprise Resource Planning) solutions.** There are a range of strong solutions in the ERP and procurement space that have robust capabilities in third-party transactions and spend analytics. However, these solutions may be weak in overall third-party governance, risk management, and compliance.

- **Enterprise GRC platforms.** Many 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 a complete view of performance management of third parties. These solutions often miss key requirements such as third-party self-registration, third-party portals, and established relationships with third-party data and screening providers.

- **Third-party GRC management platforms.** These are solutions that are built specifically for third-party GRC management and often have the broadest array of built-in (versus built-out) features to support the breadth of third-party management 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, or may be provided by a procurement solution, 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.

Most homegrown systems are the result of starting with tools that are readily available and easy: documents, spreadsheets, emails, and desktop databases. Too many organizations take an ad hoc approach to third-party risk management by haphazardly using documents, spreadsheets, desktop databases, and emails, which then dictates and limits what their third-party risk management process will be limited to. This approach then grows and expands quickly, outgrowing these desktop tools to the point where it grows cumbersome.

The right third-party risk technology choice for an organization is a 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 risk management technology that fails to connect all the dots and provide context to analytics, performance, objectives, and strategy in the real-time that the business operates within. The right third-party risk management technology architecture choice for an organization involves an integrated platform to facilitate the correlation of third-party risk assessments, information, analytics, and reporting.

Some of the core capabilities organizations should consider in a third-party risk management platform are:

- **Internal integration.** Third-party management 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. 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 delievering 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 appropriately routed to the right subject matter expert to establish workflow and tasks for review and analysis—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.

ProcessUnity Vendor Risk Management

ProcessUnity Vendor Risk Management (VRM) is a third-party risk management solution that GRC 20/20 has researched and evaluated that can manage third-party risk in complex, distributed, and dynamic business environments. ProcessUnity 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 an enterprise platform to manage the range of risks across all organization's third parties. GRC 20/20 finds that the ProcessUnity VRM solution enables organizations to be efficient, effective, and agile in their third-party management strategy and processes. VRM 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 ProcessUnity VRM reveals that it enables:

- *Identification* of the range of third parties across the organization
- *Evaluation* of third-party risks across the organization
- *Prioritization* of control and mitigation efforts in the context of third-party risk exposure
- *Management* of the lifecycle of third-party relationship process from onboarding to off-boarding
- *Continuous* due diligence efforts of third parties based on risk exposure
- *Monitoring* of individual third-party relationships as well as groups of relationships (e.g., type of relationship, type of risk, geography)
- *Provision* of a robust system of record and audit trail to provide evidence when under legal or regulatory scrutiny

After interviewing several ProcessUnity clients, GRC 20/20 finds the following to characterize organizations that utilize the ProcessUnity VRM platform:

- **Before ProcessUnity VRM.** 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. These clients come from two different scenarios:

- *Documents, spreadsheets, and emails.* They struggled to manage hundreds to thousands of third-party management-related documents, spreadsheets, and emails that became cumbersome and required considerable time to manage and report on.

- *Enterprise GRC platforms.* Some clients switched to ProcessUnity VRM from Enterprise GRC Platforms that they found limited and costly to use to manage third-party risks.

- **Why organizations choose ProcessUnity VRM.** Clients choose VRM as they desire full end-to-end enablement 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 activies throughout the third-party lifecycle.

- **How organizations are using ProcessUnity VRM.** Clients are managing a range of third-party risk and compliance activities and functions. They are integrating risk, compliance, continuous monitoring, and assurance activities to drive third-party management to make it more efficient and resilient. The ability to integrate the full scope of third-party risks with controls and assurance activities in one platform provides them with 360° contextual third-party intelligence.

- **Where ProcessUnity VRM has excelled for organizations.** Organizations utilizing the ProcessUnity platform 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 ProcessUnity VRM Does

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

ProcessUnity VRM Enables the Third-Party Management Lifecycle

ProcessUnity effectively and efficiently enables an organization's end-to-end third-party management strategy by providing a platform to manage the lifecycle of third-party relationships and risks. This lifecycle that ProcessUnity VRM automates includes:

- **Onboarding process.** ProcessUnity automates onboarding processes by collecting required third-party information and conducting appropriate due diligence in the nature of the relationship.

- *Relationship documentation.* ProcessUnity enables the organization to document the purpose of the relationship and detail performance, risk, and compliance requirements in the context of the relationship so they can be properly governed.

- *Initial due diligence.* The platform manages the sequence of steps and integrated content to qualify and screen third parties to mitigate unnecessary risk and compliance exposure. The screening process involves due diligence steps to ensure that the third-party is the proper organization with whom to establish a relationship. This process is supported through the triangulation of information provided by third parties themselves, information from an internal stakeholder of the organization, and information, pulled from external content sources. Third-party relationships, particularly high-risk ones, are evaluated against defined criteria to determine if the relationship should be established or avoided.

- *Contracting.* Upon passing the initial qualification process, ProcessUnity VRM manages the tasks and workflow for contracting and negotiations to document the interactions and define the formal agreement of the relationship with service levels established with associated performance and risk indicators.

- *Final onboarding.* After completing contracting and negotiation, ProcessUnity streamlines the final registration process and associated tasks. This includes communication of code of conduct and other relevant policies, associated training requirements, initial audits and inspections if needed, as well as attestations.

- Ongoing assessment and monitoring processes. The platform manages the ongoing periodic tasks of communications, attestations, and interactions that happen periodically as well as when triggers and situations arise with third parties. This includes:

  - *Policies.* ProcessUnity VRM directs regular periodic communication and reminders to third parties about the code of conduct and related policies they need to follow.

  - *Training.* ProcessUnity communicates and documents the completion of training required of third parties.

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

  - *Self-assessments.* The 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.* The ProcessUnity system 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.* ProcessUnity VRM enables the management and automation of the array of tasks needed to continuously monitor third-party relationships over their lifecycle. These include:

- *Risk monitoring.* The platform 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.* ProcessUnity manages the processes to monitor relationships for ongoing conformance to compliance requirements.

- *Ongoing due diligence monitoring.* In the context of risk and compliance monitoring, ProcessUnity VRM manages the workflow and tasks with integrated content to conduct ongoing due diligence and screening processes to ensure the third party is still the right organization to be doing business with.

- Issue reporting & resolution. Even the most successful business relationships encounter issues. The ProcessUnity platform automates the process of capturing and resolving issues that arise in third-party relationships. Issue reporting processes may be internal and done by employees and management, third parties, or external sources such as customer complaints.

  - *Audit & inspections.* Organizations utilize ProcessUnity to manage audits and inspections of third parties. The organization systematically exercises the right to audit clauses and do onsite inspections of third-party premises and facilities.

- Metrics & reporting. Through a solid information architecture and reporting engine, ProcessUnity VRM brings together the third-party risk management data elements to provide end-to-end reporting and metrics on third-party relationships at the relationship level, aggregated risk, or on a specific risk.

  - *Re-evaluation.* Utilizing the detailed history of interactions, issues, performance, non-conformance, and evolving risk scenarios, the platform manages the processes to evaluate, maintain, and renew third-party relationships.

  - *Off-boarding.* All good things must come to an end, and ProcessUnity enables the management of the tasks and details many organizations neglect or forget in off-boarding relationships that are no longer needed.

Foundational Capabilities in ProcessUnity VRM

While ProcessUnity VRM can manage a broad third-party risk management process, it can also be used for specific third-party risk and compliance purposes. Specific capabilities VRM delivers that enable organizations in third party risk management, no matter the scope of their third-party strategy, are:

- **Onboarding.** ProcessUnity enables the setup of third parties, collecting information, gathering of attestations, and facilitating the entire onboarding process.
- **Due diligence.** ProcessUnity gives the organization an automated workflow of due diligence that goes beyond initial onboarding to ensure that due diligence is a regular periodic task that is conducted for each third-party relationship commensurate with the risk of that relationship.
- **Questionnaires, self-assessments, and surveys.** ProcessUnity 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.
- **Inspections and audits.** ProcessUnity allows for the management and documentation of on-site inspections and audits when organizations choose to exercise the right to audit clauses. This includes the ability to scope and manage the array of third-party audits being conducted.
- **Performance and contract reviews.** ProcessUnity integrates ongoing performance monitoring of a contract against service level agreements established. This facilitates the measurement of third-party performance and provides for intelligent contract reviews.
- **Issue reporting and management.** ProcessUnity provides issue reporting and management capabilities to document, record, and manage issues, incidents, and cases that arise in the context of third-party relationships.
- **Configurability.** The ProcessUnity platform 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.
- **Content integration.** ProcessUnity VRM can integrate with a variety of content feeds (cybersecurity ratings, financial health scores, ESG data, etc.) to keep the organization aware of news, risk, and compliance developments in the context of third-party relationships and geographic operations. This includes alerts on regulatory, environmental, economic, geopolitical, and news that can affect the success or failure of any given business relationship.

- **Internationalization.** ProcessUnity has the full internationalization and contextualization capabilities that global organizations require. Clients have localized it in over thirty languages/locales.

- **Analytics.** ProcessUnity 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.

- **Risk modeling.** The ProcessUnity platform enables organizations to provide a standardized objective calculation of risk that a third-party presents to determine whether to move forward with a new relationship, review an existing relationship, or terminate a relationship immediately.

- **Notifications.** ProcessUnity 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.** ProcessUnity provides a full range of capabilities to flexibly build workflow and tasks. This includes the ability for both linear and parallel workflows, alerts on pending tasks that are soon due, and escalation of missed tasks.

The Value of ProcessUnity VRM

GRC is the capability to reliably achieve objectives [GOVERNANCE] address uncertainty [RISK MANAGEMENT] and act with integrity [COMPLIANCE]. Successful GRC 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. GRC solutions, such as ProcessUnity VRM, should achieve stronger processes that utilize accurate and reliable information. This enables a better performing, less costly, and more flexible business environment.

GRC 20/20 measures the value of GRC initiatives, such as third-party risk management, around the elements of efficiency, effectiveness, and agility. Organizations looking to achieve value will find that the results are:

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

- **Effective.** How a solution achieves effectiveness in risk, control, compliance, IT, audit, and other processes. This is delivered through greater assurance of the design and operational effectiveness of third-party risk processes to mitigate risk, protect the integrity of the organization, and meet regulatory requirements. Effectiveness is validated when business processes are operating within the organization's controls and policies and provide greater reliability of information to auditors and regulators.

- **Agile.** How a solution delivers business agility when organizations can rapidly respond to changes in the internal business environment (e.g., employees, business relationships, operational risks, mergers, and acquisitions) as well as the external environment (e.g., external risks, industry developments, market, and economic factors, and changing laws and regulations). Agility is also achieved when organizations can identify and react quickly to issues, failures, non-compliance, and adverse events in a timely manner so that action can be taken to contain these and keep them from growing.

GRC 20/20 has evaluated and verified the implementation and value of ProcessUnity VRM with clients using the solution. It confirms that their implementations have achieved measurable value across the elements of efficiency, effectiveness, and agility. ProcessUnity VRM clients interviewed by GRC 20/20 include:

- **Financial services.** A financial services firm that operates a leading cryptocurrency exchange platform.
- **Clinical research.** A life sciences/healthcare clinical research organization.
- **Life sciences.** A biopharmaceutical company developing innovative medicines.
- **Professional services firm.** A multinational information technology consulting and systems integration company

In evaluating each of these case studies, GRC 20/20 has researched, evaluated, and verified that ProcessUnity VRM has delivered value across the TPRM (Third Party Risk Management) lifecycle:

1. *Third-Party Risk Oversight & Management*
2. *Third-Party Onboarding*
3. *Third-Party Ongoing Risk Assessment/Monitoring*
4. *Third-Party Risk Reporting, Metrics & Analytics*

Value: Third-Party Risk Oversight & Management

When organizations perform third-party risk oversight and management in manual processes encumbered by documents, spreadsheets, and emails, they spend approximately twice as much time in these activities as they do in a solution like ProcessUnity VRM. In interviewing ProcessUnity VRM clients, GRC 20/20 found that they spend approximately 50 percent less time on third-party risk oversight and management activities. This is because they have all the information they need in one application with views into third-party risk processes, outstanding tasks, and status readily available to them. Without ProcessUnity VRM, these same organizations used to have to reconcile information across disparate, disconnected, and scattered documents, spreadsheets, and emails, which took time.

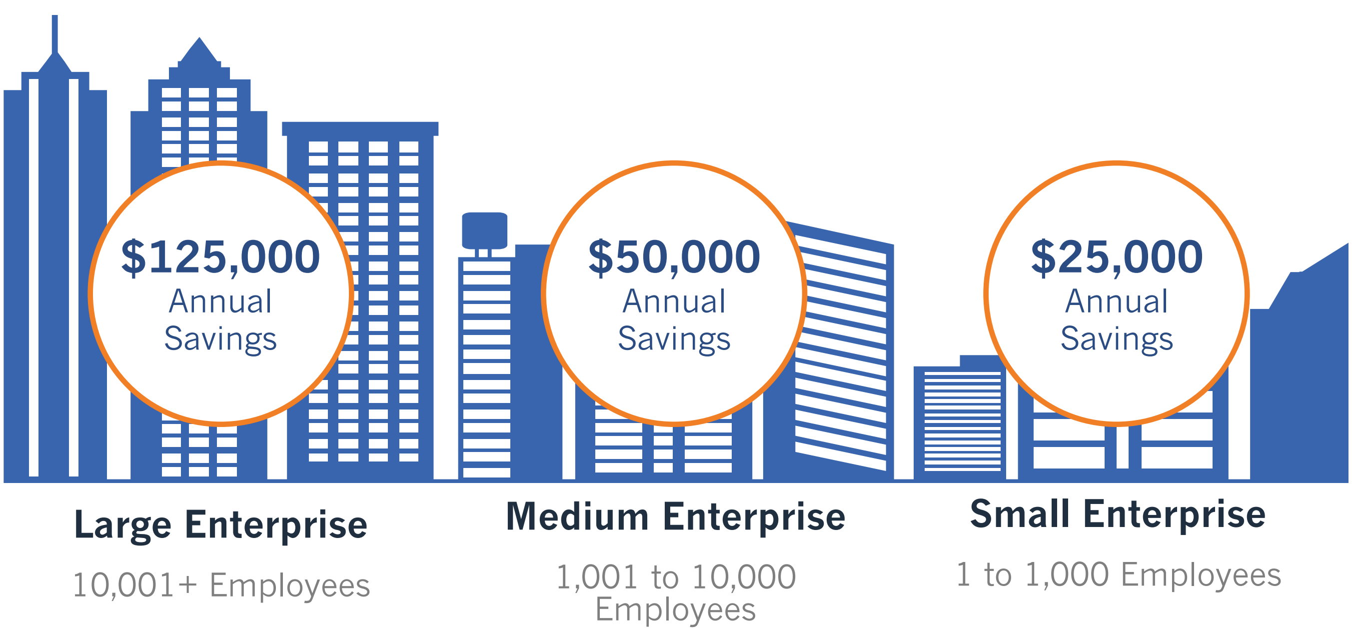
The typical large organization, with 25,000 employees managing approximately 5,000 third-party relationships in a year can expect to save approximately $125,000 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

The typical medium-sized organization, with 7,500 employees managing approximately 2,000 third-party relationships in a year can expect to save approximately $50,000 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

The typical small organization, with 2,500 employees managing approximately 1,000 third-party relationships in a year can expect to save approximately $25,000 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

Efficiency Value

GRC 20/20 has identified the following benefits and measurements of value ProcessUnity VRM clients have achieved in the context of human and financial efficiencies in case planning and administration:



- **Consistency and access to information.** Organizations using ProcessUnity VRM find that the system makes third-party risk oversight and management efficient in staff time. All third-party data is in one place, making the solution faster and easier to consolidate information across assessments, workloads, and tasks. One organization reported that they now have a single source of truth on all third parties and their risk that was previously spread across four different systems.

- **Time savings in oversight.** ProcessUnity VRM allows users to efficiently stay abreast of all third-party risk processes and activities and allows easy updates to executives and stakeholders on matters that may impact the broad business or specific business units.

- **Freeing resources to manage risk.** Organizations find that ProcessUnity VRM enables them to reduce excessive hours managing documents and manual processes that were encumbered by the reconciliation of disparate data sources and reallocate this time to improving risk management and reducing risk exposure.

Effectiveness Value

GRC 20/20 has identified the following benefits and measurements of value ProcessUnity VRM clients have achieved in the effectiveness of third-party risk oversight and management:

- **Elimination of shadow/rogue relationships.** ProcessUnity VRM enables effective third-party risk oversight and management by having a single system of record for all third-party risk processes that every relationship must adhere to. Before suffering from manual processes in scattered departments, organizations struggled with rogue relationships that were never properly assessed.

- **Risk tracking and control.** The ProcessUnity VRM solution enables organizations to track risks of individual relationships and aggregate risks to show what overall third-party risk exposure is.

- **Accuracy of information.** ProcessUnity VRM provides a single system of record for cases that effectively eliminates the need to manage third parties in disparate databases, documents, spreadsheets, and emails. This allows for consistent and accurate information that removes the chance of mismatched versions of documents and the result is corrupted data in the manual reconciliation of documents.

- **Notifications and reminders.** ProcessUnity VRM ensures that third-party risk oversight and management tasks do not slip through the cracks. The solution has detailed workflow, task management, notification, and escalation capabilities, making third-party risk oversight and management more effective. This functionality helps to ensure things get done on a timely basis, whether a specific third- party risk assessment or across third parties in overall planning and administration tasks.

- **Increased collaboration.** ProcessUnity VRM clients see greater collaboration among their third-party risk subject matter experts and relationship owners that is enabled by a single system of record for third-party risk, and real-time reports to management and the executive committees.

Agility Value

GRC 20/20 has identified the following benefits and measurement of value ProcessUnity VRM clients have achieved in the agility and responsiveness in context of third-party risk oversight and management:

- **Single source of truth.** The ProcessUnity VRM solution promotes agility by having a single system of record of all third-party risk relationships and types for administration. This eliminates errors as well as wasted time in manual reconciliation and administration of assessments in disparate databases, documents, and spreadsheets. Overall, clients are more agile with a single source of truth across third-party risk oversight and management activities.

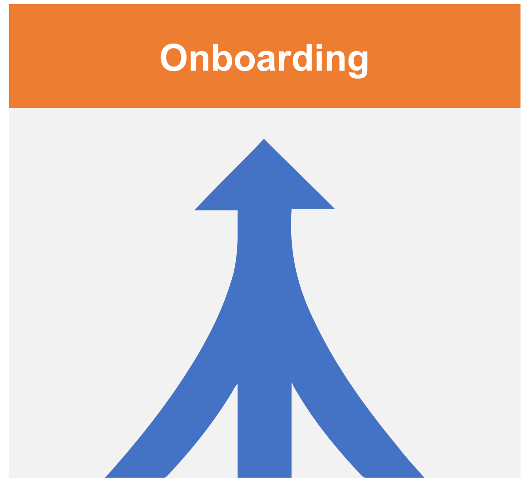
- **Resource planning, backlog, business cycles, and seasonality.** Clients are agile with ProcessUnity VRM as they can manage third-party tasks and processes to address the demands of the business in the context of business cycles/seasons that can impact risk and relationships. Organizations can manage staff, accordingly, assign resources, and know when to prioritize staff time based on the risk context of the business. This makes management of third-party risk assessments resource planning agile to a dynamic business environment.

- **Configuration and adaptability.** ProcessUnity VRM clients find the solution to be easily configured and adaptable to a changing business environment. Third-party risk oversight and management is adaptable with ProcessUnity VRM to new lines of business, acquisitions, and mergers to expand the solution to encompass the needs of a dynamic business. The ease of use and level of customization of the solution allow it to grow with the business.

- **Agile in ad hoc needs.** Clients of ProcessUnity VRM report that the solution allow them to be agile and ready to adapt to new risks and relationships. The ease with which the system is customizable allows clients to step up and assist with issues not inherently within their mission.

- **Visibility and metrics.** ProcessUnity VRM enables continuous third-party risk oversight and management and streamlines quarterly and annual reports into assessments, trending, and analytics. This allows organizations to see where they need to assign resources and where things can be improved.

Value: Third-Party Onboarding



In the context of third-party onboarding, organizations using manual processes with documents, spreadsheets, and emails spend significantly more time onboarding a third party. This typically can involve 20 hours of staff time per third-party onboarded, bringing down to 3 hours with the automation within ProcessUnity VRM. This is a result of varying processes for onboarding, the back and forth between documents and emails to onboard a third-party and following up with missing information and tracking it down. With ProcessUnity VRM, organizations cut this time significantly as the organization has a standard way of onboarding third parties that are logged and managed. This is done, so things do not slip through the cracks and integrate into other business and third-party intelligence systems to pull in information to automate risk oversight in onboarding and increase efficiency.

The typical large organization, with 25,000 employees managing approximately 5,000 third-party relationships in a year can expect to save approximately $442,000 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

The typical medium-sized organization, with 7,500 employees managing approximately 2,000 third-party relationships in a year can expect to save approximately $176,800 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

The typical small organization, with 2,500 employees managing approximately 1,000 third-party relationships in a year can expect to save approximately $88,400 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

Large Enterprise
10,001+ Employees

Medium Enterprise
1,001 to 10,000 Employees

Small Enterprise
1 to 1,000 Employees

Efficiency Value

GRC 20/20 has identified the following benefits and measurements of value ProcessUnity VRM clients have achieved in the context of human and financial efficiencies in third-party onboarding:

- **Automation and assignment.** Third-party onboarding requests registered into ProcessUnity VRM are processed with an ability to automatically do initial categorization triage and onboarding team assignment based on set inputs. This saves time and sees that onboarding is assigned and resolved more efficiently.
- **Templates.** With onboarding assignment, ProcessUnity VRM can set up the initial assessment and onboarding process through established and configurable templates that auto-assign tasks, assessments, and workflows.
- **Reduction in staff time.** One client of ProcessUnity VRM specifically reported that they were able to save several full FTE (approximately $65,000/each) in staff time in the onboarding process.
- **Integration.** ProcessUnity VRM integrates with the broader business environment, further saving time in load sharing third-party information with other systems, like ERP systems. The solution can connect with other business systems and data sources to automatically upload/download third-party information.

Effectiveness Value

GRC 20/20 has identified the following benefits and measurements of value ProcessUnity VRM clients have achieved in the effectiveness of third-party onboarding:

- **Elimination of noise.** ProcessUnity VRM enables effective onboarding by triangulating key risk areas to assess based on information and categorization of the third-party relationship, removing redundancies, and eliminating inefficiencies. All third-party relationships must be reported into the system for it to onboard and cannot be bypassed.
- **Consistency in process.** With ProcessUnity VRM, clients can define their onboarding process and have a consistent approach to the third-party onboarding processes, tasks, assessment, and information. This provides a structured process that is effective at gathering required information and moving the onboarding process along. All information must be entered for a third-party to go on to the next stage of the process.
- **Preliminary triage.** Onboarding risk issues can be flagged through an initial risk triage process in ProcessUnity VRM which conducts a preliminary risk analysis to warrant if the relationship should move on to the next stage of the third-party lifecycle.

Agility Value

GRC 20/20 has identified the following benefits and measurements of value ProcessUnity VRM clients have achieved in the agility and responsiveness in the context of third-party onboarding:

- **Focus on what is important.** The onboarding and third-party risk triage process automated in ProcessUnity VRM enables the organization to manage the range of issues, classify them, and assign resources to the most significant risk exposures in a new relationship to the organization. This enhances the agility of the organization to gather and manage third-party risks in the context of dynamic business environments.

- **Multiple pathways for reporting.** ProcessUnity VRM allows the integration of multiple pathways for the reporting of onboarding. With the solution, organizations become agile as it becomes the integration point of all onboarding assessments, reports, and critical information. Third-party risks can be quickly in the system and resolution processes initiated.

Value: Third-Party Ongoing Risk Assessment/Monitoring

Ongoing assessment and monitoring

Conducting ongoing third-party risk assessments is where organizations spend a lot of time in the lifecycle of a relationship. On average, GRC 20/20 finds that each third party annually requires about 10 hours of time utilizing manual processes with documents, spreadsheets, and emails. Some assessments take significantly longer than this average which may involve hundreds of hours if onsite inspections and audits are required. Others may be done quickly after a few hours of assessment. Twenty hours is the average time per third-party relationship when done in manual processes.

With ProcessUnity VRM, GRC 20/20 finds organizations spend less time on ongoing assessments as all information, assessments, tasks, and workflows are conveniently located in one application and readily accessible and easy to report on. This results in a minimum time efficiency savings of 85%.

Utilizing the findings of eighty-five-percent savings, the typical large organization, with 25,000 employees managing approximately 5,000 third-party relationships in a year can expect to save approximately $2,210,000 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

The typical medium-sized organization, with 7,500 employees managing approximately 2,000 third-party relationships in a year can expect to save approximately $884,000 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

The typical small organization, with 2,500 employees managing approximately 1,000 third-party relationships in a year can expect to save approximately $442,000 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

Large Enterprise

10,001+ Employees

Medium Enterprise

1,001 to 10,000 Employees

Small Enterprise

1 to 1,000 Employees

Efficiency Value

GRC 20/20 has identified the following benefits and measurements of value ProcessUnity VRM clients have achieved in the context of human and financial efficiencies in ongoing third-party risk monitoring and assessment:

- **Integration of information.** ProcessUnity VRM saves clients time by having all third-party risk assessment information in one place. This eliminates staff time spent chasing emails and documents for assessments that are not done or partially filled out. The solution further drives efficiency through an intuitive interface that allows for ease of use to get assessments completed.
- **Prepopulate information.** The ProcessUnity VRM solution allows the system to integrate with other business systems to prepopulate contact and other pertinent third-party information. Third-party assessment reports are automatically populated with relevant and current information.
- **Reduction in staff time.** ProcessUnity VRM clients report they can standardize ongoing/periodic third-party assessment steps and processes to the point they have been able to easily cross-train subject matter experts to handle a broader array of assessments. This allows organizations to consolidate previously independent groups into a single third-party risk assessment team, which allows them to significantly reduce staffing, or elect to expand an assessments reach rather than eliminate positions.

Effectiveness Value

GRC 20/20 has identified the following benefits and measurements of value ProcessUnity VRM clients have achieved in the effectiveness of ongoing third-party assessments and monitoring:

- **Organization.** With ProcessUnity VRM, clients are more effective in ongoing/periodic third-party risk assessments as the solution helps them keep all assessment documentation cataloged and organized. The solution allows for the management of all information so it is in one place. Paper trails are no longer needed as all information can be attached into the system.
- **Automation.** ProcessUnity VRM increases the effectiveness of the ongoing assessment and monitoring process through defined tasks, notifications, escalation procedures, and reminders. This ensures the process is followed and things do not slip through cracks.
- **Defensibility.** ProcessUnity VRM delivers a strong audit trail and system of record of how assessments and ongoing monitoring of third-parties were conducted. This allows for a clear chain of evidence to defend the organizations with regulators and provide assurance to stakeholders.
- **Consistency.** ProcessUnity VRM's ability to standardize the third-party risk process and ensure it is followed in a uniform manner has reduced individual interpretations and allows organizations to hold individuals accountable for third-party risk.

Agility Value

GRC 20/20 has identified the following benefits and measurements of value ProcessUnity VRM clients have achieved in the agility and responsiveness in the context of third-party assessments and monitoring:

- **Adaptability and collaboration.** ProcessUnity VRM provides a framework for agile and adaptable third-party risk assessments and monitoring that facilitate collaboration on processes. As investigations change and third parties change, the solution allows subject matter experts to collaborate and hand off work products from one to another.

Value: Third-Party Risk Reporting, Metrics & Analytics

Reporting, analytics & metrics

Third-party risk reporting and metrics can be one of the costliest areas of third-party risk management when done in manual processes of documents, spreadsheets, and emails. Organizations find that they have a significant amount of staff time that goes into manual reconciliation of hundreds to thousands of assessment records, pulling specific information out of each third party, and putting it into periodic reports for the board, regulators, relationship owners, and other stakeholders.

With ProcessUnity VRM, the time spent on case reporting and metrics is, estimated conservatively, 10 percent of the time organizations used to spend on manual processes with documents, spreadsheets, and emails. This is because all third-party risk information is in one place that is easily reported on. In fact, one organization stated that what took 2 hours per vendor/third-party to produce a report on investigations is now less than one minute with ProcessUnity VRM, so the savings can be much more significant than what GRC 20/20 models here.

Utilizing the findings of eighty-five-percent savings, the typical large organization, with 25,000 employees managing approximately 5,000 third-party relationships in a year can expect to save approximately $468,000 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

The typical medium-sized organization, with 7,500 employees managing approximately 2,000 third-party relationships in a year can expect to save approximately $187,200 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

The typical small organization, with 2,500 employees managing approximately 1,000 third-party relationships in a year can expect to save approximately $93,600 a year in time and labor costs due to the efficiency ProcessUnity brings to the organization.

Efficiency Value

GRC 20/20 has identified the following benefits and measurements of value ProcessUnity VRM clients have achieved in the context of human and financial efficiencies in third-party risk reporting and metrics:

- **Reduced individual third-party reporting time.** ProcessUnity VRM clients report a significant value in the efficiency of time spent in reporting. One client reported that a final report on a third-party risk assessment used to take about one hour to process and build and now takes them minutes, and that is just one third-party report among hundreds.

Large Enterprise

10,001+ Employees

Medium Enterprise

1,001 to 10,000 Employees

Small Enterprise

1 to 1,000 Employees

- **Reduced year-end reporting time.** Reporting efficiencies are also seen on aggregate reporting for specific business cycles/periods, such as year-end reporting on third-party risks to the board. One client stated that year-end reporting took them three weeks of FTE time to put together as they went through files and did manual reconciliation; with ProcessUnity VRM it now takes them ten minutes.

- **General efficiency in reporting.** ProcessUnity VRM clients find reporting to be highly configurable and overall faster and easier to consolidate information from their previously manual processes. Overall, they particularly find a significant efficiency gain in the analytic capabilities of ProcessUnity VRM.

Effectiveness Value

GRC 20/20 has identified the following benefits and measurements of value ProcessUnity VRM clients have achieved in the effectiveness of third-party risk reporting and metrics:

- **Benchmarking and metrics.** ProcessUnity VRM improves third-party risk processes by having detailed reporting, benchmarking, and metric capabilities to benchmark third-party risk assessment timelines, reduce gaps, and track past due tasks.

- **Flexibility of reporting.** Clients find value in ProcessUnity VRM's ability to consolidate and report on the range of data collected in the solution, accommodate changes to standard reports, and edit those reports. This is facilitated by standard report templates that are editable.

- **Regulatory and stakeholder assurance.** Clients report that they are satisfied with ProcessUnity VRM's delivery of a fully standardized and auditable tracking system to report to regulators just what actions the organization has taken to address risk and ensure compliance with law and regulations in third-party relationships.

Agility Value

GRC 20/20 has identified the following benefits and measurements of value ProcessUnity VRM clients have achieved in the agility and responsiveness in the context of third-party risk reporting and metrics:

- **Contextual awareness.** ProcessUnity VRM enables clients to gain full Insight into timeframes, statistics, cross third-party reporting, and risk aggregation. This includes overall metrics to see how things are trending and where exposure is the greatest.

- **Adaptability of reports.** The ProcessUnity VRM solution has robust capabilities to do ad hoc reporting in a simple and easy-to-use interface, with minimal training.

Total GRC Value & Return

GRC 20/20 finds that ProcessUnity VRM delivers value to organizations of all sizes. This value is quantified across issue reporting and case management lifecycle stages. This enables organizations to achieve quantitative and qualitative benefits that make them more efficient, effective, and agile.

Large Organization Value & Return

Large organizations utilizing ProcessUnity VRM can typically see a return on investment in less than one month (29 days) in the benefits of efficiency that ProcessUnity VRM brings them. Initial year implementation costs for large organizations are typically $350,000, while savings in the first year are $3,245,000. This brings a value savings of $2,895,000 in the first year. Subsequent years see ongoing licensing and maintenance costs of $280,000 with ongoing efficiency savings of $3,245,000. This brings subsequent year savings to $2,965,000 a year.

Large Enterprise

10,001+ Employees

When you factor in risk reduction in minimizing the cost of an incident exposure and reduction in cost of audit issues, it increases the value that ProcessUnity delivers.

Over a five-year period, large organizations should expect to pay about $1,370,000 in the annual subscription, initial implementation, and ongoing support/maintenance costs while seeing an efficiency savings of $16,225,000 throughout the third-party risk management process. This means a total return on investment of $14,855,000 over five years.

Item	Year 1	Year 2	Year 3	Year 4	Year 5	Total
COSTS						
ANNUAL SUBSCRIPTION FEES	$250,000	$250,000	$250,000	$250,000	$250,000	**$1,250,000**
IMPLEMENTATION COSTS	$100,000					**$100,000**
ONGOING COSTS POST-IMPLEMENTATION		$30,000	$30,000	$30,000	$30,000	**$120,000**
	$350,000	**$280,000**	**$280,000**	**$280,000**	**$280,000**	**$1,370,000**
BENEFITS						
OVERSIGHT & MANAGEMENT	$125,000	$125,000	$125,000	$125,000	$125,000	**$625,000**
ONBOARDING	$442,000	$442,000	$442,000	$442,000	$442,000	**$2,210,000**
ONGOING ASSESSMENT	$2,210,000	$2,210,000	$2,210,000	$2,210,000	$2,210,000	**$11,050,000**
PERIODIC REPORTING, METRICS & ANALYTICS	$468,000	$468,000	$468,000	$468,000	$468,000	**$2,340,000**
	$3,245,000	**$3,245,000**	**$3,245,000**	**$3,245,000**	**$3,245,000**	**$16,225,000**

Medium Organization Value & Return

Medium organizations utilizing ProcessUnity VRM can typically see a return on investment in a little over one month (33 days) in the benefits of efficiency that ProcessUnity VRM brings them. Initial year implementation costs for medium organizations are typically $130,000 while savings in the first year are $1,298,000. This brings a value savings of $1,168,000 in the first year. Subsequent years see ongoing licensing and maintenance costs of $117,500 with ongoing efficiency savings of $1,298,000. This brings subsequent year savings to $1,180,500 a year.

Medium Enterprise

1,001 to 10,000 Employees

When you factor in risk reduction in minimizing the cost of an incident exposure and reduction in cost of audit issues, it increases the value that ProcessUnity delivers.

Over a five-year period, medium organizations should expect to pay about $572,500 in annual subscription, initial implementation, and ongoing support/maintenance costs while seeing an efficiency savings of $6,490,000 throughout the third-party risk management process. This means a total return on investment of $5,917,500 over five years.

Item	Year 1	Year 2	Year 3	Year 4	Year 5	Total
COSTS						
ANNUAL SUBSCRIPTION FEES	$102,500	$102,500	$102,500	$102,500	$102,500	**$512,500**
IMPLEMENTATION COSTS	$27,500					**$27,500**
ONGOING COSTS POST-IMPLEMENTATION		$15,000	$15,000	$15,000	$15,000	**$60,000**
	$130,000	**$117,500**	**$117,500**	**$117,500**	**$117,500**	**$572,500**
BENEFITS						
OVERSIGHT & MANAGEMENT	$50,000	$50,000	$50,000	$50,000	$50,000	**$250,000**
ONBOARDING	$176,800	$176,800	$176,800	$176,800	$176,800	**$884,000**
ONGOING ASSESSMENT	$884,000	$884,000	$884,000	$884,000	$884,000	**$4,420,000**
PERIODIC REPORTING, METRICS & ANALYTICS	$187,200	$187,200	$187,200	$187,200	$187,200	**$936,000**
	$1,298,000	**$1,298,000**	**$1,298,000**	**$1,298,000**	**$1,298,000**	**$6,490,000**

Small Organization Value & Return

Small Enterprise

1 to 1,000 Employees

Small organizations utilizing ProcessUnity VRM can typically see a return on investment in a little over one month (37 days) in the benefits of efficiency that ProcessUnity VRM brings them. Initial year implementation costs for small organizations are typically $72,500 while savings in the first year are $649,000. This brings a value savings of $576,500 in the first year. Subsequent years see ongoing licensing and maintenance costs of $67,750 with ongoing efficiency savings of $649,000. This brings subsequent year savings to $58,250 a year.

When you factor in risk reduction in minimizing the cost of an incident exposure and reduction in cost of audit issues, it increases the value that ProcessUnity delivers.

Over a five-year period, small organizations should expect to pay about $329,750 in annual subscription, initial implementation, and ongoing support/maintenance costs while seeing an efficiency savings of $3,245,000 throughout the third-party risk management process. This means a total return on investment of $2,915,250 over five years.

Item	Year 1	Year 2	Year 3	Year 4	Year 5	Total
COSTS						
ANNUAL SUBSCRIPTION FEES	$58,750	$58,750	$58,750	$58,750	$58,750	**$293,750**
IMPLEMENTATION COSTS	$13,750					**$13,750**
ONGOING COSTS POST-IMPLEMENTATION		$9,000	$9,000	$9,000	$9,000	**$36,000**
	$72,500	**$67,750**	**$67,750**	**$67,750**	**$67,750**	**$329,750**
BENEFITS						
OVERSIGHT & MANAGEMENT	$25,000	$25,000	$25,000	$25,000	$25,000	**$125,000**
ONBOARDING	$88,400	$88,400	$88,400	$88,400	$88,400	**$442,000**
ONGOING ASSESSMENT	$442,000	$442,000	$442,000	$442,000	$442,000	**$2,210,000**
PERIODIC REPORTING, METRICS & ANALYTICS	$93,600	$93,600	$93,600	$93,600	$93,600	**$468,000**
	$649,000	**$649,000**	**$649,000**	**$649,000**	**$649,000**	**$3,245,000**

GRC 20/20's Final Perspective . . .

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 ProcessUnity VRM to enable organizations in consistent management of third-party risk — readers should not see this as a complete and unquestionable endorsement of ProcessUnity VRM.

GRC 20/20 finds that ProcessUnity VRM provides the greatest value to organizations that can reap the benefits of replacing thousands of documents, spreadsheets, and emails with an application that automates and enables the entire third-party risk lifecycle process.

ProcessUnity VRM is an established player in the third-party risk management segment of the GRC market. It has clients around the world managing a complex array of third-party relationships. GRC 20/20 finds that ProcessUnity VRM has what it takes to manage third-party risk to the highest industry standards and requirements in a flexible platform that is agile to the modern organization's needs to be agile.

Organizations looking to adopt ProcessUnity VRM can do so broadly or narrowly. They can implement ProcessUnity VRM as an enterprise platform to manage the range of third-party risks across the organization. Alternatively, they can start with a focused area of third-party risk management, such as IT vendor risk, and expand to other use cases and departments over time.

ProcessUnity VRM enables the organization to manage staff time more efficiently by reducing manual tasks and spending more time on third-party risk processes. ProcessUnity VRM provides a cost-efficient platform to allow third-party risk teams to better collaborate globally and share and report consistent information. This enables clients to be more agile and quickly respond to changes in their business or industry. As organizations continue to grow and have relationships globally, ProcessUnity VRM will ensure continuous low costs, information consistency, interactive global collaboration, and control and process transparency.

Organizations using ProcessUnity VRM should look to further benefits to mature their third-party risk management processes to deliver:

- **Holistic awareness of risk.** This means there is a defined taxonomy across the enterprise that structures and catalogs third-party risks in the context of business and assigns accountability. A consistent process identifies issues and keeps the taxonomy current. With ProcessUnity VRM in place, the organization aggregates third-party risk data and effectively communicates, monitors, and manages risk exposure.
- **Risk-intelligent decision-making.** This means the business has what it needs to make risk-intelligent business decisions that can drill down into the history of where third-party risk has materialized. Third-party risk management is an integral part of business responsibilities. ProcessUnity VRM enables organizations to

manage third-party risk exposure in the context of business and is structured to complement the business lifecycle to help executives make effective decisions.

- **Accountability of issues.** Accountability and issue ownership are established features of third-party risk management. Every issue in a third-party, at the enterprise and business-process level, should have clearly established owners. Risk exposure should be communicated to stakeholders and the organization's track record should illustrate successful management of issues.

- **Multidimensional third-party risk analysis and planning.** The organization needs a range of analytics, correlation, and scenario analysis. Various ProcessUnity VRM qualitative and quantitative analysis techniques enable the organization to understand third-party risk to feed into the analysis. Remediation plans must be effective and monitored for progress. Again, this allows an organization to "keep score" and know that they are winning the battle.

Appendix

Disclosures

This GRC Value Perspective research was commissioned by ProcesssUnity. GRC 20/20 Research makes no assumptions or guarantees as to the potential value and ROI that any particular organization will receive. GRC 2020 advises that readers use their own estimates with the framework provided in this research piece to determine the value of utilizing ProcessUnity. ProcessUnity reviewed and provided feedback to GRC 20/20 Research, but GRC 20/20 maintained editorial control over the reserarch and findings and does not accept changes to the study that contradict GRC 20/20's findings or obscure the meaning of the study. ProcessUnity provided the customer names for the interviews but did not participate in the interviews.

GRC Value Perspective Methodology

GRC 20/20 interviewed 4 ProcessUnity clients to determine the value and benefits they received from implementing ProcessUnity. From the findings provided in these interviews, GRC 20/20 constructed an economic model of value ProcessUnity clients cans exepct to achieve from utilizing ProcessUnity for issue reporting and case management. This model details the cost and benefits clients typically can expect. Benefits were measured in measured efficiency, effectiveness, and agility organizations achieved with ProcessUnity.

GRC 20/20 conducted the following tasks to define and measure the value of ProcessUnity in clients:

- *Reviewed* ProcessUnity solution and related collateral materials to understand how the solution works and types of problems it solves.
- *Interviewed* four organizations utilizing ProcessUnity to determine the benefits and values each of them received over how they previously approached issue reporting and case management.
- *Developed* a financial model from the findings of the interviews to determine the value received by the typical small, medium, and large organization utilizing ProcessUnity. This financial model is composed of the cost and benefit data obtained from these interviews.
- *Published* this research paper on the value of ProcessUnity for issue reporting and case management.

Further details on the model and specific assumptions and parameters used to caculate value can be obtained from GRC 20/20 Research by emailing info@grc2020.com.

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.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com