PROCESS UNITY

VENDOR RISK MANAGEMENT:

CONDUCTING PRE-CONTRACT DUE DILIGENCE IN A DIGITALLY CONNECTED WORLD

HEADQUARTERS
33 Bradford Street
Concord, MA 01742
PHONE: 978-451-7655

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

VENDOR RISK MANAGEMENT: CONDUCTING PRE-CONTRACT DUE DILIGENCE IN A DIGITALLY CONNECTED WORLD

YOU WANT TO BEGIN WITH YOUR BEST FOOT FORWARD — BUT DO YOU KNOW WHERE ALL YOUR VENDOR RISKS REALLY STAND?

Today's global, digital economy opens up a world of opportunities—and a whole new world of risk exposure. Few businesses can scale, or even survive, without a significant chain of vendors and/or suppliers—third parties who contribute essential elements to our enterprises. Many large industries—such as financial services, health-care/health insurance, oil and gas, and consumer goods—rely on a vast web of vendor relationships to conduct day to day operations.

But when important parts of your business can be fulfilled anywhere, risks may be everywhere—and responsibility cannot be deferred. In the minds of regulators, partners, investors and, perhaps most importantly, your clients and customers, the buck stops with you.

When one of your vendors takes a hit, you could take the fall. But do you have a clear picture of your vulnerability?

What happens when things go wrong…

Consider the executive of a substantial Boston bank who believed his customers' personally identifiable information (PII) was perfectly secure; after all, this VP had trusted a reputable data center to host his financial applications. What he didn't know was that his own vendor had subcontracted data recovery operations to a "fourth party" that was not scrupulously vetted. When this weak link was hacked, damage traveled all the way up the chain, compromising the bank's reputation—and exposing it to regulatory fines and other legal actions.

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

WHO'S WATCHING YOU?

This is just a sampling of the many regulatory bodies to whom many companies must demonstrate responsible compliance:

- Consumer Financial Protection Bureau (CFPB)
- Federal Deposit Insurance Corporation (FDIC)
- Office of the Comptroller of the Currency (OCC)
- U.S. Securities and Exchange Commission (SEC)
- State Insurance Agencies, and more…

Best protection: Get it right from the start

In business as in health, prevention is the best medicine. Pre-contract vendor due diligence is the key to intercepting risks before they become problems. The contract itself can be a powerful lever for ensuring compliance. By articulating precise commitments and expectations in the Service Level Agreement (SLA)—and adding potential financial penalties and other recourses for compensation—companies give themselves an important layer of protection, an opportunity that is no longer available *after* the contract is signed.

That's why effective due diligence:

- Probes every area of potential risk and requires confirmation of assurance
- Interprets vendor responses at appropriate levels of analysis, based on engagement, scope and potential threat levels
- Requests and archives appropriate documentation
- Creates a rational process for rejecting, approving, or conditionally approving a vendor relationship

Frankly, due diligence has many moving parts, and managing them all can be complicated. In this paper, you'll find important tools for making the process both simpler and more accountable. In *Conducting Pre-Contract Due Diligence in a Digitally Connected World* we'll point out all the important pieces you must pull together, and show you a model for replacing expensive—and vulnerable—manual processes with automated due diligence systems that can save you time, money, and a whole lot of trouble.

CREATE A RATIONAL DUE DILIGENCE PROGRAM

Establishing confidence in your vendor relationships begins by imposing order internally on your own vendor risk management (VRM) process. Random requests and ad hoc workflows must be substituted with documented, repeatable processes that are clearly understood within your company—and demonstrate accountability to regulators.

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

At a minimum, pre-contract due diligence, consistently fulfilled *before* contracts are signed, involves the following steps:

1. **Line of Business Request:** An internal line of business, seeking a new service or a change in service, submits a request for certification to its organization's VRM team, who assume responsibility for vetting potential vendors, assuring compliance with the company's standards, and for making recommendations regarding engagement.

2. **Classification:** The VRM team examines the request and classifies its type of service, which informs the level, nature and extent of the due diligence process. A low-risk request, such as for a cafeteria service, would require far less investigation than a data application host, which would be privy to sensitive information.

3. **Due Diligence:** After classification, the team directs the appropriate vendors through a two-stage process:

   a. **Internal:** The first wave of pre-contract inquiry is conducted in-house to determine the level of risk the company may be exposed to, and to research potential vendors via publically available sources, such as government watch lists and third-party databases like Thomson Reuters, Dow Jones, Dun & Bradstreet, LexisNexis, or Rapid Ratings, to name a few.

   b. **External:** The second wave submits inquiries directly to the vendors who made the first cut. Here, the vendors themselves answer potentially hundreds of questions, and submit relevant documents, to demonstrate capability with regulatory demands and company standards.

4. **Assessment:** Informed by the internal and external due diligence results, risk analysts decide on status: to reject the vendor, to accept the vendor without further clarification, or to accept the vendor with conditions—modified contracting terms and SLAs that sufficiently address the issues exposed in the due diligence process.

THE EXPERTS SPEAK...

On the scope of vendor relationships:
IT and business services outsourcing in US banking and financial services is expected to mushroom by more than 25% by 2016. **Deloitte**

On the ineffectiveness of current vendor due diligence:
71% of companies say they are confident that their security activities are effective, yet only 32% require third parties to comply with their policies. **PWC**

On the advice they have for enterprises:
Stop awarding work to third parties based solely on price or financial value. **Deloitte**

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

For a comprehensive risk picture, we recommend addressing nine categories of due diligence, four for internal review, five for external review:

IDENTITY Are they for real?	**FINANCIAL** Financially viable?	**REPUTATION** Negative Press?
GEOGRAPHIC Where does our data go and who performs the services?	**INFORMATION SECURITY** Will our data be secure?	**BUSINESS CONTINUITY** Are they prepared for the worst?
COMPLIANCE Do they dot the i's and cross the t's?	**FOURTH-PARTY** How much risk is out of sight?	**CONFLICT OF INTEREST** Do I need to worry about corruption?

Internal Due Diligence

A request for certification triggers the internal half of the formal review, fulfilled by company employees or agents who investigate four areas of due diligence:

I. Identity

Are your potential vendors who they say they are? Is the picture they create consistent with the underlying reality—or are they posting a false front?

II. Financial

What about their financial status? Do they have outstanding debts or weak revenue streams that call their viability into question? They're here today, but can you trust they won't be gone tomorrow?

III. Reputation

How are they regarded by others and by the media? Do they have skeletons that could fall from their closets and rattle your brand? Are they worthy of your confidence—and the trust of your customers?

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

IV. Geographic

Are they located in trouble-spots vulnerable to violence or disruption? If the relationship involves sharing customer data, are they in countries that, by US law, can accept that data?

After investigating these four due diligence domains, internal teams can classify potential vendors on a scale with tentative approval on one extreme to outright rejection on the other, with varying degrees of potential risk in between.

By doing so, the company can eliminate vendors who fail to meet fundamental standards, or can flag vendors who may remain worthy of consideration, but require further inquiry and/or clarification.

External Due Diligence

The external half of the review pursues information, usually in the form of questionnaires and document requests, from the vendors themselves, across the following five areas:

V. Information Security

Will the data you share with them be secure? Will that security meet regulatory standards? What controls do they have in place to ensure that security?

VI. Business Continuity

In the event of disaster, natural or man-made, do they have plans, resources and facilities in place to restore operations?

VII. Compliance

Do they have formal, documentable policies, procedures and processes to ensure and demonstrate compliance?

VIII. Fourth-Party

What about your vendors' vendors? How exposed are you to vendors you cannot see? Have your vendors performed and documented due diligence on their vendors?

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

HOW WIDE DO YOU HAVE TO CAST YOUR DUE DILIGENCE NET?

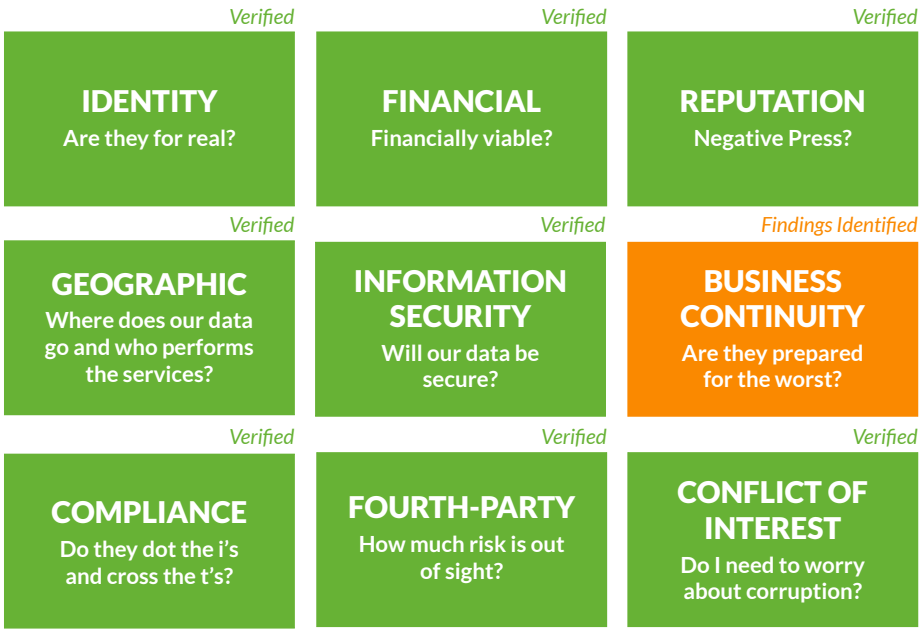
The answer depends on the nature of your industry and the regulatory obligations it must fulfill. The following list is just a sample of the many regulations and standards many companies have to consider:

- OCC 2013-29 Third Party Relationships
- HIPAA
- CFPB Bulletin 2012-03
- Payment Card Industry Data Security Act
- Sarbanes-Oxley

IX. Conflict of Interest

Do they have relationships with your executives, employees, partners, trustees, board members or other parties that might be seen as conflicts of interest? If so, have they placed restrictions or other limitations that prevent corruption or even the appearance of conflict?

Internal due diligence tells you how much further investigation—and in which domains—need to be pursued before contracting with a vendor.



When the process is fulfilled correctly, companies arm themselves with sufficient information for exercising sound judgment: whether to proceed with the vendor, amend service level agreements (SLAs) to compensate for potentially problematic areas, or to decline doing business with the vendor altogether.

Given the scope of the due diligence process, and complexity of the documentation requirements, even the best intentions can be undermined by failures in execution—gaps and inconsistencies in the workflow that compromise risk management.

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

WARNING: MANUAL IS NOT MANAGEABLE

Comprehensive and consistent investigation and analysis is the key to successful due diligence. But the way most companies approach vendor risk management opens new risks, threatening the integrity of the process.

In ProcessUnity's experience nine out of ten customers manage pre-contract due diligence through manual processes. On one level, there is the issue of inefficiency; you could calculate the cost of manual processing by multiplying the number of resources dedicated to due diligence by their number of work hours, multiplied again by the opportunity cost of this consumption of time and talent.

Resources X hours X opportunity cost = inefficiency of manual due diligence

But even if inefficiency could be dismissed as the cost of doing business, there can be no excuse for ineffectiveness. Manual management cannot keep pace with the scope and scale of contemporary due diligence, exposing the company to unnecessary errors and risks. Here's why:

Scale: An average of 28,000 questions

The principal instrument of external due diligence is a questionnaire packed with questions, lots of questions: The average Standard Information Gathering (SIG) questionnaire sits at 1,300 questions, and we have found our customers' average assessment sits at **400 questions**. Multiply that by an average number of vendors to vet, 70, the VRM team is looking at **28,000** questions to review.

Worse, not every industry category, nor even every vendor in the same category of service, merits the same set of questions. Each vendor query, therefore, requires hand-customization of the questionnaire to assure relevance.

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

WHAT DOES THE OCC WANT TO SEE?

As one of the leading (and most demanding) federal regulatory bodies, the Office of the Comptroller of the Currency has a lot to say about VRM and how due diligence is represented to them.

While the OCC has not explicitly ruled out the use of spreadsheets, today's dominant due diligence tool, it has expressed discomfort with contemporary, manual workflows.

The OCC wants to see repeatable VRM processes that display a consistency of interpretation. The goal? To reduce or eliminate subjectivity.

In the context of maturing digital technologies, and increasing OCC frustration with inconsistent due diligence policies, manual VRM methods can expect greater scrutiny and regulatory dissatisfaction.

Workflow: No means of tracking completions, omissions

Sure, many questionnaires, like surveys, can be posted online. But online posting is not true automation—not even close. Vendors have to be directed to the appropriate link. Whether distributed as Excel, Word or PDF files, or hosted on the Web, email serves as the principle workflow tool. The VRM team has to send out the emails, then track the responses as they come in.

That means someone has to manually record, usually via a spreadsheet, the progress of questionnaire completions: How many have been returned? And by whom? And are the returned questionnaires genuinely complete? If not, the VRM team has to pursue each unanswered question, each unfulfilled request for supporting documentation.

Analysis: No way to query results, compile reports

The primary value of the questionnaire lies in its power to inform contracting decisions and to bring transparency to the decision-making process. Yet when the answers must be compiled, compared, and analyzed by hand, there's no prompt and easy way to query the responses—as you would a database—to get the answers you, and the regulators, want. At best, the process is slow and expensive. At worst, the process misses potential gaps or shortcomings, exposing the company to regrettable contracts and partners.

GO WITH THE FLOW: THE POWER OF AUTOMATION

According to the OCC, a thorough and fully accountable due diligence process is your VRM ideal; automation is the practical way to achieve it. By shifting from manual, spreadsheet-based practices to an automated process facilitated by applications and cloud connectivity, you immediately resolve the tactical impediments to success:

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

Scale: No limits on volume of questions or vendors

With digital applications, you eliminate the problem of scale. Now you can draw upon a database of previously created questions and templates to customize your questionnaires by industry, or by the express needs of the line of business requesting the vetting. By using the cloud as the hosting vehicle, you eliminate the need for complex and time-consuming third-party authorizations; outside vendors can fulfill information requests without crossing firewalls or DMZs (online neutral zones).

Workflow: Dashboards track progress

The program follows the progress of individual vendor participants, producing reports that indicate completion status and identify potential problems that require resolution.

Analysis: System pushes alerts

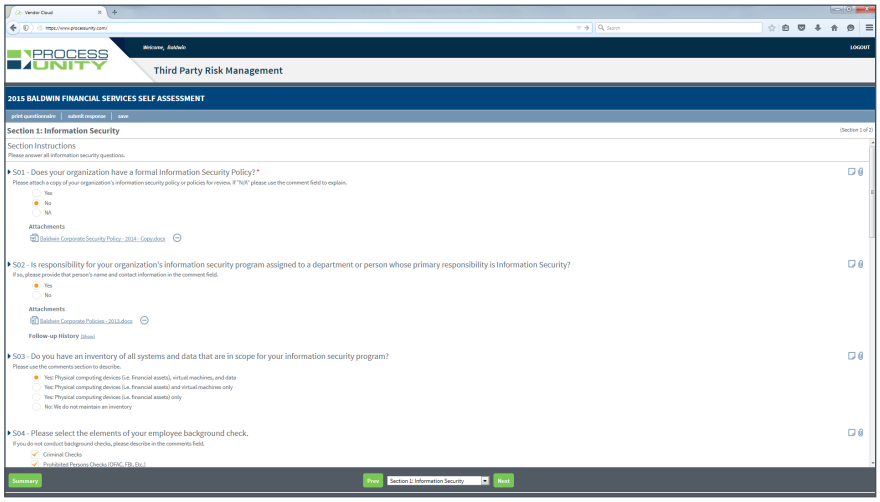
Automated applications can not only respond to queries, but can be set to generate alerts that signal the vendor's relative threat or risk level on any of the nine domains of due diligence.

Initiating Internal Due Diligence

In an automated sequence, due diligence begins with a vendor request from an internal line of business. This first step captures all the necessary basic information about the internal originator and the potential vendor, and clarifies the risk threshold through a series of inquiries regarding the potential for risk exposure and the relative severity of consequences for the company.

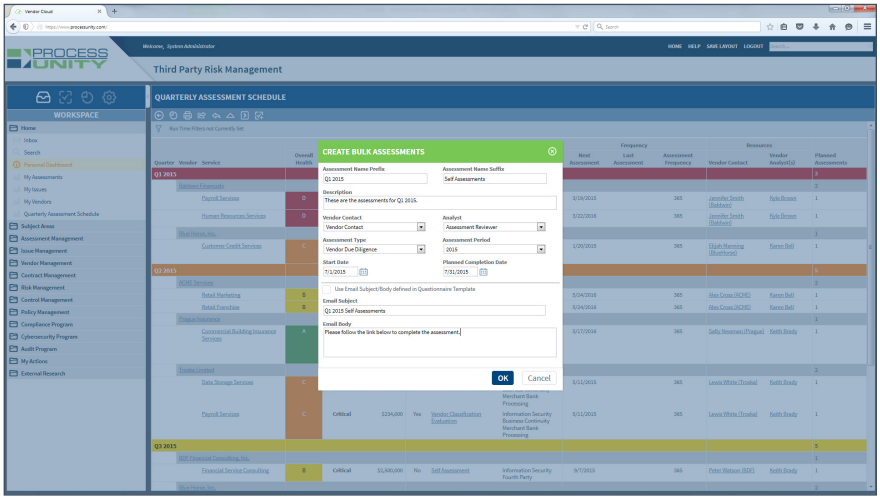
© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

In ProcessUnity's experience, nine out of ten customers manage pre-contract due diligence through manual processes.



The first form initiates due diligence with nuts-and-bolts inquiries and basic probes into potential risks.

Based on the answers to the Vendor Request Form, risk analysts get a streamlined, yet precise picture of the potential risk the vendor may represent to the firm. The application generates a recommendation for the level of necessary due diligence based on classifications in four risk areas: strategic, physical, information security, and business continuity.

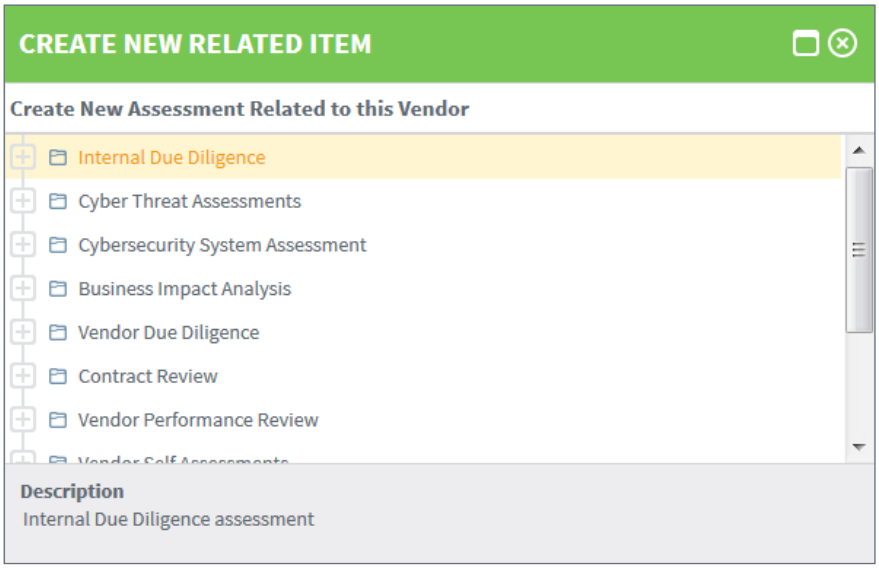


The initial vendor classification quickly answers a crucial question: How much due diligence, if any, is necessary?

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

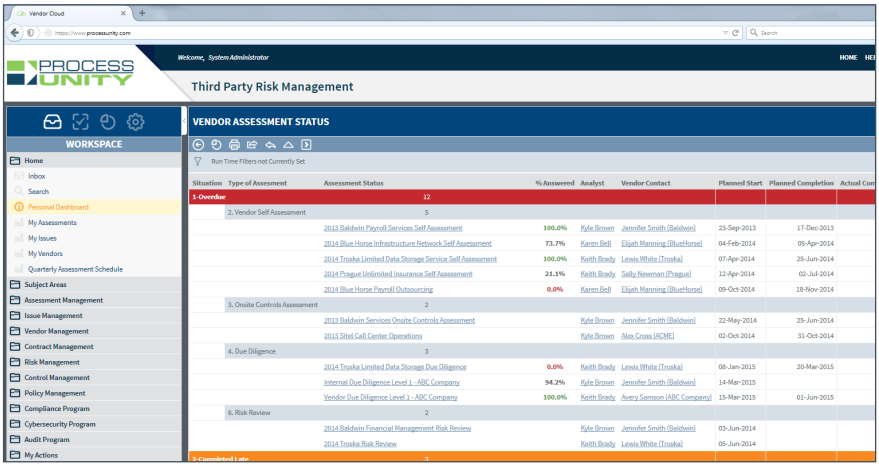
Capturing External Due Diligence

After the internal portion of the workflow is complete, risk analysts can assemble an appropriate vendor questionnaire, based on the level of potential risk that draws upon a database of pre-established questions.

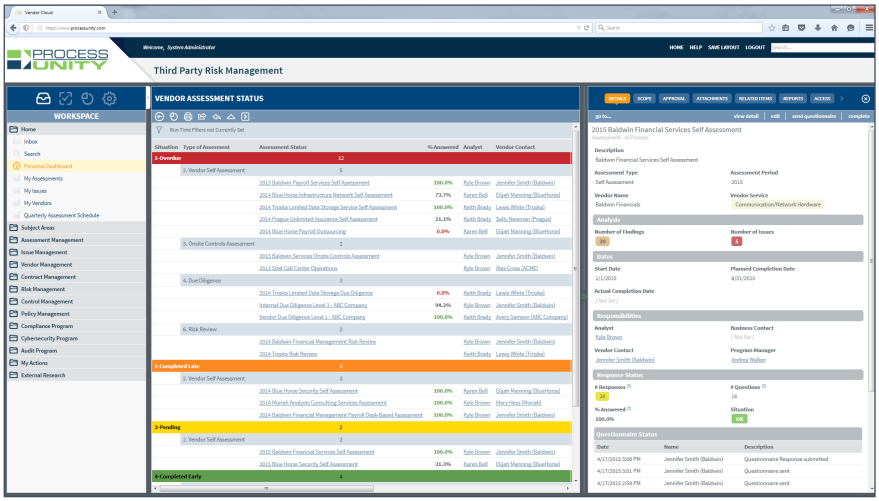


Automation makes it easy to create customized questionnaires fast.

The resulting questionnaire can include multiple-choice and/or open response questions, plus appropriate places for submitting/uploading supporting documentation.

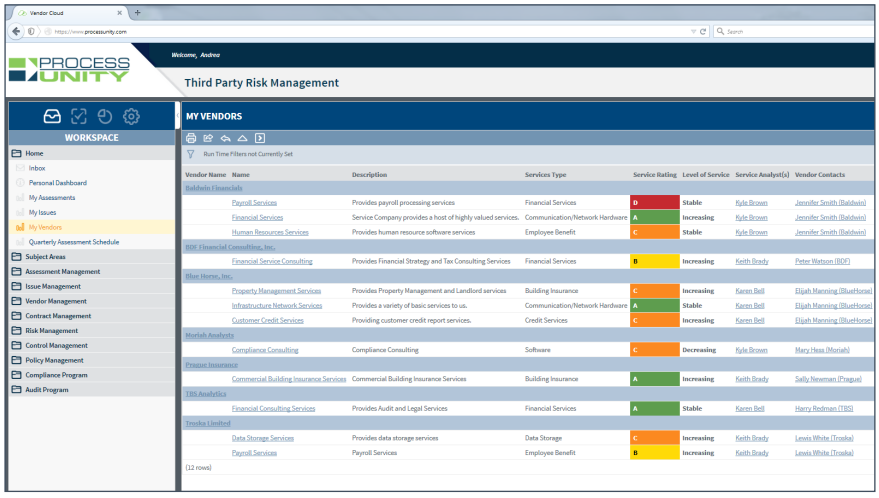


© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com



Step-by-step, the automated questionnaire guides vendors through the relevant due diligence categories and offers tools for submitting necessary documents.

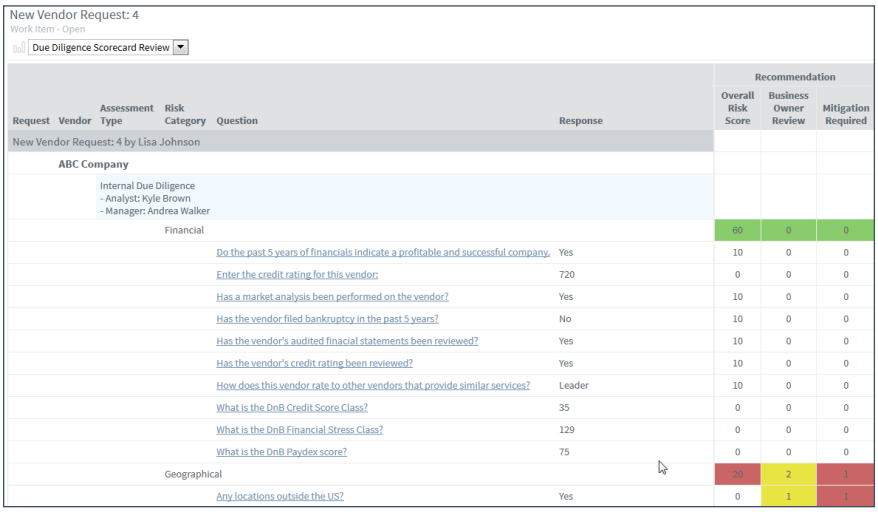
On the originator's side, risk analysts access dashboards that instantly reveal the progress of the due diligence process and track questionnaires to completion.



In a glance, VRM teams can see which assessments are complete, which are pending, and which are overdue.

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

At the end the workflow, analysts review scorecards, ranked according to their own organization's risk taxonomy (classification system), with recommendations that are both objective and transparent—two of the most important qualities regulators want to see in the due diligence process.



New Vendor Request: 4

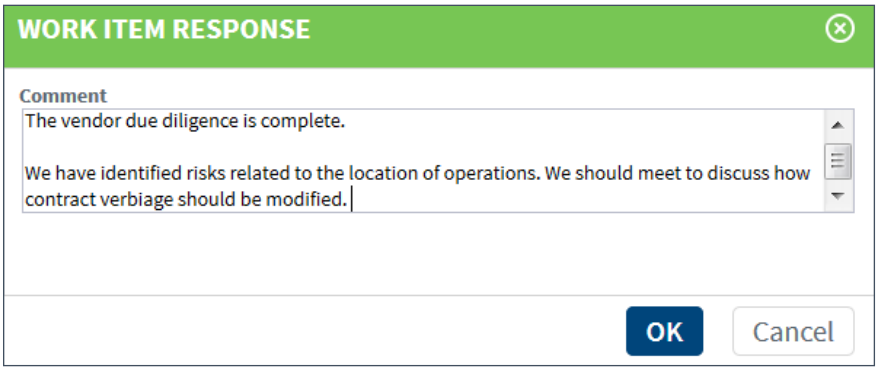
Work Item - Open

Due Diligence Scorecard Review

Request	Vendor	Assessment Type	Risk Category	Question	Response	Recommendation: Overall Risk Score	Recommendation: Business Owner Review	Recommendation: Mitigation Required
New Vendor Request: 4 by Lisa Johnson								
	ABC Company							
		Internal Due Diligence - Analyst: Kyle Brown - Manager: Andrea Walker						
			Financial			60	0	0
				Do the past 5 years of financials indicate a profitable and successful company.	Yes	10	0	0
				Enter the credit rating for this vendor:	720	0	0	0
				Has a market analysis been performed on the vendor?	Yes	10	0	0
				Has the vendor filed bankruptcy in the past 5 years?	No	10	0	0
				Has the vendor's audited finacial statements been reviewed?	Yes	10	0	0
				Has the vendor's credit rating been reviewed?	Yes	10	0	0
				How does this vendor rate to other vendors that provide similar services?	Leader	10	0	0
				What is the DnB Credit Score Class?	35	0	0	0
				What is the DnB Financial Stress Class?	129	0	0	0
				What is the DnB Paydex score?	75	0	0	0
			Geographical			20	2	1
				Any locations outside the US?	Yes	0	1	1

In this example, the firm classifies vendors as unrestricted (green), restricted (yellow), or denied (red). Your firm can configure the system in conformance with its own classification taxonomy.

While automation streamlines due diligence and provides a documented trail for accountability, it by no means displaces human judgment. On the contrary, rapid access to questionnaire results gives analysts more agency, allowing them to make informed recommendations for amending contracts or adjusting SLAs, as indicated by the vendor's responses.



Analysts gain the power to make informed recommendations based on the unique responses of each vendor.

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

HOW WELL ARE YOU MANAGING VENDOR RISK EXPOSURE?

The best way to manage vendor risk is by intercepting it at the start. In *Conducting Pre-Contract Due Diligence in a Digitally Connected World* we've encouraged you to formalize your pre-contract due diligence process, and to automate that process for efficiency, transparency, and consistency.

What's the status of your current VRM process? And what steps could you take to improve it? Take a moment now to assess your due diligence procedures—and uncover opportunities for making it both faster and stronger.

- [ ] Is your pre-contract due diligence process consistent, vendor by vendor? Can your internal lines of business initiate due diligence quickly?
- [ ] Do these lines have an easy way of articulating their needs, and the company's potential exposure to vendor risks?
- [ ] Are you able to capture relevant information across all nine domains of due diligence?
- [ ] Have you established risk thresholds for approving, restricting, or denying a vendor relationship?
- [ ] Do you have a repository of questions and templates you can use to assemble external questionnaires?
- [ ] Have you created an easy way for collecting supporting documentation?
- [ ] Can you quickly track vendor progress on the questionnaire?
- [ ] Have you automated your workflow for efficiency and accountability?
- [ ] Do your risk analysts have access to dashboards that represent vendor status in a glance?
- [ ] Does your process create scorecards that represent vendor risk thresholds—and potential next steps?
- [ ] Can you defend the objectivity of your vendor risk assessments to regulators?

If you cannot answer "yes" to all these questions, you may benefit from a review of your VRM procedures.

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

PROCESS UNITY

- Cloud-based, Third-party Risk Management
- Vendor Service Catalog
- Powerful, Automated Assessment Tools
- Interactive Dashboards & Reports

Get Started on the Road to Automation with a Custom Demo
www.processunity.com/contact

vendor cloud
Powered by ProcessUnity

ABOUT PROCESSUNITY

ProcessUnity is a leading provider of cloud-based applications for risk management and service delivery management. The company's software as a service (SaaS) platform gives organizations the control to assess, measure, and mitigate risk and to ensure the optimal performance of key business processes. For public companies and regulated industries, ProcessUnity Risk Suite delivers effective governance and control, vendor risk mitigation, and regulatory compliance. For benefit plan administrators and other financial service firms, ProcessUnity Service Delivery Risk Management (SDRM) controls complex product offerings and strengthens client service experience. ProcessUnity is used by the world's leading financial service firms and commercial enterprises. The company is headquartered outside Boston, Massachusetts and is funded by Rose Park Advisors and other private investors.

HEADQUARTERS
33 Bradford Street
Concord, MA 01742
PHONE: 978-451-7655

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com