Vendor Risk Management

June 7, 2019

ISSA Central Plains

BETH STROBEL & MICHAEL BLUMREICH

- Beth has worked at a global aerospace and defense company, working with legal compliance and ethics and in both technical and sales roles for GRC and cybersecurity software companies.

- Michael has worked as a GRC consultant, implementing Vendor, Audit, Risk and Compliance processes for Fortune 100 and 500 companies across a variety of platform software tools.

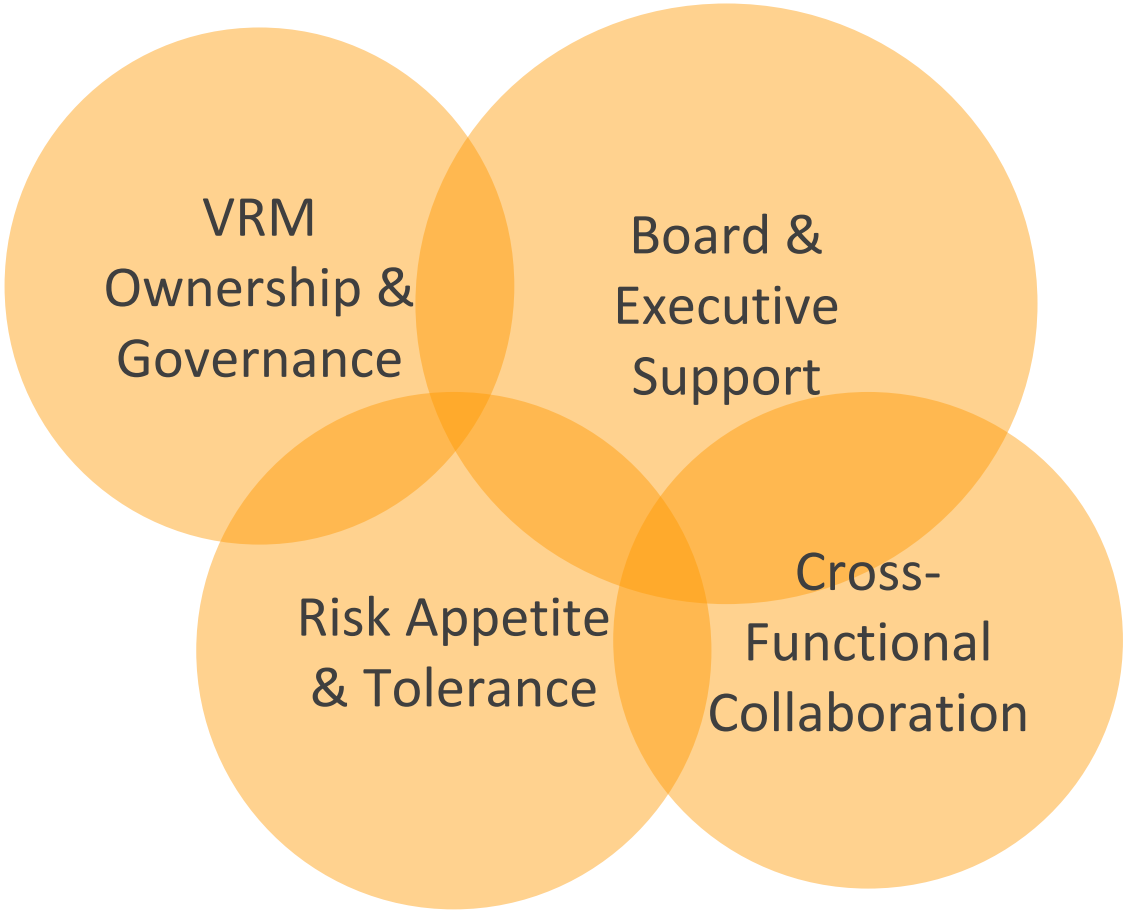
AGENDA

- Definitions
- Organizational considerations
- Elements of a Vendor Risk Management (VRM) program
- Technology to fuel VRM

GETTING ON THE SAME PAGE

- Vendor & Supplier Risk Management are generally the same.
- Third Party Risk Management is broader – encompassing vendors/suppliers + other third parties, such as:
  - Customers
  - Partners
  - Counterparty in joint venture
  - Government regulatory agencies

ORGANIZATIONAL CONSIDERATIONS



ELEMENTS OF A VRM PROGRAM

- Policies and procedures
- Initiating a vendor relationship
- Vendor risk assessments
- Risk management and mitigation
- Contract review requirements
- Cadence for review of vendor risks and obligations over time

POLICIES AND PROCEDURES

- Policy Scope
  - Determine where the requirements for managing vendors already exist in company policies
  - What are the requirements for vendors in each area of the business?
  - Who governs the policies specific to Vendor Management practices?
- Procedures and Process Flows
  - How will VRM become engaged prior to vendor evaluation and contract signing?
  - When and how will various functions engage with vendors?

INITIATING A VENDOR RELATIONSHIP

Critical factor: establish Vendor Risk Assessment as part of the business process.

INITIAL BUSINESS IMPACT / RISK ANALYSIS

- **Access to Sensitive Information:** Will the vendor handle your client or employee data, financial statements, intellectual property or other confidential information?
- **Operational Impact:** Would a disruption to the vendor's products or services harm your ability to carry out your own operations?
- **Revenue Impact:** Would a disruption to the vendor's products or services significantly impact your ability to generate revenue?
- **Reputational Impact:** Could misdeeds, negligence or malpractice on the part of the vendor damage your organization's reputation? (Think in terms of your clients, employees and the public at large.)
- **Resource Impact:** In the event of a disruption or issue with the vendor, how significantly would your internal resources be impacted?
- **Regulatory Impact:** Does the vendor relationship expose you to additional regulatory requirements (HIPAA, PCI, GDPR, etc.)? Would a disruption to the vendor's products or services impair your ability to demonstrate regulatory compliance?
- **Personnel Practices:** Does the vendor conduct background checks and policy training and awareness? What are the vendor's termination practices?
- **4th Party Risk:** How well does the vendor manage ***its own*** vendor relationships? What policies and procedures does the vendor have in place to ensure that you're not exposed to excessive 4th party risk?

VENDOR RISK ASSESSMENTS

Internal questionnaire

- Confirm the business's expectations
- Ensure vendor-provided information aligns

External questionnaire

- Questions about processes, controls, insurance, security and contract terms
- Objective is to identify risk ahead of signing a contract
- May choose to use the Shared Assessments SIG or HITRUST CSF Assurance

External Review

- Legal, HR, IT, Security, Compliance, etc. review of what vendor and the business have provided

Level of due diligence depends on:

- Criticality
- Initial risk indicators
- Type, level and duration of engagement

Learn more:
https://sharedassessments.org/sig/
https://hitrustalliance.net/thirdparty/

RISK MANAGEMENT AND MITIGATION

- Due diligence may uncover risks related to the vendor that must be communicated with the business / vendor relationship owners.
- Two main paths for identified risks:
  - Accept (sign-off by the business is required, and an expiration date assigned)
  - Mitigate (a mitigation plan and completion date must be agreed assigned).
- Engagement with the business and the vendor are critical to proper risk management and mitigation.

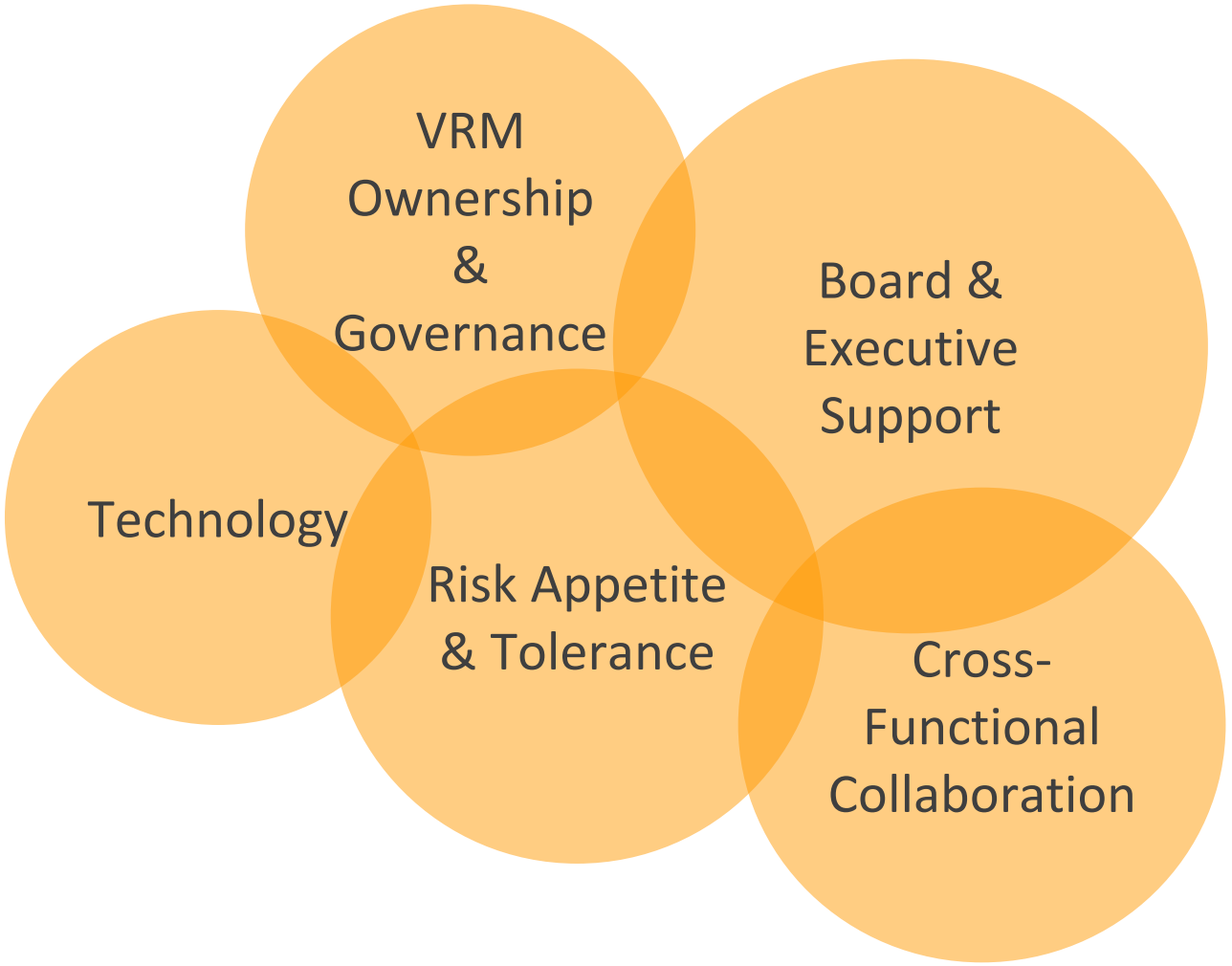
CONTRACT REVIEW REQUIREMENTS

- Formal contract review process & central repository are helpful
- Review contracts for potential risks
  - **Duration** of agreement, options for termination by either side, and post-termination terms
  - **Total Value** / cost of agreement, payment terms, and overage protection
  - **Performance Tracking** including quantifiable metrics, milestones and documentation, with measures to hold the vendor accountable
  - **Special Clauses** for things like termination, damages, indemnity, and exclusivity that conflict with internal standards
  - **Warranty Restrictions** that are unclear or may be voided under certain circumstances
  - **Insurance** coverage that is not commensurate with the risk associated with the product or service being provided
- Tracking Contract Meta-Data

CADENCE FOR REVIEW OF RISK & OBLIGATIONS

Onboarding	Resolution of Findings	Status / SLA Measurement	Onsite Audits	Satisfaction Surveys
• Complete vendor profile • Document vendor's system and data access • Vendor is linked to relevant Contracts & Engagements	• Ensure all findings are mitigated to company's satisfaction	• Request regular updates on achievement of milestones • Request documentation that Service Level Agreements are being met	• May be required to ensure controls and procedures are being adhered to	• Survey the relationship owner annually (and/or before contract renewal) to determine if there are concerns or open issues

ORGANIZATIONAL CONSIDERATIONS



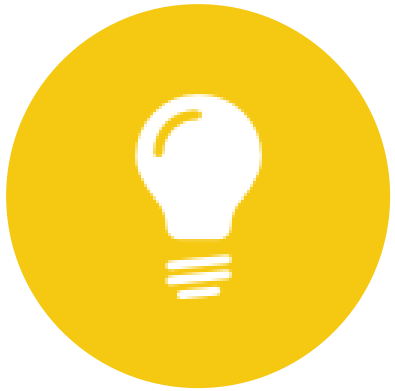
Our Mission: To empower business users to innovate and solve problems for themselves.

FLEXIBILITY

Easily adapt solutions to your specific processes, organizational structure, needs and goals

PERFORMANCE

Enjoy sub-second response time from a platform that ***never*** slows you down

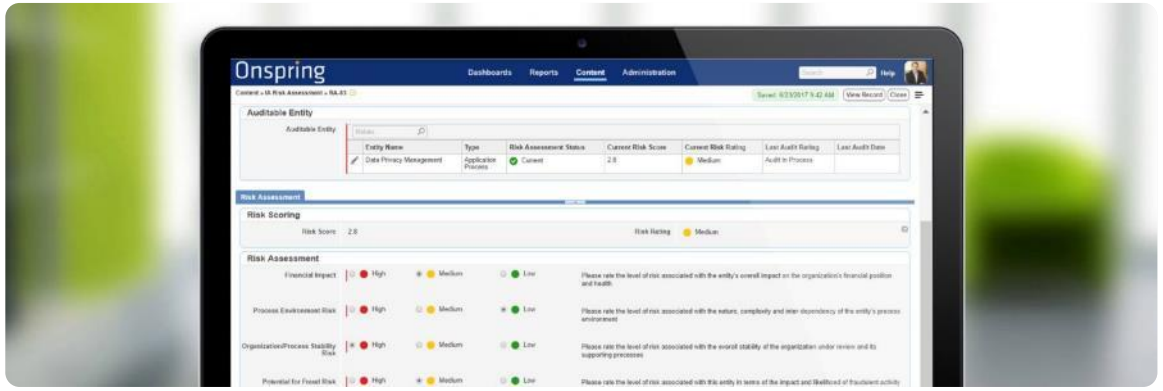


USER EXPERIENCE

Get your team working right away with an intuitive interface and minimal learning curve

PLATFORM COMPONENTS

Real-Time Reports and Dashboards



App and Survey Builder

Content Management and Dynamic Documents

Process Automation and Structured Workflow

PRE-CONFIGURED SOLUTIONS

Audit & Assurance
Build your internal audit plan, manage projects, track findings and report in real-time

Controls & Compliance
Document controls, map them to regulations and standards, and perform design and operating tests

Risk Management
Identify and evaluate risks, assign ownership, develop response plans, and track mitigation activities

Vendor Management
Centralize third-party data and use automated workflow for due diligence, assessments and contract review

Policy Management
Manage policy authoring and review, track attestations and manage exceptions

Continuity & Recovery
Document, test and monitor business continuity and disaster recovery plans across your enterprise

Incident Management
Capture incidents, analyze their impact, engage responders, and monitor outcomes and KPIs

Contract Management
Document, track, review and monitor contracts with efficiency, integrity and confidence

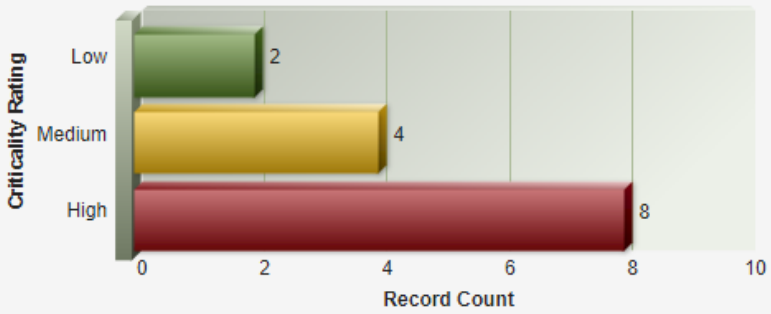
Corporate Counsel
Manage legal service requests, contracts, transactions and litigation from a central portal

Human Resources
Use automated workflow and role-based security to manage your organizational structure, employee documentation and performance evaluation

Request a New Vendor

Search Vendors

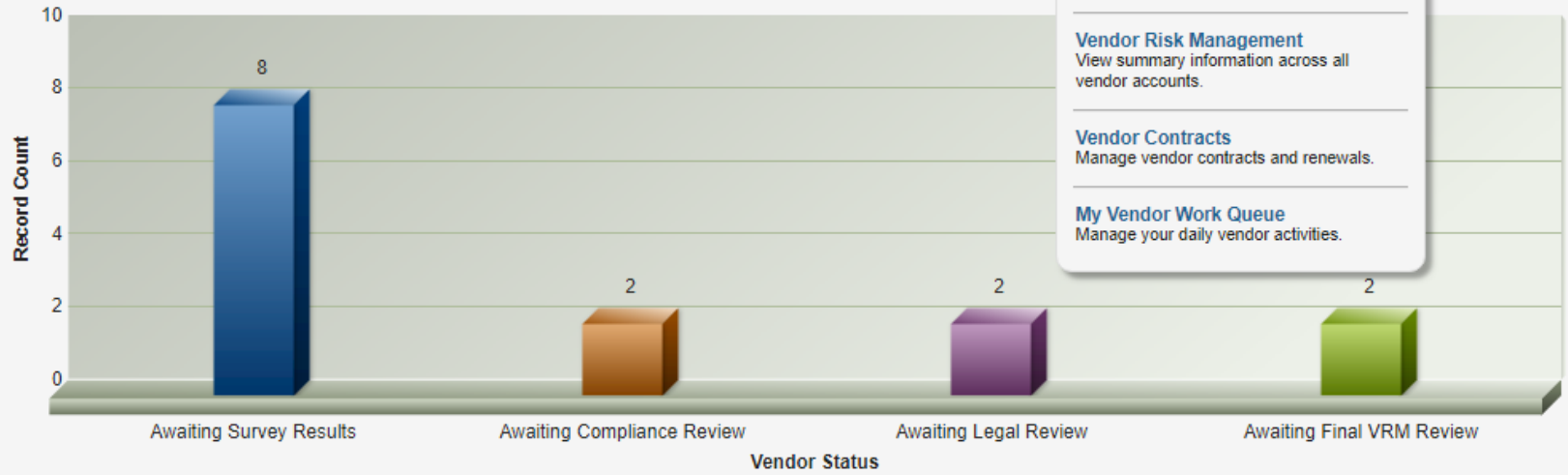
Potential Vendors by Criticality Rating



	Vendor ...	Submit...	Criticali...	Legal R...	Compli...	Vendor ...
	ABC Hosting	Jason Rohlf	High	Yes	Yes	Awaiting Survey Results
	BMID	Jason Rohlf	Medium	Yes	No	Awaiting Legal Review
	Calahan,	Jason	High	Yes	Yes	

1 - 14 of 14 items

Vendors in Onboarding Review



Vendor Onboarding
Enables users to request new Vendors and monitor overall review status

Vendor Risk Management
View summary information across all vendor accounts.

Vendor Contracts
Manage vendor contracts and renewals.

My Vendor Work Queue
Manage your daily vendor activities.

	Vendor Name	Submitted By	Criticality Rating	Legal Review Required	Compliance Review ...	Vendor Status
	ABC Hosting	Jason Rohlf	High	Yes	Yes	Awaiting Survey Results
	BMID	Jason Rohlf	Medium	Yes	No	Awaiting Legal Review
	Calahan, Drake and Thompson	Jason Rohlf	High	Yes	Yes	Awaiting Survey Results
	Cloudify	Jason Rohlf	High	Yes	Yes	Awaiting Survey Results
	GRC Systems Inc.	Jason Rohlf	High	Yes	Yes	Awaiting Survey Results
	Housing Lending Corporation	Jason Rohlf	High	Yes	Yes	Awaiting Survey Results
	InfoTech	Jason Rohlf	Medium	No	No	Awaiting Final VRM

1 - 14 of 14 items

About

General Information

General Information

Company Id	V-9	Vendor Status	Awaiting Survey Results
Vendor Name	Cloudify	Vendor Type	Software
Relationship Owner		Relationship Start Date	10/31/2013

Relate

Full Name	Title	Email Address
Jason Rohlf	VP, Solutions	jason@onspring.com

Description of Services: Cloudify provides virtualization software.

Primary Vendor Contact

Relate

Name (Full)	Title	Email Address
Jen Busant	VP	noreply@onspring.com

Vendor Address

Street Address	7582 Walnut	Street Address 2	
City	Chicago	State	IL
Zip/Postal Code	42578	Country	United States

About

General Information

General Information

Company Id	V-9	Vendor Status	Awaiting Survey Results
Vendor Name	Cloudify	Vendor Type	Software
Relationship Owner		Relationship Start Date	10/31/2013

Relate

Full Name	Title	Email Address
Jason Rohlf	VP, Solutions	jason@onspring.com

Description of Services: Cloudify provides virtualization software.

Primary Vendor Contact

Relate

Name (Full)	Title	Email Address
Jen Busant	VP	noreply@onspring.com

Vendor Address

Street Address	7582 Walnut	Street Address 2	
City	Chicago	State	IL
Zip/Postal Code	42578	Country	United States

About

General Information

General Information

Company Id: (auto-generated)

Vendor Status: Draft

Vendor Name:

Vendor Type:

Relationship Owner: Relate

	Full Name	Title	Email Address
	Michael Blumreich		michael.blumreich@onspring.com

Relationship Start Date:

Description of Services:

Primary Vendor Contact: Relate

	Name (Full)	Title	Email Address

Vendor Address

Street Address:

Street Address 2:

City:

State: Select a value

Zip/Postal Code:

Country: Select a value

Related Vendors

Parent Company

Relate

Vendor Name	Vendor Type

Subsidiaries

Relate

Vendor Name	Vendor Type

Qualifying Information

Please provide the following information regarding the nature of the company's relationship with this vendor.

More

Vendor Access to Information: Select a value

Level of Customer Impact: Select a value

Critical Services and System Provider: Select a value

Onsite Vendor: Select a value

Estimated Annual Spend:

Qualifying Information Score: 0

Criticality Rating: Low

Submission

Submit Vendor for Review

Set the Submission Status to Submitted to notify the VRM team that the requested vendor is ready for review.

Submission Status: Awaiting Submission

Date Submitted:

Submitted By

Relate

Full Name	Email Address

Risks, Findings and Incidents

Vendor Documentation

Tasks

Risks, Findings and Incidents

Related Risks

Related Risks

Relate

Risk Title	Risk Category	Business Owner	Inherent Risk Rating	Residual Risk Rating

Vendor Finding Information

Vendor Findings

Relate

Record Id ↓	Created Date	Title	Primary Owner	Overall Status	Vendor Risk Assessment

Incidents

Incidents

Create New Record | Quick Add

Incident Id	Type	Overall Status	Date/Time Reported	Date/Time Occurred	Subtype	CI Accessed?	Submission Date	Days Open

Vendor Documentation

Vendor Documentation

Document Repository

Create New Record

Name	Type	Description	Status

Attachments

Drag and Drop Attachments here

Select File(s)

Name	Type	Modified ↓	Owner	Notes

No attachments have been uploaded

Link to Documentation

Tasks

Task Information

Tasks

Create New Record | Quick Add

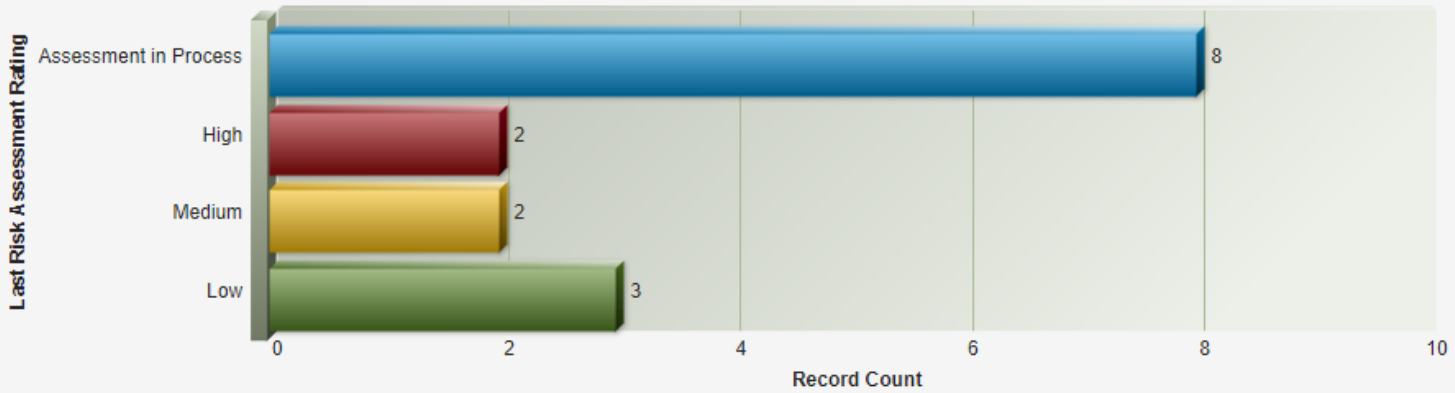
Name	Owner	Due Date ↑	Status

Search Vendors

Request a New Vendor

Add a Vendor Finding

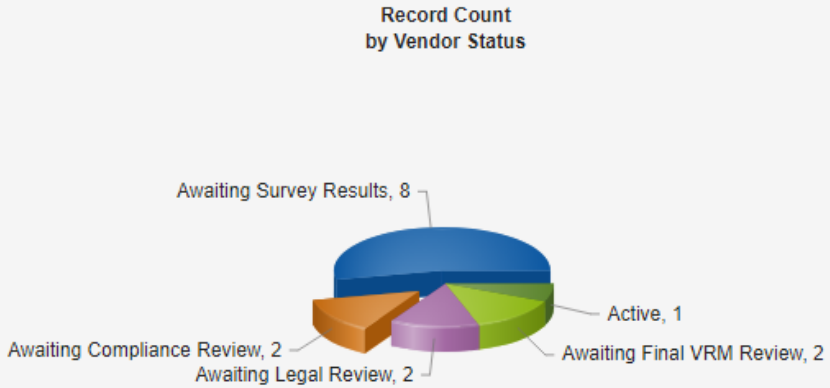
Vendors by Risk Assessment Rating



Vendor Name	Vendor Type	Relationship Owner	Spend - Total 3 Ye...	Criticality Rating	Last Risk Assess...
ABC Company	Consulting Services	Chris Pantaenius	$178,750	High	Low
ABC Hosting	Telecom and Networking	Kyle Graves	$1,500,000	High	Medium
Calahan, Drake and Thompson	Business Services Legal	Chris Pantaenius	$0	High	Low
Cloudify	Software	Jason Rohlf	$275,000	High	Assessment in Process
GRC Systems Inc.	Consulting Services Software	Jason Rohlf	$0	High	Assessment in Process
			Total: $9,003,750		

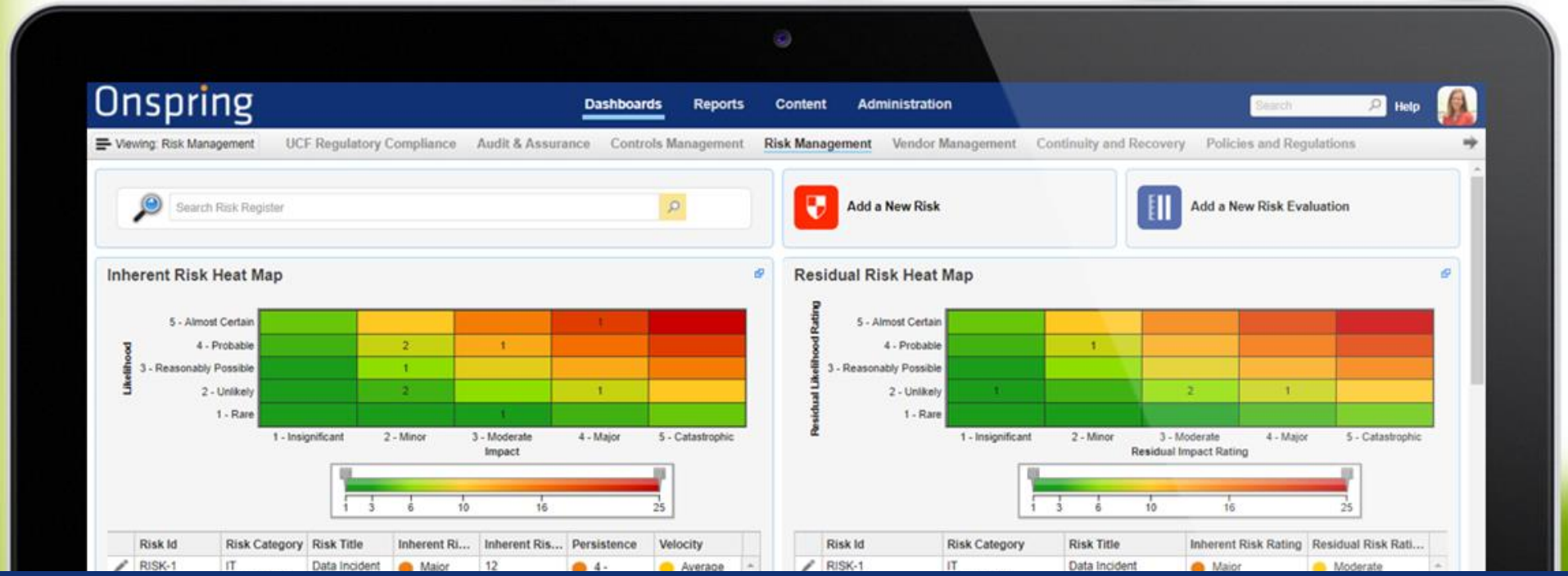
1 - 15 of 15 items

Vendors by Status



Total: 15

Vendors by Criticality



CONTACT US WITH QUESTIONS

Beth Strobel
Regional Sales Manager
+1 913.940.6094 (m)
beth.strobel@onspring.com

Michael Blumerich
Solutions Engineer
+1 913.633.5485 (m)
michael.blumerich@onspring.com