

# Tips, Pitfalls and Best Practices for Managing Nonprofits' Risk with Third Parties



Vendor Centric



Lewis  
Baach  
Kaufmann  
Middlemiss  
PLLC



# Today's Speakers



**Tom Rogers, CPA**  
Founder & CEO  
**Vendor Centric**



**Jeff Tenenbaum, Esq.**  
Chair of the Nonprofit  
Organizations Practice  
**Lewis Baach Kaufmann**  
**Middlemiss PLLC**



**Renee Stock**  
Account Executive  
**AHT Insurance**

# Agenda



What is a third party and what is third-party risk management?



5 top influencers driving third-party risk management



12 best practices for managing risk with your third parties



Closing thoughts



Vendor Centric



Lewis  
Baach  
Kaufmann  
Middlemiss  
PLLC



# Section I:

# What Is a Third Party and What Is Third-Party Risk Management?



# What Is a Third Party?



Any *company* or *individual* with which or whom you have entered into a business relationship to:



Provide goods and services for your own use



Perform outsourced functions on your behalf



Provide access to markets, products and other types of services



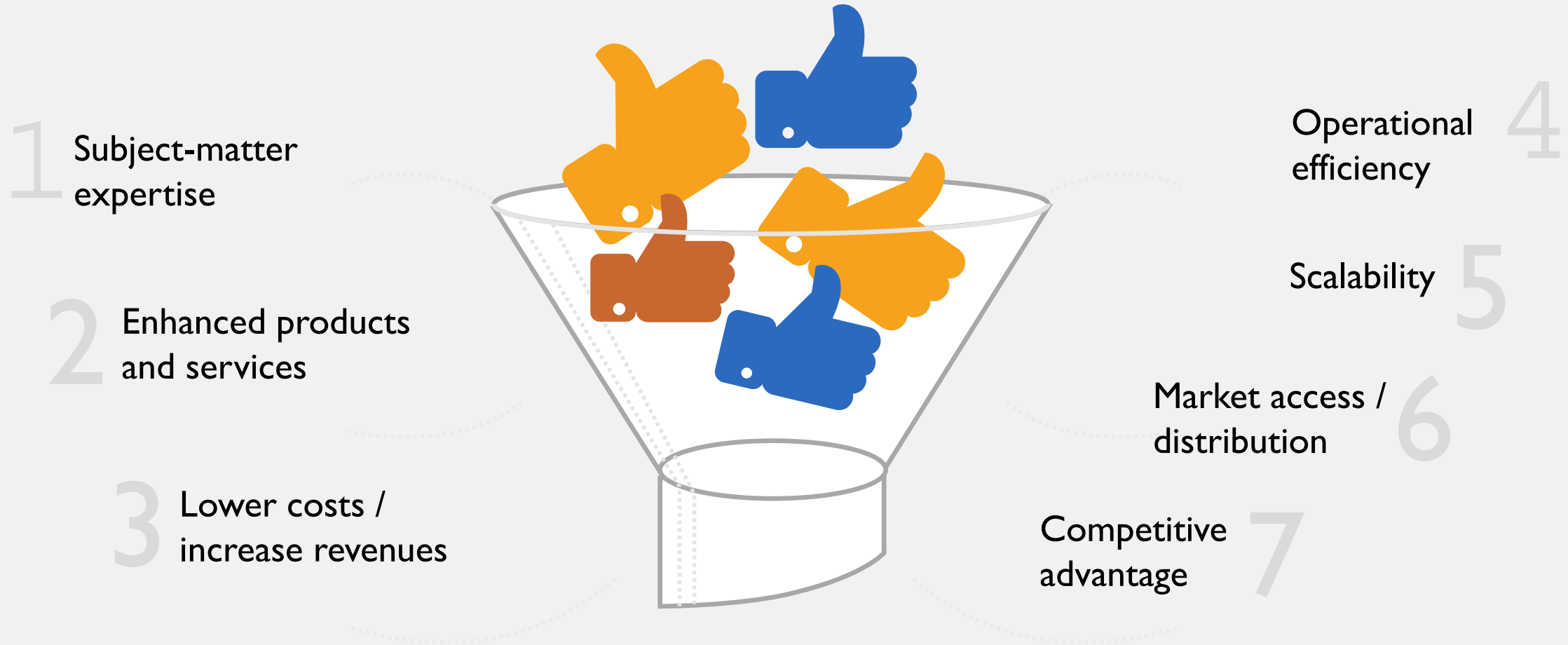
Vendor Centric



Lewis  
Baach  
Kaufmann  
Middlemiss  
PLLC

AHT  
INSURANCE

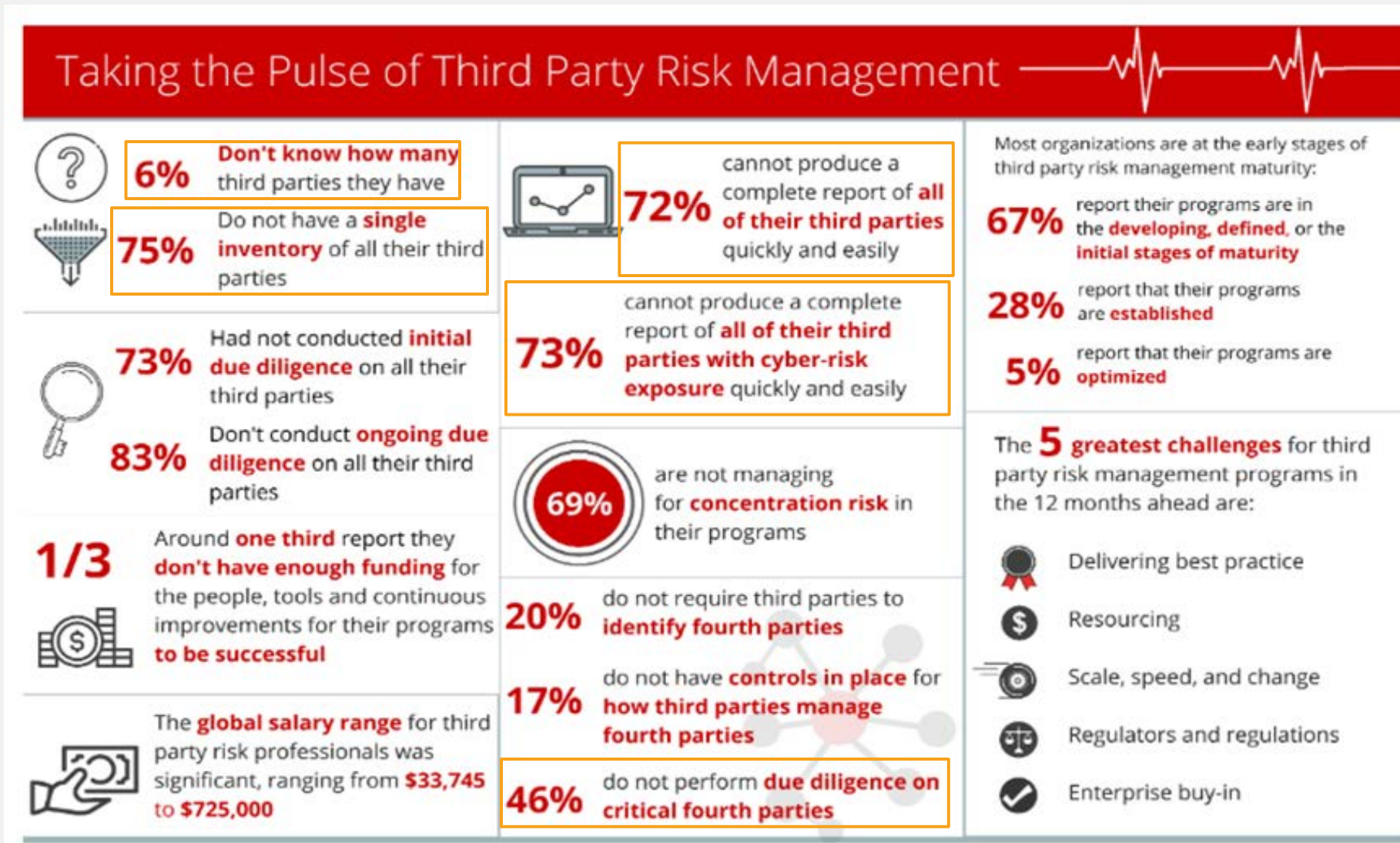
# Benefits of Third-Party Relationships



# Examples of Nonprofit Third Parties

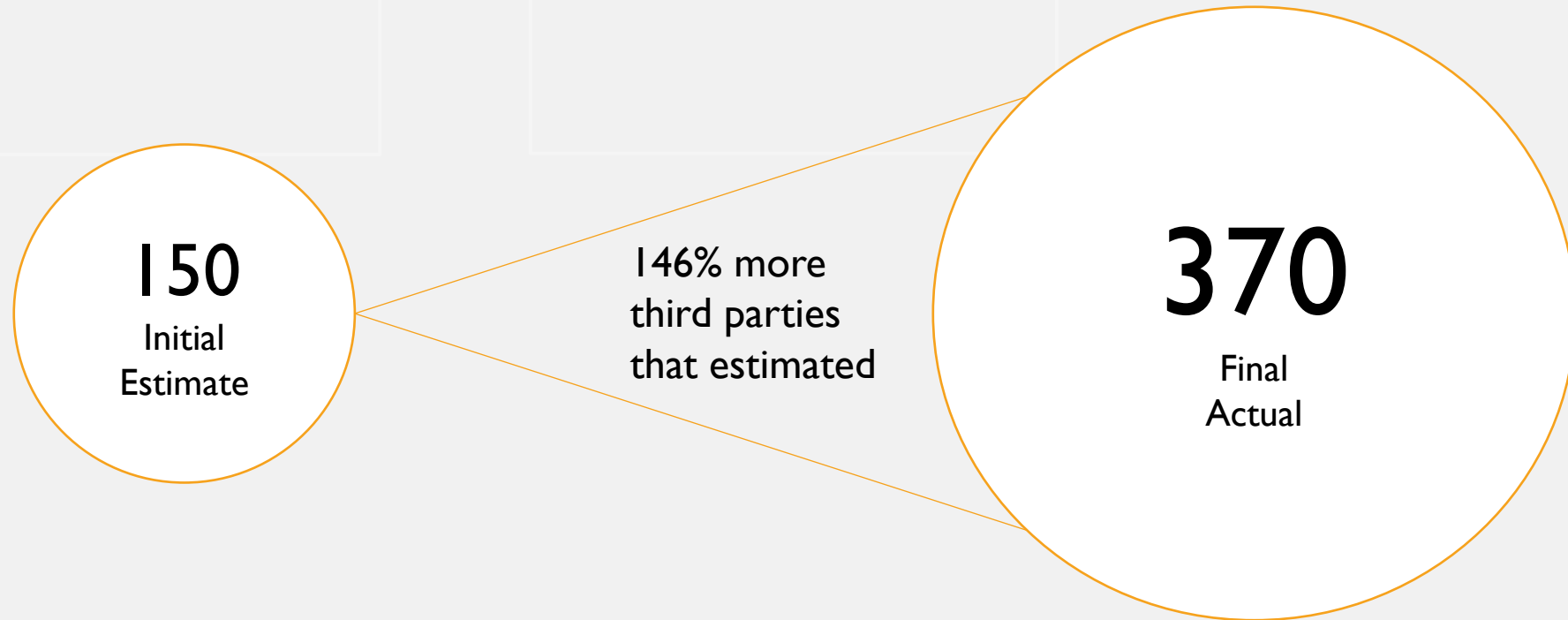
- Software manufacturers such as membership, donors, grants, accounting, learning
- Software hosting
- Credit card processing
- Printing and publications
- Fulfillment and mail houses
- Meeting / event-related vendors
- Fundraisers
- Temporary agencies
- Subrecipients
- Subcontractors
- Consultants and independent contractors
- HR and payroll companies
- IT hardware, services and support
- Accountants and auditors
- Lawyers
- Agents and brokers

# Do you know your third parties?



Source:  
Aravo, Key Findings from Global Third Party Risk Benchmarking Survey, 2018

# You May Have More Third Parties Than You Realize



Source:  
Actual nonprofit organization, \$70M annual revenue

# What Is Third-Party Risk?

## Third-Party Risk

The potential exposure to problems, harm or loss that arise from relying on outside parties to perform services or activities on your behalf.



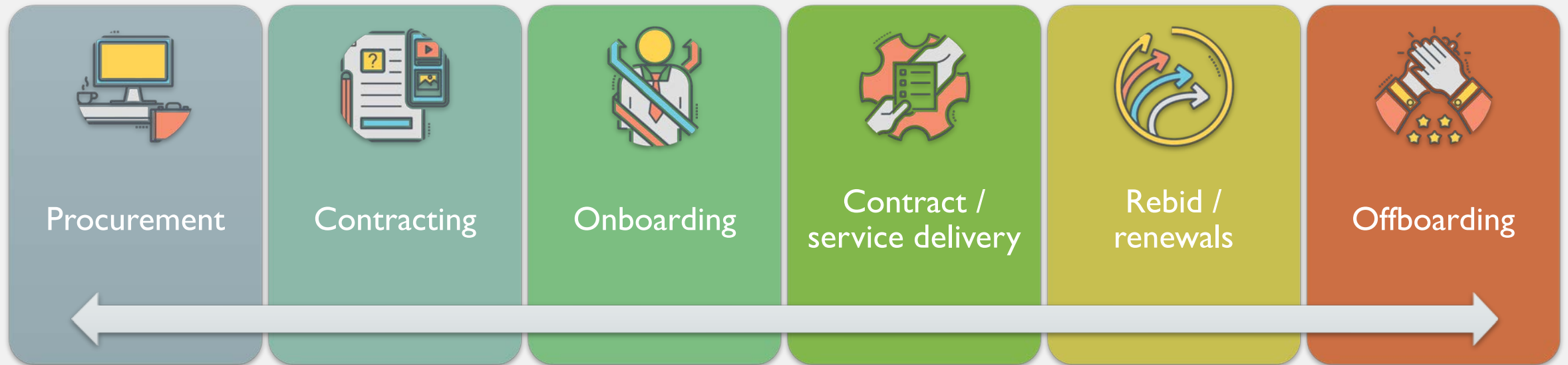
## Third-Party Risk Management

The process whereby an organization monitors and manages interactions with all external parties with which it has a relationship. This may include both contractual and non-contractual parties.



# When Are Third Parties Risky?

## All of the Time!



# 6 Types of Risks You Need to Manage



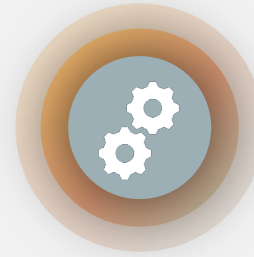
## Reputational

Risk of your organization receiving *negative public opinion* due to problems with, or failure of, a vendor.



## Strategic

Risk arising from your *inability to implement strategies* or strategic initiatives due to vendor advice/failure.



## Operational

Risk of *disruption to operations* due to the failure in a vendor's processes, people or systems.



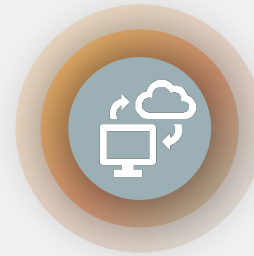
## Transactional

Risk of *financial loss or damage to credit* due to your inability to deliver important services, or transact business, due to problems created by a vendor or even fraud.



## Compliance

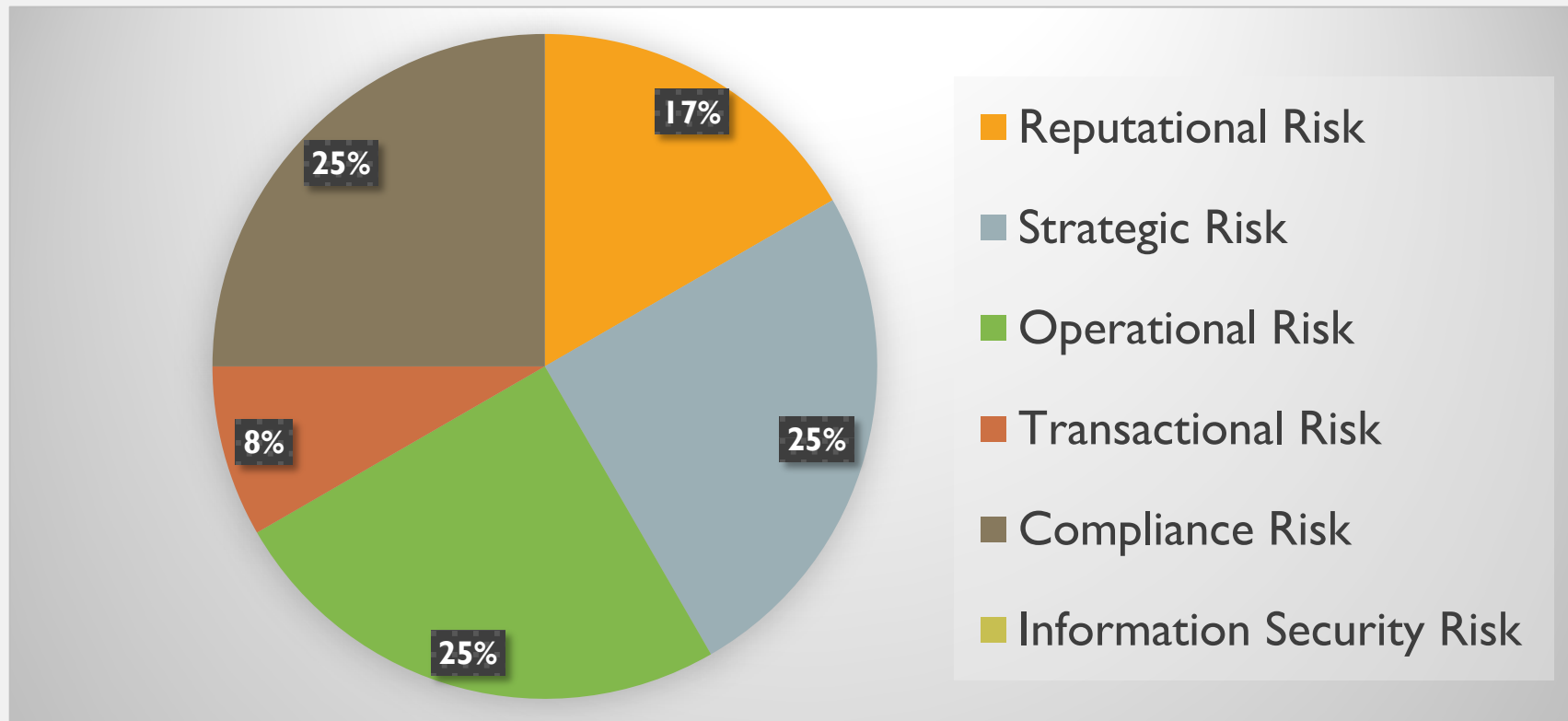
Risk related to your *violation of laws, policies, or regulations* due to something the vendor does (or doesn't do).



## Data Information Security

Risk related to the *exposure of non-public information* (yours and your members, customers, clients') information due to breach or other fault of a vendor.

# Poll #1. Risk you are most concerned with (or we can rank them)

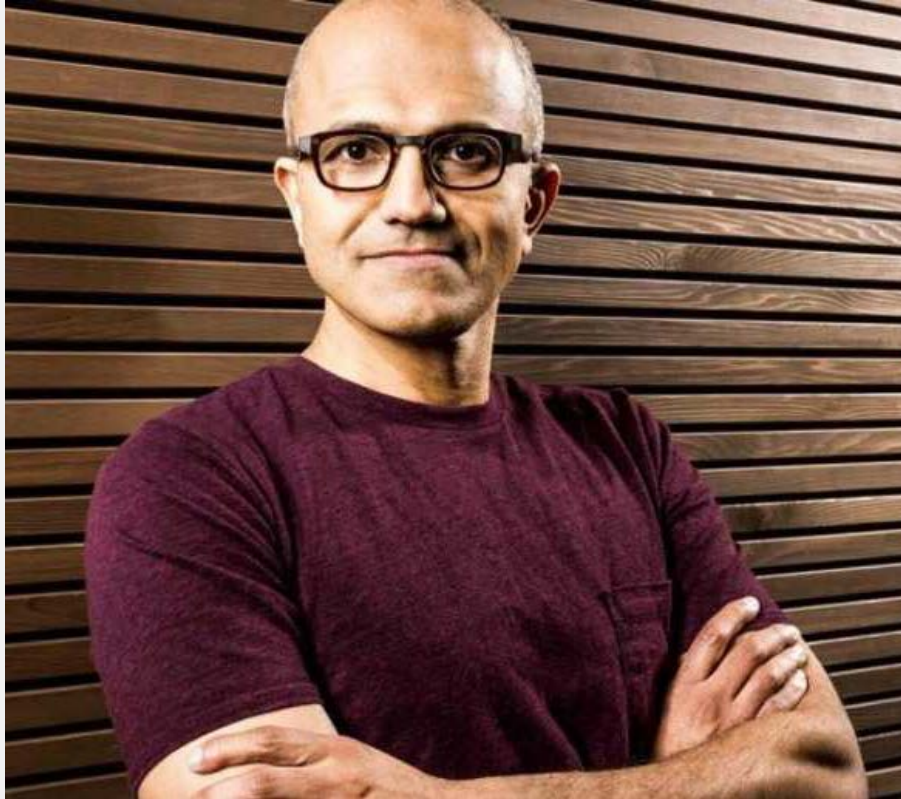


# Section 2:

## 5 Top Influencers Driving Third- Party Risk Management



# #1. Relationships Are More Complex & Intertwined



"There's a secular movement that's happening... more to an annuity relationship as well as a subscription relationship. These are the long-term relationships we want to have with all customers."

- Satya Nadella  
CEO, Microsoft

# #2. Third Parties Have Lots of Data

SECURITY & FRAUD

## Third-Party Data Breaches Rise To 61 Pct In US

By PYMNTS

Posted on November 15, 2018

### Security: Third-Party Suppliers Major Source of Business Data Breaches

[Home](#) > [Security](#) > Security: Third-Party Suppliers Major Source of Business Data Breaches

By Dick Weisinger

Third party vendors and suppliers are the source of more than 60 percent of data breaches according to a survey by Ponemon Institute and Opus.

The survey by Ponemon found that the number of third-party incidents is growing. The number of third-party suppliers increased by 25 percent

### 16 Breach at Goodwill Vendor Lasted 18 Months

SEP 14

C&K Systems Inc., a third-party payment vendor blamed for a credit and debit card breach at more than 330 Goodwill locations nationwide, disclosed this week that the intrusion lasted more than 18 months and has impacted at least two other organizations.

On July 21, 2014, this site broke the news that multiple banks were reporting indications that Goodwill Industries had suffered an apparent breach that led to the theft of customer credit and debit card data. Goodwill later confirmed that the breach impacted a portion of its stores, but blamed the incident on an unnamed "third-party vendor."



## Third-Party Data Security Breach Affects Approximately 650 Delawareans

Insurance Commissioner | News | Date Posted: Monday, January 28, 2019

Listen



## Vendor error causes major patient record leak at New York hospital

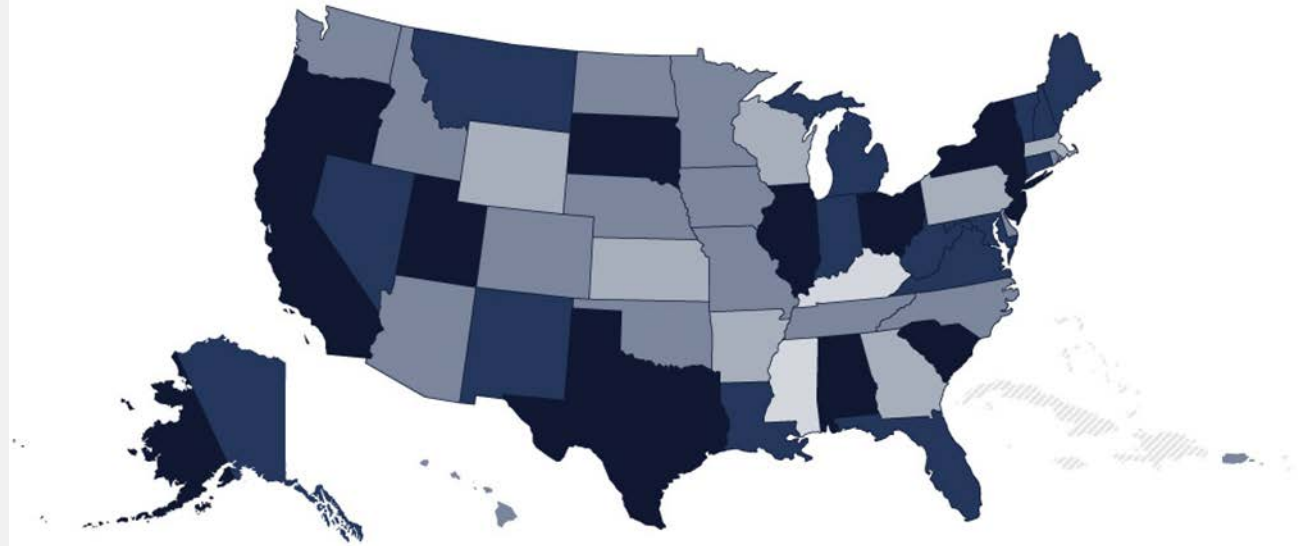
Cause of Bronx-Lebanon Hospital Center breach tied to misconfigured rsync backup that was managed by iHealth Innovations.

By Bill Siwicki | May 09, 2017 | 12:42 PM



# Data Breach Laws

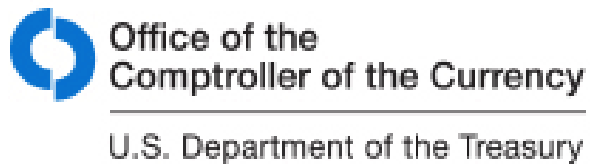
in States, Territories, and the U.S. Capital



Stricter laws			Less strict laws		
5	Alabama	5	Texas	4	Michigan
5	California	5	Utah	4	Montana
5	Illinois	4-5	Alaska	4	Nevada
5	New Jersey	4	Connecticut	4	New Hampshire
5	New York	4	Florida	4	New Mexico
5	Ohio	4	Indiana	4	Vermont
5	Oregon	4	Louisiana	4	Virginia
5	South Carolina	4	Maine	4	West Virginia
5	South Dakota	4	Maryland	3	Arizona
				3	Colorado
				3	Delaware
				3	Hawaii
				3	Idaho
				3	Iowa
				3	Minnesota
				3	Missouri
				3	Nebraska
				3	North Carolina
				3	North Dakota
				3	Oklahoma
				3	Rhode Island
				3	Tennessee
				3	Washington
				3	Guam
				3	Puerto Rico
				2	Arkansas
				2	Georgia
				2	Kansas
				2	Massachusetts
				2	Pennsylvania
				2	Wisconsin
				2	Wyoming
				2	Washington, D.C.
				2	U.S. Virgin Islands
				1	Kentucky
				1	Mississippi

Source:  
Digital Guardian, 2018

# #3. Third-Party Regulations Are Increasing

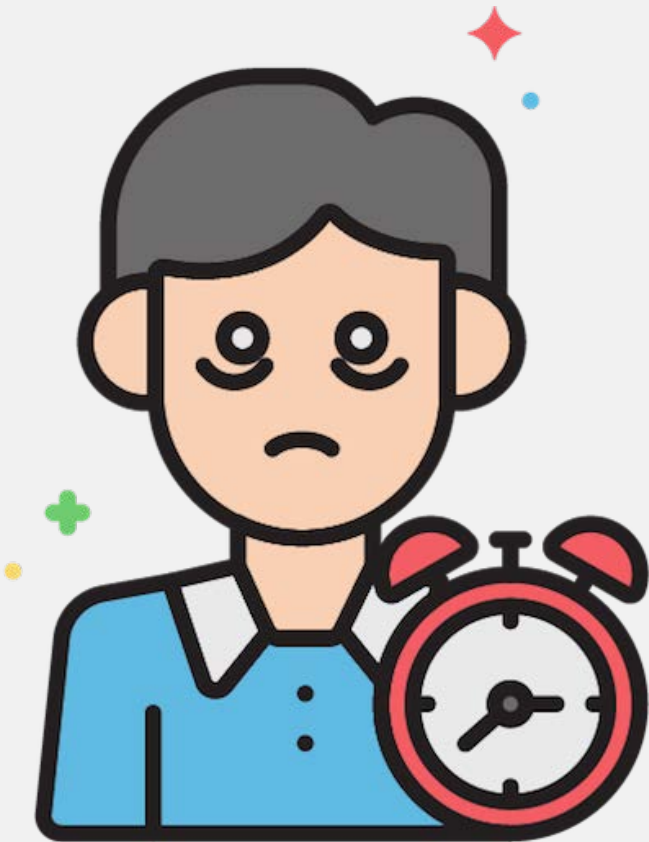


# Two Examples of State Proposals That Would Affect Third-Party Risk Management



Proposals	Relevancy to Third Party Management
A bill proposes new requirements for businesses to "take all reasonable steps to dispose of, or arrange for the disposal of, consumer records."	<ul style="list-style-type: none"><li>• Contractual clauses regarding data retention/destruction.</li><li>• May need to have third parties attest to destruction after the fact.</li></ul>
Proposal that ransomware attacks would be considered a security breach, and a breached entity would need to notify the state attorney general's office within 30 days.	<ul style="list-style-type: none"><li>• Contractual provisions requiring breach notification.</li></ul>

# #4. Increased Scrutiny by Auditors

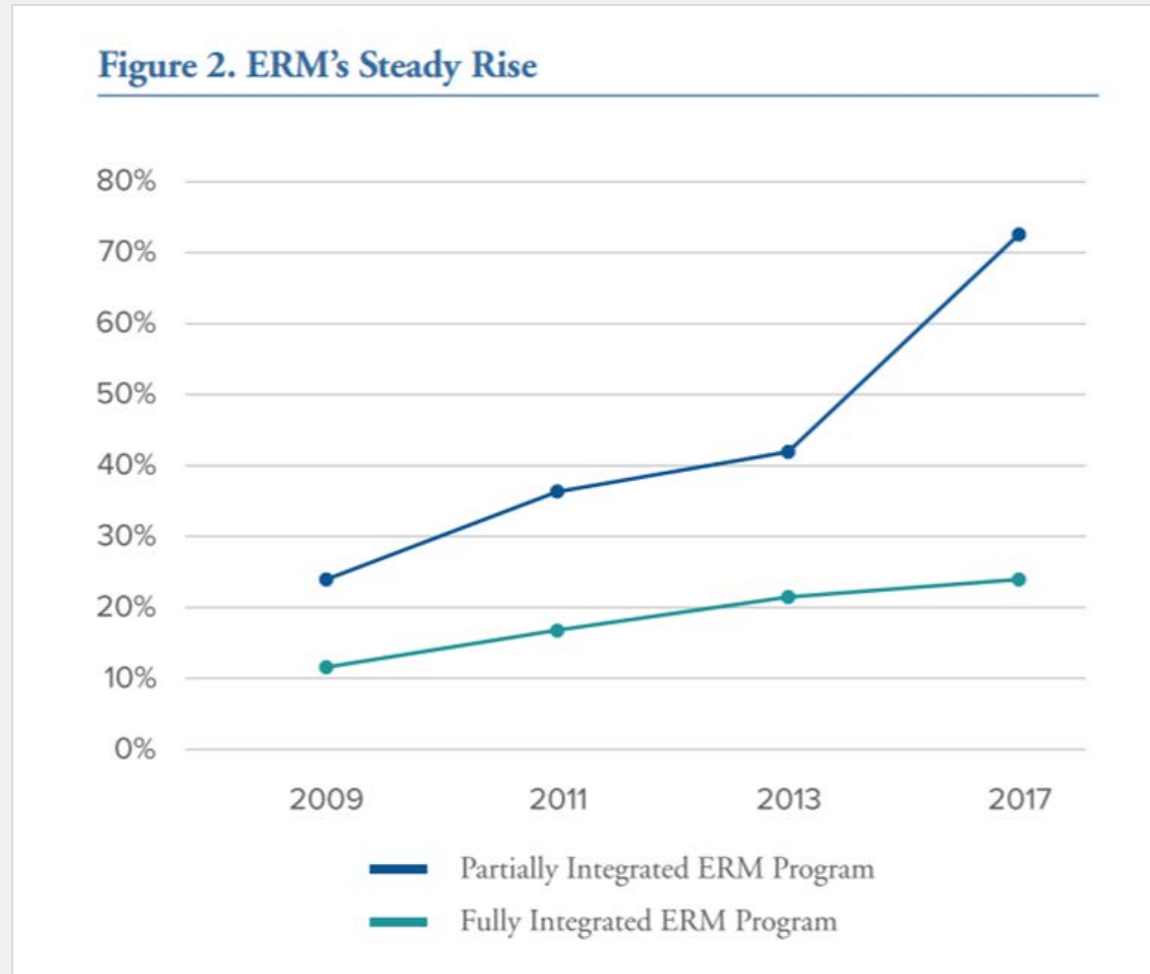


## 10 Things Keeping Nonprofit Auditors up at Night

1. Changes to operations or strategy
2. Organizational culture
3. *New technology*
4. *Cybersecurity*
5. *Compliance with funder requirements*
6. Financial controls
7. *Reliance on third parties*
8. *Procurement procedures*
9. Transportation and distribution
10. Fraud and corruption

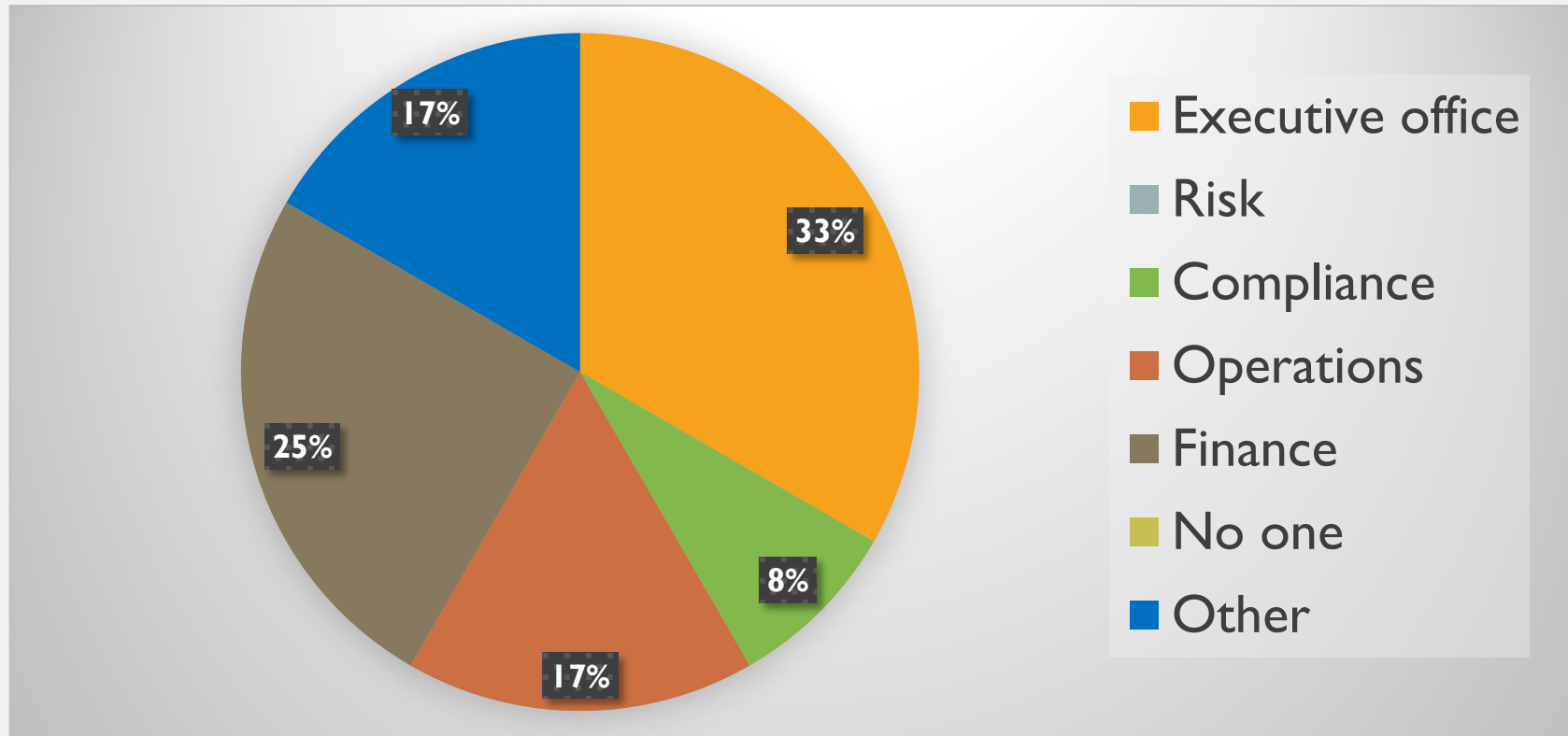
Source:  
The NonProfit Times, October 2018

# #5. Risk Management Is Growing in Adoption



Source:  
Risk & Insurance Management Society, 2018

# Poll #2. Who Owns Third-Party Risk?



# Section 3:

## 12 Best Practices for Managing Risk with Your Third Parties



# 12 Best Practices for Managing Risk with Third Parties

## Before the Contract Signing

1. Stop sleeping on your RFP
2. Share terms and conditions up front
3. Understand your risk exposure
4. Conduct risk-based due diligence
5. Establish cyber security standards
6. Include SLAs in your contract
7. Evaluate insurance requirements

## After the Contract Signing

8. Assign a contract manager
9. Standardize onboarding
10. Employ risk-based oversight and continuous monitoring
11. Have a formal offboarding process
12. Maintain continuous visibility into all of your third parties and contracts

# #1. Stop Sleeping on Your RFP



## Why It's Important

- Ensures clarity of expectations
- Improves accuracy and completeness of vendor proposals and statements of work
- Teases out issues early on
- Makes it easier to evaluate vendors and solutions

# Components of a Solid RFP

- 1 Executive overview** – frames purpose and objectives
- 2 Company background** – provides context about your organization
- 3 Functional, technical and business requirements** – details everything that the solution needs to do
- 4 Pricing information** – defines all components preferred methodology
- 5 Deliverables and timelines** – what you expect to be produced and by when
- 6 Responsibilities of both parties** – what resources you will provide and what you expect of them
- 7 Evaluation process and key factors** – how you'll evaluate proposals and what factors are most important to you
- 8 Guidelines for proposal submission** – makes it easier to compare apples-to-apples

# #2. Share Your Terms and Conditions up Front



## Why It's Important

- Allows you to communicate your desired terms and conditions early on so you can identify any potential deal breakers before you get too far down the road
- Gives you leverage in the contract negotiation process
- Speeds up the contracting process when/if you get there

# Key Terms and Conditions to Define

- Term and termination
- Fees and expenses
- Intellectual property ownership and licensing
- Confidentiality, conflicts of interest, non-competition, non-solicitation of your employees
- What is each party responsible to do under the contract?
- Authority (including limits thereon) to act on your behalf?
- How can the vendor describe its relationship with you?
- Indemnification and limitation of liability
- Insurance requirements
- Post-termination/expiration obligations and restrictions
- Dispute resolution
- Others – each contract needs to be tailored to each matter/transaction

Table 2: Top ten most negotiated terms 2018

	'18	'15	'13	'12	'11	'10	'09	'08	'07
1 Limitation of Liability	-	1	1	1	1	1	1	1	1
2 Indemnification	-	2	3	2	2	2	2	2	2
3 Price/Charge/ Price Changes	-	3	2	3	3	3	3	3	4
4 Termination		9	4	8	11	7	6	7	11
5 Scope and Goals/ Specification		11	5	6	5	6	8	8	9
6 Warranty		7	8	7	4	4	4	4	3
7 Performance/ Guarantees/ Undertakings		8	7	9	12	10	11	13	14
8 Payment		5	9	16	7	18	-	15	15
9 Data Protection/ Security/Cybersecurity		18	17	18	15	5	5	10	7
10 Liquidated Damages		13	6	20	14	13	12	5	5

Table 3: Top ten most important terms 2018

1. Scope and Goals/Specification
2. Responsibilities of the Parties
3. Price/Charge/Price Changes
4. Delivery/Acceptance
5. Service Levels
6. Performance/Guarantees/Undertakings
7. Limitation of Liability
8. Payment
9. Data Protection/Security/Cybersecurity
10. Change Management

Source:

International Association of Contract & Commercial Management

# #3. Understand Your Risk Exposure



## Why It's Important

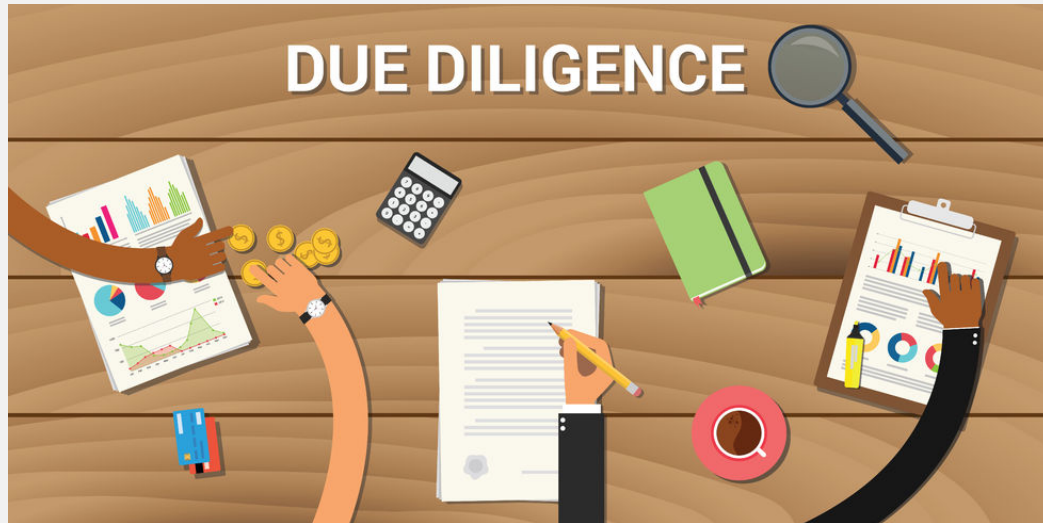
- Creates clarity on where to focus your due diligence
- Drives level of post-contract oversight

# 7 Risk-Related Questions You Should be Asking

Will the third party:

1. Be providing mission critical software or services?
2. Store, process or otherwise have access to non-public information?
3. Have direct access to our systems?
4. Be interacting directly with members/donors/customers?
5. Have unsupervised access to your physical premises?
6. Use downstream vendors (4th parties) to deliver their goods or services?
7. Create a severe financial impact (contract costs, lost revenue, people time) if something went wrong?

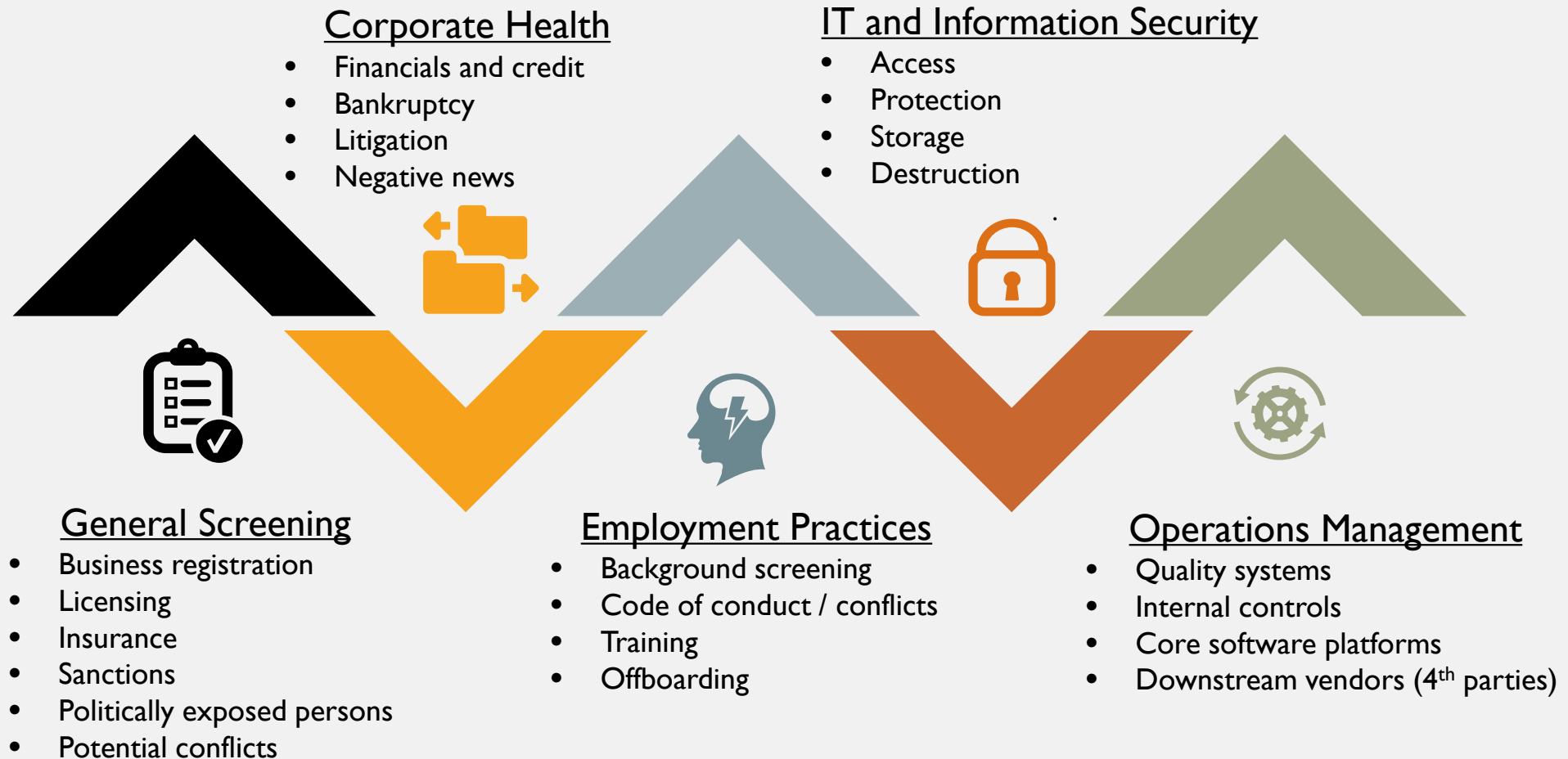
# #4. Conduct Risk-Based Due Diligence



## Why It's Important

- Identifies size and scope of risk exposure
- Verifies controls are in place to mitigate your big risks and identifying the size of the risk
- Identifies issues requiring remediation, contract language, or compensating controls
- Prevents contracting with high-risk third parties

# Types of Due Diligence



# #5. Establish Cybersecurity Standards



## Why It's Important

- Provides a basis from which you can evaluate third parties
- Aligns third parties with your own data protection standards

Only 52% of companies have security standards for third-parties.

[CLICK TO TWEET](#) 

Source:  
PWC, Global State of Information Security Survey, 2018

# Sample Cyber Security Requirements for Third Parties

- Written information security program (WISP)
- Code of Conduct
- Security awareness training
- Firewalls
- Anti-virus protection
- Multi-factor authentication
- Data encryption when transmitting NPI
- Decommissioning and destruction policy

## Example of a Written Standard

“Third parties must have a *process* to ensure that their users (e.g., employees, subcontractors and/or temporary workers) with access to [organization’s] nonpublic data are bound by non-disclosure agreements and/or code of conduct agreements.”

# #6. Include Service-Level Agreements in Your Contracts

SAAS Agreement; service credit...

Heavy Pro... Software a... Obligation...

[Copy to Clipboard](#) | [Share Example](#)

## 1. Service Levels

**1.1. Applicable Levels.** [PARTY A] shall provide the Service to [PARTY B] with a System Availability of at least [98]% during each calendar month.

**1.2. System Maintenance.** [PARTY A] may

- (a) take the Service offline for scheduled maintenances that it provides [PARTY B] the schedule for in writing (though this scheduled maintenance time will not count as System Availability), and
- (b) change its schedule of maintenances on [one] month written notice to [PARTY B].

**1.3. Service Credits**

- (a) **Eligibility for Service Credits.** Subject to paragraph [NOTICE REQUIRED] directly below, for each full percentage point that the availability of the Services does not meet the System Availability percent, [PARTY A] shall provide one additional days' service to [PARTY B] (each additional day a "Service Credit"), up to a maximum of [10] Service Credits, to be added to the end of the Term and at no additional charge to [PARTY B].
- (b) **Notice Required.** If [PARTY B] does not give [PARTY A] written notice that it is eligible for Service Credits within [30] Business Days' after the end of a month it is eligible to

## Why It's Important

- Creates clarity on service level expectations
- Establishes quantifiable measures for service delivery
- Allows for inclusion of credits and refunds
- Can support compliance with regulations

# #7. Evaluate Insurance Requirements

B. The Buyer and Owner, along with their respective officers, agents and employees, shall be named as additional insureds for Ongoing Operations and Products / Completed Operations on the Subcontractor's and any Sub-Subcontractor's Commercial General Liability Policy. The Subcontractor shall continue to carry Completed Operations Liability Insurance for at least three (3) years after either ninety (90) days following Substantial Completion of the Work or final payment to the Subcontractor, whichever is later. . .

**D. COMMERCIAL GENERAL LIABILITY & UMBRELLA LIABILITY:** In addition to the primary limits listed in A, B and C above, Subcontractor shall maintain an umbrella liability policy in the amount of Four Million Dollars (\$4,000,000.00) Per Location.

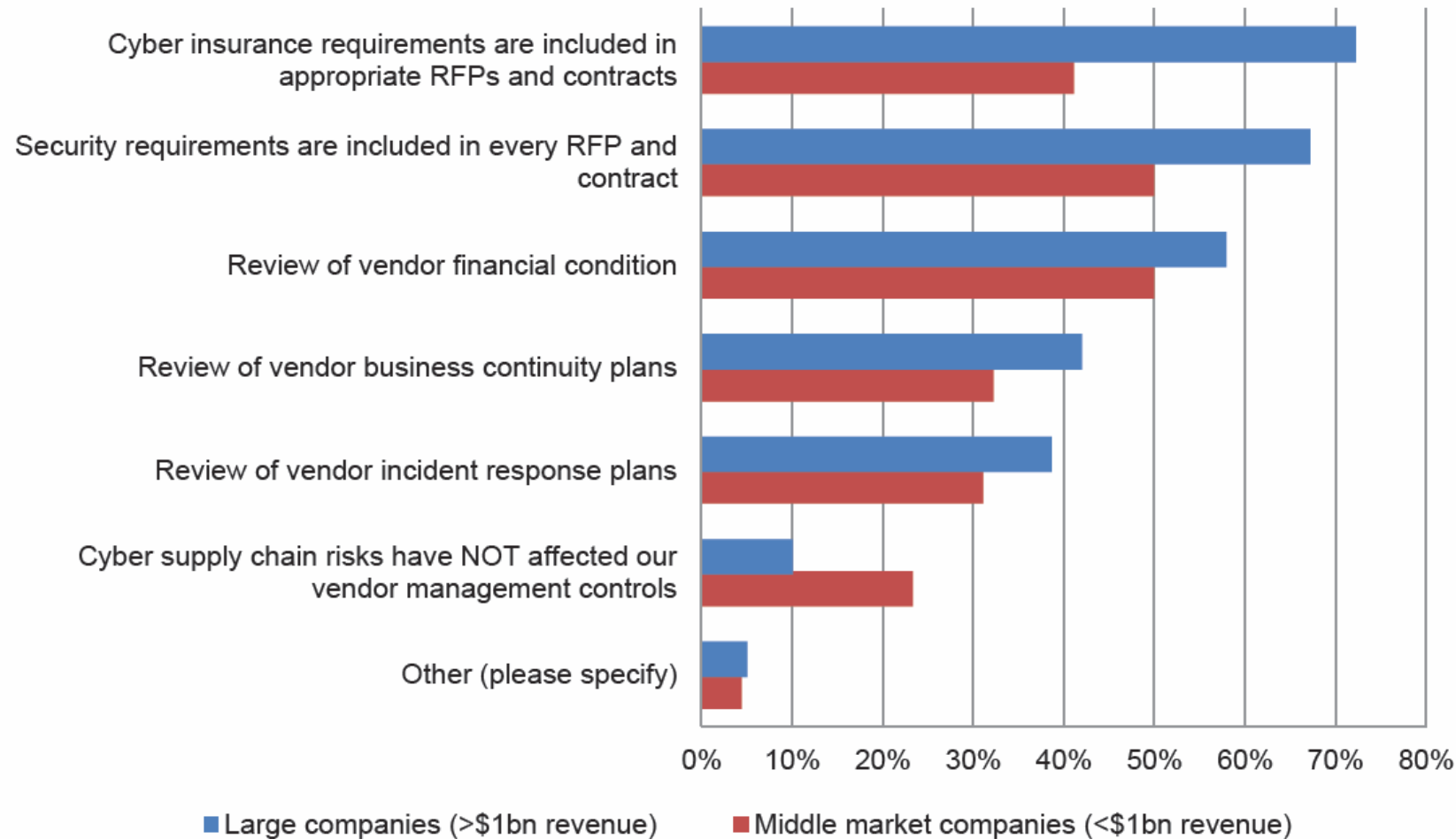
With respect to the policies providing coverage under subsets B, C and D above, Buyer (and the fee owner of each property together with any and all mortgagees or other parties having privity of interest of the fee owner) shall be named as an Additional Insured on a primary and non-contributing basis; and for all of the policies listed above (under subsets A, B, C and D), above, there shall contain a waiver of subrogation in Buyer's favor. All companies providing Subcontractor's insurance shall have and maintain a minimum AM Best rating of A- or better.

## Why It's Important

- Contractual Transfer (Indemnification) is key to who pays for negligence in a claim scenario
- Are your limits sufficient?
  - Have you priced increased limits and written them into the cost of the contract?
- There are typical contract terms in RFPs that are not advisable on certain policies
  - Additional Insured
  - Waiver of Subrogation
  - Primary Non-Contributory

## WHICH VENDOR MANAGEMENT CONTROLS HAVE YOU IMPLEMENTED TO MANAGE CYBER SUPPLY CHAIN RISKS?

*(Please select all that apply)*



Source:  
Zurich, Information Security and Cyber Risk Management Survey, 2018

# Project Matrix Insurance Risk Transfer

<b>Statutory</b>	<b>Contractual</b>	<b>Business Purposes</b>
Workers' Compensation / USL&H / DBA	General Liability and Excess Liability	Third-Party Employment Practices Liability
Automobile Liability	Property Exposures	Environmental Liability
ERISA Compliance	Errors & Omissions Liability	Intellectual Property
State Laws, i.e. (NY Disability)	Third-Party Crime	Business Interruption / Time Element



# Common Contract Terms

## Additional Insured

- When [client] agrees per contractual requirement to add a third party as an insured under a policy, but does not give full policy grants
- Frequently requested on General Liability
- Not applicable to all policies

## Waiver of Subrogation

- When [client] agrees to waive the right (for both [client] and its insurer) to subrogate against another in the event of a loss
- Frequently requested on General Liability and Workers Compensation
- Not applicable to all policies; different implications depending on scope of work, contract, agreement



## Primary Non-Contributory

- When agreed to, [client] would agree to respond as “primary” to a claim of negligence and not request another party to contribute
- Should be stricken whenever possible
- Only available on liability-type policies

# #8. Assign a Contract Manager



## Why It's Important

- Establishes accountability for oversight and results
- Ensures that your organization's contract protocols are followed consistently
- Creates a staff person with above-average knowledge of the contracting process

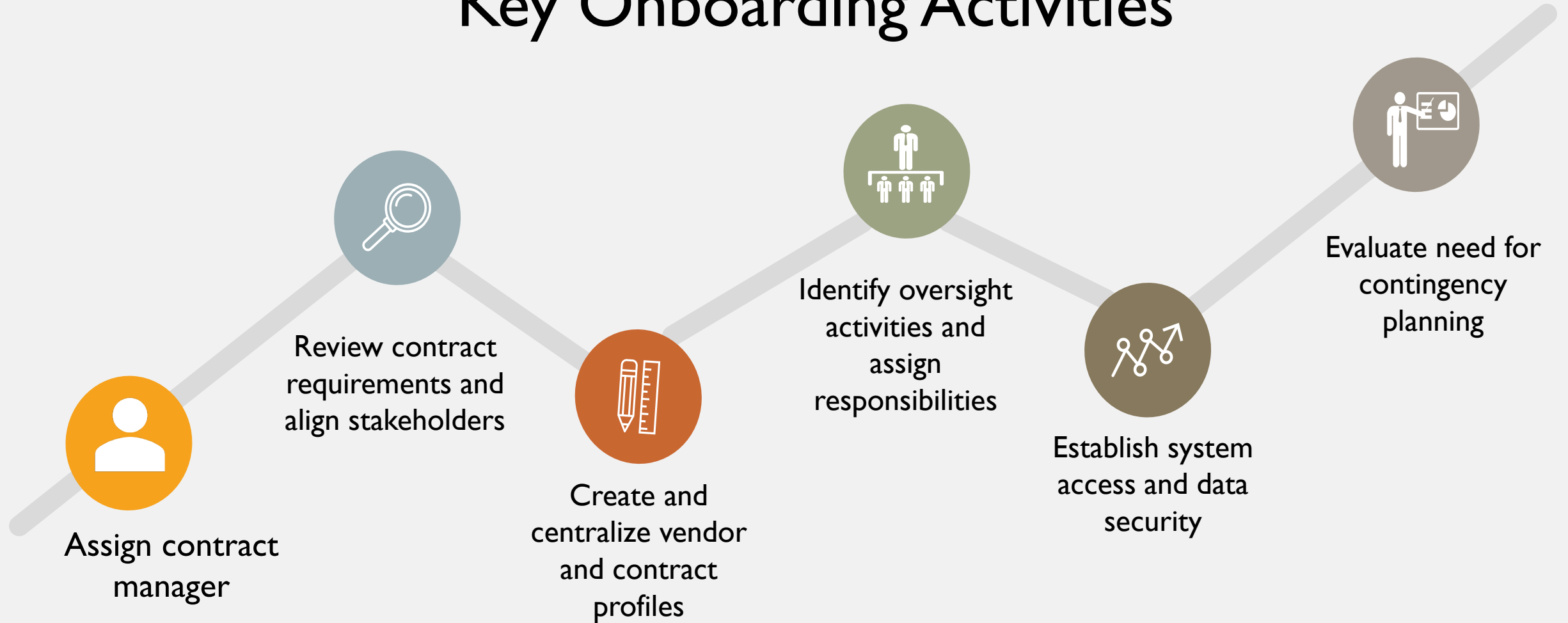
# #9. Standardize Onboarding

## Why It's Important

- Aligns stakeholders
- Supports policy compliance
- Creates basis for a more successful relationship



# Key Onboarding Activities



# #10. Employ Risk-Based Oversight and Monitoring



## Why It's Important

- Establishes a baseline for general oversight and monitoring
- Aligns resources with the riskiest third parties
- Increases compliance with contractual terms and conditions

# Oversight Activities Should Expand with Risk

- **Basic Oversight**

- Ensuring goods and/or deliverables conform to agreement with vendor
- Ensuring invoices are complete, accurate and reconciled to purchase order or contract
- Ensuring timely payment of vendor according to payment terms

- **Expanded Oversight**

- Monitoring contract auto-renewal and expiration dates
- Monitoring compliance with service level agreements
- Conducting surveys of internal stakeholder (and perhaps the vendor)
- Facilitating business reviews and issue remediation meetings
- Onsite visits and control testing
- Developing contingency plans

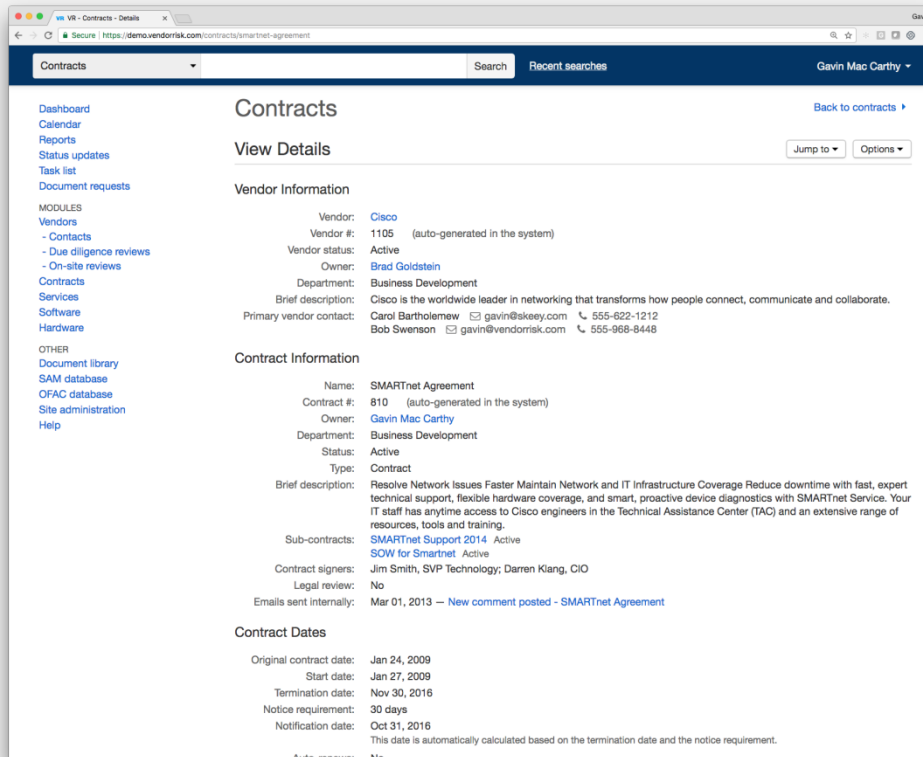
# #11. Have a Formal Offboarding Process



## Why It's Important

- Validates all contractual obligations are completed
- Ensures data is properly returned and/or destroyed
- Allows for effective knowledge capture and transition

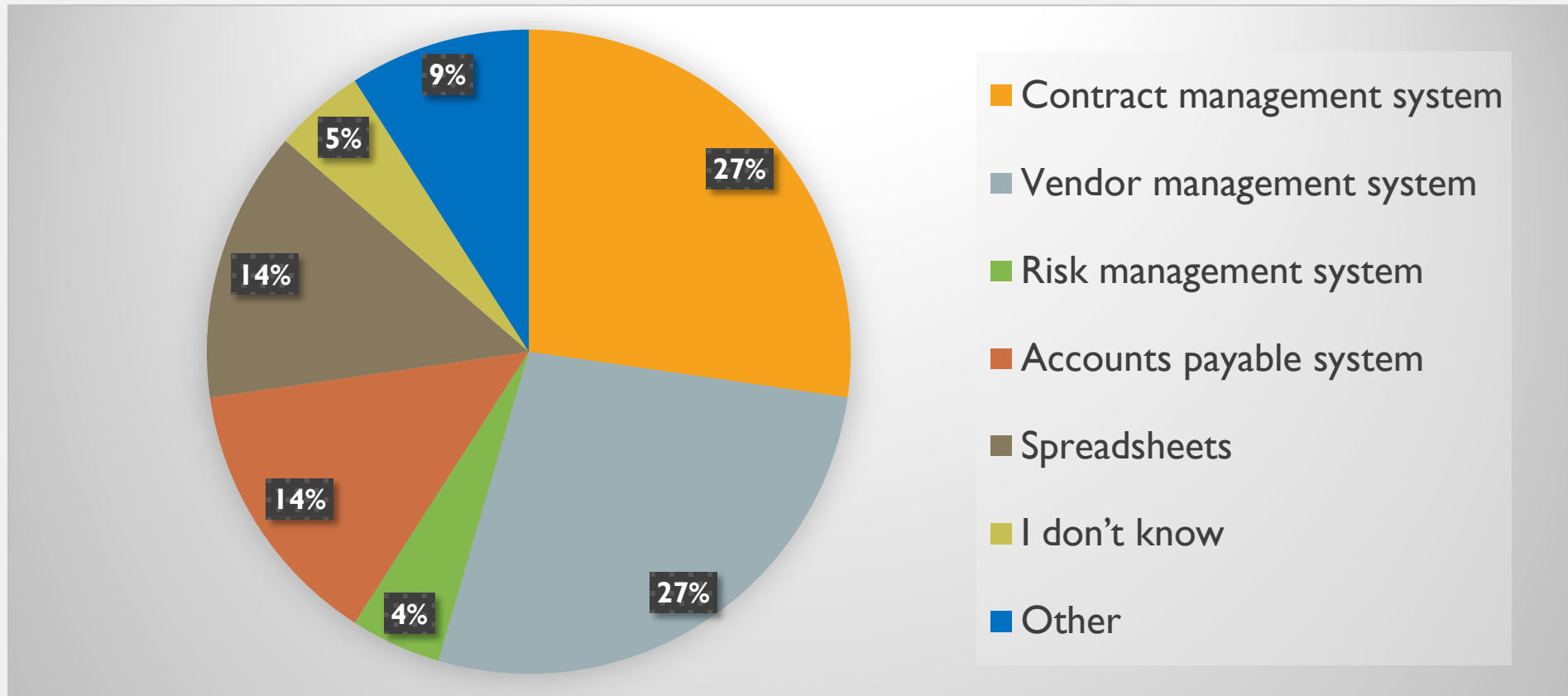
# #12. Maintain Continuous Visibility into All of Your Third Parties and Contracts



## Why It's Important

- It's the only way you will know who you're working with, what your exposure is, and whether all contractual and compliance requirements are being met

# Poll #3. How do you currently track information on your vendors and contracts? (Check all that apply)



# Section 4:

# Closing Thoughts



Vendor Centric



Lewis  
Baach  
Kaufmann  
Middlemiss  
PLLC

AHT  
INSURANCE

# Taking the Pulse of Third Party Risk Management



Source: Third Party Risk: A Journey Towards Maturity: Results of the 2018 'Taking the Pulse of Third Party Risk Management' Survey  
<http://info.aravo.com/cefpro-third-party-risk-survey>





# Contact Information




**Tom Rogers, CPA**  
**Vendor Centric**

 [trogers@vendorcentric.com](mailto:trogers@vendorcentric.com)


 [www.vendorcentric.com](http://www.vendorcentric.com)

 301-943-8624


 9841 Washingtonian Blvd #200,  
Gaithersburg, MD 20878




**Jeff Tenenbaum, Esq.**  
**Lewis Baach Kaufmann**  
**Middlemiss PLLC**

 [jeff.tenenbaum@lbkmlaw.com](mailto:jeff.tenenbaum@lbkmlaw.com)

 <http://www.lbkmlaw.com/>

 202-659-6749


 1101 New York Avenue, NW, #1000  
Washington, DC 20005




**Renee Stock**  
**AHT Insurance**

 [rstock@ahtins.com](mailto:rstock@ahtins.com)

 [www.ahtins.com](http://www.ahtins.com)

 703.737.2258

 20 South King Street  
Leesburg, VA 20175