# Today's Speakers

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

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

# Agenda

Who are third parties and what is third-party risk management?

4 top influencers driving third-party risk management

9 trends and innovations for managing risk with your third parties

Closing thoughts

VendorCentric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

# Section 1:
# Who Are Third-Parties and What Is Third-Party Risk Management?

The typical mid-sized organization has over 1,000 third-party relationships.

# 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

# 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

VendorCentric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

# What Is Third-Party Risk Management?

The process whereby an organization monitors and manages the potential exposure to problems, harm or loss that arise from interactions with all external parties with which it has a relationship. This may include both contractual and non-contractual parties.

# 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).
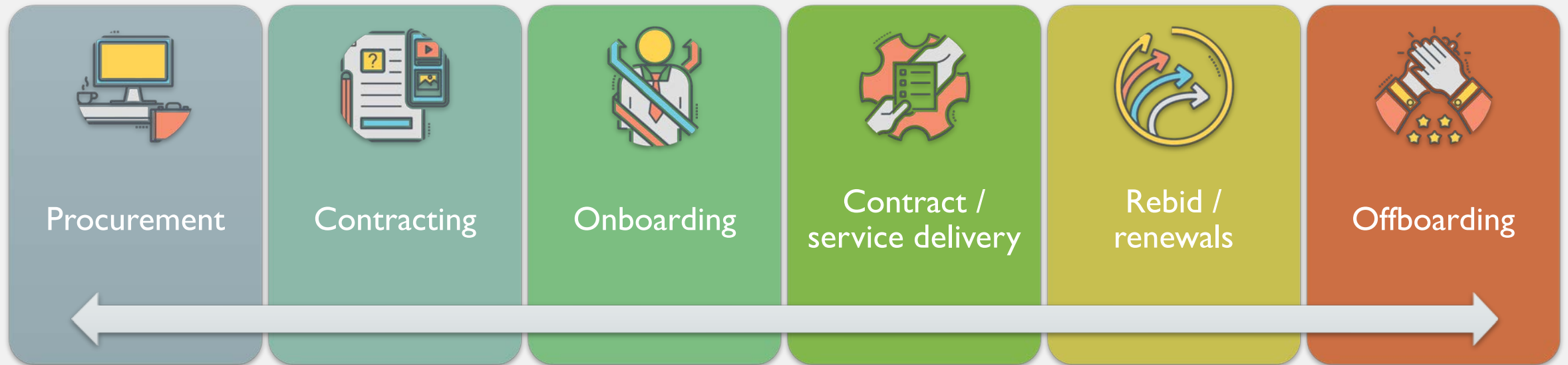
**Information Security**

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

VendorCentric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

8

# When Are Third Parties Risky?

# All of the Time!

| Procurement | Contracting | Onboarding | Contract / service delivery | Rebid / renewals | Offboarding |



VendorCentric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

9

**Section 2:**

# 4 Key Influencers Driving Third-Party Risk Management

# Driver #1. Increasing Reliance on Third Parties

**What is your organization's level of dependence on external entities that might include third, fourth or fifth parties?**

Votes Received: 3,129

Don't know/Not applicable 11%

Little or no level of dependence 18%

High level of dependence 19%

Moderate level of dependence 52%

Copyright © 2018 Deloitte Development LLC. All rights reserved.

2019 Extending the risk management ecosystem poll : 3

Vendor Centric

Lewis Baach Kaufmann Middlemiss PLLC
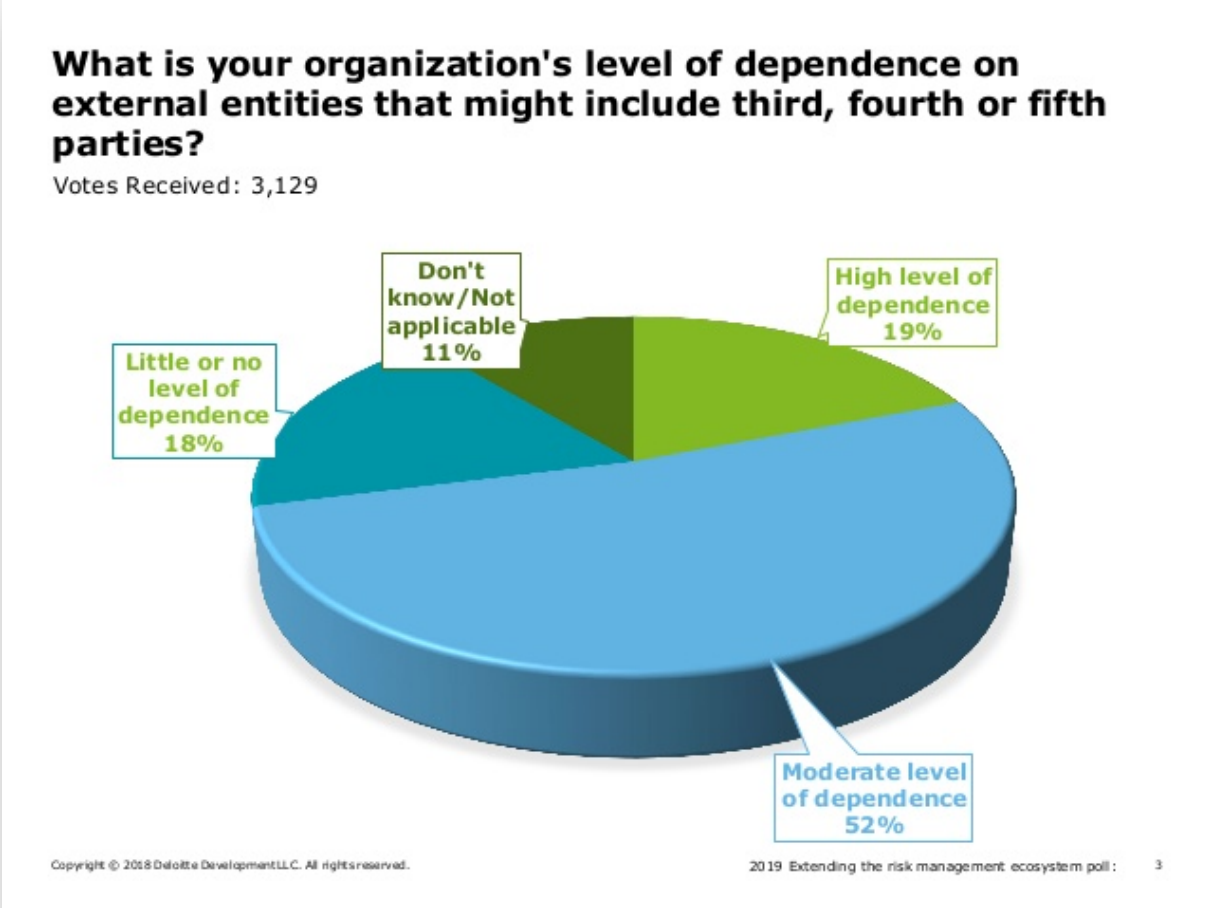
# Driver #2. Increased Complexity of Relationships



"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

Vendor Centric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

12

# Driver #3. Increased Data-Sharing

# Driver #4. Increased Regulatory Oversight

**83%** of organizations experienced a third-party incident in the last 3 years.

**46%** of those experienced a **moderate to severe impact** on customer service, financial position, reputation or regulatory compliance.

Vendor Centric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

# Section 3:
# 3 Themes & 9 Trends in Third-Party Management

Theme 1

# Expanded Risk Management Activities During Procurement

Vendor Centric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

17

# 1. Organizations Are Being More Deliberate About Adding New Third Parties

| Master Vendor List | | |
|---|---|---|
| Last updated: 12/4/2018 | | |
| | | |
| Vendor | Status | Notes on goods/services |
| Actuarial Careers | Active | Recruiter |
| Addison Group | Active | Recruiter |
| Adecco | Active | Recruiter |
| Aerotek Professional Services | Active | Recruiter |
| Alta IT Services | Active | Recruiter |
| Andover Research | Active | Recruiter |
| Beacon Recruiting | Active | Recruiter |
| Bridgeway | Active | Recruiter |
| Capstone Search | Active | Recruiter |
| CPA Search Inc. | Active | Recruiter |
| D.W. Simpson | Active | Recruiter |
| ECS (Employment Contractor Services Inc.) | Active | Recruiter |
| Executive Network, LLC | Active | Recruiter |
| Frank Consulting | Active | Recruiter |
| Group One Consultants | Active | Recruiter |
| Hanover Search | Active | Recruiter |
| Hire Strategy | Active | Recruiter |
| Kaye Bassman International | Active | Recruiter |
| KD&G | Active | Recruiter |
| KDG (Kathy Gibney) | Active | Recruiter |
| Latitude, Inc. | Active | Recruiter |
| MRI Network | Active | Recruiter |
| Neos LLC | Active | Recruiter |

## Key Reasons Why

- Avoid introducing unnecessary risks from new relationships

- Reduce the # of vendors, contracts and compliance requirements to manage

## 2. Organizations Are Developing Risk-Mitigating RFPs



### Key Reasons Why

- Improve accuracy and completeness of vendor proposals and statements of work

- Identify and remediate risk issues early on

- Comply with regulatory requirements

# Components of a Solid RFP Package

**1** **Executive overview** – frames purpose and objectives

**2** **Organizational 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** **Standard terms and conditions** – teases out risk issues at the beginning of the process

# 3. Organizations are <u>Significantly</u> Expanding Pre-Contract Due Diligence

| Employment Practices | | Completed? |
|---|---|---|
| 1. | Will services be provided by subcontractors, instead of employees? | -- |
| 2. | Are employees, subcontractors and temporary workers with access to client data, bound by non-disclosure agreements (whether separately or as part of their code of conduct)? | -- |
| 3. | Does your company conduct background checks (that include credit, criminal, drug and employment checks) for all employees, consultants, temporary workers and external providers before they are hired and are granted access to sensitive data? | -- |
| 4. | Is there a termination checklist to ensure employees return assets upon termination, (laptop, desktop, PDA, cell phones, access cards, tokens, smart keys, proprietary documentation)? | -- |
| **Technology** | | **Completed?** |
| 1. | Does your company have a SOC 1 – Type 2 report? If yes, please submit. | -- |
| 2. | Provide details on all locations where data is stored (including backup or replicated sites). List all locations, including any which may be data or portion of data taken offsite by an employee, contractor, on a laptop, etc. | -- |
| 3. | Briefly describe the process used to determine when a client should be notified after an incident or event. | -- |
| 4. | Has your company experienced any security breach in the past 3 years (internal or external)? | -- |
| 5. | How does your company ensure security of portable devices that potentially has Company's data and information (i.e. laptops, removable storage, mobile phones, etc.). Does this includes both firm and employee's own device? | -- |
| **Disaster Recovery/Business Continuity** | | **Completed?** |
| 1. | Does your company have a Business Continuity Plan and/or Disaster Recovery? If Yes, please upload. | -- |

## Key Reasons Why

- Understand risks that are inherent in the relationship

- Assess the adequacy of policies, controls and contractual terms to mitigate those risks

- Prevent contracting with third parties whose risk exceeds your tolerance

# Where Companies Are Focusing Their Due Diligence
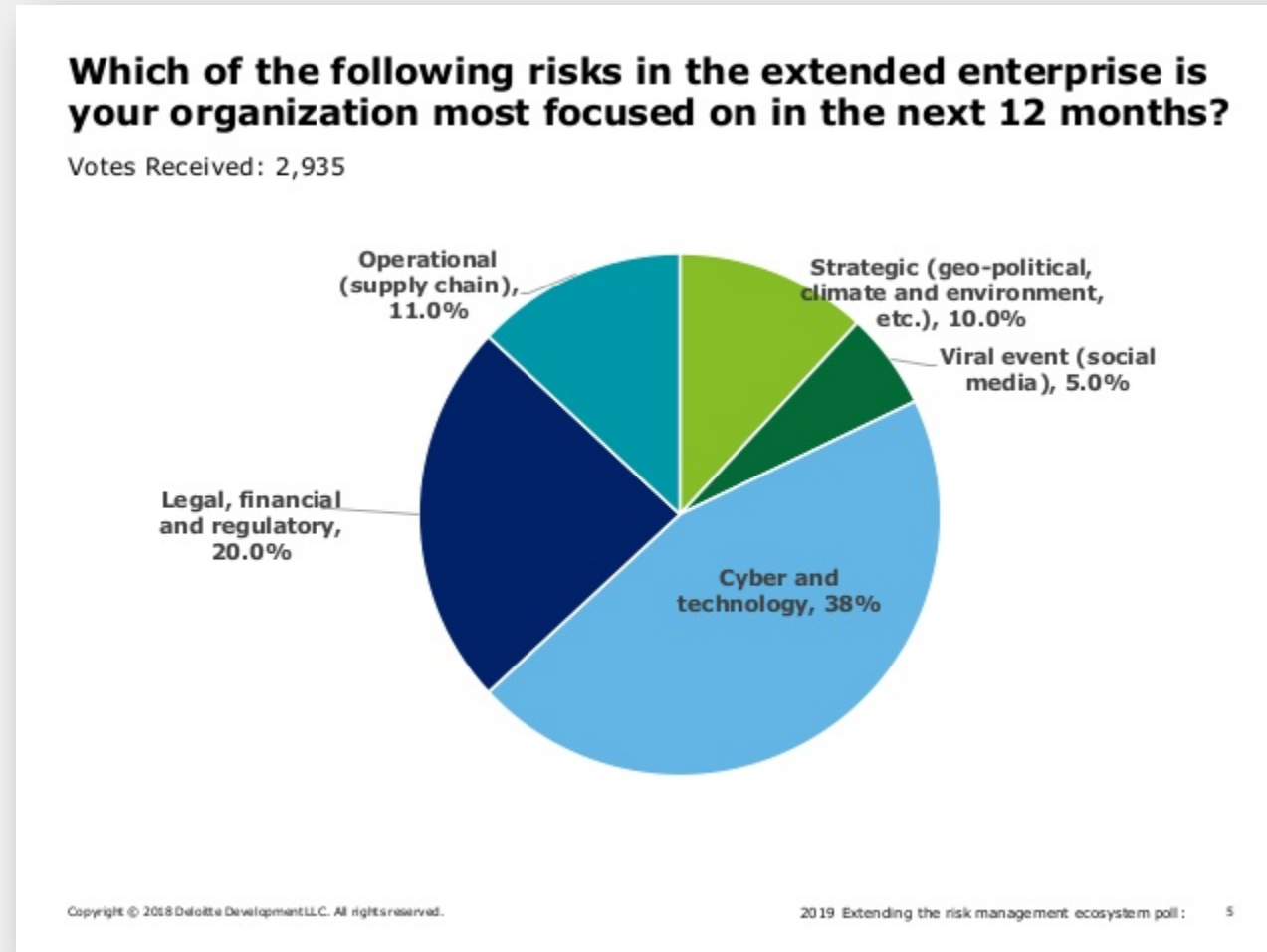


Source: Deloitte Third-Party Management Global Survey

# Types of Due Diligence that May Be Needed

## Corporate Health
- Financials and credit
- Bankruptcy
- Litigation
- Negative news

## IT and Information Security
- Access
- Protection
- Storage
- Destruction

## General Screening
- Business registration
- Licensing
- Insurance
- Sanctions
- Politically exposed persons
- Potential conflicts

## Employment Practices
- Background screening
- Code of conduct / conflicts
- Training
- Offboarding

## Operations Management
- Quality systems
- Internal controls
- Core software platforms
- Downstream vendors (4th parties)

VendorCentric

Lewis Baach Kaufmann Middlemiss PLLC

# 4. Organizations Are Establishing Standards for Their Third-Party Relationships

**APPENDIX C – MINIMUM CYBERSECURITY PRACTICES**

The following minimum requirements should be applied in assessing whether to proceed to use a vendor with access to any form of ▇ non-public information ("NPI"). Based on its Risk Assessment, these minimums shall be implemented by the vendor, unless the CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Note that as a vendor's risk level increases, additional cybersecurity practices and standards apply.

**Organization and Human Resources**
- Vendors shall have an information security program implemented with policies and procedures to support the security of confidentiality, availability, and integrity of systems and data. At a minimum, the organization must have the following implemented:
  - Non-Disclosure Agreements / Confidentiality Acknowledgement
  - Code of Conduct
  - Security Awareness Training

**Infrastructure and Application Security**
- The vendor's computing environment must involve a defense in depth approach with tools and technologies that can detect and prevent potential intrusions. A defense-in-depth solution includes having firewalls, anti-virus protections, as well as utilizing secure protocols (i.e. SSH) to connect to systems securely).
- Vendors must have a process to utilize encryption when transmitting sensitive data over insecure networks. At a minimum, data must use the Cryptography Standard using a secure channel (e.g. HTTPS, SFTP, VPN). In addition, all credentials and/or passwords must be stored using encryption.
- All data designated as non-public by ▇ must be encrypted in transit and at rest.
- Vendors must have controls implemented to manage access to applications/systems and/or data. Accounts should be configured to lock after a pre-determined number of failed logins and remote

- Cybersecurity standards

- Licensing standards

- Insurance standards

- Employment screening standards

- Performance/reliability standards

- Contracting standards

VendorCentric

Lewis Baach Kaufmann Middlemiss PLLC

# Theme 2
# Standardization of Contracting and Contract Management

Vendor Centric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

# 5. Organizations Are Standardizing Contractual Terms and Conditions

**Table 2: Top ten most negotiated terms 2018**

| '18 | | '14/'15 | '13 | '12 | '11 | '10 | '09 | '08 | '07 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Limitation of Liability | - | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | Indemnification | - | 2 | 3 | 2 | 2 | 2 | 2 | 2 |
| 3 | Price/Charge/Price Changes | - | 3 | 2 | 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

## Key Reasons Why

- Create guidelines for contract signers
- Reduce overall risk exposure
- Address concerns when using vendor contractual templates

Source: IACCM

Vendor Centric

Lewis Baach Kaufmann Middlemiss PLLC

# 13 Common, Standard Terms and Conditions

1. Term and termination

2. Fees and expenses

3. Intellectual property ownership and licensing

4. Confidentiality, conflicts of interest, non-competition, non-solicitation of your employees

5. What is each party responsible to do under the contract?

6. Authority (including limits thereon) to act on your behalf?

7. How can the vendor describe its relationship with you?

8. Indemnification and limitation of liability

9. Insurance requirements

10. Post-termination/expiration obligations and restrictions

11. Dispute resolution

12. Service-level agreements

13. Others – each contract needs to be tailored to each matter/transaction

VendorCentric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

# 6. Organizations are Standardizing Third-Party Onboarding

## **Key Reasons Why**

- Align stakeholders

- Support policy compliance

- Create basis for a more successful relationship

Vendor Centric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

28

# Key Onboarding Activities



Assign contract manager

Review contract requirements and align stakeholders

Create and centralize vendor and contract profiles

Identify oversight activities and assign responsibilities

Establish system access and data security

Evaluate need for contingency planning

# 7. Organizations Are Using Risk Standards to Determine Level of Contractual Oversight and Management

**Key Reasons Why**

- Focus on the riskiest contracts

- Scale oversight activities based on the level of risk

- Increase compliance with contractual terms and conditions

# Types of Oversight Activities

- **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
  - Monitoring contract auto-renewal and expiration dates

- **Expanded Oversight**
  - 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
  - Formal offboarding

VendorCentric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

Theme 3
# Establishing Resources and Infrastructure for the Third-Party Risk Management Function

# Third-Party Risk Management Framework

Third-party risk management

| 1. Sourcing | 2. Due Diligence | 3. Contracting | 4. Onboarding | 5. Monitoring | 6. Termination |

To manage third-party risks, it is critical to establish foundational components within TPRM Program.

## TPRM foundational components

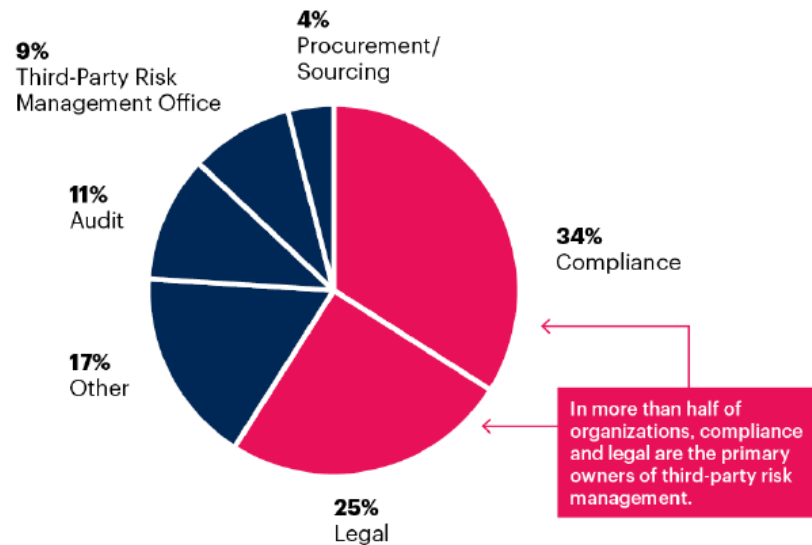| Governance and oversight | Policies and standards | Third-party inventory and contracts | Risk approach and models | TPRM processes | Technology, automation and reporting |
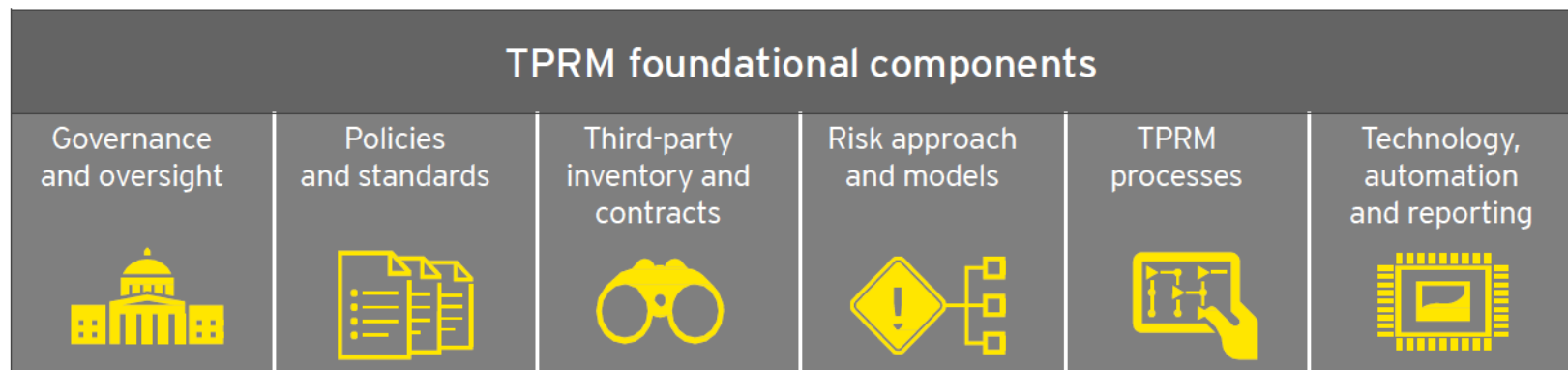
Source: EY

# 8. Organizations Are Establishing Functional Owners of TPRM



## Managing Third-Party Risk

### Primary Functional Owner of Third-Party Risk Management

- 9% Third-Party Risk Management Office
- 4% Procurement/Sourcing
- 11% Audit
- 34% Compliance
- 17% Other
- 25% Legal

In more than half of organizations, compliance and legal are the primary owners of third-party risk management.

n = 256 legal and compliance leaders
Source: 2019 Gartner Third-Party Risk Management Model

## Key Reasons Why

- Provide governance and oversight
- Clarify roles and responsibilities
- Assign accountability
- Meet regulatory requirements

Source: Deloitte Third-Party Management Global Survey

VendorCentric

Lewis Baach Kaufmann Middlemiss PLLC

34

# 8. Organizations Are Implementing Third-Party Management Software
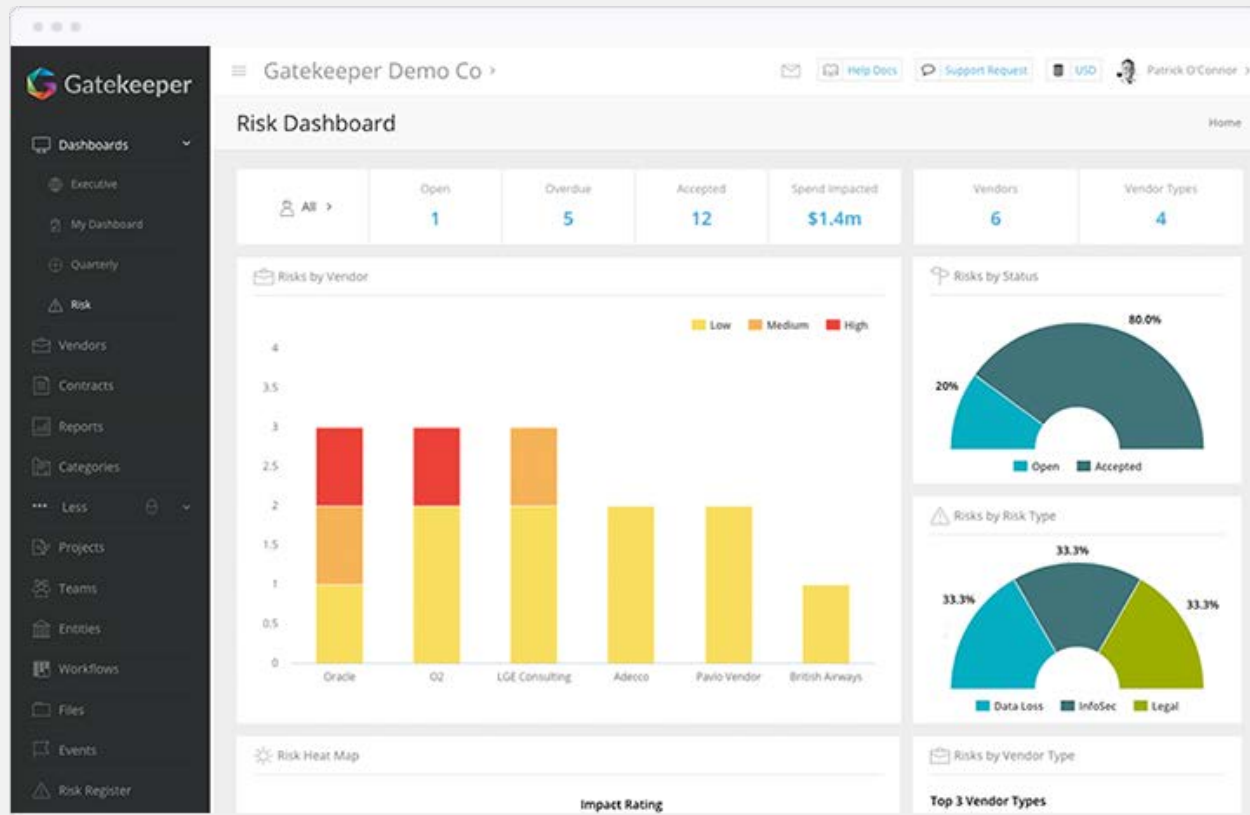


## Key Reasons Why

- Create central inventory of third parties and contracts

- Build profiles of the relationships

- Store contracts and related documents

- Assess risk and perform due diligence

- Run reports to easily show compliance

Source: Gatekeeper

Vendor Centric

Lewis Baach Kaufmann Middlemiss PLLC

# 9. Organizations Are (Starting) to Leverage External Data Intelligence Tools
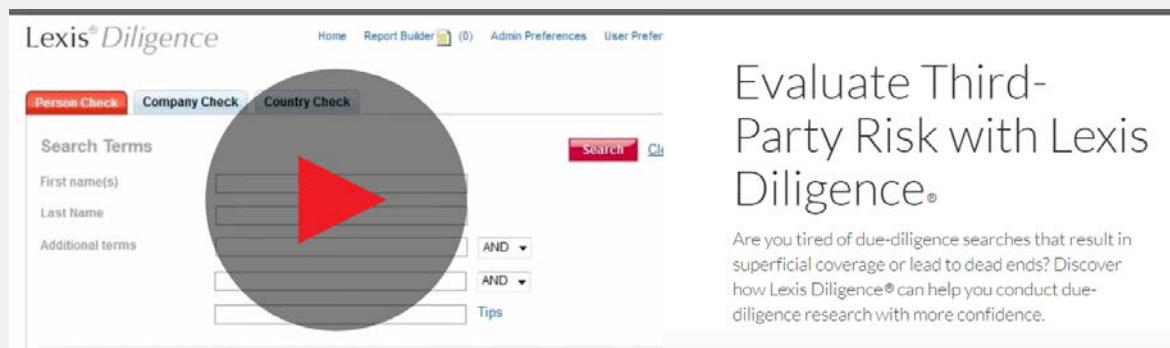


## Current and Emerging Tools

- Business verification screening

- Background screening

- Licensing and certification screening

- Sanctions screening

- Cyber risk monitoring

- Financial health monitoring

Source: Lexis Nexis

Vendor Centric

Lewis Baach Kaufmann Middlemiss PLLC

36

# Section 4:
# Closing Thoughts

**1** Instill oversight and governance
Establish a clear governance structure so that sound risk management practices are embedded into your culture. Set the tone at the top.

**2** Get a fully view of your third-party inventory
Identify, categorize and assess your existing third-party population to effectively manage your third-party inventory.

**3** Establish a risk approach and models
Adopt Risk models according to your organization's risk appetite and culture. determine the level of risk your organization is willing to take.

**4** Implement policies and standards
These should outline the purpose and phases of TPRM framework and define the roles and responsibilities of accountable stakeholders.

**5** Establish and execute TPRM processes
These should be cascaded into each phase of the third-party risk management life-cycle.

**6** Leverage technology automation and reporting
Use technology to automate processes, analyze data and report metrics to improve decision making and understand the operational effectiveness of the TPRM function.

Vendor Centric

Lewis
Baach
Kaufmann
Middlemiss
PLLC

# Contact Information

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

✉ trogers@vendorcentric.com

🌐 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

🌐 http://www.lbkmlaw.com/

📞 202-659-6749

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

Vendor Centric

Lewis
Baach
Kaufmann
Middlemiss
PLLC