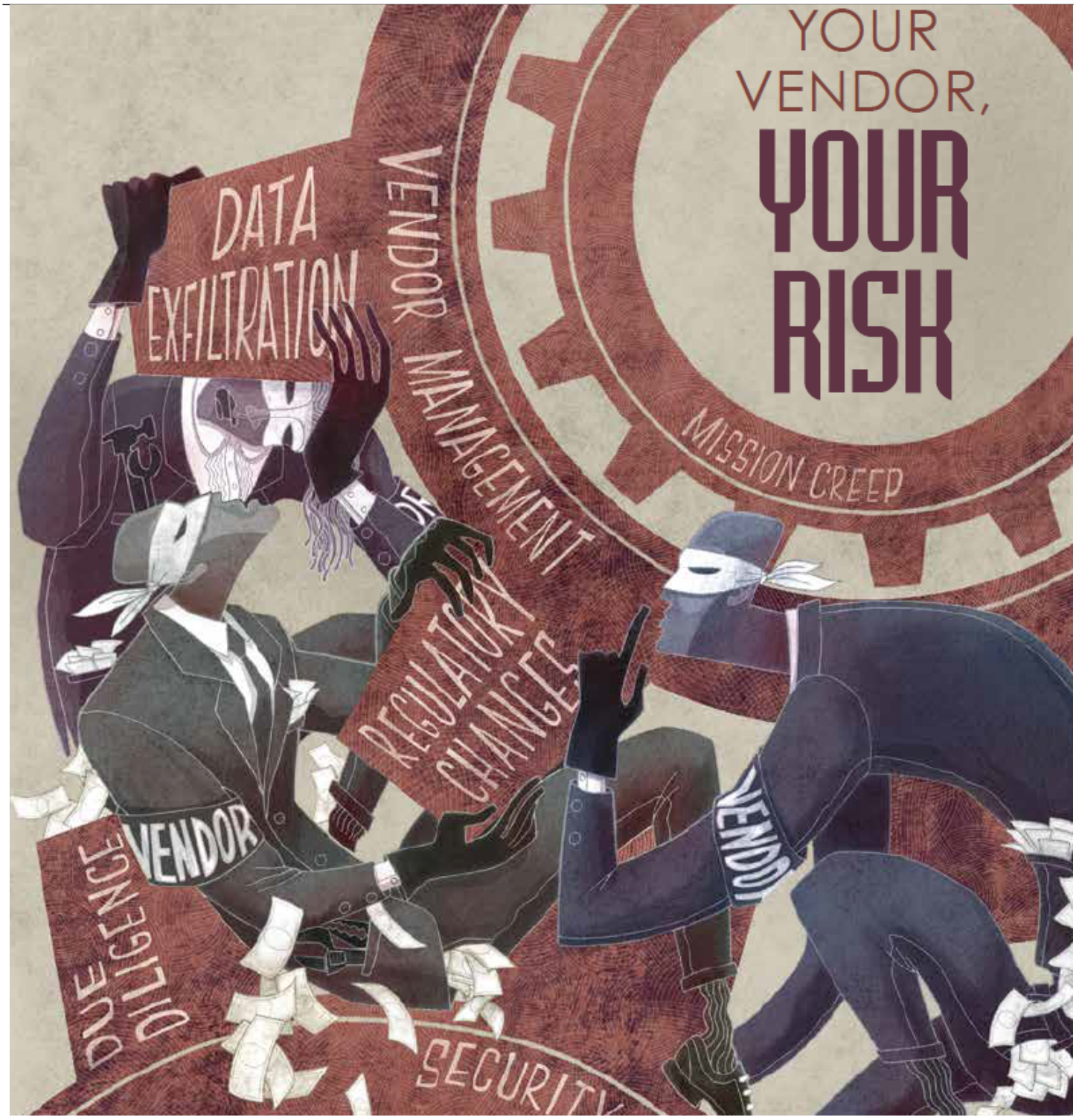
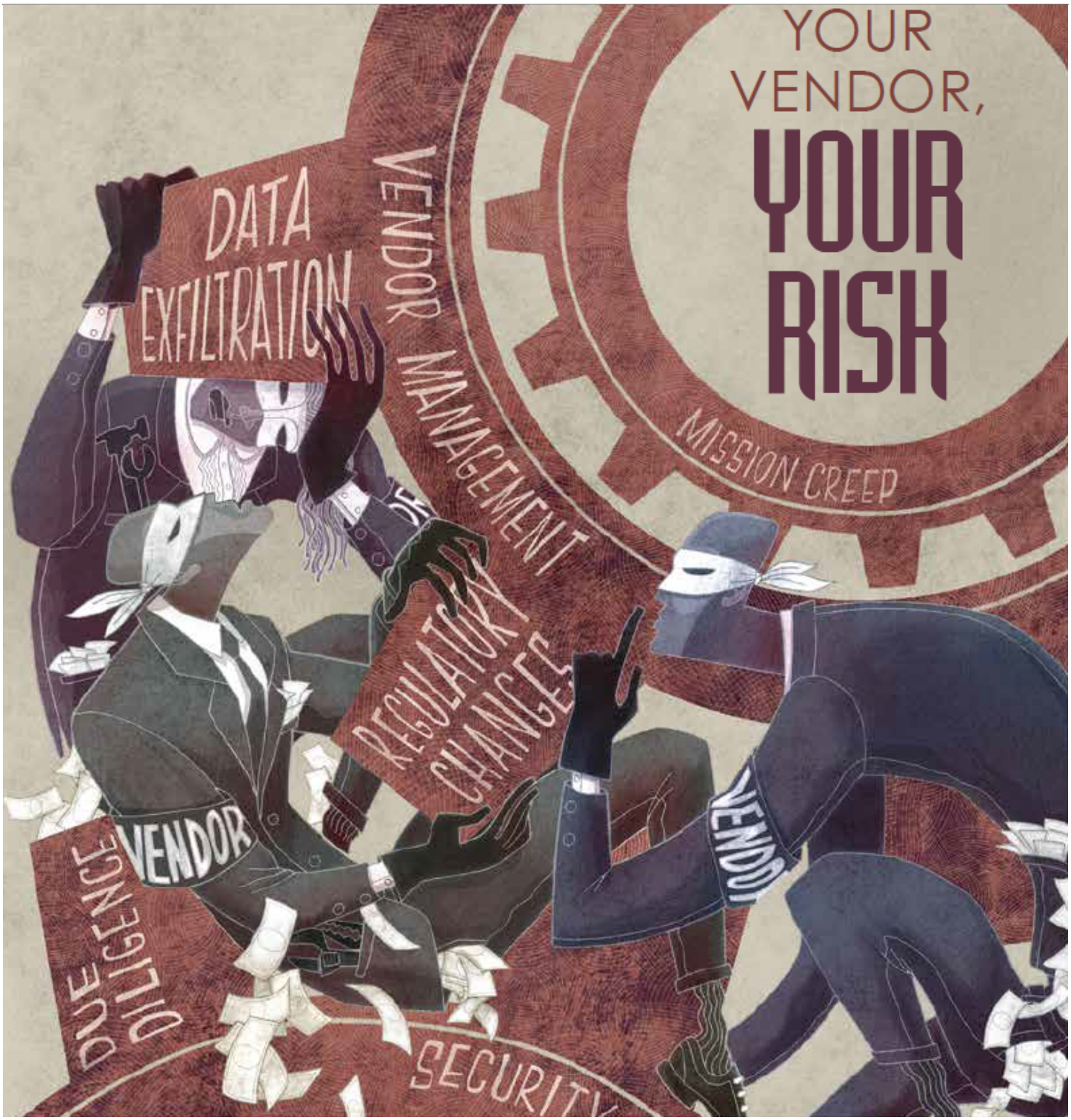
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Your Vendor, Your Risk

Law Department Management


YOUR VENDOR,
YOUR RISK
DATA EXFILTRATION
VENDOR MANAGEMENT
REGULATORY CHANGES
MISSION CREEP
DUE DILIGENCE
VENDOR
SECURITY



CHEAT SHEET

- ***Company onus.*** In many jurisdictions, responsibility lies with the controlling company if a vendor mismanages data, making vendor management instrumental in the protection of data and brand.
- ***Before.*** Prior to engaging a vendor, establish risk tolerance criteria, conduct a vendor landscape assessment, determine a due diligence process, and address remediation and

contractual issues.

- ***During.*** Conduct ongoing reviews, seek feedback on the vendor's performance from internal and external clients, and monitor vendor tasks to ensure they are within the agreed-upon scope.
- ***After.*** Always have an exit strategy ready to avoid renewals or penalties, and if data is involved, confirm that the vendor does not keep it.

Nearly all businesses face the same basic problem: They can't do it all. Businesses rely on vendors to provide various services or products to support not only their clients, but also their own business requirements. The challenge is how to balance the benefit with the associated risks.

An analogy is the phrase, "a chain is only as strong as its weakest link." A variation of the idiom first appeared in Thomas Reid's "Essays on the Intellectual Powers of Man," published in 1786. The original expression was first printed in 1868. This example is applicable to relationships between companies and their third-party providers — particularly as it relates to protecting confidential information. Are your vendors the weakest link in your information chain?

> Accessing and/or viewing databases in one country from another is considered a cross-border transfer. Most notably, the European Union places significant restrictions on such transfers.

In this article, we will first provide an overview of some key concepts that apply to vendor management before discussing the regulatory landscape and the lifecycle of vendor management. We will cover the entire lifecycle: before, during, and after, along with legal requirements and special circumstances.

Key concepts

The terms "vendor," "third party," and "service provider" are often used interchangeably, and in many ways, it is appropriate to do so.

In the supply-chain world, a vendor is the last entity that sells the service or product to the end user. In most cases, the term is used alongside service provider, because the business is the end user — the consumer of the product or service. However, all vendors and service providers are typically external third parties, but not all third parties are vendors or service providers. Third parties include governmental reporting agencies, parties that request information, and other external entities that have not been hired to provide services or products to the company.

In addition, it is common for one area of the business to service another. This creates internal customers. When data flows from one area to another, even within a company, it creates liability and responsibility that can be similar to external sharing of data.

In this article, we will use the term "vendor" for simplicity, but where necessary, we will identify the important nuances.

"Cross-border transfers" refer to the transmission of personal data from one jurisdiction to another.

The transfer can be either physical or digital. Accessing and/or viewing databases in one country from another is considered a cross-border transfer. Most notably, the European Union places significant restrictions on such transfers. The European Union requires that the receiving jurisdiction be judged to have "adequate" data protection practices. The European Commission has so far recognized Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United States as providing adequate protection. If cross-border transfers are regulated and can only occur under certain conditions, make sure you understand and are familiar with your vendor's data practices. In addition to the European Union, the Asia-Pacific region is also working to ensure the protection of personal information when it moves across borders. Its standards are prescribed by the APEC Privacy Framework.

Sometimes, it is not about the written law but about the norms in that area. For example, not all countries are heavily reliant on contracts. Your field units may start doing business while the home office is still reading the paper. Relationships may be the most important factor in selecting a vendor rather than pricing or service delivery. Aside from cultural nuances such as expected behaviors, greetings, etc., be aware of the nuances in doing business. These come into play throughout the vendor lifecycle.

The other critical concepts relate to the legal requirements for companies to exercise appropriate control or oversight or where the law in question holds vendors directly accountable.

Regulatory landscape

The regulatory landscape has changed drastically in the past few years. Laws are adopted that are directed at both privacy and security to protect the personal information that a company processes as well as confidential company data. This is in addition to other laws and requirements that apply to vendor relationships, such as anti-bribery, money laundering, conflicts of interest, and others. This article will focus on data protection, but the recommendations apply to all vendors.

With the introduction of Europe's General Data Protection Regulation (GDPR) in May 2018, and many countries adopting the same approach to protect their residents, organizations can no longer abdicate and shift their responsibilities. In the United States, the New York Department of Financial Service (NYDFS) 23 NYCRR 500.11 requires a covered entity to perform a risk assessment of their third-party service providers and continue to perform periodic assessment of third-party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.

Section 500.11 Third Party Service Provider Security Policy(a)(4)

US states are considering (or have already passed) laws that include oversight of service providers and third parties. Companies are currently focused on the California Consumer Privacy Act (CCPA) that comes into effect January 1, 2020. Likewise, Latin America has been assertive in its data protection laws, and Brazil passed the General Data Protection Law (LGPD), effective in early 2020. Other countries, such as Colombia and Chile, have similarly increased their presence in data protection regulation with GDPR-like elements, and Mexico has been the most active in its enforcement of data laws.

The ABCs of vendor management

A AUDIT AND ASSESSMENT.
The right to audit vendors for compliance.

B BOARDROOM.
Is your board engaged?

C CYBERSECURITY COVERAGE.
Do vendors have coverage, and how much?

D DATA BREACH/SECURITY BREACH.
Do you have a plan in place?

E EXIT PLAN.
Do you have one for ending the relationship?

F FINANCIALS.
How financially stable is your vendor?

G GOVERNMENT REGULATED.
Are you prepared for an investigation?

H HOMOGENEITY.
Are they consistent in their approach across multinational locations, joint ventures, and affiliates?

I INDUSTRY REGULATION.
How will sectoral or regional laws affect your company?

J JUDGMENT AND ENFORCEMENTS.
Did you check if there are any against the vendor or its executives?

K KNOWLEDGE–FRAMEWORK/CERTIFICATION.
Does the vendor abide by an established knowledge base or framework?

L LIMITATION OF LIABILITY.
Are they willing to negotiate?

M MERGERS, ACQUISITION, AND DIVESTURES.
How will these impact your
third-party relationship?

P POLICIES AND PROCEDURES.
Do you have the necessary policies in place?

O OFFSHORING AND OUTSOURCING.
Do they outsource (or offshore) services?

Q QUICK ONLINE SEARCH.
Have you done a quick online search on their reputation/brand risk?

R RETENTION.
Did you document the retention period?

S STRATEGIES AND SYNERGIES.
Are they your partner, and is this going to be a long-lasting relationship?

T THIRD-PARTY REPORTS.
When and how often should you do them?

U UP-AND-COMING TECHNOLOGY.
Is it proven tech?

V VENDOR MANAGEMENT PROGRAM.
Does the company have its own program?

X CROSS BORDER TRANSFERS.
How, when, and where is data transferred, and is it regulated?

Y YOUR RISK PROFILE.
What are you willing to tolerate?

Z ZONE.
Are they representing your zone of influence or able to add to your zone?

The GDPR and the US Health Insurance Portability and Accountability Act of 1996 (along with its subsequent amendments, HIPAA) are two examples of laws that hold vendors directly accountable for the protection of data. However, if the controlling company (or covered entity) has not performed its own due diligence and examined the vendor's data practices and security controls, it is likely that it will be held accountable for selecting a vendor that was not suitable. In many jurisdictions, the onus is directly on the controlling company to exercise the appropriate amount of management and control over their chosen vendors. This amount can vary based on risk — and risk changes based on the legal regime, upline reporting, reliance on supply chain, and types of data being exchanged.

Vendor breaches are increasing

According to the third annual Ponemon Institute Data Risk in the Third-Party Ecosystem (2018),5 59 percent of companies said they have experienced a data breach caused by one of their vendors or third parties. These numbers are even higher in the United States — 61 percent — up five percent over

the 2017 study and a 12 percent increase since 2016. Almost a quarter of the respondents (22 percent) admitted they didn't know if they had a third-party data breach over the past year. Overall, more than three-quarters of organizations believe that third-party cybersecurity incidents are increasing.

One reason for the increase is the growing complexity of the vendor landscape. Companies are increasing their reliance on third parties and sharing an increasing amount of sensitive data outside their own walls. Furthermore, fewer than 50 percent of companies claim that their third-party management program is effective or even a priority. Most have no idea if their vendor safeguards are enough to prevent a breach.

It is no longer the responsibility of just the vendor or just the customer; each organization now has a vested interest to ensure that they protect their data as well as their brand and reputation.

In recent years, we have seen a shift in business operations. Companies are searching for ways to reduce their infrastructure costs by moving to a cloud-based computing model (Infrastructure as a Service or IaaS). The cloud offers flexibility and scalability for any business so they can adapt to changing business needs. Special considerations for cloud providers are discussed further below.

With changes in the regulatory landscape, companies must ask themselves: Do I know who I am doing business with, and how do I hold my vendors accountable?

Cloud vs. co-location

Businesses are turning to the cloud and data center co-location to cut costs, gain efficiencies, deliver on-demand services, and provide the business with a competitive advantage. Both the cloud and a co-located data center can help — and they are not the same.

The cloud is a set of services, technologies, and tools that can help you transform the way you do business whereas co-location is a place. It's the data center where your actual IT environment lives. Building and maintaining your own data center can easily run into the millions — and companies search for predictable, cost-effective ways to manage that need.

You can have both co-location and the cloud, but having one doesn't automatically mean that you have the capability for the other. For example, your co-location provider may not offer cloud, managed services, or migration services. You can also use the cloud without being in a co-location facility. The key is to find the right mix that works for your company.

The world of vendor relationships: Before, during, and after

There is a lack of confidence in third parties' data safeguards, security policies, and procedures for responding to a data breach or cyber attack. Organizations often rely on contractual obligations

instead of audits and assessments to evaluate the privacy and security practices of vendors.

An average of 63 percent of a company's personal and sensitive data is disclosed to or managed by third parties spanning a wide range of functions, including human resources, law firms, legal service providers, payroll, accounting, marketing, customer services, software development, engineering, and many more.

As in-house counsel, your role may or may not manage vendors directly. Large companies in particular tend to have procurement departments and certainly contract management teams. Often, the privacy counsel or privacy officer must be involved in vendor management — from assessment to termination. However, you are viewed as the expert in legal matters and much of vendor management falls under the umbrella of legal matters.

Further, as you engage in conversations with key personnel or projects, you may learn about potential or actual vendors that carry legal implications due to the sensitive nature of the data, the critical nature of the project, or elements as simple as the vendor's geographical location or a vendor's lack of legal review due to low cost.

Your heightened awareness of the full lifecycle of vendors is important.

Can you confidently answer "yes" to these questions?

- Are your vendors subject to data privacy and cybersecurity regulations?
- Do you know the specific types of personal data you disclose to each vendor?
- Do you know how all your vendors manage and use that data?
- Are your vendors complying with applicable regulations?
- Do you trust your vendors to know this information about their vendors?

How to leverage technology to manage vendors

Contract management systems are important to managing vendor contracts, but they have not developed to address the current needs of business — mainly privacy and security. Do you know which clients you are required to notify within 24 hours of a potential data breach? Most systems cannot tell you that. Can you track the mitigation measures contractually required of vendors? Can you identify what requirements are in place in case of a potential merger, acquisition, or divestiture? Technology is the solution to this. Building from the basics of eDiscovery, we are starting to see sophisticated tools, such as Planet Data's Exego platform, that use a combination of massive processing power and active learning to identify not only words, but contextual phrases for whatever is needed across thousands of electronic documents (no matter what form those documents take).

Not all companies have the budget to engage such vendors, but if you have contract management, review it to see what capabilities it has to provide you the information you need, quickly, without special programming. You may find that like most cloud providers, the vendor can provide an expertise at a cost-effective and efficient manner. That peace of mind — confidence in the end result — may balance the budget constraints.

Remember that ‘I know him; we went to high school together,’ or similar personal connections, do not constitute appropriate due diligence.

Before engaging a vendor

When we consider the vendor engagement model, what level of due diligence is conducted and who is performing the assessment? In large organizations, teams may be dedicated to performing this function. In small to mid-size companies, it is included as a portion of another job function — if at all. In many cases, vendor due diligence is reliant upon the business unit that is engaging the vendor. These individuals are often not well trained in recognizing the legal risks, business red flags, or assessing privacy and security measures. It is not uncommon for a key individual to have a relationship with a potential vendor. Remember that “I know him; we went to high school together,” or similar personal connections, do not constitute appropriate due diligence.

Here are the five points to address before engaging a vendor:

1. Establish business alignment

Set a risk tolerance based on the sensitivity of the data, the profile of the company, the history, the board preferences, the industry, and the market. Make sure business partners understand that a favorite vendor may need to be cut because it does not meet standards. Also, set the process upfront — whether it is the amount of a contract that needs legal review, outsourced to the business units, when to conduct a privacy impact assessment, what triggers a security review, etc.

2. Know your current landscape

Many companies have not conducted or maintained a thorough data inventory, which includes internal sharing and replication as well as external sharing and replication. This includes retention, security measures, reasons for collecting and keeping data, and destruction processes. Knowing this will help companies identify duplication in vendor types and provide intelligence on where to streamline resources and recognize cost savings and efficiencies. Before hiring a new vendor, check to see if the business is already using a vendor that offers those services or products. Being a known entity is an easy way for a vendor to expand its reach inside the company — which increases relationships through trust and satisfaction. It may also highlight problematic vendors to avoid.

3. Determine an assessment process

Some organizations may have purchased third-party software to assist with this process. However, if you have a limited budget and resources, you may have to create your own questionnaire. Regardless, this is your due diligence process, which needs to include these elements as a baseline — and the people over each area must coordinate:

- Privacy;
- Security;
- Business model and history (number of clients);
- Key business plans: expansion, acquisitions, to be sold, etc.;
- Physical location and location of data you provide them;
- Key personnel;
- News reports and reputation;

- Relationship with competitors; and
- Insurance coverage (types, exclusions, amount).

4. Address remediation measures

Should the assessments above identify any areas of concern, determine how to address them and critically evaluate if they should be addressed. For example, if your company is governed under HIPAA and the system implementer you are hiring is not HIPAA-compliant, you may be facing millions in costs to control this risk. Perhaps the vendor needs to satisfy your concern before contracting or insert mitigation requirements into the contract. If you do the former, make sure someone has responsibility to verify that the vendor successfully completes this on time. If the vendor does not, what are the repercussions? This is a point in the business alignment above — counterparts must be on board to exit a relationship if predetermined criteria are not met.

5. Contractual issues

Aside from the issues mentioned above, there are numerous elements that must be addressed in the contract, such as indemnification (you cannot indemnify away negligence or gross misconduct), limitations of liability, definitions of key terms (watch out for circular definitions — they do matter), insurance coverage, audit rights and cost, standards to meet, knowledge and compliance with laws, data handling, dispute resolution, subcontracting or outsourcing, and termination. Please also consider addressing advance notice of a potential merger, acquisition, or divestiture. Have the ability to push down new requirements on you that feed into what the vendor does for you — whether it is a customer requirement, legal decision, or other controlling party. You may also be able to discover if they are working with or for a competitor and control that information flow.

This is a short list of essential requirements. Make sure you have this documented to (1) know that you have a complete “before” view and where agreement or exceptions were noted and (2) that you have all the information in one spot for future reference. Most companies have no one place to find all vendors.

At the start of a vendor engagement, you need to have a vendor onboarding of some sort. Based on the risk profile you established above, this may be a quick process or it may be long and drawn out. If the vendor is stocking your paper supplies, they may only need orientation to the delivery location and to learn your delivery process (e.g., submitting invoices, key contacts, etc). If the vendor is your co-located data center or your cloud service provider, there is quite a bit more to do to get the relationship working smoothly.

During the relationship

The three essential items during the relationship are:

1. Ongoing due diligence

All the actions you took above need to continue. Based on the risk profile, you may need to review them quarterly or annually (try not to go beyond every other year for the least risk) and determine what level that review warrants. Some vendors may require an in-person visit annually, some may only need a desktop review (get a copy of policies, certifications, etc.) or a telephone interview. But don’t over-emphasize certifications — they are not the Holy Grail of vendor approval — they are just another tool. Make sure you trust the entity performing the certification. If a vendor is in the news for

a data breach, your data inventory should show you exactly what data this vendor has from your company. If a prior vendor has a data breach, be confident (and verify) that you have no data remaining with that vendor. Watch out for mergers, acquisitions, and divestitures to see how they impact you. Finally, pay attention to enforcement and legal activity that may indicate a need for a change on your side.

2. Relationship management

Check in with the business partners, invoicing, and other key departments to see if the vendor is performing satisfactorily. Identify and address key issues. Be comfortable about whether they are working for or with a competitor and if you are assured that no corporate confidential information (e.g., strategic plans) are in danger of being passed along. If you relied on key personnel — are they still there or have they slipped in another individual? Regardless of how well the relationship is going, be aware of two things: (1) the desire for an ongoing relationship, and (2) the ease of switching to another vendor. Have a plan for continuing and a plan for exiting. Watch for automatic renewals and have the critical dates controlled.

3. Mission creep

Once a vendor is approved and in your system, your colleagues may think that is approval to use that vendor for any reason. That may not be the case. This vendor may have been approved on a low-risk item and the new expansion is high risk. It is extremely important to document what services the vendor is contracted to provide so that a colleague doesn't add new services that are beyond the scope of the vendor. This information should be captured in a central database with details.

The key component during the relationship is to identify this vendor's importance. If you are in manufacturing, this may be a requirement of your quality management, but that doesn't mean everyone does it well. In enforcement activity, regulators identify the issues that are of most concern — ranging from inadequate control records and documentation to poor vendor criteria.

Ending the relationship

You should always have an exit strategy. In this operating model of frequent buying and selling, enforcement activity, and corporate misconduct or mistakes, there is no excuse for burying your head in the sand. As noted above, you should be monitoring the relationship throughout to prepare for an unexpected ending. On the other hand, this may simply be the end of the contracted service and everyone parts on amicable terms.

If data was involved, they should not keep it. Data that was backed up at an offsite facility is often overlooked. You may, if there is a need for the vendor to maintain data, require them to provide you a list of the types of data, the reasons for retention (possible regulatory requirement), and how long it is anticipated. Have them provide a certificate of irretrievable destruction that is not based on your request (unless you have a solid system to follow up in a timely fashion like the mitigation actions outlined earlier).

Make sure you take the appropriate steps to end the relationship to avoid renewals or penalties. Even in an amicable termination, there are likely required steps to follow. During an unfriendly split, you need to make sure that the termination is appropriate, backed up by evidence, as part of a process that includes notification of key departments, including how other services will be impacted, whether or not a replacement is necessary, and, depending on the scope of the termination, if counsel should

be involved.

Also, follow through on any items that need to be changed — data inventories, subcontractors, upstream partners, documentation, and processes that might be impacted. Transitioning to a new vendor may not be easy or quick. Try not to be in a position of negotiating during a trauma — you are never in a strong bargaining place in emergency situations.

Special circumstances

In addition to the lifecycle above, be aware that there are some circumstances where you may need to add more diligence, oversight, or considerations. Most of these are not uncommon, but just because outpatient surgery is fast and simple does not mean it doesn't have risks.

Cloud services. We partially addressed this earlier. It is very common now to engage software, infrastructure, or platform as a service (respectively SaaS, IaaS, and PaaS). Most businesses do not enter the market to manage software, infrastructure, or platforms — but it is a necessary component of doing business. The cloud service providers specialize in what they do. That may alleviate concerns about managing those services in-house when lacking the special knowledge or skills to do so, but it also adds a level of oversight. Don't be blasé about contracting with cloud providers. Do the diligence. Know where they are located, where their servers are located, where they have disaster recovery and business continuity rollover, and where they push overflow (cloud bursting is where designated servers get too busy, so it pushes to another). Usually, they will have certifications, but look up the certifiers. If possible, go visit.

Co-lo data centers. This is short for co-location (or co-located) data centers. These data centers are subject to the same recommendations and comments as the cloud providers above. They are generally the experts where you are not. It helps with cost and efficiencies but do the diligence and exercise a high level of oversight.

Outsourcing overseas. Another common practice is to outsource software development and customer service overseas. This one can be sensitive as it is very helpful in saving costs, but is the outsourced location in a country that is known for its corruption?

The World Population Index issues a Corruption Perception Index report annually. This can be of some assistance in gauging the potential for corrupt practices

In recent news articles, companies have been fined over foreign corruption charges and the fines are significant. This does not mean you cannot do business, it just means that you need to exercise care and oversight. Have a solid process for secure software development review, don't let actual data be used in development, go visit in person, have your outsourced business in a secure environment — physically — and instill physical deterrents to theft or misconduct. Certain countries also address corruption through antibribery, such as the UK Anti-bribery Act and the US Foreign Corrupt Practices Act. You should make sure to have a solid process for addressing these requirements.

Unequal bargaining powers. Some well-known vendors are much larger than the companies who hire them. This generally means negotiating contractual terms is infeasible. However, with many of these large vendors, they also provide a great deal of transparency into their practices, make documentation publicly available, and have finetuned their agreements to a certain degree of commercial reasonableness. Not always. It is always worth trying if there is something in the terms, contracts, or other documents that you find objectionable. If you dislike the majority, and they won't

negotiate, make your decision for what is best for your company. You must still do your diligence and exercise oversight. Do not take it for granted that they are doing everything right.

Parents-subsidiaries out of alignment. This situation can happen due to a parent company being in one country with subsidiaries in others. Thus, individual companies may be subject to different laws and may be in conflict — especially when it is likely one is the controller and the other a processor (under the many laws that use those terms, such as GDPR). Many companies have successfully navigated this with the expert assistance of local attorneys in each impacted country coming to a commercially reasonable and well-negotiated strategy, typically involving some sort of intracompany agreement around data, controllership, liability, and commitment that local law shall override any standard practices.

These are certainly not the only special circumstances and yours may very well be similar to some and vastly different from others. Resources abound on this topic as it is one that is critical to operating a successful company.

The bottom line

With this vendor management lifecycle, key concepts, brief regulatory oversight, and special circumstances, you should have a simple framework to adopt or improve your vendor management program. Whether you are directly involved in vendor management, indirectly involved in certain aspects, or merely maintain an awareness of critical issues, as in-house counsel, you need to know how to manage vendors.

ACC EXTRAS ON… Vendor management

ACC Docket

The Legal Department's New Nightmare: Your Vendors (Oct. 2018).

Verifiable Vendor Management: 4 Tips to Avoid Risk (Aug. 2017).

Articles

Working with Vendors Without Waiving Privilege (United States) (March 2018).

Sample Forms, Policies, and Contracts

Template Letter of Technology Vendor Requesting Improvements (April 2018).

Code of Conduct Regarding Suppliers and Vendors (May 2017).

Further Reading

Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of

Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks

Cybersecurity Checklist

Untangling Third-Party Data Privacy and Cybersecurity Risks

Maggie Gloeckle

VP of Privacy and Compliance Counsel

A+E Networks

K Royal

Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.