THIRD-PARTY RISK MANAGEMENT:
TAMING THE BEAST USING INFORMATION GOVERNANCE

By

Sofia Empel, PhD, CRM

Project Underwritten By:
ARMA International Education Foundation

December 21, 2021

www.armaedfoundation.org

Table of Contents

Introduction

Organizations of all sizes, from global conglomerates to small firms, are increasingly leveraging third-party relationships to improve competitive advantage and control costs. During these third-party engagements, an organization's data, and in some cases its clients' data, may be shared, transferred, processed, or stored outside the contracting organization's environment. Stakeholders such as regulators, clients, shareholders, and the organization itself expect each third-party to manage and protect data under its control to the same degree as the contracting organization (the "Organization").[1] To mitigate risks that may result from these third-party relationships, including any data-related risks, Organizations must exercise internal and external controls.

In the aftermath of the U.S. 2008 financial crisis, the Federal Deposit Insurance Corporation (FDIC) stressed that "A bank can outsource a task, but it cannot outsource the responsibility."[2] Beyond this notion, the Federal Reserve emphasized that risks may be created by more than the outsourced activity itself: risks may arise by simply being involved with a third-party.[3] Going a step further, when a client agrees to do business with an Organization, there is an implicit promise of trust that must be kept,[4] including trust that the Organization will not do business with third parties who may present a "clear and present danger" to an Organization's data.[5] Meeting these expectations requires Organizations to implement robust third-party risk management processes, policies, training, controls, diligence, audits, and remediation. If an Organization does not

[1] "Organization" is used throughout this paper to refer to any entity, regardless of size, industry, or ownership, from small family-owned businesses to large multinational conglomerates, as well as municipal, state or provincial and federal government bodies who enter a contractual relationships with third-party providers.

[2] "Guidance for Managing Third-Party Risk," Federal Deposit Insurance Corporation (FDIC), accessed January 20, 2021, https://www.fdic.gov/news/news/financial/2008/fil08044a.html

[3] "Guidance on Managing Outsourcing Risk," Division of Banking Supervision and Regulation Division of Consumer and Community Affairs Board of Governors of the Federal Reserve System, December 5, 2013, https://www.federalreserve.gov/supervisionreg/srletters/ sr1319a1.pdf

[4] Mark Sangster, "It's Time to Take Third-Party Risk Seriously," *The American Lawyer*, September 1, 2019.

[5] John Thomas A. Malatesta III and Sarah S. Glover, 2016, "A Clear and Present Danger: Mitigating the Data Security Risk Vendors Pose to Businesses," *Sedona Conference Journal* 17 (761).

implement an effective third-party risk management process, third-party risks could snowball into serious issues that affect the Organization's mission, profitability, and reputation.

Although an Organization's board and its management team ultimately bear responsibility for exercising diligence before entering into third-party relationships and the oversight of controls afterward,[6] third-party management is primarily implemented by internal functions such as third-party risk, vendor management, strategic sourcing, procurement, supply chain management, extended enterprise risk management, information security, compliance, or something else.[7] Regardless of its name, Organizations must mobilize this internal function to help protect the Organization against third-party risks. While they provide oversight from their own perspectives, the subject matter experts in this third-party risk function may not be qualified to address information governance issues that may arise from an Organization's data being retained by an outside party. As data-specific subject matter experts, records and information governance professionals are uniquely qualified to add value to the third-party risk management process, particularly the governing of an Organization's data and documents (together the "Data")[8] under the control of its third parties.

Generally, third parties may be categorized into three main groups: vendors, intermediaries, and business partners.[9] Vendors include suppliers, manufacturers, contractors, staffing agencies, software developers, hardware and software sellers and resellers, and other goods or services providers, whereas intermediaries encompass professional services such as consultants, accountants, lawyers, engineers, designers, advisors, brokers, agents, sales representatives, and others. Business partners consist of entities with which an Organization collaborates, for example

---

[6] Ralph Sharpe and Meredith Boylan, 2012, "Operational Risk: Increased Regulatory Focus on BSA/AML Compliance and Third-Party Relationships," *Journal of Taxation and Regulation of Financial Institutions*, 25(41).

[7] "Building Trust with Your Third Parties in a Technology Driven and Disruptive World: EY Global Third-Party Risk Management Survey 2019-20," Ernst & Young, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-trpm-survey-2019-20-update-final.pdf

[8] "Data" is used throughout this paper to refer to any data or documents received by the third-party from the contracting organization on behalf of the organization or its clients.

[9] Shaswat Das, "Conducting KYC of Third Parties: Best Practices for Conducting Due Diligence," Hunton Andrews Kurth, April 2018, https://www.huntonak.com/images/content/3/6/v4/36714/best-practices-for-conducting-due-diligence.pdf

co-investors, joint venture partners, and strategic partners. Typically, third parties do not include client relationships. This paper focuses on vendors and intermediaries, although the described approach that follows can be applied to business partners as well. In this paper, a third-party is broadly defined as an entity engaging in a potential or existing contractual relationship to provide products or services to an Organization or to perform professional services.[10]

The purpose of this paper is to provide information governance and records and information management professionals (the "IG Officers") and other interested stakeholders with an approach to integrate Data-focused diligence and monitoring into an existing third-party risk management program or to stand up an entirely new program (together the "Framework"). To achieve this goal, the Generally Accepted Recordkeeping Principles (the Principles"),[11] which apply to an Organization's Data as a best practice, should also be used to govern Data in the possession of and under the control of third parties. As such, IG Officers who use the Framework are expected to have an intermediate to advanced understanding of these Principles, as well as practical experience implementing them in a decision-making capacity at an enterprise level. This paper will also be helpful to novice IG Officers interested in professional development, as well as students who want to explore future opportunities.

Seasoned third-party risk management practitioners *without* information governance experience may also find this paper useful. However, such users are cautioned that "the devil is in the details." Applying the Principles within an Organization is challenging, even for experienced IG Officers. Likewise, third-party diligence and monitoring are often complex. For example, Data under the control of a third-party may be governed by the same regulatory requirements as the Organization, but not always. In addition, third parties operate independently, often with low levels of information governance maturity, limited transparency into data management execution, and minimal accountability for non-compliance. Nonetheless, this paper will provide practitioners

[10] "Guidance for Managing Third-Party Risk," Federal Deposit Insurance Corporation (FDIC).

[11] The Generally Accepted Recordkeeping Principles, also referred to as the Principles, are a set of eight principles that when considered together comprise a global standard that identifies the critical characteristics and best practices for records management, records and information management (RIM), and information governance programs. The eight principles include accountability, transparency, integrity, protection, compliance, availability, retention, and destruction. "The Principles," ARMA International, 2017, https://www.arma.org/page/principles

without information governance experience insight into the third-party diligence and monitoring needed to mitigate associated risks.

This paper does *not* provide IG Officers with a one-size fits all approach to third-party risk management. Every Organization and third-party is unique; third-party relationships are structured to suit specific business needs; and regulatory requirements may vary not only from one relationship to another, but also from one engagement to another. Nevertheless, this paper outlines a scalable Framework that can be adopted by an Organization of any size or a member of any industry and applied to a wide variety of third parties and engagements. It should be noted that the Data-related monitoring addressed in this paper is for data-at-rest, not data-in-transit which is the domain of information security professionals. Moreover, the Framework concentrates on governance or activities related to compliance and policymaking. In other words, the Framework emphasizes "what" should be done, rather than being a step-by-step "how-to" guide.[12]

The Framework focuses on Data-related diligence and monitoring in the context of the five stages of the third-party risk management lifecycle, specifically: planning; diligence; contracting; monitoring; and contract renewal or termination (see Figure 1).

[12] Information management professionals debate the difference between records and information management (RIM) and information governance (IG), sometimes arguing there is no difference at all. The author's view is that the two fields are distinct, yet related disciplines. While the information governance function develops organizational policies and the supporting activities such as training and oversight, the records management function operationalizes these polices. To explain this distinction more fully, analogies between corporate and country governance are useful. Legislators create laws that citizens must follow; similarly, information governance professionals generate corporate policies that employees must abide by. Further, enforcement agencies implement laws, while records management professionals implement information-related corporate policies. For example, state legislators create speed limit laws, while police departments execute speed limit controls such as issuing traffic tickets. Similarly, information governance creates corporate retention policies, and records and information management personnel operationalize these retention rules within the business units. For a discussion on the differences between governance and management, see Lynda Bourne, "The Six Functions of Governance," PM World Journal, Volume III, Issue XI, November 2014, https://www.mosaicprojects.com.au/PDF_Papers/P188_Six_Functions_of_Governance.pdf

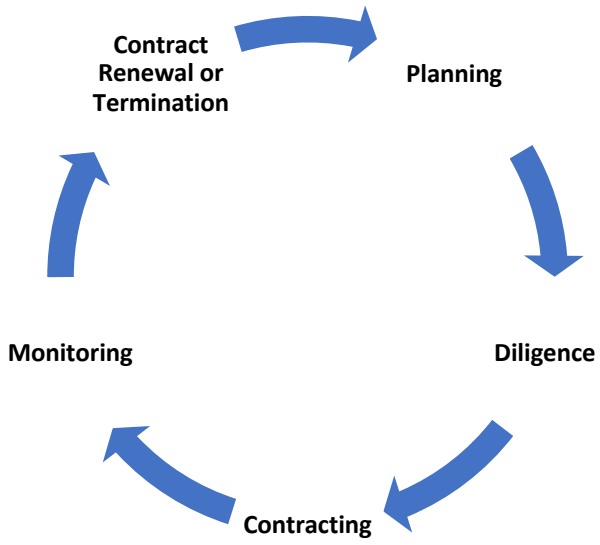

Figure 1: Third-Party Risk Management Lifecycle

Finally, the Framework described in this paper is based on the author's experience and provides insight into "what" Data-related diligence might look like, as well as "what" is needed to implement ongoing monitoring while supporting successful third-party relationships. Although this Framework is applicable to most Organizations and situations, IG Officers are responsible for adapting the Framework to their Organization's objectives, structure, and culture, and for making the necessary programmatic modifications to ensure the Framework operates effectively for their Organization.

Chapter 1: Planning

"It does not do to leave a live dragon out of your calculations, if you live near him."[13] In this quote, author J.R.R. Tolkien suggests that risks should not be overlooked, and minimally, they should be acknowledged when planning a course of action. Keeping this in mind, Chapter 1 addresses several key planning issues.

Understand Compliance and Regulatory Concerns

The Organization's primary regulators and any corresponding regulations that may include third-party requirements or implications should be identified and analyzed by the IG Officer. If the Principle of Compliance[14] has been applied in the normal course of business, the Organization's regulatory environment will be known already and codified in a matrix of global regulations and corresponding requirements. What may not be known are which, if any, of the applicable regulations contain requirements that compel the Organization to "flow-down" its obligations to its third parties. Even if a regulation does not specify third-party requirements, such obligations may be implied by the law's intent. For example, a reasonable assumption can be made that retention requirements for human resource records apply not only to records stored in-house by the Organization, but also to Data retained on behalf of the Organization in a third-party's software-as-a-service (SaaS) solution. For these reasons, applicable regulations, some of which may not seem to directly apply to third parties, must be analyzed in the context of the business relationship, the specifics of the engagement, and the type of Data being retained by the third-party.

If an information governance regulatory analysis has not been completed, another Organization's analysis should not be copied given that every Organization, third-party, and engagement is

---

[13] Tolkien, J.R.R. 2017. Chapter 12: Inside Information in *The Hobbit.* Houghton Mifflin Company: New York. After the protagonist Bilbo Baggins breaks into the dragon's lair and steals a cup from Smaug's treasure, his wizard advisor Gandalf rebukes him for not planning how to deal with Smaug, even while the dragon plots his revenge.

[14] The Principle of Compliance states that an organization's information governance program shall be constructed to comply with applicable laws, other binding authorities, and the organization's policies. "The Principles," ARMA International.

unique.[15] This is not to say that another Organization's regulatory analysis may not be employed as a model: Organizations in the same industry are subject to similar regulations; therefore, another Organization's analysis may be useful as a starting point. Some resources for identifying regulatory requirements include an Organization's existing third-party risk management function, legal department, outside counsel, or internal or external subject matter experts. Identifying applicable regulations is the first necessary step in determining third-party compliance requirements, but the crux of the analysis lies in understanding how each requirement applies in the context of each third-party relationship and each engagement. This type of targeted third-party analysis will be explained as part of the Framework in later chapters.

While regulatory guidance varies among government bodies, all agencies agree that robust diligence and continuous monitoring are critical to reducing third-party risk. Organizations should ensure their third parties conduct business ethically, protect confidential information, mitigate operational risks, and more. At the same time, Organizations should establish third-party compliance with regulations such as the Gramm-Leach-Bliley Act; Anti-Money Laundering (AML) requirements; Foreign Corrupt Practices Act (FCPA); UK Bribery Act; Federal Trade Commission (FTC) Act; Dodd-Frank Act; General Data Protection Regulation (GDPR); Health Insurance Portability and Accountability Act (HIPAA); HITECH Act; and Medicare and Medicaid contract provisions; to name a few.[16] Note that the regulatory environment of a third party's host country also presents challenges for third-party relationships.[17] For example, India currently does not have adequate regulatory controls and enforcement related to data breaches, which poses high risk challenges for clients located in Europe and the United States.[18]

---

[15] "Third Party Risk Management," Security Industry and Financial Market Association (SIFMA), accessed August 27, 2020, https://www.sifma.org/resources/general/third-party-risk-management/

[16] For a list of some government agencies that require third-party diligence and oversight, as well as sample regulations and standards, see Appendix A.

[17] Prashant Palvia et al, 2002, "Global Information Technology: A Meta-Analysis of Key Issues," *Information and Management*, 39(5): 403-414.

[18] Peter Engardio et al, "Fortress India," *Business Week*, February 14, 2004; Anupam Kumar Nath, 2018, "Towards Understanding the Factors and Their Effect on Offshored Data Privacy," *Journal of Business and Management*, 24(2): 1-18. DOI: 10.6347/ JBM.201809_24(2).0001

Currently, governments do not specify a standardized approach that Organizations must adopt to comply with third-party regulatory requirements. As a result of this lack of coordination, Organizations design and implement their own third-party risk programs,[19] often employing best practices from compliance programs generally. For example, regulators expect compliance programs to follow common-sense requirements that can be evaluated by asking three fundamental questions:[20]

- Is the Organization's program well-designed?
- Is the program applied in good faith, adequately resourced, and empowered?
- Does the compliance program work in practice? [21]

The answers to these questions determine whether, and to what extent, an Organization's program was effective at the time of an offense. Violations for non-compliance can be expensive. For example, penalties for a HIPAA data breach range from $100 to $50,000 per violation (per person), depending on the level of negligence, with a maximum penalty of $1.5 million per year, with certain violations subject to criminal charges that may result in jail time.[22]

Heightened regulator expectations reflect the increasing number of Organizations doing business with third parties in interconnected environments that make these engagements more difficult to control than ever before.[23] When critical activities are involved such as sharing, transferring, processing, or storing Data outside an Organization's environment, regulators expect

---

[19] "Third Party Governance and Risk Management: Turning Risk into Opportunity," Deloitte Global, 2015, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-third-party-governance-risk-management-report.pdf

[20] "Evaluation of Corporate Compliance Programs," U.S. Department of Justice, updated June 2020, https://www.justice.gov/criminal-fraud/page/file/937501/download

[21] For a complete description of the requirements for compliance programs, see "Department of Justice Manual 9-28.800," Department of Justice, accessed August 21, 2020, https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations

[22] "HIPAA Violations and Enforcement," American Medical Association, accessed August 31, 2000, https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

[23] Thomas J. Curry, "Remarks Before RMA's Governance, Compliance, and Operational Risk Conference" Speech, Cambridge, Massachusetts, May 8, 2014, https://www.occ.treas.gov/news-issuances/speeches/2014/pub-speech-2014-69a.pdf

comprehensive and rigorous third-party diligence and monitoring.[24] To ensure compliance and avoid financial penalties, costly investigations, and reputational damage when third parties fail to meet their obligations, Organizations should prepare for government and other audits by identifying regulatory requirements (see Appendix A) and employing a robust third-party risk management program to implement the applicable requirements.

Define Organizational Objectives for Third-Party Risk

Third-party relationships vary widely from one Organization to another. An Organization may outsource products, lines of business, or entire functions. Third-party relationships may involve simple or complex transactions; include foreign or domestic entities; comprise big or small suppliers; traverse a wide variety of industries and sectors; and span time periods from a few minutes to many decades. Organizations may engage third parties for their subject matter expertise or utilize them geographically to concentrate workers, facilities, or goods. An Organization may depend on a single third-party to such an extent that the third-party becomes a vital component of an Organization's operations.[25] Third parties even may be engaged to tackle deficiencies in an Organization's operations or to ensure compliance with regulations.[26] Regardless of organizational objectives, third-party relationships pose risks to an Organization, albeit that some third-party activities are riskier than others. Everyone is responsible for protection of the Data—executive leaders, boards, employees who "own" the third-party relationships, third-party risk management functions, and even the third parties themselves.[27] In a recent study, companies reported that during

[24] "OCC Bulletin 2013-029, Third-Party Relationships: Risk Management Guidance," Office of the Comptroller of the Currency (OCC), October 30, 2019, https://www.occ.gov/news-issuances/bulletins/2013/ bulletin-2013-29.html

[25] "Third Party Risk Management," Security Industry and Financial Market Association (SIFMA).

[26] Ibid.

[27] Maria Moskver, "Navigating the Pitfalls of Third-Party Service Provider Oversight," The *Mortgage Banker Magazine*, February 8 2019, https://www.mortgagebankermag.com/loan-servicing/navigating-the-pitfalls-of-third-party-service-provider-oversight/

government reviews regulators focused primarily on third-party oversight and governance activities.[28]

Unfortunately, many boards and executive leaders hesitate to redirect their attention and resources from current challenges to third-party regulatory compliance that may not presently be affecting them.[29] Regulators have no patience for such executive "balancing-acts" and reinforce time and again that boards and executive leaders are accountable for controlling third-party risk.[30] A good rule of thumb is that boards and executive leaders should set the "tone-at-the-top" and extend oversight to third parties just like any other function in the Organization, regardless of a third-party's reputation or outward ability to comply with relevant regulations.[31] Further, enterprise-wide policies governing the use of third parties should be approved by the board of directors or an executive committee. These policies should establish clear objectives for third-party risk management, hold stakeholders accountable,[32] outline the Organization's risk appetite, and authorize a team to implement the program. After organizational objectives are defined, a cross-functional third-party risk management team, including an IG Officer, should align the third-party risk management program with the Organization's objectives.

Leverage an Existing Third-Party Risk Management Process

Information governance-related diligence and monitoring of third parties should be integrated into an existing centralized third-party risk management program, if available. Many Organizations operate such programs due to regulatory requirements or past enforcement actions, but these

---

[28] "Building Trust with Your Third Parties," Ernst & Young Global Limited; "Global Financial Services Third-Party Risk Management Survey," 2018, Ernst & Young, https://ey-global-financial-services-third-party-risk-management-survey.pdf

[29] Subhashis Nath,"The Coming Regulatory Wave: Vendor Risk Management," Genpact, accessed November 28, 2020, https://www.genpact.com

[30] See for example, "Comptroller's Handbook: Consumer Compliance, Version 1.0," June 2020, Office of the Comptroller of the Currency, https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/unfair-deceptive-act/pub-ch-udap-udaap.pdf

[31] Cathryn Judd and Mark Jennings, 2012, "Vendor Risk Management—Compliance Considerations," *Consumer Compliance Outlook*: Fourth Quarter 2012.

[32] The Principle of Accountability states that a senior executive (or a person of comparable authority) shall oversee the information management to appropriate individuals, "The Principles," ARMA International.

programs may have different levels of maturity. In a benchmark study, four in ten companies reported having a fully mature third-party risk management program, while approximately one-third of companies had ad hoc or no programs at all.[33] Regardless of program maturity, connecting information governance to the Organization's wider objectives by joining an existing third-party risk management program increases the probability of successfully implementing the Framework described in this paper.

According to Linda Tuck Chapman,[34] one of the biggest challenges to a third-party risk management program is a lack of internal resources to execute the program.[35] Connecting third-party management to other risk domains, while networking with the Organization's other subject matter experts increases efficacy and decreases duplication and inconsistencies. For example, during a third-party diligence review, an Organization's security function may address data-in-transit with the third-party, but if they also review data-at-rest for topics such as data retention, data organization, and destruction, the analysis may be superficial, misinterpreted, or even unacknowledged. For the Organization to "fire on all cylinders," information governance objectives should be incorporated into an existing third-party risk management program, and the IG Officer should be a member of the cross-functional team, serving as the data-at-rest subject matter expert.

Know the Organization's Risks

Risk management is a process that involves identifying risks, evaluating the probability that a vulnerability will occur, and implementing controls to avoid or minimize potential harms posed

---

[33] "Vendor Risk Management Benchmark Study: Running Hard to Stay in Place," Shared Assessments and Protiviti, 2019, https://www.protiviti.com/ sites/default/files/2019-vendor-risk-management-benchmark-study sharedassessments-protiviti.pdf

[34] Linda Tuck Chapman is a recognized expert in third-party risk management. She was the former Chief Procurement Officer for three major banks; President of ONTALA Performance Solutions Ltd.; and author of "Third-Party Risk Management: Driving Enterprise Value." "About," ONTALA Performance Solutions, accessed August 21, 2020, https://ontala.com/

[35] "Regulatory Requirements and the Third-Party Threat," LexisNexis, 2014, https://www.lexisnexis.com/pdf/Nexis-Diligence/Financial-Services.pdf

by those vulnerabilities.[36] There are many definitions of risk; however, the two characteristics common to most definitions include: (1) uncertainty that an event may occur and, (2) unwanted consequences from vulnerabilities that can be avoided or prevented.[37] There may be numerous risks that arise from an Organization's use of third parties. Some risks are amplified by involvement with a third-party, while other risks are associated with the underlying activity itself.[38] The Framework described in this paper addresses two distinct, yet related types of risks: (1) risk to the Organization based on the quality and comprehensiveness of its third-party risk management program and, (2) risks posed to the Organization by the third-party relationships and engagements themselves.

The first type of risk is programmatic risk, which deals with the efficacy and completeness of the overall process used by an Organization to diligence and monitor its third parties. To withstand scrutiny from regulators and other stakeholders, the third-party risk management process should define what steps should be completed by the third-party review team and other stakeholders based on a good faith effort. Once the third-party risk management process is defined, process steps should be followed consistently and the same tools, such as diligence questionnaires, should be used to minimize subjectivity. Process steps include all parts of the third-party risk management lifecycle from how an Organization interprets relevant laws through onboarding, maintenance, and eventual offboarding. For a third-party risk management program to be defensible against challenges and complaints, it should be objective, fair, consistent, and documented.

Even heavily regulated industries such as financial services or healthcare do not specify what constitutes acceptable quality and comprehensiveness of a third-party risk management program, but some best practices for diligence, contractual negotiation, and monitoring are available.[39] For

---

[36] "What is Risk? Definition and Meaning." *Market Business News,* accessed November 21, 2020. https://marketbusinessnews.com/financial-glossary/risk-definition-meaning/

[37] Michael G. Campbell, 2011, *The Complete Idiot's Guide to Project Management, 5th edition*. London: Penguin Books.

[38] "Guidance for Managing Third-Party Risk," Federal Deposit Insurance Corporation (FDIC).

[39] Malatesta, "A Clear and Present Danger.

example, the Federal Council's regulations for implementation of the Gramm-Leach-Bliley Act (GLBA) by banks and other financial institutions specifies that businesses should:

1. Utilize a diligence process to select appropriate third parties;
2. Compel third parties by contract to implement appropriate controls to meet regulatory requirements and industry best practices; and
3. Where indicated by a risk assessment, monitor the third parties to confirm their obligations were satisfied.[40]

Organizations can mitigate programmatic risks by implementing a third-party risk management program that meets the requirements of a compliance program generally as described earlier in this chapter, and by instituting a defensible process described in this section, as well as throughout this paper.

The second type of risk relates to the third-party relationships and engagements themselves. Although regulators do not categorize risk in the same the way, there are seven categories of risk that recur with frequency.[41] All of these risks do not apply to every third-party, either directly or indirectly; however, there are four categories of risk that are particularly germane when third parties are in control an Organization's Data, including:

- ***Transaction risk*** relates to a third-party's failure to perform as expected by the Organization or its clients due to problems with service or product delivery. For example, a third-party may lack an effective data destruction process or fail to employ qualified

[40] 12 C.F.R. § 570 III(D). Appendix B, Interagency Guidelines Establishing Information Security Standards. Available https://www.law.cornell.edu/cfr/text/12/appendix-B_to_part_30

[41] In addition to the four risks mentioned in the body of the paper, the other common categories of third-party risk are: ***Strategic risk*** is the risk that occurs when a third-party fails to offer products or services that are not compatible with the organization's strategic goals or do not provide an adequate return on investment. ***Reputational risk*** is risk arising from negative public opinion caused by dissatisfied clients, inappropriate actions, violations of law, data breaches, or publicity from other adverse events. ***Operational risk*** is the risk of loss from inadequate internal or external people, processes, or technology, including data-related activities. "OCC Bulletin 2013-029," Office of the Comptroller of the Currency (OCC).

personnel who can execute defensible data destruction as specified in contractual requirements.

- ***Compliance risk*** is posed by violations of laws, rules, or regulations, or from non-compliance with policies, procedures, ethical standards, and contractual obligations. For example, a third-party may not comply with regulatory obligations that require certain types of records be retained for specified periods of time in accordance with applicable laws.
- ***Country risk*** occurs when a third-party based in a foreign country exposes an Organization to the economic, social, and political conditions of the foreign country. For example, a third-party's protection of Organizational Data of a personal nature might be influenced by lax or ineffective regulations in the third-party's home country, even if Data protection controls are specified in the contract.
- ***Legal risk*** arises from third-party activities that expose an Organization to lawsuits, investigations, audits, or otherwise cause the Organization to incur legal expenses. For example, if Data under a third-party's control becomes subject to a legal hold, the third-party may not have the process or knowledgeable resources to preserve, collect, or produce the legal hold data.

A group of risk categories is known as the "risk universe"—a base list of the risks that the Organization faces[42]—which may be further divided into sub-categories based on other criteria such as Data-related risks as described in Table 1.

[42] Risk categories included in the risk universe depend on factors specific to the Organization such as industry, regulations and other legal requirements, third-party engagement activities, countries involved, and others.

Table 1: Examples of Data-Related Information Governance Risks	
Risk	**Description of Data**
Retention[43]	Retention of organizational and/or client Data provided to and controlled by the third-party that must be retained to satisfy a business need or regulatory requirement
	Retention of the third-party's business records to demonstrate compliance with the contract and applicable legal and regulatory requirements
Email	Retention and destruction of Data stored in the third-party's email system that may be classified as official company records or organizational or client Data provided to and controlled by a third-party
Disaster Recovery Backups	Retention and destruction of disaster recovery backup copies of organizational and/or client Data, used to restore systems in the event of an adverse event (electrical interruption, natural disaster, etc.)
Data Classification	Classification of organizational and/or client Data provided to and controlled by the third-party; or third-party's business records to demonstrate compliance with the contract and comply with a regulatory requirement
Destruction[44]	Destruction of organizational and/or client Data destroyed in the normal course of business
	Destruction of organizational and/or client Data destroyed as specified by contract in the normal course of business
	Destruction of organizational and/or client Data at contract termination as specified by contract
Legal Holds	Preservation of Data relevant litigation, investigation, or audit, or as otherwise subject to a legal hold
Downstream Entities[45]	Retention and destruction of organizational or client Data provided by the third-party to downstream fourth parties, fifth parties, etc.
Cloud Computing	Retention and destruction of organizational or client Data stored in a cloud (the organization's cloud) that is used as part of the organization's IT infrastructure and controlled by the Organization's personnel
	Retention and destruction of organizational Data stored in a Software-as-a-Service (SaaS) solution where the organization's data is retained in a third-party system

[43] The Principle of Retention states that an organization shall maintain its information assets for an appropriate time, taking into account its legal, regulatory, fiscal, operational, and historical requirements. "The Principles," ARMA International.

[44] The Principle of Disposition states that an organization shall provide secure and appropriate disposition for information assets no longer required to be maintained, in compliance with applicable laws and the organization's policies. "The Principles," ARMA International.

[45] Regulations do not differentiate between third, fourth, fifth, etc. parties, typically referring to them as "downstream entities." Regulators and other relevant parties hold organizations accountable for managing risks related to their engagements with downstream entities.

Another facet of risk focuses on the difference between inherent and residual risk, which help quantify the effectiveness of risk mitigation. Inherent risk represents the current risk level given an existing set of controls; whereas residual risk is whatever risk level remains after additional controls are applied.[46] For instance, a free soloing rock climber experiences a high degree of inherent risk, while the same rock climber with a harness, ropes, and protective gear (the mitigating controls) encounters residual risk, or a fraction of the risk compared to free soloing. Another metaphor to visualize the relationship between these two facets of risk is water flowing through a filter as seen in the Figure 1.[47]

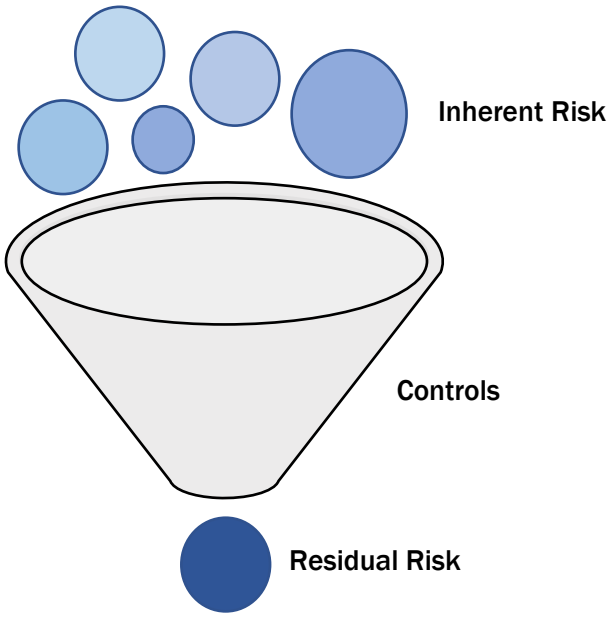

Figure 2: Inherent v. Residual Risk

Inherent risk is represented by water above the filter and includes the third-party's existing controls; the filter represents the application of additional controls required by the Organization, typically through contractual provisions; and the smaller pool of risk below the filter is the residual

[46] Rachel Slatbotsky, "Inherent Risk vs. Residual Risk Explained in 90 Seconds," Fair Institute, accessed November 23, 2020, https://www.fairinstitute.org/blog/inherent-risk-vs.-residual-risk-explained-in-90-seconds

[47] "Inherent and Residual Risk," Tennessee State Government, accessed October 22, 2020, https://www.tn.gov/content/dam/tn/finance/accounts/Inherent-vs-RisidualRisk.pdf

risk that remains after the mitigating controls are applied by the third-party. The IG Officer can help the Organization mitigate third party relationship and engagement risk by analyzing each third-party's risk universe, applicable information governance risks, and inherent and residual risks; identifying weaknesses that create risks; and applying controls to mitigate those risks.

Define Controls

Controls are a combination of people, processes, tools, and activities undertaken by an Organization to prevent, reduce, or counteract exposure to risk. The subject matter experts of a third-party risk management team are responsible for specifying controls in their respective domains. During a third-party evaluation, an IG Officer may specify certain information governance controls to protect an Organization's or client's Data and to mitigate any Data-related risks.[48] Information governance controls might be standardized such as templated contract language for the right to audit a third-party, and other times controls need to be tailored to specific engagements. For example, an Organization may specify a retention period for a particular type of organizational Data being retained by the third-party. Controls may be internal and applied within the Organization such as when an Organization requires its technical resources to configure a data feed to transmit only certain types of Data to a third-party. Conversely, controls may be external such as requiring a third-party to train its employees in procedures to suspend automated destruction in the event of a legal hold. In ideal circumstances, responsibilities for determining controls should be clear, but often the lines of responsibility are blurred.

An understanding of the Three Lines Model, adopted in 2013 by the Institute of Internal Auditors and revised July 20, 2020, can be useful in understanding an Organization's risk management eco-system.[49] Different groups within an Organization, or "lines," play unique roles in managing risk.

---

[48] The Principle of Protection states that an information governance program shall be constructed to ensure an appropriate level of protection to information assets that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection. "The Principles," ARMA International.

[49] Jeffrey P. Taft et al, "The Blurred Lines of Organizational Risk Management," Mayer Brown, July 31, 2020, https://www.mayerbrown.com/en/ perspectives-events/publications/2020/07/the-blurred-lines-of-organizational-risk-management

In the context of third-party risk management, the first line is the business that engages the third-party, and therefore "owns" the risks and corresponding controls. The second line consists of the third-party risk management function that identifies risks and provides diligence in the form of frameworks, policies, processes, and other tools that support risk management activities. The third line provides objective auditing and monitoring to ensure the first and second lines are operating effectively and the "control culture across the Organization is effective in its design and operation."[50] The three lines are accountable to an Organization's senior leadership and its governing body.

The Three Lines Model has been widely adopted within the financial services industry, and in some instances, it may be mandated by regulators.[51] Many Organizations in other industries follow similarly organized risk management models, although the "lines" in smaller Organizations may not be well-defined. The second line, or third-party risk management, typically encompasses subject matter experts from the Organization's governance functions[52] such as those in the list below (together "the Team").[53]

- ***Compliance*** ensures third parties have adequate controls, policies, and procedures in place to conduct business ethically and in accordance with the law. It also reviews contracts to confirm they reference appropriate regulations and other requirements (i.e., Organization's Code of Conduct) for the third-party to follow when providing services or products to the Organization.
- ***Information Governance*** ensures third parties have adequate controls, policies, and procedures in place to comply with applicable regulations, contractual obligations, and industry best practices for the retention, destruction, and preservation of a third-party's

[50] "Modernizing the Three Lines of Defense Model," Deloitte, accessed September 24, 2020, https://www2.deloitte.com/us/en/pages/advisory/articles/modernizing-the-three-lines-of-defense-model.html

[51] See 12 CFR Appendix D to Part 30 - OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches.

[52] "Governance functions" are those business units that create frameworks, objectives, policies, values, culture, accountabilities, and performance targets. Some typical governance functions are security, privacy, compliance, information governance and human resources.

[53] "Team" is used throughout this paper to refer to the cross-functional members of the group designated to conduct third-party diligence and monitoring activities.

business records, as well as data-at-rest controlled by and provided to the third-party by or on behalf of the Organization.

- ***Information Security*** ensures third parties have adequate controls, policies, and procedures in place to prevent the unauthorized access, use, transmission, disruption, modification, inspection, recording, or destruction of Data in accordance with applicable regulations, organizational policies, and industry best practices.
- ***Legal*** drafts and executes contracts between third parties and the Organization, in collaboration with the business owner and the governance stakeholders (e.g., Compliance, Security, Privacy, Information Governance) to contractually obligate third parties to comply with applicable regulatory requirements, organizational policies (i.e., retention schedule, privacy policy, Code of Conduct), industry best practices (i.e., information security, disaster recovery, business continuity), and operational risk needs (i.e., indemnification, right-to-audit, insurance).
- ***Privacy*** ensures third parties have adequate controls, policies, and procedures in place to protect the confidentiality and unauthorized disclosure of the sensitive personal information of individuals in accordance with consent from the owner of the sensitive data, applicable regulations, and contractual obligations.
- ***Procurement*** is responsible for negotiating contractual agreements with third parties that protect the strategic objectives of the Organization and mitigate risks.

Incorporating a broad range of subject matter experts into a third-party risk management process ensures a wide spectrum of risk will be addressed,[54] and appropriate controls implemented. Organizations may assign responsibilities for specific controls differently than described in this section. Generally, the function assigned to a particular control is not as important as ensuring that all risks and corresponding controls are addressed appropriately. As stated earlier, some subject matter experts may be aware that certain controls are needed, but they may not have the in-depth knowledge needed to apply the controls correctly.

[54] Andrew Kenney, 2016, "Third-Party Risk: How to Trust Your Partners." *Journal of Accountancy* May (2016): 57-61.

As an initial step to specifying third-party information governance controls, the IG Officer reviews the Organization's policies, which codify the Organization's regulatory requirements, business needs, and industry best practices. Additionally, the Organization's client contracts may include legal obligations related to Data provided by the Organization on a client's behalf to a third-party. For example, a law firm may provide the Data of one of its clients for which it is completing a security investigation to a third-party forensic firm. The contract between the law firm and its client might specify data retention and destruction for such Data. As a best practice, information governance controls should be standardized across all client contracts to allow contractual provisions to defer to the Organization's policies, which comply (or should comply) with applicable laws and regulations. In turn, the Organization's policies should contain specific legal requirements such as retention periods. If a law or regulation changes, then only the policy needs to be updated, not all the client contracts. As a point of reference, some common information governance controls are listed in Table 2.

Table 2: Examples of Data-Related Information Governance Controls	
Third-Party's Internal Controls	
Control	**Description**
Third-Party's Policies	Establish a *written* framework of information governance expectations for the workforce and others by setting clear standards for desired behavior, ensuring compliance with laws and regulations, and providing guidance for decision-making
Third-Party's Procedures	Support the implementation of information governance policies through *written* step-by-step processes to help the workforce and others complete daily work actions in accordance with those policies
Third-Party's Training Content	Prepare the workforce and others to comply with relevant laws, regulations and internal information governance policies and instruct them how to adhere to the policies in their daily work
Third-Party's Awareness Campaign Content	Raise awareness and inform the workforce and others of appropriate behavior and of the various elements of the information governance program
Organization's Internal Controls	
Control	**Description**
Contract Requirements	Document and communicate an Organization's expectations for the third-party's performance, internal controls to manage risks, and compliance with applicable laws and regulations, including during termination of contract and post-termination, if applicable
Right to Audit Contract Clause	Permit an Organization to access and review information about a third-party's internal controls periodically, usually annually, to ensure these controls comply with legal and contractual requirements and provide a mechanism for the Organization to require the third-party to mitigate any identified deficiencies
Change Orders	Document bilateral agreements between an Organization and a third-party for any contract amendments that might pose additional risks or affect a third-party's internal controls
Contract Monitor	Designate an organizational employee, usually the business owner, to assess and continuously monitor the third-party's performance, internal controls to manage risks, and compliance with the contract
Periodic Monitoring/Audits	Exercise the Organization's right-to-audit by conducting assessments and monitoring of the third-party's performance, internal controls to manage risks and compliance with the contract
Statement of Destruction from the Third-Party	Confirm compliance with contractual terms for destruction of specified electronic or physical Data during the engagement, but more commonly at contract termination
Certificate of Destruction from the Third-Party's Data Destruction Vendors	Confirm compliance with contractual terms for destruction of specified electronic Data or physical media when carried out by a third-party's vendor (fourth-party to an Organization) in the normal course of business and typically requested during an audit
Workforce Empowerment	Educate the business owner and others who play a role in the third-party relationship on the critical terms and conditions of the contract and the risks and controls, while empowering them to ask questions

Assign Third Parties to Tiers

Organizations can ease some of the burden of risk management by categorizing third parties into tiers based on the relative risk they pose to the Organization.[55] Tiering is a ranking system that uses a grading matrix based on business criticality and other criteria. The Team uses tiers to focus on the full spectrum of risks posed by third parties within the Organization's ecosystem. Based on an evaluation, third parties are categorized into one of three risk tiers: low, medium, or high (see Figure 3).[56]

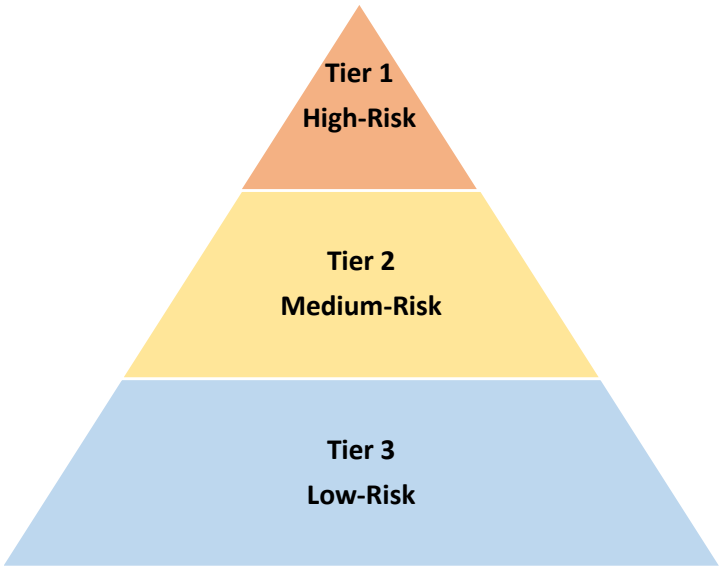

Figure 3: Third-Party Risk Tiers

The most important information governance criteria that determines tiering is whether a third-party stores and controls an Organization's or its clients' Data outside of the Organization's environment. The type, volume, and purpose of the Data will also be prominent when determining tiers. A third-party who accesses data solely within the Organization's environment might be classified as moderate risk, whereas a third-party who stores the Organization's Data in its data center might be classified as medium- to high-risk, depending on the type of data. An example of

[55] Adam Cummings, "Inherent Risk Tiering for Third-Party Risk Assessments." MindPoint, Group Blog, June 10, 2018, https://www.mindpointgroup.com/blog/breach/inherent-risk-tiering-for-third-party-vendor-assessments/

[56] Alternatively, organizations may choose a scoring model that uses a four-tier system: low, medium, high, and critical. Third parties categorized as critical pose the greatest risk and therefore, they receive the most frequent, rigorous and comprehensive diligence and oversight.

a high-risk tier is a third-party medical laboratory that receives patient Data on a weekly basis from a pharmaceutical company to perform diagnostic tests. The nature and volume of the Data make this third-party relationship very risky. Conversely, a third-party who provides career development training to the Organization's employees using its own proprietary materials with no access to the Organization's Data meets the criteria for a low-risk tier. This third-party does not store, or even interact with the Organization's Data making the risk low from an information governance perspective. Tiers help the Team determine the level and frequency of diligence and monitoring required for a particular third-party. Tiers also establish escalation paths such as the level of seniority required to accept third-party risks. Most importantly, tiering assists business owners and other stakeholders decide which third parties to contract with and how to structure engagements.

To illustrate why tiering is essential, one only needs to consider the 2013 data breach of Target,[57] a retailer based in the United States. Target granted an HVAC supplier access rights to its network to complete remote tasks like monitoring energy consumption and temperatures at various retail facilities. Unfortunately, hackers used the HVAC supplier's credentials to link to Target's network, exploit weaknesses in information systems, access the customer service database, install malware on the system, and steal sensitive customer data. If tiering was used, the third-party risk evaluation would have identified the HVAC supplier as a high-risk third-party based on access to Target's network. And, as a third-party in the high-risk tier, Target may have required more stringent controls for the engagement such as structuring HVAC system connectivity to limit risk.[58]

---

[57] During the cyberattack, the hackers stole 40 million credit card numbers. The HVAC vendor's services were unrelated to the credit card data and therefore, the realized risk arose from the relationship, not the services themselves. Target paid $18.5 million to settle claims by 47 states and the District of Columbia and $202 million dollars to investigate the breach. Stephanie Mlot, "HVAC Vendor Confirms Link to Target Data Breach," PC, February 7, 2014, https://www.pcmag.com/news/hvac-vendor-confirms-link-to-target-data-breach; Greg Zimmerman, "Target Settles HVAC Data Breach for $18.5 Million," FacilitiesNet, May 25, 2017, https://www.facilitiesnet.com/hvac/tip/Target-Settles-HVAC-Data-Breach-for-185-Million--39237; and "Target Settles 2013 Hacked Customer Data Breach For $18.5 Million," NBC News, May 24, 2017, https://www.nbcnews.com/business/ business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031

[58] Rhys Dipshan, 2017, "Three Things to Consider in Vendor Risk Management," *Legal Tech News,* https://www.law.com/legaltechnews/sites/legaltechnews/2017/12/07/3-things-to-consider-in-vendorrisk-management/?slreturn=20210102060213

Chapter 2: Diligence

After the first stage of third-party planning is complete, the second stage of diligence can begin. In the context of third-party risk management, diligence is the investigation or exercise of reasonable care that an Organization undertakes before contracting with a third-party for services or goods.[59] Chapter 2 focuses on implementation of the diligence process from this perspective.

Identify Third Parties to be Reviewed

An Organization's diligence methodology should be capable of managing large numbers of third parties with available resources and without disproportionate time and effort focused on low-risk third parties.[60] Performing diligence on which and how many third parties is a matter of debate. On the one side, there are some stakeholders who argue that "the onus is on companies" to ensure all third parties are reviewed for risk, while the naysayers feel that "managing every instance of risk is a bridge too far."[61] This paper takes the position that Organizations should conduct diligence on the complete universe of their third parties before entering into contractual agreements. First, some industry regulations, such as those enacted for U.S. healthcare, require Organizations to screen all third parties without exception against certain government exclusion lists.[62] Next, some third-party engagements may appear to pose minimal risks, while they may really be a "train wreck" waiting to happen. One only needs to consider the HVAC supplier that contributed to Target's massive data breach in 2013. Further, selecting which third parties to diligence based on

---

[59] "Third Party Anti-Corruption Due Diligence Guidelines," CreateCompliance, 2018, https://ethisphere.com/wp-content/uploads/Third-Party-Due-Diligence-7.2.18.pdf

[60] "Global Anti-Bribery Guidance: 13 Managing Third Parties," Transparency International UK, accessed August 27, 2020, https://www.antibriberyguidance.org/guidance/13-managing-third-parties/guidance

[61] Some of the in-house professionals who attended the session of ALM's CyberSecure conference titled "Enforcing Third Party Vendor Compliance" participated in a survey for a *LegalTech News* article. As part of the survey, Catherine Castaldo, global chief privacy officer at Nuance Communications reported being in favor of conducting diligence on all vendors, while Noga Rosenthal, chief privacy officer at Epsilon felt that total protection against third-party risk was not possible. Dipshan, "Three Things to Consider in Vendor Risk Management.

[62] 42 U.S.C. 1320a–7 states that any organization that contracts with a third-party that the organization knows or should know is excluded from participation in a Federal health care program for the provision of items or services for which payment may be made under such a program shall be subject to monetary penalties, and in some instances of malfeasance the organization itself may be excluded from participation in Medicare and state health care programs.

subjective criteria may backfire. The size of a third-party is a good example. A 2020 data breach trend was that small, less secure third parties provided the means of unauthorized access for bad actors.[63] Another "cut-off" criteria for diligence review might be engagement cost, even though dollar amount is not a good indicator of risk. For instance, one research study found a 71 percent increase over the last five years in data breaches from free open-source software.[64]

Another consideration in the debate on which third parties to diligence is the notion of defensible third-party risk management. A defensible process is a well-defined documented approach that is consistently applied and can be audited, making it suitable as evidence that all relevant conditions and requirements of the process were met.[65] Subjecting all third parties to the same intake process not only supports a defensible process, but also increases the likelihood of successful risk assessments. The phrase "a chain is no stronger than its weakest link"[66] seems particularly relevant to this argument. When an Organization casts its net as wide as possible, third parties are more likely to be scrutinized appropriately to ensure they can perform their contractual obligations in compliance with applicable laws and regulations and in a safe, secure manner. Regardless of an Organization's position on which third parties to review, the degree of diligence should be commensurate with the level of risk and complexity of the engagement.

Extensive diligence, for example on-site visits to fully understand the third-party's operations, may be necessary when a third-party engagement involves critical activities such as ingesting and storing an Organization's Data.[67] If additional scrutiny is warranted, the Organization should broaden the scope of its diligence as needed. On the flip side, value-driven Organizations or those

---

[63] Phoebe Fasulo, "5 Data Breach Statistics and Trends to Look Out for in 2020," Security Scorecard, December 9, 2019, https://securityscorecard.com/blog/5-data-breach-statistics-and-trends-to-look-out-for-in-2020

[64] Charlie Osborne, "Open-source software breaches surge in the past 12 months." ZDNet, March 4, 2019, https://www.zdnet.com/article/open-source-software-breaches-surge-in-the-past-12-months/

[65] "Defensible Process," Queensland Government, February 27, 2019, https://www.forgov.qld.gov.au/glossary/defensible-process

[66] This idiom may have originated from the ancient Basque proverb, "a thread usually breaks from where it is thinnest." A variation of this phrase appeared in Thomas Reid's "Essays on the Intellectual Powers of Man" that was published in 1786. The full saying "a chain is no stronger than its weakest link" was first printed in Cornhill Magazine in 1868. Elyse Bruce, "A Chain is Only as Strong as its Weakest Link," Ideomation, April 23, 2010, https://idiomation.wordpress.com/2010/04/23/a-chain-is-only-as-strong-as-its-weakest-link/

[67] "OCC Bulletin 2013-029," Office of the Comptroller of the Currency (OCC).

subject to less regulatory oversight may determine diligence based on criteria such as country, region, or business line, and choose a monthly or quarterly cadence rather than reviewing third parties in real time.[68] In the end, how wide to cast the net of third-party diligence review is a decision that each Organization must make depending on its industry, goals, and risk appetite.

Collect Key Data

Once an Organization decides which third parties are "in scope" for review, the main process of diligence begins. The three key elements to conduct a comprehensive third-party diligence review are data collection, verification and validation of data, and evaluation of results (covered in the next section). One approach to data collection is a two-step process: *internal* data collection from the business unit that wants to retain the third party and *external* data collection from the medium- to high-risk vendors themselves. For high-risk third parties, the Organization should conduct a comprehensive analysis of all publicly available information and a detailed in-country investigation of the third-party's operations,[69] as well as other pertinent information such as business structure, ownership, financials, sanctions/watch list review, references, and subcontractors, to name a few. In some cases, assistance of an external diligence provider may be needed to obtain information about the third-party's owners, operators, and key principals; conduct live, local-language research and litigation checks; and obtain reputational intelligence through local investigators.[70] Before an exchange of information can begin, most Organizations and third parties sign nondisclosure agreements to protect the non-public information that they will share before and after the engagement. The objective of data collection is to gather key information needed to conduct a risk assessment.

---

[68] Vera Powell and Alice Hsieh, 2020, "Effective Monitoring of Compliance Programs: A Guide for Practitioners," *Corporate Counsel*, January 13, https://www.law.com/corpcounsel/2020/ 01/13/effective-monitoring-of-compliance-programs-a-guide-for-practitioners/

[69] Das, "Conducting KYC of Third Parties."

[70] Ibid.

As part of the first step, the Team performs an initial *internal* screening to separate low-risk from medium- and high-risk third parties.[71] One way to accomplish this is by administering a short, standardized questionnaire to the *internal* business owners who want to engage the third-party at the start of third-party selection and before contracting. Since third-party diligence is a cross-functional process, the questions will deal with a variety of issues including compliance, privacy, information governance, security, etc. The questionnaire must ask for a complete and understandable description of the services or goods, as well as key risk-related questions from each function. For example, the compliance function might ask if a third-party has a Code of Conduct,[72] while security might need to know about third-party access to the Organization's systems. It is imperative that business owners answer the questions completely and accurately.[73] After all, the Team can only be effective if they understand the engagement (description of the services and goods) and how it will be implemented (key questions). The *internal* questionnaire should be limited to the minimum number of questions necessary to assess the engagement and to categorize the third parties into tiers based on the risk they pose to the Organization.

The business owner's description of the third-party's services or goods is needed by all the subject matter experts on the Team to conduct their analyses. The description, as well as responses to other questions, is used by the Team to assess each third-party from their function's perspective in the context of the engagement. Many of the questionnaire responses will be useful to the IG Officer, but a key response is whether the third-party will maintain any organizational or client Data outside the Organization's environment. If a third-party will store such Data, then it will likely be classified by the IG Officer as a medium- to high-risk, depending on the type and volume of Data. Based on pre-determined criteria for each governance function (compliance, privacy, information governance, etc.), such as a "yes" response for IG's question about Data outside the environment,

---

[71] "Third Party Anti-Corruption Due Diligence Guidelines," CreateCompliance.

[72] "Fraud, Third-Party Risks Still Top Concerns for Chief Compliance Officers," *Corporate Counsel (Online),* January 31, 2020, https://www.law.com/corpcounsel/2020/01/31/fraud-third-party-risks-still-top-concerns-for-chief-compliance-officers/

[73] The Principle of Integrity states that an information governance program shall be constructed so the information assets generated by or managed for the organization have a reasonable guarantee of authenticity and reliability. "The Principles," ARMA International.

the Team will collectively categorize each third-party into a tier. Third parties in the low-risk tier continue to the next step in the procurement process without a further diligence review, while medium- and high-risk third parties are subjected to a more rigorous diligence review (step 2).

Step two is to gather *external* information from the third parties designated for more rigorous review. The main purpose for gathering external information is to understand the third-party's enterprise-wide controls. To accomplish this, the business owner in cooperation with the Team provides a customized questionnaire or other information gathering tool such as a SIG (Standardized Information Gathering) questionnaire to the third party to complete. The SIG, developed and maintained by Shared Assessments, is a comprehensive set of questions covering eighteen risk domains that is designed to assess a third-party's compliance with regulations and adherence to industry standards and best practices. The SIG is used by over 15,0000 companies worldwide to drive third-party risk assurance and is updated annually.[74] Although the SIG contains data-related questions, the questionnaire is primarily targeted to security subject matter experts, who may address third-party risks differently than IG Officers. For this reason, the information governance function should add pertinent information governance questions whenever possible, either through a customized diligence questionnaire or by adapting the Data-related questions in the SIG.[75]

The information governance questions should be focused on the risks identified in the planning stage such as retention, destruction, etc. (see Table 1), as well as the third-party's enterprise-wide controls (see Table 2). Contingent on responses to the main information governance questions, documentation or sub-questions should be requested to support answers. For example, if the response to the question, "Does your company have an email retention policy?" is "yes", then a

---

[74] "SIG Questionnaire Tools," Shared Assessments, accessed October 15, 2020, https://sharedassessments.org/sig/

[75] The Standard Information Governance (SIG) questionnaire may not be customizable for information governance questions for several reasons. First, the questions map back to standards such as ISO 27002:2013, PCI, NIST SP 800-53 Rev 4, Health Insurance Portability and Accountability Act (HIPAA), Global Data Protection Regulation (GDPR), etc. Therefore, revising any questions may affect the validity of the SIG in relation to those standards. Secondly, third parties often complete the SIG annually with interim updates as needed to improve efficiency. Specifically, they complete the SIG once, but they provide it multiple times to many organizations who require diligence reviews. Finally, companies that provide vendor risk management tools to organizations to help streamline their third-party risk reviews provide functionality for vendors to auto-populate SIGs into the organization's instance of the tool. SIG customization may not be supported to enable such an auto-populate feature.

copy of the email retention policy should be requested from the third-party and submitted to the Organization with the completed diligence questionnaire. If the response is "no", a follow up sub-question may be "How long is email retained?" Either way, the IG Officer needs the information to conduct a risk assessment. Reviewing and verifying the third-party's policies, procedures, training transcripts, etc. provides evidence of controls, albeit that some controls are more effective than others. The Team may find that some third parties are not willing to provide copies of internal business documents. In those instances, the Team should request the documents be shared on-site or in a virtual meeting through a secure screen-sharing session.

Third parties will vary in their level of cooperation when responding to requests for diligence information. Some third parties may be more inclined to provide requested information because they want the business. Yet other third parties may leverage their unique services or goods, or the fact they are the only provider, for a "take it or leave it" approach. Another issue is an uneven power balance such that the third-party has significantly more power than the Organization.[76] For example, Google Cloud services, used by many companies to extend storage capacity, does not respond to diligence questionnaires. Instead, Google posts a one-size-fits-all SIG on their website.[77] Even though Google's questionnaire answers 956 questions scoped to CSA CCM[78] and ISO 27002[79] controls, the responses may not include the information needed by the Team's subject matter experts to conduct their review. Cultural differences may also create obstacles.[80] For

---

[76] Anju Mehta and Nikhil Mehta, 2017, "Moving Toward an Integrated Framework of Offshore Information Technology Outsourcing Success," *Journal of Global Information Technology Management* 20(3) 171-94.

[77] For more information about Google's SIG or to view its questionnaire responses, see "Standardized Information Gathering Questionnaire," Google, accessed October 22, 2020, https:// cloud.google.com/security/compliance/sig

[78] The Cloud Security Alliance (CSA) is a global organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA created the Cloud Control Matrix (CCM) to respond to and simplify the process of responding to risk assessments for the overall security risk of a cloud provider. CCM provides a controls framework that provides information about security concepts and principles as outlined in the "Clouds Matrix V4," 2021, Cloud Security Alliance, https://cloudsecurityalliance.org/ artifacts/cloud-controls-matrix-v4/

[79] ISO 27002 provides best practices for information security controls used by those responsible for initiating, implementing or maintaining information security management systems. "ISO/IEC 27002:2013 — Information Technology, Security Techniques, Code of Practice for Information Security Controls," International Standards Organization (ISO), accessed October 17, 2020, https://www.iso.org/standard/54533.html

[80] Adam Alami, Bernard Wong and Tom McBride, 2000, "Outsourcing Shows the Limited Impact for Strategic HR," *Employee Benefit News*, 14(10) 70.

example, a third-party may object to responding to diligence questionnaires because of the belief that only laws in the third-party's home country apply to the third-party and the corresponding engagement. Ultimately, the business owner who wants to engage the third-party is responsible for ensuring the external questionnaire and the corresponding supporting documentation is provided by the third-party to the Team. Each Organization must determine the degree of diligence information required to move forward with a third-party engagement and when less than the required amount of information will be accepted, or an exception granted.

Conduct the Risk Assessment

After data collection is complete, the Team reviews, verifies, and validates the information that was provided by the third-party. The evidence that must be reviewed by the Team depends on what types of documents were required to be submitted as support for responses in the *external* questionnaire. These items are typically information governance policies, procedures, and transcripts of training content. For instance, the Organization's compliance officer may review the third-party's compliance policies to ensure the vendor has an effective compliance program in place, if required.[81] Likewise, the IG Officer reviews the third-party's retention schedule policy to confirm that business records demonstrating compliance with the contract will be retained as specified by regulation, when required.[82] Similarly the third-party's business records should be retained for the duration of the statute of limitation period for breach of contract in the event of a

[81] U.S. Federal Sentencing Guidelines, 18 U.S.C.A. §8B2.1 requires many organizations to have an effective compliance program consisting of seven elements that include: 1) implementing written policies and procedures; 2) designating a compliance officer; 3) conducting training and education; 4) developing effective lines of communication through a hotline or established reporting processes; 5) conducting internal monitoring and auditing; 6) publicizing and enforcing disciplinary guidelines; and 7) promptly responding to detected problems and undertaking corrective actions. The U.S. Department of Justice (DOJ) updated its guidance in June 2020 to include additional requirements such as those related to third-party management. See "Evaluation of Corporate Compliance Programs," U.S. Department of Justice Criminal Division. The effective compliance program standard is required in various countries, although the issued guidance varies. However, there are key themes common among many of them such as the U.S. Sentencing Guidelines, the official guidance relating to the UK Bribery Act, or the Good Practice program guidelines endorsed by the Organization for Economic Co-operation and Development. "Five Essential Elements of Corporate Compliance: A Global Template," Baker & McKenzie, 2015, https://www.bakermckenzie.com/~/media/Files/BDSUploads/Documents/global%20corporate%20compliance/bk_global_5elements_20150721.pdf

[82] For example, see 42 CFR § 422.504. Medicare Advantage (MA) Contract provisions require MA organizations to retain certain compliance, financial and performance records for a specified period time, and to "flow down" these requirements to any of the organization's First-tier, downstream and related entities (FDRs).

dispute or litigation. The IG Officer reviews the key data to identify where the third-party lacks controls to mitigate risks, and then specifies the controls required to compensate for those shortcomings.

The third-parties questionnaire responses and supporting documents collected in Step 1 should be tested against a "red flag" checklist developed by the IG Officer (see Table 3). Red flags indicate situations where the third-party has insufficient controls to comply with regulations, meet the Organization's expectations, or conform with industry best practices. The information received from the third-party may be incomplete, vague, or not comprehensive. To resolve this deficiency, the IG Officer, alone or as part of the Team, should meet with the third-party to get clarification for any red flags that indicate increased risk such as a "permanent" retention period for organizational Data. In some cases, the IG Officer may request additional documents from the third-party, for example a data diagram that illustrates types of organizational Data retained, storage location(s) (e.g., SFTP server, in-house server, third-party cloud, offshore, etc.) and associated retention period(s). Additionally, if responses in the internal questionnaire completed by the business owner differ from those in the external questionnaire, a meeting with the business owner and/or third-party may be needed to explain these red flag discrepancies. For each risk assessment, the IG Officer is responsible for not only collecting enough information from the third-party though a standardized means such as a diligence questionnaire, but also following-up with additional information requests as needed to adequately identify and address any risks.

Table 3: Examples of Information Governance-Related Red Flags

Description	What to Watch For
No information governance program	Information governance is an afterthought with no data management oversight
No information governance function or officer or data management personnel to ensure compliance	Information governance is a side job; "We have a security officer that deals with that"
No policies or procedures	"Sorry, we don't share that information"; "I'll send it after our legal review"

Table 3: Examples of Information Governance-Related Red Flags	
Description	**What to Watch For**
Policies with vague, incomplete, or missing controls	Policy language does not include the level of detail needed for the workforce to understand its responsibilities and to implement controls
Procedures with vague, incomplete, or missing steps	Procedures do not contain the level of detail needed for the workforce to follow the process
Training transcripts that do not include key topics	No formal training and awareness program; "Our security training covers that"
Retention periods that are too long or too short	"We retain data indefinitely"; "We do not have any retention requirements"; "Those retention requirements do not apply to us"; "Retention periods apply to business records, not client data" or vice versa
Missing or vague records series or retention periods	Client/customer Data not included in retention policy; business records not included in retention policy; no specific retention stated (e.g., years, months, etc.); no trigger event to start the retention period countdown (e.g., x years from end of contract; x months from the date of creation, etc.)
No email retention period	"We retain email forever"; mailboxes of terminated employees are not destroyed in a timely manner
Disaster backup data retained too long	"We retain backups forever" or "We retain backup data for long-term retention requirements"
Methods of data destruction are vague, incomplete, missing, or do not meet industry standards	"We use a data destruction vendor" but there is no mention of how electronic data is destroyed; Focus on "media" rather than "data"
No system of data classification	"We do not retain any personal data, so data classification does not apply"; "We classify all data the same"
Missing, incomplete, or vague legal hold process	"Legal holds apply to business records, not customer Data or vice versa"; "Legal holds are the responsibility of our Legal Department"
No supporting documents provided	"We do not share proprietary information outside of the company" or only table of contents are provided
Third-party wants to work with vague, incomplete, or missing controls	"Let's gets started and take care of the paperwork later"

Organizations cannot scrape by with assessments that are narrowly focused on third-party data collection with no meaningful scrutiny or application of controls. A suitable methodology, molded by the Organization's risk appetite and matched against diligence norms, should be used by the IG Officer to specify controls that are proportionate to the risks and which may need to be coordinated among Team members. For instance, in some cases data destruction may be both a privacy and an information governance red flag, although the reasons for concern may be different. The privacy

officer may need to address data destruction from the standpoint of minimum necessary data for a business purpose, while the IG Officer may focus on preventing the over-retention of data. Although the control is the same, in this case data destruction, the reasons for implementing the control from each perspective may be different. The Privacy Officer may require a privacy-related agreement such as a Business Associate Subcontractor Agreement (BASA),[83] while the information governance officer may require a specific retention period in the third-party's retention schedule policy. The point here is that risks may not be exclusive to a particular Team member and therefore, coordination is needed to ensure controls are harmonized.

Regardless of whether the control requirements are provided independently or in tandem with other Team members, the IG Officer must make qualitative judgements using a methodology that is *not* a "check-the-box" activity. The IG Officer should challenge and question the nuances of the engagement and remain alert to new risks, including any risks not previously identified. When new or unusual risks are identified, innovative controls may need to be implemented. There are no "one size fits all" controls in third-party risk management. When assessing a particular engagement, the IG Officer should map the risks (Table 1) to the controls (Table 2) to ensure all red flags (Table 3) are addressed. Typically, information governance controls are addressed by contract, but certain controls may be required for the business owner who wants to engage the third-party. For example, if a statement of destruction at contract termination is a required control, the business owner, as the person who knows when the engagement will end, sends a written request to the third-party to destroy the relevant Data and ensures receipt of a confirmation statement. Red flags do not necessarily mean the Organization cannot move forward with a third-party engagement. However, all red flags must be addressed and resolved through mitigating controls, preferably before contract execution and before the engagement begins.[84] Sometimes there may be an agreement that states

[83] A Business Associate Agreement (BAA) or a Business Associate Subcontractor Agreement (BASA) is a written arrangement required by Health Information Portability and Accountability Act (HIPAA) that requires covered entities (e.g., hospitals, doctors, pharmacies, health plans, health exchanges,) and their business associates to safely handle Protected Health Information (PHI). Once Covered Entities, Business Associates, and Business Associate Subcontractors have identified their relationship with one another, it is necessary to ensure that any third parties safeguard the PHI they receive. "Business Associate Contracts," U.S. Department of Health and Human Services, accessed September 17, 2020, https://www.hhs.gov/hipaa/for-professionals/covered-entities/samplebusinessassociate-agreement-provisions/index.html

[84] Das, "Conducting KYC of Third Parties."

the third-party will implement the needed controls after contract execution by a specified due date, with the Organization using a follow-up mechanism to ensure compliance. For those cases where high residual risks remain, the decision whether to engage a third-party may be referred to legal or compliance or to a special committee for resolution.

Findings are provided to the internal stakeholders in the form of a formal report that minimally includes a description of the third-party and the related engagement, methodology of evaluation, list of key data collected, risk tier assignment, risks identified, and required controls. The Team provides the risk assessment findings to the business owner, as well as the other stakeholders who have actions, such as the Legal Department for contracting, or to those who simply have an interest such as the business owner's manager. The entire diligence process should be transparent to provide all parties the opportunity "to do the right things."[85] Diligence findings reveal information the stakeholders need to protect the Organization and tighten third-party controls when needed.

Document and Retain Evidence

"If it isn't documented, then it didn't happen" sums up why documenting the third-party risk management process is necessary. Regulators, auditors, or other stakeholders require proof not only that a third-party risk management process exists, but also that it is followed. Proper documentation also facilitates operation of the required diligence and monitoring activities, helps the Team collaborate among themselves, and communicates requirements to various stakeholders including business owners and third parties. It helps to build a defensible record, and provides the foundation for future decisions, auditing and monitoring, and analysis for future improvements.[86] Some examples of documents include internal and external questionnaires; supporting documents submitted by the third-party such as policies, procedures, and training transcripts; outside documents provided by advisors or investigators; notes detailing any relevant information or

[85] Principle of Transparency states that an organization's business processes and activities, including its information governance program, shall be documented in an open and verifiable manner, and that documentation shall be available to all personnel and appropriate, interested parties. "The Principles," ARMA International.

[86] "Third-Party Screening and Monitoring are Critical for Health Care and Life Science Companies," Ropes and Gray, August 29, 2019, https://www.ropesgray.com/en/newsroom/alerts/2019/08/Third-Party-Screening-and-Monitoring-Are-Critical-for-Health-Care-and-Life-Science-Companies

observations; attestations; exclusion screenings;[87] meeting minutes; Team diligence reports of findings; and valid contracts with explanations of any redlines if needed. In addition, records that document dispute resolution, risk acceptance, or decisions not to proceed with the third-party must be retained. If the Team deviated from normal diligence practices while conducting its risk assessment, an explanation of why the deviation was necessary should be documented and approved by an appropriate Team leader.

The Framework described in this paper functions for either a manual process or a technology assisted process that utilizes software tools. The Organization's approach will depend on the resources available, both financial and human, as well as the maturity of the third-party risk management program. A manual process typically involves freestanding files such as spreadsheets for documentation, email for collaboration and communication, and a centralized Team library for document storage. On the other hand, many VRM tools run an end-to-end process that includes all or most stages of the vendor risk management lifecycle.[88] These tools also may add value with functionality such as automating rote, repetitive information gathering tasks; mapping to specific regulatory frameworks; creating dashboards that automatically tier third parties based on key information; providing real time metrics about the Organization's risk posture; integrating with an Organization's other systems; facilitating collaboration and communication through in-platform chats and automated notifications; and generating automated data driven reports for decision-making. Regardless of approach, all third-party diligence and monitoring evidence should be

[87] 42 CFR § 455.436 - Federal database checks. Exclusion screening is the process of verifying that a current or potential entity is not classified as an excluded entity who is prohibited from participation in Medicare, Medicaid, and all other Federal healthcare programs. The Office of the Inspector General (OIG) requires organizations to screen entities prior to contracting and with monthly thereafter, against certain lists including OIG's List of Excluded Individuals and Entities (LEIE); General Service Administration's (GSA) Excluded Parties List Service (EPLS); and the U.S. Treasury's Office of Foreign Assets Control's (OFAC) List of Specially Designated Nationals and Blocked Persons. "Medicaid Program Integrity," Centers for Medicare and Medicaid Services (CMS), accessed October 4, 2020, https://www.cms.gov/Medicare-Medicaid-Coordination/FraudPrevention/FraudAbuseforProfs/Downloads/fftoolkit-federal-database-checks.pdf

[88] Mikkelsen, "Improving Third-Party Risk Management."

retained in a central location available to authorized stakeholders for the time specified in the Organization's retention schedule and be accessible for reference when needed.[89]

[89] Principle of Availability states that an organization shall maintain its information assets in a manner that ensures their timely, efficient, and accurate retrieval. "The Principles," ARMA International.

Chapter 3: Contracting

After diligence is complete, the contracting stage of the risk management lifecycle can begin. The use of contracts to manage risks posed by third parties is not just a best practice, it may also be a legal requirement.[90] Chapter 3 addresses contracting as a key component of third-party risk management.

Understand the Power of Contracting

A third-party contract should clearly specify rights and responsibilities and include provisions that protect both the Organization and the third-party. A well-written contract clarifies engagement expectations, supports enforceability, limits risks, and helps mitigate performance and compliance disputes.[91] It serves as the mechanism that ensures the needs and requirements of all stakeholders are considered, addressed, and documented. For a third-party contract to be an effective control mechanism, contract terms and timing must minimize risk. For instance, the Office of the Comptroller of the Currency identified cases in which bank management failed to properly implement third-party contracts, specifically:

- Contracts were executed without completing third-party risk assessments;
- Contracts incentivized third parties to take risks that were detrimental to the bank or its customers to maximize the third party's revenues; and
- Banks engaged in informal third-party relationships or started engagements without a contract in place.[92]

---

[90] Peter Arant and Steve Kreitner, 2016, "Feature Story: Understand the Risks and Benefits When Using Third Party Vendors for IT Needs," *Montana Lawyer* 42(14):1-4. For example, 45 CFR §165.504(e) of the Health Insurance Portability and Accountability ACT of 1996 (HIPAA) requires covered entities to execute business associate agreements with outside parties who create, store, maintain or transmit protected health information (PHI) on their behalf. Example of other laws requiring similar agreements include 16 CFR §314.4(d)(2) of the Safeguards Rule under the Gramm Leach Bliley Act and 201 CMR § 17.03(f)(2) of the Massachusetts Standards for the Personal Protection of Personal Information of Residents of the Commonwealth.

[91] "OCC Bulletin 2013-029," Office of the Comptroller of the Currency (OCC).

[92] Ibid.

Contracts not only minimize risk when they are executed appropriately, they are binding and legally enforceable. They also outline a shared understanding of business relationship and engagement expectations, so misunderstandings cannot be claimed later, although anticipating all situations that may occur in the future is not always possible.[93]

Each Organization determines what function leads its third-party contract negotiations, who participates in contract review, and who signs-off on contract terms. As the person most vested in engaging the third-party, the business owner serves as the central stakeholder in the contracting process. Contracting tends to be the responsibility of the legal department or a shared responsibility between the legal department and the business owner. The IG Officer may be called upon to assist during contract creation or negotiation to the extent that IG controls specified in the risk assessment findings need clarification or revision in the draft contract.

Provide Contract Input

The contract template used for the engagement determines the level of effort needed to customize the contract to the engagement. Third parties may request, or even require, use of their standard contracts; however, these contracts may not specify the controls required by an Organization. In fact, some of the provisions may conflict with the Organization's expectations. Contracting is complex and sometimes the underlying structure of a third-party's standardized contract may be such that the number and extent of "redlines" are overly burdensome to the Organization. Contract revisions are to be expected as negotiations progress, but Organizations are in a better position using their "own paper" whenever possible. The Organization's "own paper" is a template contract containing pre-approved and pre-populated standardized provisions, including third-party controls commonly required by the Organization. When used as the base contract, Organization templates add another layer of diligence to contracting, in addition to saving time and effort. The Team's subject matter experts, including the IG Officer, provide guidance to Legal for the development of standardized contract provisions related to their area of expertise. Even if an Organization uses its

[93] Kenney, "Third-Party Risk: How to Trust Your Partners."

"own paper," template provisions will likely need to be revised, depending on the details of an engagement. For example, the retention period for personnel records that must be retained in a software-as-a-service solution will be quite different from how long a client's paper medical chart must be retained after being digitized by a third-party scanning vendor. Another unique contracting challenge is presented by "click-through-agreements" for paid or "free" services, which must not be permitted to bypass the Organization's third-party risk management review process.

To be effective, the IG Officer should possess at least a high-level understanding of how diligence analysis correlates to third-party contracting. With respect to information governance diligence, analyzing the third-party *relationships*, although useful, is not the determinant unit of analysis. Instead, the IG Officer must evaluate each *engagement's* risks to specify data-related controls. To explain this further, the differences between the third-party relationship and the associated engagement should be examined from a contracting perspective. A legal agreement covers (or should cover) a third-party relationship (Master Services Agreement or "MSA"). That one MSA may govern one or multiple engagements, which are represented by Statements of Work (SOWs).

From a control perspective, this contracting structure matters. Specifically, the initial engagement may not be high-risk from an information governance perspective in the sense that the third-party will not store organizational or client Data. However, later engagements, represented by additional SOWs under the same MSA, may involve Data. For example, a third-party may be engaged to provide software development within the Organization's environment. From an information governance perspective, this arrangement by itself is not risky to the Organization, as the data will be stored on the Organization's servers. If later an additional SOW is added for implementation support that requires logs containing organizational Data to be provided to the third-party, then the risk related to the support component of the engagement increases substantially. Consequently, although the risk evaluation should examine the overall third-party relationship, the primary focus of the diligence review and subsequent contractual controls should be completed at the engagement level.

Contract provisions should be based on identified risks, contain controls for compliance with applicable laws, regulations, and other requirements, and include the right to request information

to demonstrate compliance with the contract.[94] Although there are many potential requirements that may need to be included in third-party contracts, this paper focuses on those provisions that most likely contain an information governance component (see Table 4).

Table 4: Examples of IG-Related Contract Provisions

Name	Description
Nature and Scope of the Data	Specifies and describes the type(s) of organizational and client Data to be retained and may include a list of data elements
Operating Procedures	Stipulates responsibilities for the retention of organizational and client Data, including retention periods, and destruction of such data when subject to a legal hold
Retention of Business Records	Requires the third-party to retain timely, accurate and comprehensive financial, performance, and business records to demonstrate compliance with the contract and applicable laws
Ongoing Monitoring	Ensures the Organization's right to audit, request third-party reviews and require remediation if issues are identified
Regulatory and Legal Compliance	Requires compliance with relevant laws and regulations applicable to the specific engagement
Disaster Recovery Backup	Stipulates coordinated (but not the same) retention periods for production and redundant copies of organizational or client Data
Default and Termination	Specifies Data transfer in-house or another third-party and data destruction at termination or expiration of the engagement or business relationship
Fourth (fifth, sixth, etc.) Parties	Ensures "flow-down" requirements from the third-party contract to the fourth-party contract, when such subcontracting is approved by the Organization

Some contractual "gotcha" items demand special attention. For example, business records to be retained by the third-party to protect the Organization may not be easy to identify. Certainly, the third-party's financial and performance records demonstrating compliance with the contract are important. They even may be required to be retained for a certain time in accordance with applicable regulations.[95] What about other less-obvious business records such as system or activity logs that may be needed in the aftermath of a security event? Another consideration for how long

[94] Judd, "Vendor Risk Management—Compliance Considerations."

[95] For example, 42 CFR §§ 422.503, 422.504 Medicare Advantage Contract Provisions.

to require a third-party to retain its business records is the statute of limitations for breach of contract in the jurisdiction governing the contract. In most cases, the longer of the regulatory or limitations retention period should prevail, keeping in mind that the regulatory retention period is required by law, whereas keeping records for the limitations period is prudent, but not required. The statute of limitations ensures that in the event of a dispute, investigation, or litigation, the appropriate records will be available. Every contract, regardless of risk level, should contain a provision related to the retention of business records.

By far, the most critical data that the IG Officer must protect is organizational or client Data retained by the third-party. A common "rookie mistake" is to lump the third-party's business records in with any organizational or client Data. For example, customer Data provided to a third-party to develop artificial intelligence (AI) capability is not the third-party's business records. Instead, the customer Data was provided to the third-party by the Organization for the purpose of creating AI rules. When that work is complete, the customer Data is no longer needed by the third-party for a business purpose and should be destroyed in a timeframe specified by the Organization in the contract. The retention period for organizational or client Data should be as short as possible to reasonably allow the third-party to complete its work including any quality control, but not long enough to increase risk in the case of a privacy, security, or other adverse event. Another "gotcha" item is that retention periods should be coordinated with the timeframe for the right to audit, so that the third-party's records needed for an audit are available. For example, Medicare Contract provisions require that "'HHS', the Comptroller General's, or their designee's right to inspect, evaluate, and audit any pertinent information for any particular contract period will exist through 10 years from the final date of the contract period or from the date of completion of any audit, whichever is later."[96] In order for the government to audit such records, they must be retained for the specified time.

Where organizational or client Data is retained by the third-party, the contract should have a data destruction provision for both the normal course *and* at contract termination. If a third-party receives organizational or client Data on an on-going basis, then that Data should be destroyed on

[96] 42 CFR § 422.504(i)

a rolling basis or other appropriate interval as specified by a retention period in the contract. Alternatively, the Organization may also accept a retention period specified in the third-party's retention schedule policy. Depending on risk posed by the retention of the Data, both the Organization's control (the contract) and the third-party's control (the retention schedule policy) may be prudent. From a risk perspective, exposing 50,000 records during a data breach is much riskier than exposing 5,000 records. At contract termination, data may need to be returned so the Organization can satisfy its regulatory recordkeeping requirements. For example, if the Organization uses a software-as-a-service accounting solution, the finance Data within the third-party solution will need to be transferred back to the Organization or to another third-party.

The contract should require the third-party to provide to the Organization a statement of destruction signed and dated by an authorized officer to ensure compliance. Another "gotcha" item at contract termination is the retention period for disaster recovery backup data, which should not be confused with long-term archival retention. Some third parties, particularly those that have few or no internal information governance controls, may retain disaster recovery backup data for a "permanent" or unspecified retention period. To avoid indefinite retention of organizational or client Data after the contract ends, the retention periods for disaster recovery backup copies should be specified in the contract, usually a short period of time such as 60 to 90 days after contract termination.

If the IG Officer is integrating into an existing third-party risk management program, a retroactive review of third-party contracts may be needed. The key to reviewing existing agreements is to pinpoint high-risk third-party relationships in which organizational or client Data is stored by and in control of a third-party. The IG Officer should focus on specific information governance-related contract sections within the contracts, such as "records retention," "right to audit" and "termination," to complete each risk assessment analysis. Depending on the risks posed to the Organization, a contract amendment that includes the required controls may need to be implemented immediately or at contract renewal. Contract revisions also may be needed when there is a change in scope of the engagement or if regulations change. For example, Organizations

subject to General Data Protection Regulation (GDPR)[97] or California Consumer Privacy Act (CCPA)[98] requirements probably needed to amend contracts when the legislation was enacted. Contracts should be reviewed periodically, particularly those related to high-risk engagements, to ensure they continue to include the appropriate controls and legal protections. Where problems arise, the Organization should seek to renegotiate the contract at the earliest opportunity.

Clarify Contract Expectations with the Third-Party

Since regulators and auditors are increasingly focused on third-party risk management, it is prudent for the Organization to take a proactive stance in helping a third-party meet its obligations. For engagements with complicated contractual controls, all or part of the Team may need to meet with third-party stakeholders after contract execution to reaffirm expectations and clarify requirements. Certain industry regulations, although specified in the contract, may need to be explained to the third-party who may not have the ability to interpret applicable regulations correctly. Third parties, particularly smaller ones, or those in different host countries, may not have the depth, breadth, or quality of subject matter expertise available to the Organization. Accordingly, the Organization's subject matter experts who conducted the risk assessment and specified the controls may fill this knowledge gap by meeting with third parties to explain expectations that will increase compliance and reduce risk.

[97] Data Protection Act 2018 (EU) 2016/679 also referred to as the General Data Protection Regulation (GDPR) GDPR contains explicit requirements for documenting processing activities including data processing purpose and "time-limit for storing" this information (GDPR Art. 30); data processing (GDPR Art. 5), data protection (GDPR Art. 32); and right to erasure (GDPR Art. 17).

[98] California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375). This California law allows California consumers to see all data an organization has saved on them, as well as a full list of all the third parties that data is shared with. Additionally, CCPA permits consumers to sue organizations if the privacy guidelines are violated, even if there is no breach.

Chapter 4: Monitoring

Monitoring mirrors the diligence process described in Chapter 2 in many ways, but monitoring involves activities such as on-site audits, desk-audits, and attestations. Organizations might assign dedicated personnel to conduct monitoring, such as auditors in the third line of defense, or as assumed in this paper, other qualified personnel such as the Team. Chapter 4 focuses on enforcing the Organization's contractual rights through monitoring.

Understand Monitoring Activities

While pre-engagement diligence is critical, post-contract monitoring is equally important as a strategic component of a robust third-party risk management program.[99] Monitoring involves verification activities to assess, evaluate, and inspect a third-party's risks and controls to ensure compliance with requirements. Regulatory guidance emphasizes that Organizations must monitor their third parties beyond initial diligence screening. For example, the U.K. Bribery Act states the importance of "continued and regular monitoring,"[100] and the Foreign Corrupt Practices Act (FCPA) Guide notes that "companies should undertake some form of ongoing monitoring" and where appropriate, conduct "diligence periodically."[101] Although regulators expect Organizations to monitor third parties during the term of the engagement, they do not give guidance on what constitutes appropriate monitoring. Organizations must take the initiative to establish a risk-based approach to third-party monitoring, including deciding which third parties to monitor. One research study found that only 6% of financial services companies had "all" third parties in scope for review, down from 19% three years earlier, while 75% of companies reported fewer than 10% of their third parties were in their highest risk tier, up from 50% in 2016.[102] This sharp decline in

[99] "OCC Bulletin 2013-029," Office of the Comptroller of the Currency (OCC).

[100] "The Bribery Act 2010," UK Ministry of Justice, accessed December 23, 2020, https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf

[101] "FCPA Resource Guide," U.S. Department of Justice, November 14, 2012, p.60, accessed December 23, 2020, https://www.justice.gov/sites/ default/files/criminalfraud/legacy/2015/01/16/guide.pdf

[102] "Global Financial Services Third-Party Risk Management Survey," Ernst & Young.

scope suggests that financial companies are focusing their resources on higher risk third parties to reduce the time and costs needed to conduct monitoring.

Monitoring ranges from basic reviews such as having third parties periodically update diligence information to more comprehensive monitoring such as on-site audits. Regulators differentiate between initial diligence reviews and post-onboarding monitoring, suggesting that the role of monitoring is to update initial diligence efforts ensuring they do not "become stale."[103] Unlike diligence reviews which occur prior to onboarding, presumably for all third parties, post-contract monitoring is conducted periodically and usually for a subset of the total third-party population. Comprehensive monitoring for all or most third parties is not always appropriate or practical. In practice, monitoring should be proportionate to the risk posed by the third-party to the Organization, with more extensive monitoring for those third parties in higher risk tiers. Should any red flags be discovered during monitoring, Organizations have an obligation to take timely action to correct any deficiencies. Further, a defensible third-party risk management program necessitates that a defined monitoring process be applied consistently to all third parties, with the ability to adapt to any changes in the third-party relationship or engagement as needed.

Establish the Monitoring Schedule

Organizations cannot monitor their third parties unless they know who they are, their risk tier, and other related information. A surprising number of Organizations do not have a comprehensive third-party inventory, and if they do have one, it may be incomplete, spread across multiple systems or functions, or lack a single source of truth.[104] The average company shares sensitive data with approximately 583 third parties, but only 34% of companies have a comprehensive inventory of those third parties.[105] To build an inventory retroactively, Organizations can leverage existing information such as invoice or payment data, contract management databases, or enterprise

[103] "FCPA Resource Guide," U.S. Department of Justice, p.62.

[104] VigneshVeerasamy et al, 2018, "Can You Transform Your Third Parties Risk to Competitive Advantage?" Ernst & Young, https://assets.ey.com/content/dam/ey-sites/ey-com/en_ie/topics/ advisory/transforming-your-third-party-risk-into-a-competitive-advantage.pdf

[105] Ilia Sotnikov, "Simplifying Third-Party Risk Management," *Risk Management* July/August (2019): 8-9.

resource planning (ERP) systems. Organizations with more mature third-party risk management programs tend to maintain inventories with detailed information such as third-party contacts, engagement details, business owner, key dates, spend information, contracts, list of fourth parties, as well as a summary of key risks. Once established, inventories should be updated in real-time and reviewed annually for new, terminated, inactive, and any "rogue" third parties that were engaged outside of the third-party risk management process.

With an inventory list in hand, the Team should define monitoring categories based on risk tiers (as described in Chapter 1) with anticipated monitoring frequencies for each category. Ultimately, audit provisions of the governing contract establish the frequency and type of monitoring for each third party; however, the Team is responsible for exercising the "right to audit" at the stated intervals. Key dates such as effective, renewal, or termination dates may be used to trigger monitoring start times. Monitoring may also be prompted by events such as changes in relationship, applicable regulations, or business risk. Other triggering events may surface during the engagement including customer complaints, regulatory investigations, enforcement actions, or civil litigation brought against the third-party, even if unrelated to the engagement with the Organization.

As a best practice, all third parties should be monitored on a set schedule, typically annually for critical or high-risk third parties and approximately every two years for the remaining third parties. Periodic monitoring demonstrates an Organization's commitment to managing third-party risk and facilitates year-to-year comparisons that provide opportunities to flag potential lapses in the application of controls. Monitoring covers everything from the opening to the closing communications with the third-party. It consists of multiple activities including data collection; understanding risks and controls posed by the engagement; verifying that the controls work through activities such as onsite audits, desk audits, and attestations; producing findings with expectations for mitigating shortcomings; and communicating results.

Apply Point-in-Time Auditing

Critical and high-risk third parties typically are required to participate in on-site audits, the most rigorous form of monitoring.[106] The Team prepares for each on-site audit by analyzing existing documentation prior to the visit including the contract and other relevant agreements; initial diligence documents; monitoring reports from earlier audit cycles; third-party's policies and procedures from previous submissions; and any other information that might be useful, including publicly available information. Based on the pre-visit analysis and the Organization's procedures, the Team outlines a plan for the on-site audit specifying key information such as the monitoring period; processes that will be the target of the monitoring; dates and times of on-site visits; names and roles of Team members; and any pre-audit documentation required from the third-party.

In advance of the on-site visit, the Team may request supplementary information. For example, the IG Officer might ask a third-party for a written list of its data destruction vendors (fourth parties to the Organization) that were active during the audit period with dates when data destruction occurred. Based on the gathered information, the IG Officer develops questions and a list of potential observations to be used during the onsite audit to test compliance. For instance, while onsite the IG Officer might pick a vendor from the advance list of data destruction vendors and choose random dates to ask that those certificates of destruction be provided by the end of the day. This test case shows how the IG Officer can verify that data destruction controls were implemented as required in the contract to protect the Organization. Another on-site observation might be to have the third-party demonstrate a standard operating procedure in practice. For example, the third-party might show the step-by-step process of suspending destruction in the event of pending or potential litigation to avoid the destruction of data subject to a legal hold.

On-site audits are costly and time consuming to conduct. With affordable web conferencing technologies, bandwidths with good definition capable of live streaming, and virtual data room repositories with suitable security, the same level of data collection and verification as an on-site

[106] For a description of auditing, see "What is Auditing," adapted from *The ASQ Auditing Handbook*, ASQ Quality Press, American Society for Quality, accessed December 2, 2020, https://asq.org/quality-resources/auditing

visit can be accomplished from anywhere for a fraction of the time and cost. Remote audits are conducted in very much the same way they would be carried out in person. Even from afar, the Team must ensure a thorough understanding of the third-party's processes and controls to complete a comprehensive audit. However, there are some circumstances when it would be prudent for the Team to be physically on-site for an audit. Technical or policy restrictions may limit a reliable method of information sharing between the Organization and its third-party. The third-party may have no audit or reporting mechanisms in place which make it difficult for the Team to effectively conduct remote monitoring. Another concern occurs when a third-party has experienced a data breach or other serious performance issue and firsthand assurance of risk mitigation or operational processes is needed. When an Organization determines that onsite or remote audits are not required each year, they may intersperse them with other monitoring activities such as desk audits or attestations in the intermittent years.

Before starting a desk audit, which is appropriate for medium-risk third parties, the IG Officer identifies key risk areas and develops queries in a standardized format such as a post-contract monitoring questionnaire, alone or in coordination with the Team, to use as the main tool to assess how risks are being managed. Depending on their responses in the questionnaire, third parties are instructed to provide documentation such as policies, reports, certifications, risk assessments, and other artifacts to support their answers. Often the Team will ask the third-party for certifications such as a SOC report,[107] HITRUST assessment,[108] ISO 27001 certification,[109] the PCI DSS

[107] SOC (Service Organization Controls) is a security-focused report from an independent auditor that details information about an organizations controls relevant to security, availability, and processing integrity of the systems the organization uses to process data. There are two types of SOC reports: type 1 is a point in time audit, while a type 2 is more in depth and a period of time audit. For example, a SOC 2 Type 2 might be focused on an organization's practices over the past year. "SOC 2® - SOC for Service Organizations: Trust Services Criteria," AICPA, accessed October 2, 2020, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

[108] HITRUST (Health Information Trust Alliance) is a healthcare-related certification used to streamline the third-party risk management process by harmonizing multiple standards such as HIPAA, HITECH, state, and business associate requirements into a single assessment that may be reported out in multiple ways. HITRUST is a privately held company located in Frisco, Texas that collaborates with healthcare, technology and information security organizations to establish the HITRUST CSF certification. "CSF Assurance Program," 2021, HITRUST Alliance, accessed January 1, 2021, https://hitrustalliance.net/csf-assuranceprogram/?gclid=CjwKCAiAr6ABhAfEiwADO4sfSZc14xNkN1cpTJb6FHnW6A90VMetBHekrXicIjX3O_yREWHVxnEtBoC8egQAvD_BwE

[109] ISO 27001 (ISO ISO/IEC 27001:2013) is an international standard created jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001 is the international equivalent of SOC 2, and both standards aim to ensure certified organizations have mature security controls in place to adequately protect data. One key difference between these two standards, which is common between many

assessment,[110] or a Cloud Security Alliance controls matrix.[111] These security-focused reports are produced and certified by independent parties and can be cost-prohibitive, particularly for smaller third parties. They contain limited information governance-related information from a security perspective. Nonetheless, some of the report findings may be useful to the IG Officer, especially if any red flags related to organizational or client Data are identified.

During a desk audit, it is not enough just to ask the third-party if certain policies are in effect. The Team should verify that the policies provided by a third party contain the required controls. When it comes to audits, sound advice is to "Trust but verify. Ask for copies. And read them."[112] For example, the IG Officer might ask if a third-party has a legal hold policy and if it does, the IG Officer should read the policy to verify that retention schedule requirements are suspended for legal hold data until resolution of the legal matter. Careful review of the supporting documentation is needed to ensure the third-party's controls meet or exceed the Organization's own policies. If any controls are found to be deficient, corrective actions to remediate the deficiencies will be required. Sometimes third parties only provide table of contents of needed policies, procedures, or other documents. For the reasons previously stated, this limited information does not provide enough detail to conduct a thorough review. When third parties are reluctant to share written materials, a video conference with the Team will be needed for the third-party to screen share the supporting documentation.

European and American standards and regulations, is that ISO 27001 is principles-based while SOC 2 is prescriptive. "ISO/IEC 27002:2013, Information Technology, Security Techniques, Code of Practice for Information Security Controls, International Organization for Standardization (ISO), accessed October 17, 2020, https://www.iso.org/standard/54533.html

[110] A PCI (Payment Card Industry) assessment validates compliance with the Payment Card Industry Data Security Standard (PCI DSS), a set of security standards for merchants who accept, process, store or transmit credit card information. Satya Rane, "What are the 12 requirements of PCI DSS Compliance?" Controlcase.com, accessed January 15, 2021, https://www.controlcase.com/what-are-the-12-requirements-of-pci-dss-compliance/

[111] The Cloud Security Alliance (CSA) is a global organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA created the Cloud Control Matrix (CCM) to respond to and simplify the process of responding to risk assessments for the overall security risk of a cloud provider. CCM provides a controls framework that provides information about security concepts and principles. "About," Cloud Security Alliance, accessed October 15, 2020, https://cloudsecurityalliance.org/about/

[112] Royal, K., "Chapter Seven: Saturn," International Association of Privacy Professionals (IAPP), accessed December 2, 2020, https://iapp.org/news/a/monitoring-third-party-vendors-means-managing-your-own-risk-chapter-seven/

The Organization also may use compliance attestations to monitor lower risk third parties or for intermittent monitoring of higher risk third parties, although such attestations may be required by law.[113] By completing an attestation, an authorized third-party individual certifies on behalf of the vendor that it adheres to regulatory and contractual requirements. Third parties attest, usually on an annual basis, that they understand their legal obligations and will fulfil them. An attestation consists of a short template created by the Team, which is delivered as a stand-alone document or as an on-line form, that lists third-party requirements with brief descriptions and references to applicable regulations. The questions are formatted as "yes" or "no" responses, with free text explanations where a required control is reported as "no" or "not applicable." The IG Officer might include questions related to records retention requirements that "flow down" to the Organization's third parties to get written assurances that the third-party is implementing information governance controls as required. For example, regulations require healthcare Organizations to provide on-hire and annual privacy and security training to the workforce and to keep records of compliance for each employee.[114] Attestations are cost effective to implement and can be processed by administrative staff. However, all "no" responses and other red flags must be reviewed by qualified individuals such as the subject matter experts of the Team to determine what corrective actions are needed to remediate any deficiencies.

Corrective actions are *reactive* activities undertaken to eliminate or reduce the causes of an *existing* nonconformity, defect, or other undesirable situation to prevent *recurrence*, while preventive actions are *proactive* activities undertaken to eliminate the causes of a *potential* nonconformity, defect, or other undesirable situation to *prevent occurrence*. Since corrective actions may not be finished during the time of the audit, the Team may require follow-up monitoring to verify that corrective actions were completed satisfactorily. Due to effort and cost, follow-up monitoring may be combined with the third-party's next scheduled monitoring. Other times, Organizations may forward identified performance issues to the business owner for follow-up. Regardless, all

[113] For example, Medicare Prescription Drug Benefit Manual Ch. 9 §50.6.6.

[114] For example, 42 CFR §§ 422.503, 422.504 Medicare Advantage Contract Provisions.

decisions about follow-up activities should be appropriate and based on the risk level of the finding.

To communicate the results of monitoring activities, findings are issued in the form of a report to the third-party and business owner. The report provides accurate and clear information that helps the third-party address any identified risks and assists the business owner in making decisions. Responses from third parties run the gamut, from being defensive to graciously acknowledging the findings and accepting responsibility. There are three common types of third-party risk management findings:

1. Deficiencies in the third-party's internal controls related to business processes;
2. Non-compliance with regulations or contract requirements; or
3. Areas of concern not quite deserving of a finding, but in need of improvement.

The third-party can respond in three ways: agreement, disagreement, or no response. If the third-party agrees with the audit finding, it moves forward with a corrective action plan to remediate identified deficiencies. The Team conducts follow-up monitoring to ensure the third-party completed all corrective actions as agreed-upon. If the third-party disputes the finding, the Team must evaluate whether the disagreement is valid and substantiated. If the third-party's explanation is not accepted, the Team responds with further clarification on why the finding is valid. Finally, third parties may not respond, which should be viewed negatively by the business owner and put the relationship in jeopardy of termination. The monitoring process ends either when the monitoring report is issued with no actions required or after corrective or preventive actions specified in the report are implemented by the third-party.

Plan for the Next Cycle

Rigorous monitoring deters risky activities,[115] but the process is burdensome for many third parties, particularly those who are smaller and have limited resources. Organizations should

[115] "Global Anti-Bribery Guidance," Transparency International UK.

schedule monitoring in intervals proportionate to the risks. Organizations should be mindful of "audit fatigue," which may affect a third-party of any size. Audit fatigue occurs when third parties are audited year after year for the same audit criteria and maybe even by the same individuals.[116] With each passing year, the useful information that Organizations obtain from their third parties diminishes with the results sometimes being predictable and of limited value. Nevertheless, some industries require an Organization's third parties to be monitored regularly.

Planning for the next audit cycle should be part of the monitoring process. As a condition to renewing a third-party relationship, the Team assigns expiration dates for risk assessments and updates diligence periodically. They adjust the degree of scrutiny as the relationship or engagement changes and problematic activities are detected. Risk-based monitoring is scheduled in advance, including any reminders to exercise audit rights where appropriate. Most importantly, Organizations should use the findings from monitoring activities to strengthen third party controls, including reporting to senior management and the Board with an appropriate level of detail to facilitate oversight by these bodies.

[116] Dennis Ryan,"Yes, There is a Cure for Audit Paralysis," Compass Health and Safety Limited, accessed January 14, 2021, http://compasshealthandsafety.com/whats-new/compass-articles/yes-cure-audit-fatigue-audit paralysis/

Chapter 5: Renewal or Termination

Contract renewals and contract terminations are handled differently; the first restarts the third-party risk management lifecycle, while the latter ends the relationship. Third party offboarding might be assigned to a variety of stakeholders, but in this paper, we assume that the business owner and Team address end-of-lifecycle activities. As the final step in a well-functioning third-party risk management process, Chapter 5 focuses on third-party contract renewal and exit strategies.

Identify Contract Renewals or Terminations

As the main stakeholder, the business owner who engaged the third-party provides offboarding leadership for unbundling business processes, adherence to contractual obligations, and compliance with the Organization's procedures. A system to identify renewal and termination dates should be implemented to ensure required actions are executed in a timely manner. "The deeper the third-party is embedded in and uses the confidential information of the company and its customers, the greater the risks presented by failing to design a smooth transition process."[117] Longer and more complex relationships require greater effort to renew or separate. The Team should use available resources, such as the Organization's third-party inventory (as discussed in Chapter 4) or a contract management system, to generate alerts or reports that identify third-party contract renewal and termination dates. The reports should be created at regular intervals, minimally once per month, and be provided to relevant stakeholders such as the business owner, Legal, the Team, and others.

When a business owner opts to renew a contract, there is an opportunity for both the Organization and the vendor to reset the third-party relationship and the engagement terms. Renewals have two main reentry points back into the risk management lifecycle. First, the Organization may require the third-party process to begin again with a refresh of the initial diligence documentation and an updated review. This reentry point is appropriate when the product or services are substantially different from the initial engagement and increase risk to the Organization: additional contract

[117] Ibid.

terms may be needed to mitigate such risk. Secondly, if the engagement remains essentially the same, the reentry point might be to renew the existing contract without adding additional contract provisions and resume the third-party's previous monitoring activities and schedule. Regardless of reentry point, the business owner and Team should have the opportunity to evaluate third-party renewals that substantially differ from the initial engagement to ensure any additional risks are identified and mitigated.

"Contract termination is an inevitable phase in the third-party relationship lifecycle. As many risks as there are in the active phase of a third-party relationship," there are new risks that might "arise when the relationship is ending."[118] The Office of Comptroller of the Currency advises banks to develop a termination plan "to ensure that the bank can transition the activities to another third party, bring the activities in-house, or discontinue the activities when a contract expires" and to confirm that "the terms of the contract have been satisfied" in accordance with the bank's and third party's business strategy.[119] Third-party contracts that clearly specify contract termination rights are the first step for orderly offboarding. Ideally, the expectations and obligations of each party should be stated in the contract with enough detail to facilitate a smooth transition. Apart from the contract, the third-party risk management process should outline end-of-lifecycle procedures covering change management, contingencies, designation of transition team members, and provisions for adequate resources.

Confirm Contract Compliance at Termination

A "rookie mistake" for IG Officers at contract termination is not recognizing the difference between "return *or* destroy" and "return *and* destroy" Data, where the first is applicable to physical records, while the latter is *not* appropriate for electronic Data. After a third-party returns or destroys paper records, the third-party no longer physically possesses such records. Whereas it is possible for the third-party to return electronic Data to the Organization, but *not* destroy the source Data from its systems. Contracts should be written as "return *and* destroy data" to ensure data

[118] Carole Switzer, "Breaking Up is Hard to Do – Avoiding Pain by Planning for the End of a Third-Party Relationship," OCEG Blog, July 19, 2014, https://go.oceg.org/third-party-management

[119] "OCC Bulletin 2013-029," Office of the Comptroller of the Currency (OCC).

destruction requirements for electronic Data are clear. The IG Officer should flag for action any terminating third parties that have data destruction obligations at contract termination. At the appropriate time, but in advance of the contract termination date, the business owner or other designated internal stakeholder notifies the third-party of pending data destruction obligations to allow enough time for the return, transfer to another third-party, or destruction of data to be completed. If the terminated third-party possesses paper records, there must be a plan for their secure return. For example, original paper business records provided to a law firm for a case will need to be returned to the Organization. The law firm no longer has a business purpose for these records once the third-party relationship terminates. If the third-party has duplicates, not original paper records, the Organization might require them to be destroyed instead of being returned.

If the Data is electronic, it should be returned (only when requested) to the Organization or the new third-party replacement in an agreed-upon format specified in the contract. Data provided in proprietary formats is not useful to the Organization and in fact, it will be useless if it cannot be read. A common scenario is Data retained in a third-party's software-as-a-service (SaaS) solution that needs to be transferred to a new third-party replacement. The terminated third-party's cooperation may be needed to collect and deliver the Data successfully to a replacement third-party. For example, an Organization's human resource records retained in a third-party SaaS solution should be transferred back to the Organization or a new third-party replacement to ensure compliance with relevant regulations. In no case whatsoever should an Organization's records be left to "live out" the retention period in the possession of a third-party, since the Organization, not the third-party, is responsible for fulfilling its own records retention requirements.

When Data must be destroyed on contract termination, the business owner in collaboration with the IG Officer should confirm the third-party's compliance through a written attestation that specifies:

- *All* iterations of the Data regardless of format or location were destroyed including disaster recovery backup copies.
- Data was destroyed in a manner that rendered it unusable, unrecoverable, and unreadable for any purpose.

- Data was destroyed in "[x] days from the contract termination date," typically between 30 to 90 calendar-days with sensitive personal data being destroyed as soon as possible.
- Upon written notification by the Organization, the third-party must provide a written statement of destruction signed and dated by an authorized officer confirming destruction of the Data.

Another "gotcha" item is the statement of destruction itself. Rather than allowing the third-party to provide its own statement of destruction which may not be robust, the IG Officer should develop a standardized statement of destruction form for third parties to sign at termination. By creating an in-house form, the Organization can ensure all the nuances around data destruction are included such as description of the data, reference to the governing contract and termination date, and other relevant information as described in the bullet points above. The signed statements of destruction should be retained by the Organization with the third-party's contract as evidence of contractual compliance and for reference in the event of a potential dispute. Finally, it is important to note that successful third-party terminations are highly dependent on contract provisions as demonstrated in this chapter. Therefore, when providing input into the contract (as described in Chapter 4), the IG Officer should anticipate what actions and documentation will be needed at contract termination, and require robust contract controls to meet those needs and avoid a messy termination.

Final Thoughts

Current trends indicate that third-party relationships are not only here to stay, but they are projected to accelerate "with the speed of digital evolution."[120] In fact, finding a company today that does *not* do business with at least a few third parties is increasingly rare. As the need for third-party services and goods grow, so do the risks. However, these risks lie not only in the third-party relationships themselves, but also in the engagements where organizational or client Data is stored by a third-party outside of the Organization's environment. The Framework described in this paper provides a starting point for IG Officers to build a program from the ground up or to integrate into an existing third-party risk management program. To be effective contributors, IG Officers must be involved in the third-party risk management process during all five stages of the lifecycle, from planning through termination. Further, they must apply the tenets of the Generally Accepted Recordkeeping Principles, which govern the Organization's Data, to the Data in the possession of and under the control of third parties. As data-specific subject matter experts, information governance professionals are not only uniquely qualified to add value to the third-party risk management process, but they also have a responsibility to do so. The boundaries of information governance are expanding and evolving, and it is up to information governance professionals to march the profession forward into third-party risk management opportunities and beyond.

[120] "Can You Transform Your Third Parties' Risk into a Competitive Advantage?" Ernst & Young, accessed January 20, 2021, https://assets.ey.com/content/dam/ey-sites/ey-com/en_ie/topics/advisory/transforming-your-third-party-risk-into-a-competitive-advantage.pdf

Appendix

Third Party Risk Management Guidance, Regulations, Standards

Third-Party Risk Management Guidance, Regulations, Standards by Topic Area	
Anti-Bribery and Corruption	
Agency	**Guidance, Regulations, Standards**
U.S. Department of Justice, USA	• Foreign Corrupt Practices Act (FCPA), 15 U.S.C. 78dd-1 *et seq.*
U.K. Ministry of Justice, UK	• The Bribery Act of 2010 (March 2011)[121]
International Anti—Corruption Unit, Canada	• Fighting Corruption Act, Bill S-14
Agence Française Anticorruption (AFA, the French Anticorruption Agency), France	• The Sapin II Law, French Commercial Code: Article L-233-3
Parliament of India, India	• Prevention of Corruption Act, 1988, No. 49 of 1988
National Anti-Corruption Commission (NACC), Thailand	• Amendment No. 3 (B.E. 2558) to the Act Supplementing the Constitution Relating to the Prevention and Suppression of Corruption B.E. 2542 (also known as "The Organic Act on Counter Corruption")
Vietnam	• The New Penal Code, Anti-Corruption, Law No. 36/2018/QH14
National Peoples' Congress (NPC) Standing Committee, China	• Anti-Unfair Competition Law, 2017, 2019. 31
Brazil	• Clean Company Act 2014 (CCA), Law No. 12,846
Organization for Cooperation and Economic Development	• Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (1999)[122]
International Standards Organization (ISO)	• 37001:2016 - Anti-Bribery Management Systems – Requirements with Guidance for Use (October 2016)[123]

[121] "The Bribery Act 2010," UK Ministry of Justice, accessed January 20, 2021, https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf

[122] "OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions," Organisation for Economic Co-operation and Development, accessed January 20, 2021, https://www.oecd.org/corruption/oecdantibriberyconvention.htm

[123] "ISO 37001:2016: Anti-bribery Management Systems: Requirements with Guidance for Use," International Standards Organization, accessed January 20, 2021, https://www.iso.org/standard/65034.html

Third-Party Risk Management Guidance, Regulations, Standards by Topic Area	
Financial Services	
Agency	**Guidance, Regulations, Standards**
Office of the Comptroller of the Currency (OCC), USA	• OCC Bulletin 2013-029, Third-Party Relationships: Risk Management Guidance (October 30, 2019)[124] • OCC Bulletin 2017-07, Third-Party Relationships: Supplemental Examination Procedures (January 24, 2017)[125] • OCC Bulletin 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-029 (March 5, 2020)[126]
The Federal Reserve, USA	• FED SR 13-19 / CA 13-21: Guidance on Managing Outsourcing Risk (December 5, 2013)[127]
Federal Financial Institutions Examination Council (FFIETC), USA	• FFIEC IT Examination Handbook: Vendor and Third-Party Management[128] • FFIEC IT Examination Handbook Appendix J: Strengthening the Resilience of Outsourced Technology Services[129]
Federal Deposit Insurance Corporation (FDIC), USA	• FIL-44-2008: Guidance for Managing Third-Party Risk (updated June 6, 2008)[130]

[124] "OCC Bulletin 2013-029, Third-Party Relationships: Risk Management Guidance," Office of the Comptroller of the Currency (OCC), October 30, 2019, https://www.occ.gov/news-issuances/bulletins/2013/ bulletin-2013-29.html

[125] "OCC Bulletin 2017-07, Third-Party Relationships: Supplemental Examination Procedures," Office of the Comptroller of the Currency (OCC), January 24, 2017, https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-7.html

[126] "OCC Bulletin 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-029," Office of the Comptroller of the Currency (OCC), March 5, 2020, https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html

[127] "Guidance on Managing Outsourcing Risk," Division of Banking Supervision and Regulation Division of Consumer and Community Affairs Board of Governors of the Federal Reserve System, December 5, 2013, https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf

[128] Federal Financial Institutions Examination Council (FFIEC) includes five banking regulators—the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). "Retail Payment Systems," FFIEC IT Examination Handbook Infobase, accessed January 20, 2021, https://ithandbook.ffiec.gov/it-booklets/retail payment- systems/retail-payment-systems-risk-management/

[129] "Appendix J: Strengthening the Resilience of Outsourced Technology Services," Federal Financial Institutions Examination Council (FFIEC), accessed January 20, 2021, https://www.ffiec.gov/press/PDF/FFIEC_Appendix_J.pdf

[130] "Guidance for Managing Third-Party Risk," Federal Deposit Insurance Corporation (FDIC), accessed January 20, 2021, https://www.fdic.gov/news/news/financial/2008/fil08044a.html

Third-Party Risk Management Guidance, Regulations, Standards by Topic Area	
Financial Services (continued)	
Agency	**Guidance, Regulations, Standards**
Consumer Financial Protection Bureau (CFPB), USA	• Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), 12 U.S.C. §§ 5514-5516
Consumer Financial Protection Bureau (CFPB), USA	• CFPB Bulletin 2012-03, Service Providers (April 12, 2020)[131]
Financial Industry Regulatory Authority (FINRA), USA	• Rule No. 3190, Regulatory Notice 11-14 (May 19, 2011)[132] • NASD Rule 3010, FINRA Notice to Members 05-48[133] • Notice to Members 11-14 and Letters to Members (March 1, 2010 and March 9, 2009)
Securities and Exchange Commission (SEC), USA	• Investment Advisers Act of 1940, 17 CFR § 275.206(4)-7 - Compliance Procedures and Practices
Securities and Exchange Commission (SEC), USA	• Investment Company Act of 1940, 17 CFR § 270.38a-1 - Compliance Procedures and Practices of Certain Investment Companies
National Credit Union Administration, USA	• Supervisory Letter No.: 07-01, Evaluating Third-Party Relationships (October 2007)[134]
New York State Department of Financial Services, USA	• Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500
Monetary Authority of Singapore (MAS), Singapore	• Guidelines on Outsourcing (October 5, 2018)[135]
European Banking Authority, EU	• EBA/GL/2019/02: Final Report on EBA Guidance on Outsourcing Arrangements (February 25, 2019)[136]

[131] "CFPB Bulletin 2012-03: Service Providers" Consumer Financial Protection Bureau (CFPB), April 12, 2012, https://files.consumerfinance.gov/f/20120212_cfpb_ServiceProvidersBulletin.pdf

[132] "Third Party Service Providers 11-14," Financial Industry Regulatory Authority (FINRA), March 2011, https://www.finra.org/sites/default/files/NoticeDocument/p123398.pdf

[133] "Notice to Members 05-48: Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers," Financial Industry Regulatory Authority (FINRA), accessed January 20, 2021, https://www.finra.org/rules-guidance/notices/05-48

[134] "Supervisory Letter No.: 07-01, Evaluating Third-Party Relationships," National Credit Union Administration, October 2007, https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/evaluating-third-party-relationships-0

[135] "Guidelines on Outsourcing," Monetary Authority of Singapore, October 5, 2018, https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing

[136] "EBA/GL/2019/02: Final Report on EBA Guidelines on Outsourcing Arrangements," European Banking Authority, February 25, 2019, https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

Third-Party Risk Management Guidance, Regulations, Standards by Topic Area	
Financial Services (continued)	
Agency	**Guidance, Regulations, Standards**
Basel Committee on Banking Supervision, EU	• Basel Committee on Banking Supervision Outsourcing in Financial Services (February 2005)[137]
Financial Conduct Authority (FCA), UK	• Financial Authority Conduct Handbook, SYSC 13.9 - Outsourcing[138] • Considerations for Firms Thinking of Using Third-Party Technology (off-the-shelf) Banking Solutions (July 2014)[139] • Cyber and Technology Resilience: Themes from Cross-Sector Survey 2017/2018 (updated 2019)[140] • FG16/5: Guidance for Firms Outsourcing to the 'Cloud' and Other Third-Party IT Services (updated January 2019)[141]
The Bank of England, Prudential Regulation Authority (PRA), and Financial Conduct Authority (FCA), UK	• Operational Resilience: Impact Tolerances for Important Business Services, Discussion Paper, Consultation Paper 29/19, Discussion Paper 1/18 (December 5, 2019)[142]
China Banking Regulatory Commission (CBRC) (Now the China Banking and Insurance Regulatory Commission), China	• Notice on Issuing the Guidelines on Internal Control of Commercial Banks - Article 25 (2014)

[137] "Outsourcing in Financial Services," Basel Committee on Banking Supervision, February 2005, https://www.bis.org/publ/joint12.pdf

[138] "SYSC 13.9 Outsourcing," Financial Conduct Authority, accessed January 20, 2021, https://www.handbook.fca.org.uk/handbook/SYSC/13/9.html

[139] "Considerations for Firms Thinking of Using Third-Party Technology (off-the-shelf) Banking Solutions," Financial Conduct Authority (FCA), July 2014, https://www.fca.org.uk/publication/barriers-to-entry-third-party-technology-considerations.pdf

[140] "Cyber and Technology Resilience: Themes from Cross-Sector Survey 2017/2018," Financial Conduct Authority (FCA), updated January 14, 2019, https://www.fca.org.uk/publications/research/cyber-technology-resilience-themes-cross-sector-survey-2017-18

[141] "FG16/5: Guidance for Firms Outsourcing to the 'Cloud' and Other Third-Party IT Services," Financial Conduct Authority (FCA), updated January 2019, https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-cloud-and-other-third-party-it

[142] "Operational Resilience: Impact Tolerances for Important Business Services, Discussion Paper, Consultation Paper 29/19, Discussion Paper 1/18," Bank of England, December 5, 2019, https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper

Third-Party Risk Management Guidance, Regulations, Standards by Topic Area	
General	
Agency	**Guidance, Regulations, Standards**
Securities and Exchange Commission (SEC), USA	• Sarbanes Oxley Act (SOX), 15 U.S.C. §§ 7241 - Sections 302 – Disclosure Controls; 404 – Assessment of Internal Control
U.S. Department of Justice, USA	• Evaluation of Corporate Compliance Programs (updated June 2020)[143]
Institute of Internal Auditors	• Practice Guide: Auditing Third-Party Risk Management (November 2018)[144]
Healthcare	
Agency	**Guidance, Regulations, Standards**
U.S. Department of Health and Human Services, USA	• Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308
U.S. Department of Health and Human Services, USA	• The Health Information Technology for Economic and Clinical Health Act (HITECH), See H.R. 1 (111th Cong., 1st Sess.), amending the Public Health Service Act (42 U.S.C. 201 et seq.) by adopting 42 U.S.C. 13001 et seq.
Centers for Medicare and Medicaid Services (CMS), USA	• Medicare Advantage Contract Provisions, 42 CFR §§ 422.503, 422.504 • Medicare Managed Care Manual, Chapter 21: Compliance Program Guidelines and Prescription Drug Benefit Manual, Chapter 9: Compliance Program Guidelines (January 11, 2013)[145]
Centers for Medicare and Medicaid Services (CMS), USA	• Standards for Qualified Health Plan Issuers on Federally Facilitated Exchanges and State-Based Exchanges on the Federal Platform, Downstream and Delegated Entities, 45 CFR § 156.340

[143] "Evaluation of Corporate Compliance Programs," U.S. Department of Justice, updated June 2020, https://www.justice.gov/criminal-fraud/page/file/937501/download

[144] "Practice Guide: Auditing Third-Party Risk Management," The Institute of Internal Auditors, November 2018, https://global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Auditing-Third-Party-Risk-Management-Practice-Guide.aspx

[145] "Medicare Managed Care Manual, Chapter 21: Compliance Program Guidelines and Prescription Drug Benefit Manual, Chapter 9: Compliance Program Guidelines," Centers for Medicare and Medicaid Services (CMS), January 11, 2013, https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/ Downloads/mc86c21.pdf

Third-Party Risk Management Guidance, Regulations, Standards by Topic Area	
Information Security	
Agency	**Guidance, Regulations, Standards**
International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)	• ISO/IEC 27001:2013 Information technology - Security Techniques - Information Security Management Systems – Requirements (2013, last reviewed 2019)[146]
National Institute of Standards and Technology (NIST)	• Federal Information Security Management Act of 2002 as amended (FISMA), 44 U.S.C., Sec. 3541 et seq
Insurance	
Agency	**Guidance, Regulations, Standards**
National Association of Insurance Commissioners (NAIC), USA	• MDL-668: Insurance Data Security Model Law (2017)[147]
Legal	
Agency	**Guidance, Regulations, Standards**
American Bar Association, USA	• ABA Model Rules of Professional Conduct 1.1, 1.6, 4.4(a) – (b), 5.1, 5.3, 5.7
The Sedona Conference, USA	• The Sedona Conference Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers, Volume 17, No. 1 (2016)[148]

[146] "ISO/IEC 27001:2013 Information Technology - Security Techniques - Information Security Management Systems – Requirements," International Standards Organization (ISO), accessed January 20, 2021, https://www.iso.org/standard/54534.html

[147] "MDL-668: Insurance Data Security Model Law," National Association of Insurance Commissioners (NAIC), 2017, https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf

[148] Sedona Conference, 2016, "The Sedona Conference Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers," Volume 17, No. 1, https://thesedonaconference.org/sites/default/files/publications/Commentary%20on%20Privacy%20and%20Information%20Security.17TSCJ1.pdf

Third-Party Risk Management Guidance, Regulations, Standards by Topic Area	
Life Sciences	
Agency	**Guidance, Regulations, Standards**
Food and Drug Administration (FDA), USA	• Food Drug and Cosmetic Act (FD&C), 21 C.F.R. § 820.50 – Purchasing Controls • 21 CFR Part 211, Subpart B – Organization and Personnel • 21 C.F.R. § 117.435
International Organization for Standardization (ISO)	• ISO 9001:2015 Section 8.4[149]
International Conference on Harmonisation of Technical Requirements (ICH)	• EMA/CHMP/ICH/24235/2006 – ICH Guideline Q 9 on Quality Risk Management (December 2015)[150] • Pharmaceutical Quality System – ICH Q10, Section 2.7 (June 4, 2008)[151]
Privacy	
Agency	**Guidance, Regulations, Standards**
U.S. Department of Health and Human Services, USA	• Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.308
State of California Department of Justice, USA	• California Consumer Privacy Act 3§§ 1798.140(o)(1), 1798.100
European Parliament and Council of the European Union, EU	• General Data Privacy Regulation (GDPR), Chapter 3
Organization for Cooperation and Economic Development (OECD)	• OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (2013)[152]
Federal Trade Commission (FTC), USA	• Children's Online Privacy Protection Act (COPPA), 16 CFR Part 312

[149] "ISO 9001:2015(en) Quality Management Systems – Requirements," International Standards Organization (ISO), accessed January 20, 2021, https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:en

[150] "ICH Guideline Q 9 on Quality Risk Management," International Conference on Harmonisation of Technical Requirements (ICH), December 2015, https://www.ema.europa.eu/en/documents/ scientific-guideline/international-conference-harmonisation-technical-requirements-registration-pharmaceuticals-human-use_en-3.pdf

[151] "Pharmaceutical Quality System – ICH Q10," International Conference on Harmonisation of Technical Requirements (ICH), June 4, 2008, https://database.ich.org/sites/default/files/Q10%20 Guideline.pdf

[152] "OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data," Organization for Cooperation and Economic Development (OECD), 2013, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Third-Party Risk Management Guidance, Regulations, Standards by Topic Area	
Other	
Agency	**Guidance, Regulations, Standards**
Payment Card Industry Security Standards Council, USA	• Payment Card Industry Data Security Standard, PCI DSS 3.2[153]
Federal Trade Commission (FTC), USA	• Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act - GLBA), 12 C.F.R. § 1016.13 and 16 CFR §314.4 (d)
Federal Trade Commission (FTC), USA	• Fair and Accurate Credit Transactions Act of 2003 (FACT Act), 15 U.S.C. §§ 1681-1681x

[153] "Requirements and Security Assessment Procedures, Version 3.2.1," PCI Security Standards Council, May 2018, https://commerce.uwo.ca/pdf/PCI_DSS_v3-2-1.pdf

References

Alami, Adam, Bernard Wong and Tom McBride. 2000. "Outsourcing shows the limited impact for strategic HR." *Employee Benefit News* 14(10) 70.

American Institute of Certified Public Accountants (AICPA). "SOC 2® - SOC for Service Organizations: Trust Services Criteria." Accessed October 2, 2020. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

American Medical Association. "HIPAA Violations and Enforcement." Accessed August 31, 2000. https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

American Society for Auditing. "What is Auditing," adapted from *The ASQ Auditing Handbook*. ASQ Quality Press. Accessed December 2, 2020. https://asq.org/quality-resources/auditing

Arant, Peter and Steve Kreitner. 2016. "Feature Story: Understand the Risks and Benefits When Using Third Party Vendors for IT Needs." *Montana Lawyer* 42(14):1-4.

ARMA International. 2017. Generally Accepted Recordkeeping Principles. ARMA International: Kansas. https://www.arma.org/page/principles

Baker & McKenzie. 2015. "Five Essential Elements of Corporate Compliance: A Global Template." https://www.bakermckenzie.com/~/media/Files/BDSUploads/Documents/global% 20corporate%20compliance/bk_global_5elements_20150721.pdf

Bank of England. "Operational Resilience: Impact Tolerances for Important Business Services, Discussion Paper, Consultation Paper 29/19, Discussion Paper 1/18." December 5, 2019. https://www.bankofengland.co.uk/ prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper

Basel Committee on Banking Supervision. "Outsourcing in Financial Services." February 2005. https://www.bis.org/publ/joint12.pdf

Bourne, Lynda. "The Six Functions of Governance." *PM World Journal*, Volume III, Issue XI. November 2014. https://www.mosaicprojects.com.au/PDF_Papers/P188_Six_Functions_of_Governance.pdf

Bruce, Elyse. "A Chain is Only as Strong as its Weakest Link." Ideomation. April 23, 2010. https://idiomation.wordpress.com/2010/04/23/a-chain-is-only-as-strong-as-its-weakest-link/

Campbell, Michael G. 2011. *The Complete Idiot's Guide to Project Management, 5th edition*. London: Penguin Books.

Centers for Medicare and Medicaid Services (CMS). "Medicaid Program Integrity." Accessed October 4, 2020. https://www.cms.gov/Medicare-Medicaid-Coordination/FraudPrevention/FraudAbuseforProfs/Downloads/ fftoolkit-federal-database-checks.pdf

Centers for Medicare and Medicaid Services (CMS). "Medicare Managed Care Manual, Chapter 21: Compliance Program Guidelines and Prescription Drug Benefit Manual, Chapter 9: Compliance Program Guidelines." January 11, 2013. https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/ Downloads/mc86c21.pdf

Cloud Security Alliance (CSA). "About." Accessed October 15, 2020. https://cloudsecurityalliance.org/about/

Cloud Security Alliance. 2021 (CSA). "Clouds Matrix V4." https://cloudsecurityalliance.org/artifacts/ cloud-controls-matrix-v4/

Consumer Financial Protection Bureau (CFPB). "CFPB Bulletin 2012-03: Service Providers." April 12, 2012. https://files.consumerfinance.gov/f/20120212_cfpb_ServiceProvidersBulletin.pdf

CreateCompliance. "Third Party Anti-Corruption Due Diligence Guidelines." 2018. https://ethisphere.com/wp-content/uploads/Third-Party-Due-Diligence-7.2.18.pdf

Cummings, Adam. "Inherent Risk Tiering for Third-Party Risk Assessments." MindPoint Group. June 10, 2018. https://www.mindpointgroup.com/blog/breach/inherent-risk-tiering-for-third-party-vendor-assessments/

Curry, Thomas J. "Remarks Before RMA's Governance, Compliance, and Operational Risk Conference." Speech. Cambridge, Massachusetts, May 8, 2014. https://www.occ.treas.gov/news-issuances/speeches/2014/pub-speech-2014-69a.pdf

Deloitte. "Modernizing the Three Lines of Defense Model." Accessed September 24, 2020. https://www2.deloitte.com/us/en/pages/advisory/articles/modernizing-the-three-lines-of-defense-model.html

Deloitte. "Third Party Governance and Risk Management: Turning Risk into Opportunity." 2015. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/ deloitte-uk-third-party-governance-risk-management-report.pdf

Dipshan, Rhys. "Three Things to Consider in Vendor Risk Management." *Legal Tech News*, December 7, 2017. https://www.law.com/legaltechnews/sites/legaltechnews/2017/12/07/3-things-to-consider-in-vendor-risk-management/

Division of Banking Supervision and Regulation Division of Consumer and Community Affairs Board of Governors of the Federal Reserve System. "Guidance on Managing Outsourcing Risk." December 5, 2013. https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf

Engardio, Peter, Josey Puliyenthuruthel and Manjeet Kripalani. "Fortress India." *Business Week*, February 14, 2004.

Ernst & Young. "Building Trust with Your Third Parties in a Technology Driven and Disruptive World: EY Global Third-Party Risk Management Survey 2019-20." 2020. https://www.google.com/search?client=firefox-b-1d&q=global+financial+services+third-party+risk+management+survey

Ernst & Young. "Can You Transform Your Third Parties' Risk into a Competitive Advantage?" Accessed January 20, 2021. https://assets.ey.com/content/dam/ey-sites/ey-com/en_ie/topics/advisory/transforming-your-third-party-risk-into-a-competitive-advantage.pdf

Ernst & Young. "Global Financial Services Third-Party Risk Management Survey." 2018. https://ey-global-financial-services-third-party-risk-management-survey.pdf

European Banking Authority. "EBA/GL/2019/02: Final Report on EBA Guidelines on Outsourcing Arrangements." February 25, 2019. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3702423665479/EBA% 20revised%20Guidelines% 20on%20outsourcing%20arrangements.pdf?retry=1

Fasulo, Phoebe. "5 Data Breach Statistics and Trends to Look Out for in 2020." Security Scorecard. December 9, 2019. https://securityscorecard.com/blog/5-data-breach-statistics-and-trends-to-look-out-for-in-2020

Federal Deposit Insurance Corporation (FDIC). "Guidance for Managing Third-Party Risk." Accessed January 20, 2021. https://www.fdic.gov/news/news/financial/2008/fil08044a.html

Federal Financial Institutions Examination Council (FFIEC). "Appendix J: Strengthening the Resilience of Outsourced Technology Services." Accessed January 20, 2021. https://www.ffiec.gov/ press/PDF/FFIEC_Appendix_J.pdf

Federal Financial Institutions Examination Council (FFIEC). "Retail Payment Systems" FFIEC IT Examination Handbook Infobase. Accessed January 20, 2021. https://ithandbook.ffiec.gov/ it-booklets/retail payment- systems/retail-payment-systems-risk-management/

Financial Conduct Authority (FCA). "Considerations for Firms Thinking of Using Third-Party Technology (off-the-shelf) Banking Solutions." July 2014. https://www.fca.org.uk/publication/barriers-to-entry-third-party-technology-considerations.pdf

Financial Conduct Authority (FCA). "Cyber and Technology Resilience: Themes from Cross-Sector Survey 2017/2018." Updated January 14, 2019. https://www.fca.org.uk/publications/research/cyber-technology-resilience-themes-cross-sector-survey-2017-18

Financial Conduct Authority (FCA). "FG16/5: Guidance for Firms Outsourcing to the 'Cloud' and Other Third-Party IT Services." Updated January 2019. https://www.fca.org.uk/publications/ finalised-guidance/fg16-5-guidance-firms-outsourcing-cloud-and-other-third-party-it

Financial Conduct Authority (FCA). "SYSC 13.9 Outsourcing." Accessed January 20, 2021. https://www.handbook.fca. org.uk/handbook/SYSC/13/9.html

Financial Industry Regulatory Authority (FINRA). "Notice to Members 05-48: Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers." Accessed January 20, 2021. https://www.finra.org/ rules-guidance/notices/05-48

Financial Industry Regulatory Authority (FINRA). "Third Party Service Providers 11-14." March 2011. https://www.finra.org/sites/default/files/NoticeDocument/p123398.pdf

"Fraud, Third-Party Risks Still Top Concerns for Chief Compliance Officers." *Corporate Counsel (Online).* January 31, 2020, https://www.law.com/corpcounsel/2020/01/31/ fraud-third-party-risks-still-top-concerns-for-chief-compliance-officers/

Google. "Standardized Information Gathering Questionnaire." Accessed October 22, 2020, https:// cloud.google.com/security/compliance/sig

HITRUST Alliance. "CSF Assurance Program." 2021. https://hitrustalliance.net/csf-assuranceprogram/?gclid=CjwKCAiAr6ABhAfEiwADO4sf SZc14xNkN1cpTJb6FHnW6A90VMetBHekrXicIjX3O_yREWHVxnEtBoC8egQAvD_BwE

Institute of Internal Auditors. "Practice Guide: Auditing Third-Party Risk Management." November 2018. https://global.theiia.org/standards-guidance/recommended-guidance/ practice- guides/Pages/Auditing-Third-Party-Risk-Management-Practice-Guide.aspx

International Conference on Harmonisation of Technical Requirements (ICH). "ICH Guideline Q 9 on Quality Risk Management." December 2015. https://www.ema.europa.eu/en/ documents/scientific-guideline/international-conference-harmonisation-technical-requirements-registration-pharmaceuticals-human-use_en-3.pdf

International Conference on Harmonisation of Technical Requirements (ICH). "Pharmaceutical Quality System – ICH Q10." June 4, 2008. https://database.ich.org/sites/default/files/ Q10% 20 Guideline.pdf

International Standards Organization (ISO). "ISO 37001:2016: Anti-bribery Management Systems: Requirements with Guidance for Use." Accessed January 20, 2021. https://www.iso.org/ standard/65034.html

International Standards Organization (ISO). "ISO 9001:2015(en) Quality Management Systems – Requirements." Accessed January 20, 2021. https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:en

International Standards Organization (ISO). "ISO/IEC 27001:2013 Information Technology - Security Techniques - Information Security Management Systems – Requirements." Accessed January 20, 2021. https://www.iso.org/standard/54534.html

International Standards Organization (ISO). "ISO/IEC 27002:2013 — Information Technology, Security Techniques, Code of Practice for Information Security Controls." Accessed October 17, 2020. https://www.iso.org/standard/54533.html

Judd, Cathryn and Mark Jennings. 2012. "Vendor Risk Management—Compliance Considerations." *Consumer Compliance Outlook*: Fourth Quarter 2012.

Kenney, Andrew. 2016. "Third-Party Risk: How to Trust Your Partners." *Journal of Accountancy* May (2016): 57-61.

LexisNexis. "Regulatory Requirements and the Third-Party Threat." 2014. https://www.lexisnexis.com/pdf/Nexis-Diligence/Financial-Services.pdf

Malatesta III, John Thomas A. and Sarah S. Glover. 2016. "A Clear and Present Danger: Mitigating the Data Security Risk Vendors Pose to Businesses." *Sedona Conference Journal* 17 (761).

Mehta, Anju and Nikhil Mehta. 2017. "Moving Toward an Integrated Framework of Offshore Information Technology Outsourcing Success." *Journal of Global Information Technology Management* 20(3) 171-94.

Mikkelsen, Daniel, Angelika Reich, Emily Yueh, Caroline Coombe, and Michael Bartholomeusz. 2017. "Improving Third-Party Risk Management: A Joint Study Between ORIC International and McKinsey and Company." Whitepaper. McKinsey and Company. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Improving%20third%20party%20risk%20management/Improving-third-party-risk-management.ashx

Mlot, Stephanie. "HVAC Vendor Confirms Link to Target Data Breach." *PC.* February 7, 2014. https://www.pcmag.com/news/hvac-vendor-confirms-link-to-target-data-breach

Monetary Authority of Singapore. "Guidelines on Outsourcing." October 5, 2018. https:// www.mas.gov.sg/ regulation/guidelines/guidelines-on-outsourcing

Moskver, Maria. "Navigating the Pitfalls of Third-Party Service Provider Oversight." *The Mortgage Banker Magazine* February 8, 2019. https://www.mortgagebankermag.com/loan-servicing/navigating-the-pitfalls-of-third-party-service-provider-oversight/

Nath, Anupam Kumar. 2018. "Towards Understanding the Factors and Their Effect on Offshored Data Privacy." *Journal of Business and Management* 24(2): 1-18. DOI: 10.6347/ JBM.201809_24(2).0001

Nath, Subhashis. 2020. "The Coming Regulatory Wave: Vendor Risk Management." Genpact. Accessed November 28, 2020. https://www.genpact.com

National Association of Insurance Commissioners (NAIC). "MDL-668: Insurance Data Security Model Law." 2017. https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf

National Credit Union Administration. "Supervisory Letter No.: 07-01, Evaluating Third-Party Relationships." October 2007. https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/evaluating-third-party-relationships-0

NBC News. "Target Settles 2013 Hacked Customer Data Breach For $18.5 Million." May 24, 2017. https://www.nbcnews.com/business/business-news/target-settles-2013-hackedcustomer- data-breach-18-5-million-n764031

Office of the Comptroller of the Currency (OCC). "Comptroller's Handbook: Consumer Compliance, Version 1.0." June 2020. https://www.occ.treas.gov/publications-and-resources/publications/ comptrollers-handbook/files/unfair-deceptive-act/pub-ch-udap-udaap.pdf

Office of the Comptroller of the Currency (OCC). "OCC Bulletin 2013-029, Third-Party Relationships: Risk Management Guidance." October 30, 2019. https://www.occ.gov/news-issuances/bulletins/ 2013/bulletin-2013-29.html

Office of the Comptroller of the Currency (OCC). "OCC Bulletin 2017-07, Third-Party Relationships: Supplemental Examination Procedures." January 24, 2017. https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-7.html

Office of the Comptroller of the Currency (OCC). "OCC Bulletin 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-029." March 5, 2020. https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html

Ontala. "About," Ontala Performance Solutions. Accessed August 21, 2020, https://ontala.com/

Organization for Economic Co-operation and Development (OECD). "OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions." Accessed January 20, 2021. https://www.oecd.org/corruption/oecdantibriberyconvention.htm

Organization for Economic Cooperation and Development (OECD). "OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data." 2013. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Osborne, Charlie. "Open-source software breaches surge in the past 12 months." ZDNet. March 4, 2019. https://www.zdnet.com/article/open-source-software-breaches-surge-in-the-past-12-months/

Palvia, Prashant, Shailendra Palvia, and James Edward Whitworth. 2002. "Global Information Technology: A Meta Analysis of Key Issues." *Information and Management*, 39(5): 403-414.

PCI Security Standards Council. "Requirements and Security Assessment Procedures, Version 3.2.1." May 2018. https://commerce.uwo.ca/pdf/PCI_DSS_v3-2-1.pdf

Powell, Vera and Alice Hsieh. "Effective Monitoring of Compliance Programs: A Guide for Practitioners." *Corporate Counsel*. January 13, 2020. https://www.law.com/corpcounsel/2020/ 01/13/effective-monitoring-of-compliance-programs-a-guide-for-practitioners/

Queensland Government. “Defensible Process.” February 27, 2019. https://www.forgov.qld.gov.au/ glossary/defensible-process

Rane, Satya. “What are the 12 requirements of PCI DSS Compliance?” Controlcase.com. Accessed January 15, 2021. https://www.controlcase.com/what-are-the-12-requirements-of-pci-dss-compliance/

Ropes and Gray. “Third-Party Screening and Monitoring are Critical for Health Care and Life Science Companies.” August 29, 2019. https://www.ropesgray.com/en/newsroom/alerts/2019/08/Third-Party-Screening-and-Monitoring-Are-Critical-for-Health-Care-and-Life-Science-Companies

Royal, K. “Chapter Seven: Saturn.” International Association of Privacy Professionals (IAPP). Accessed December 2, 2020. https://iapp.org/news/a/monitoring-third-party-vendors-means-managing-your-own-risk-chapter-seven/

Ryan, Dennis. “Yes, There is a Cure for Audit Paralysis.” Compass Health and Safety Limited. Accessed January 14, 2021. http://compasshealthandsafety.com/whats-new/compass-articles/ yes-cure-audit-fatigue-audit paralysis/

Sangster, Mark. “It’s Time to Take Third-Party Risk Seriously.” *The American Lawyer*, September 1, 2019. https://www.law.com/legaltechnews/2019/09/19/its-time-to-take-third-party-risk-seriously/

Security Industry and Financial Market Association (SIFMA). “Third Party Risk Management.” Accessed August 27, 2020. https://www.sifma.org/resources/general/third-party-risk-management/

Sedona Conference. 2016. “The Sedona Conference Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers,” Volume 17, No. 1. https://thesedonaconference.org/sites/default/files/publications/Commentary%20on%20Privacy%20and%20Information%20Security.17TSCJ1.pdf

Shared Assessments and Protiviti. 2019. “Vendor Risk Management Benchmark Study: Running Hard to Stay in Place.” https://www.protiviti.com/ sites/default/files/2019-vendor-risk-management-benchmark-study-sharedassessments-protiviti.pdf

Shared Assessments. “SIG Questionnaire Tools.” Accessed October 15, 2020. https://sharedassessments.org/sig/

Sharpe, Ralph and Meredith Boylan. 2012. “Operational Risk: Increased Regulatory Focus on BSA/AML Compliance and Third-Party Relationships.” *Journal of Taxation and Regulation of Financial Institutions* 25(41).

Shaswat, Das. “Conducting KYC of Third Parties: Best Practices for Conducting Due Diligence.” Hunton Andrews Kurth LLP. April 2018. https://www.huntonak.com/images/content/3/6/v4/ 36714/best-practices-for-conducting-due-diligence.pdf

Slatbotsky, Rachel. “Inherent Risk vs. Residual Risk Explained in 90 Seconds.” Fair Institute. Accessed November 23, 2020. https://www.fairinstitute.org/blog/inherent-risk-vs.-residual-risk-explained-in-90-seconds

Sotnikov, Ilia. “Simplifying Third-Party Risk Management.” *Risk Management* July/August (2019): 8-9. http://www.rmmagazine.com/2019/08/01/simplifying-third-party-risk-management/

Switzer, Carole. “Breaking Up is Hard to Do – Avoiding Pain by Planning for the End of a Third-Party Relationship.” OCEG Blog. July 19, 2014. https://go.oceg.org/third-party-management

Taft, Jeffrey P., Megan S. Webster, Matthew Bisanz, and Joy Tsai. “The Blurred Lines of Organizational Risk Management.” Mayer Brown. July 31, 2020. https://www.mayerbrown.\com/en/perspectives-events/publications/2020/07/the-blurred-lines-of-organizational-risk-management

Tennessee State Government. “Inherent and Residual Risk.” Accessed October 22, 2020. https://www.tn.gov/content/dam/tn/finance/accounts/Inherent-vs-RisidualRisk.pdf

Tolkien, J.R.R. 2017. Chapter 12: Inside Information in *The Hobbit.* Houghton Mifflin Company: New York.

Transparency International UK. "Global Anti-Bribery Guidance: 13 Managing Third Parties." Accessed August 27, 2020. https://www.antibriberyguidance.org/guidance/13-managing-third-parties/guidance

U.S. Department of Health and Human Services. "Business Associate Contracts." Accessed September 17, 2020. https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

U.S. Department of Justice. "Department of Justice Manual 9-28.800." Accessed August 21, 2020. https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations

U.S. Department of Justice. "Evaluation of Corporate Compliance Programs." U.S. Department of Justice Criminal Division. 2020. https://www.justice.gov/criminalfraud/page/file/937501/download

U.S. Department of Justice. "FCPA Resource Guide." 2012. https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf

UK Ministry of Justice. "The Bribery Act 2010." Accessed December 23, 2020. https://www.justice.gov.uk/ downloads/legislation/bribery-act-2010-guidance.pdf

Veerasamy, Vignesh, Amy Brachio and Nitin Bhatt. 2018. "Can You Transform Your Third Parties Risk to Competitive Advantage?" Ernst & Young. https://assets.ey.com/content/dam/ ey-sites/ey-com/en_ie/topics/advisory/transforming-your-third-party-risk-into-a-competitive-advantage.pdf

"What is Risk? Definition and Meaning." *Market Business News*. Accessed November 21, 2020. https://marketbusinessnews.com/financial-glossary/risk-definition-meaning/

Zimmerman, Greg. "Target Settles HVAC Data Breach for $18.5 Million." FacilitiesNet. May 25, 2017. https://www.facilitiesnet.com/hvac/tip/Target-Settles-HVAC-Data-Breach-for-185-Million--39237

About the Author:

Sofia Empel, PhD, CRM, IGP, is the Director, Information Governance at a healthcare data analytics company located in the United States. As the company's information governance subject matter expert, she participated in creating the company's enterprise-wide third-party risk management program from the ground up and continues to contribute to its ongoing improvement. As a compliance officer, she leads the company's third-party risk management program on behalf of the Compliance Department. Dr. Empel previously worked as an independent records and information management consultant to a large variety of industries for over 20 years. She specializes in information governance program development, training, technology implementation, and other analytical services. She frequently teaches, writes, and speaks on information governance and records management topics. Dr. Empel was a 2010 recipient of ARMA International Education Foundation's graduate scholarship for advanced study in the field of records and information management and served as a member of its Research Committee from 2015 through 2018.