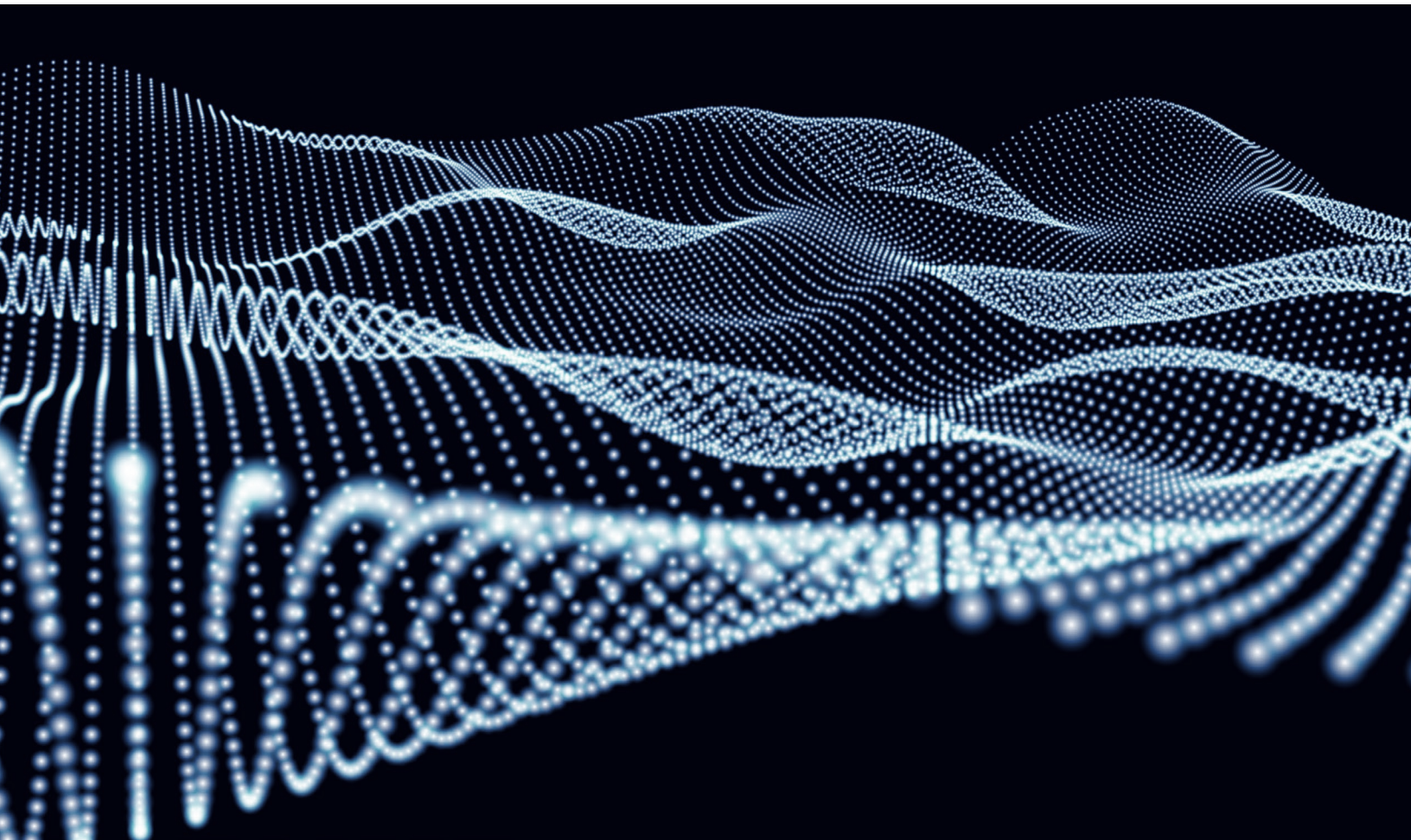
CAPCO

MITIGATING VENDOR RISK THROUGH DATA MANAGEMENT



ABSTRACT

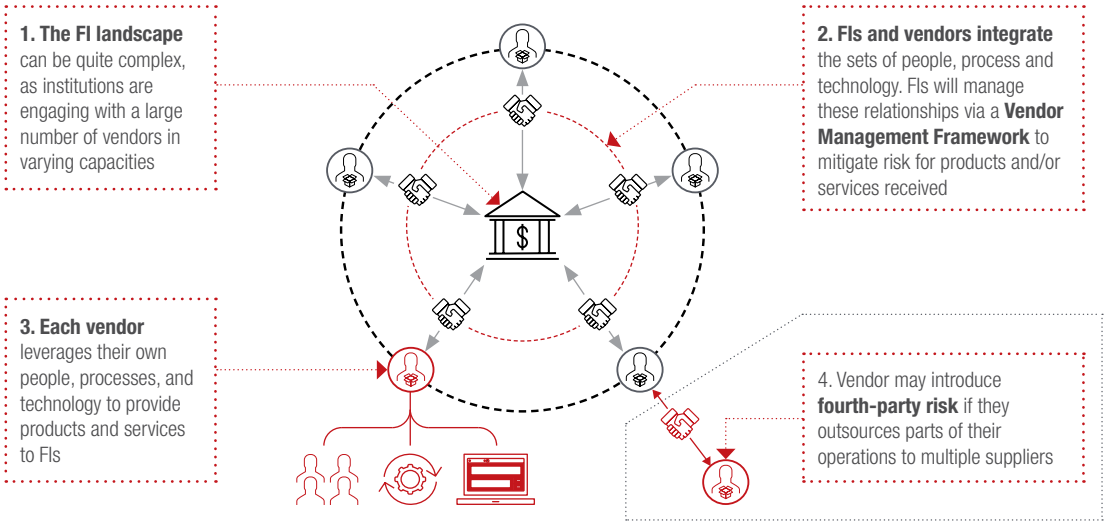
Financial institutions (FIs) frequently rely on vendors to enhance their current infrastructure, processes, and technology solutions. Vendors enable these institutions to achieve their strategic business objectives with new products and services, thereby achieving operational excellence, by increasing revenue and reducing costs. However, the outsourcing of core functions and increased use of data brings forth the need to better manage vendor risk across areas, such as cybersecurity, privacy, and information and protection laws. This paper explores enhancing a financial institution's vendor risk management (VRM) framework by incorporating data risk to drive effective data governance and management. We identify four principles utilizable to actively reduce data risk. Lastly, in this paper, the terms "vendor(s)" and "third-party(ies)" are used interchangeably to cover a broad interpretation of a contract or a business arrangement. It covers any relationship that an FI may enter with another entity or individual for the purposes of obtaining products or services.

1. INTRODUCTION

In response to the 2007 Global Financial Crisis, regulatory-authorities imposed mandates such as CCAR, Dodd-Frank, MiFID II, and BCBS 239. Now, Financial Institutions (FIs) need to quantify their credit, market, and operational risks to ensure they meet both qualitative and quantitative capital requirements across all products and services. In addition to supporting the health of the financial system, these regulations highlight the importance globally of managing data quality. However, there have been minimal adjustments on how FIs interact and manage their vendors. FIs designed vendor risk management (VRM) frameworks primarily to help control costs, drive service value, and mitigate their financial risk. As technology innovations have accelerated, there is now an industry-wide focus on data security and data privacy concerns. Regulators and FIs need to continuously monitor their risk frameworks and identify any emerging technologies that pose potential risks. At this intersection of operational and technology risk, data management is a critical foundation to mitigate financial and reputational consequences, as data is continuously exposed to people, processes, and technology. Through interactions between FIs and third-parties, data may be exposed to new vendor procedures and transformations that can compromise its integrity. These interactions quickly get intricate and create a multi-vendor landscape that produces direct or indirect risk for an FI as illustrated in Figure 1.

When FIs partner with vendors, they need an effective mechanism to maintain data quality and mitigate data risk. Regulatory oversight still holds FIs accountable for any processing by vendors and their actions. For instance, the Federal Deposit Insurance Corporation (FDIC) in the U.S. issued a formal guidance in 2008: "An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution.[1]" For any vendor-produced data, the FI thus must continue managing data quality risk to mitigate financial, operational, and reputational consequences. FIs should ensure their vendors, and any potential vendors of vendors (i.e., fourth-parties), are committed to providing products and services within an agreed framework to mitigate any data-related risks.

Figure 1: A multi-vendor landscape, requiring a transparent and strong vendor risk management framework

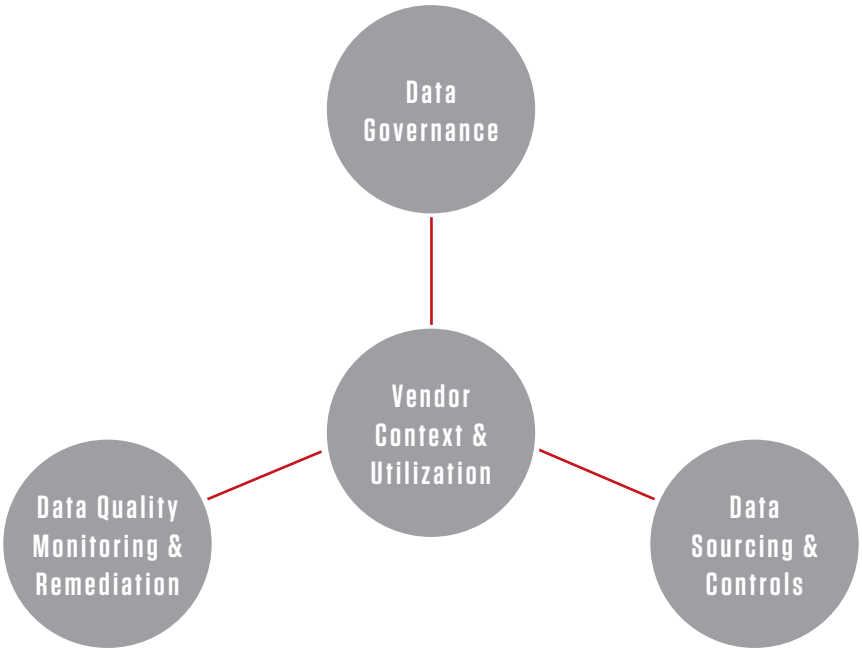


2. UNDERSTANDING DATA-RELATED VENDOR RISKS

VRM frameworks provide a structure for an FI and its vendors to work together on an on-going basis. This usually includes a day-to-day engagement model, escalation management, key performance indicators, and a joint strategic view. To manage vendor risk, institutions often tier their vendors based on contract amounts and the criticality of services received. Institutions understand that they need to periodically evaluate their vendors across key risk areas, such as compliance risk, financial risk, and reputational risk. With the rise in instances of data breaches that affect such risks, privacy and cybersecurity have quickly become indicators of confidence for consumers. In a 2019 study[2] by Ponemon Institute, the global average cost of a data breach has grown by 12% in the prior five years to $3.92 million. If a third-party caused the data breach, the cost increased by more than $370,000, for an adjusted average total cost of $4.29 million. In another 2016 survey[3] conducted by the same institute; only 31% of respondents rated their vendor risk management program as highly effective, while only 38% required an evaluation of vendor policies before starting a business relationship. There are shortfalls in the current process and FIs need to ensure they are diligently evaluating their vendors and managing vendor data quality risk.

A vendor partnership still requires FIs to maintain accountability for regulatory reporting and the accuracy of data. This can be performed by enhancing existing VRM frameworks to structure vendor relationships across four principles, as illustrated in Figure 2: 1) Vendor Context and Utilization 2) Data Governance, 3) Data Sourcing and Controls, and 4) Data Quality Monitoring and Remediation. These principles are adaptable and allow for FIs to adjust as per their strategic objectives and goals. These will enable FIs to maintain transparency, reliability, and substitutability with their vendors. We discuss the importance and purpose of each principle below.

Figure 2: Enhance existing Vendor Risk Management frameworks by incorporating key data management principles



PRINCIPLE 1: VENDOR CONTEXT AND UTILIZATION

The initial due diligence performed is a key step in managing vendor risk. Typically, the FI will evaluate the vendor in two aspects – the vendor company profile and financials; and the product or service that is being assessed for purchase. This initial assessment provides insight into the operations and technology capabilities and its viability within the FIs landscape but does not always evaluate for data risk.

As the vendor offerings can range from out-of-the-box products and services to highly customized solutions, the range of products and/or services offered by the vendor should also be evaluated for their data risk. To illustrate:

- Does the vendor only provide datasets?
- What types of data will they store and have access to?
- Would the vendor face financial or reputational damage if this data were compromised?
- Does the vendor provide a technology solution that they maintain?
- Does the vendor provide any operational support?

The solutions presented by the vendors for these queries will have a significant effect on the granularity of oversight required. The type of product and/or service provided by a vendor drives the set of controls required to maintain data quality and meet regulatory commitments. There is no one-size-fits-all data quality framework applicable to all vendors. Instead, it is important to identify the type of vendor relationship. Most vendors can be categorized into one of four relationship buckets, as shown in Figure 3.

Figure 3: Vendor Characteristics by Products and Services Offered

	Data Providers	Service providers
Standard Products	• Vendor provides the expected dataset, with no involvement from buying organization • Usually established as industry standards and provided to numerous buyers • No integration required with buying organization	• Vendor provides services across technology, operations, infrastructure, etc. • Data quality is integral to the service provided • Minimal integration may be required with buying organization
Custom Products	• Vendor provides custom datasets and/or processing tailored for the buying organization • Beyond initial engagement, no further day-to-day involvement required from buying organization	• Highly customizable service provided, requiring integration of processes and technology • Buying organization can influence design or operations • Data quality will be impacted by both organizations

Data providers supply easily consumable data sets. They will typically focus on presenting data in a desirable format and will not need significant integration with the buying FI. Most data providers can be categorized as either standard or custom:

a. Standard Data Providers offer commoditized data sets used across financial services (e.g., historical pricing, market data feeds, industry analysis across disciplines, etc.).

b. Custom Data Providers provide bespoke data sets to institutions. Many of these data providers leverage artificial intelligence and machine learning to create data sets for a specific market or product segment.

Service Providers typically offer technology, processing, or infrastructure resources, often requiring some level of either systemic or process integration. Like data providers, service providers also fall into two categories:

a. Standard Service Providers are often industry-leading companies providing commoditized solutions (e.g., trading services, administrative operations, etc.).

b. Custom Service Providers provide tailored technology solutions or advisory services to complex business problems (e.g., artificial intelligence, application development, etc.).

Figure 4 illustrates some commonly used vendors in financial services across each of these groups. Consider a data provider — such as IDC or Moody's — that distributes market data feeds in a standardized format across the industry. These datasets generally require little-to-no integration, and the vendor applies sufficient controls before distribution. Alternatively, consider a service provider — such as Finastra — that provides a technology solution to create an integrated treasury platform. The platform integration is unique per the customization required with the institution.

With this lens, it is also clear that vendors may not exclusively belong to one category. The context and basis of interaction between the vendor and FI is a critical aspect of risk management, especially for data quality. Consider a service provider, such as Salesforce, that provides standardized products and services in financial services. Due to the nature and complexity of the industry, they also offer customized solutions that are tailored versions of the standard out-of-the box solution. The complexity of managing a vendor relationship depends on the suite of products and services provided by the vendor, and how they will be utilized. Therefore, FIs must define a set of guiding principles toward identifying and managing risk associated with their vendor's data.

Figure 3: Vendor Characteristics by Products and Services Offered

PRINCIPLE 2: DATA GOVERNANCE

Existing VRM frameworks serve as a foundational construct of managing the technology eco-system between FIs and vendors. The existing process defines designated points-of-contact (contract or relationship owners) to ensure the execution of processes per contractual agreement. Contract management typically covers technology and operations components and, it should be strengthened by including data management processes. Periodic reviews of data-relevant change processes need to be conducted to ensure the vendor continues maintaining data quality. In partnerships with significant data impact, the FI should consider the following enhancements to the VRM framework, as illustrated in Figure 5:

- Establishing data oversight and ownership with designated points-of-contact across both organizations
- Operating a joint change management committee to ensure consistent usage of data across organizations and transparency of data management centric transformations
- Outlining an interaction model that defines any committees and/or working groups involved in recurring activities
- Defining communication protocols across any data sourcing or data quality processes in the context of the partnership
- Instituting key performance indicators and metrics to track the effectiveness of agreed data management processes

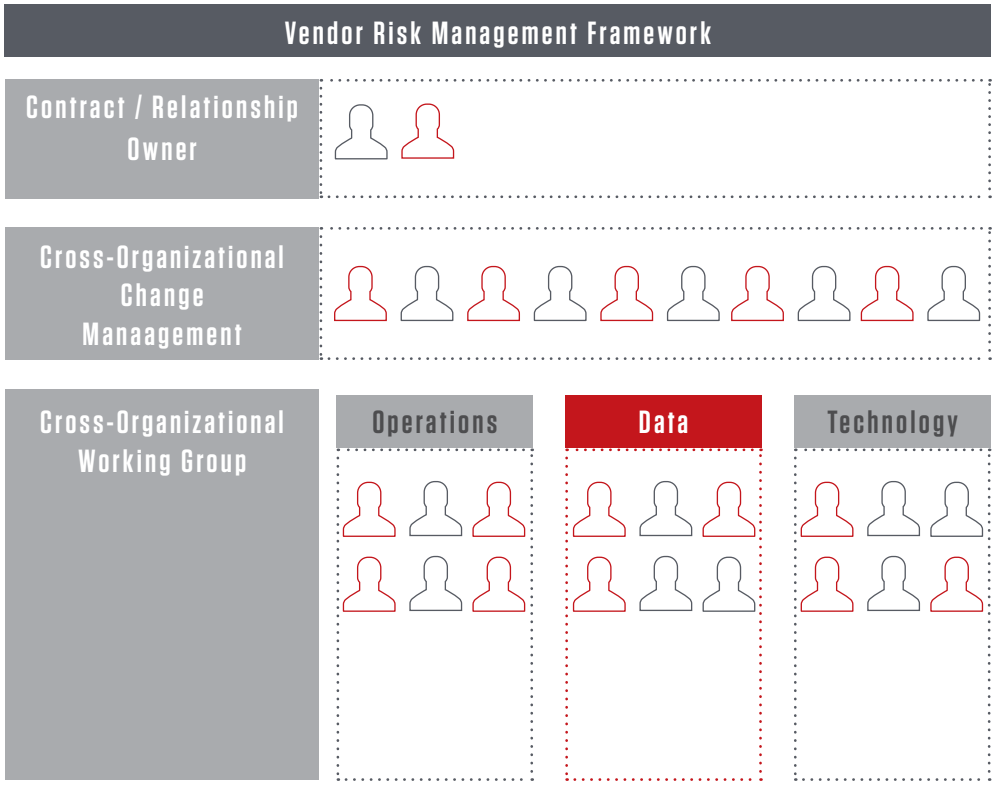
Figure 5: Mitigating Risk by Incorporating Oversight of Data Management Processes

1. **Vendor Risk Management Framework**

FIs and vendors establish Contract or Relationship Owners to provide oversight and ensure the efficient execution of change management processes

2. **Enhancing the Vendor Risk Management Framework**

For relationships with high impact to data quality, enforce data management principles through cross-organization committees and working groups



PRINCIPLE 3: DATA SOURCING AND CONTROLS

Many organizations have extrapolated this principle by capturing their data lineage through identifying the originating source and tracing routes through which the data travels. The time required and complexity of capturing data lineage can be quite intimidating. At its most granular form, data lineage has been captured with the intent of capturing all metadata instead of focusing on the result desired. Thus, significant time and effort may have been spent with minimal business impact. To avoid this pitfall with vendor data, FIs can focus on identifying where the data is being created, how it reaches the FI, and how data integrity is maintained. With this information, institutions can significantly reduce complexity of lineage capture and focus on data quality monitoring. FIs should work with their vendors to establish sourcing standards including but not limited to:

- Identifying systems responsible for originating data, and systems authorized to distribute data across organizations
- Building a data ontology with business, technical terms, and their definitions, ensuring the use of consistent terminology and strengthening transparency of data usage across firms
- Leveraging industry standards where feasible, such as the Sarbanes-Oxley Act (SOX), International Organization for Standardization (ISO), and NIST
- Receiving from the vendor a complete list of relevant data controls with clearly defined processes, SLAs, and escalation resolution procedures

Ultimately, the extent of third-party data risk depends on the type of products and services received. The FI may need to establish a baseline with any custom providers while standard providers will typically already meet industry wide minimum standards. The FI needs only to evaluate if any further stringent requirements need to be met by the vendor.

PRINCIPLE 4: DATA QUALITY MONITORING AND REMEDIATION

Privacy protection laws for the customer are continuously evolving. Regulatory bodies are constantly evaluating the customer's right of consent to use of their data; and an organization's ability to utilize the customer's data for monetization or other purposes. With the increased focus on data security and privacy, regulatory bodies frequently require FIs to measure data quality. FIs and vendors should collaborate to ensure they converge on meeting these industry standards. In any partnership, it may not be possible for the vendor to replicate an institution's controls framework under limitations of time, cost, and resources. Instead, they should focus on maintaining data quality at the source and data consistency from source to distribution. A comprehensive data quality framework between the two organizations can be achieved through the following:

- Establishing scope of focus under data management by identifying Critical Data Elements (CDEs)
- Implementing data quality standards and metrics at data origination and distribution sources
- Utilizing data quality monitoring tools to observe when data quality falls below acceptable thresholds
- Creating a clear, comprehensive process to remediate data quality issues, aligned to existing operational risk frameworks
- Using external/independent party audits to ensure vendor data quality controls and processes are consistent and sufficient

These principles integrated with the VRM framework provide a succinct view of how data quality can be managed across both organizations. Figure 6 illustrates these four principles combined can effectively reduce third-party risk.

Figure 6: Applying Data Sourcing and Data Quality Standards within the Vendor context

Vendor Risk Management Framework

1. **Vendor Context and Utilization**

Establish guidelines that help identify the data risk factor that a vendor relationship may bring

Standard Data / Service Providers | **Custom Data/ Service Providers**

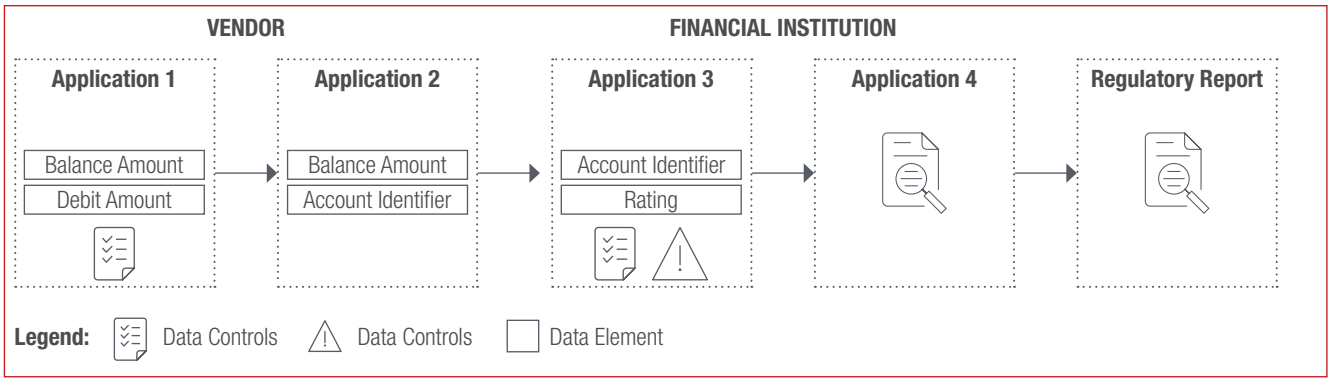
2. **Data Governance**

Strengthen vendor risk management frameworks to enforce data management principles and capabilities

Contract / Relationship Owner | **Cross-Organizational Change Management** | **Cross-Organizational Working Group**

3. **Data Sourcing and Controls**

Apply sufficient controls to ensure data quality against points of data origination and data distribution



4. **Data Quality Monitoring and Remediation**

Monitor data controls so that upon failure, data quality issues can be identified, assessed and resolved

1. Identify and document Issue | **2. Evaluate issue severity and impact** | **3. Create remediation plan** | **4. Execute controls to resolve issue**

3. CONCLUSION

Today, there is minimal guidance from regulators on how FIs must manage their relationships with vendors to mitigate data risk. Many FIs have vastly complicated vendor landscapes, and as data flows from one organization to another, there is an inherent data quality risk. This is exacerbated with direct and indirect risk stemming from relationships with third-parties, fourth-parties to N parties that are critical to maintaining their business. While current vendor risk management frameworks outline how institutions can mitigate operational and technological risk; vendors are not incentivized to sufficiently manage their data risk. Financial organizations can strengthen their vendor relationships, mitigate risk, and go beyond merely complying with regulatory reporting commitments by incorporating data management principles into their vendor due diligence.

AUTHORS

Varenya Prasad, Principal Consultant
Varenya.Prasad@capco.com

Brandon Schwartz, Consultant
Brandon.Schwartz@capco.com

REFERENCES

1. FDIC. "Third-Party Risk: Guidance for Managing Third-Party Risk." June 6, 2008. https://www.fdic.gov/news/financial-institution-letters/2008/fil08044.html
2. Ponemon Institute, IBM. Cost of a Data Breach Report. 2019 2019 Cost of a Data Breach Report (ibm.com)
3. Ponemon Institute, Data Risk in the Third-Party Ecosystem. April 2016 Data Risk in the Third Party Ecosystem_BuckleySandler LLP and Treliant Risk Advisors LLC Ponemon Research 2016 - FINAL2

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO