DATA RISK MANAGEMENT

A NEW APPROACH TO THIRD-PARTY DATA RISK

See it all, control it fully, and stay compliant

Vendia

Table of contents

When it comes to data risk management,

third-party data has long been treated as an afterthought: left to flow wild while internal and customer data sources are diligently governed and managed.

Yet times have changed, and poorly managed and unreliable third-party data flows now represent one of the fastest-growing sources of operational risk. While these essential data streams are vital to modern business, traditional methods of managing risk (and the risk management tools of years past) simply don't cut it anymore.

This eBook explores a new, more inclusive approach for managing third-party data risks: what it is, why it matters, and how to do it right.

#01

Beyond the breach:
A closer look at third-party data risks

Third-party data risks are more than just security headaches. From compliance fines to reputational damage, a single misstep can hit your business everywhere it hurts.

All up, third-party risk management (TPRM) is a well-established corporate governance activity that aims to identify, manage, and mitigate the business risks that arise when working with outside companies, such as alliance partners, vendors, suppliers, and contractors. At a broad level, TPRM programs account for a diverse range of business focuses, including risks related to data shared across one or more third parties.

This guide examines the specific risks related to managing **third-party data**, as it fits into a holistic TPRM program. Key priorities and business risks include the following:

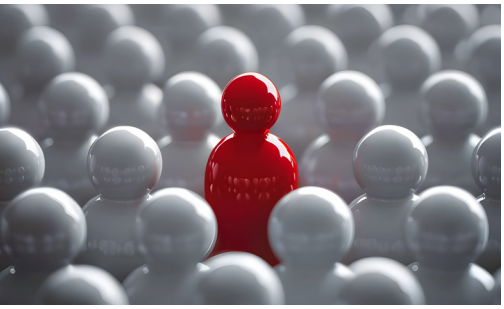
Data security

BUSINESS PRIORITY

Effectively manage all third-party data flows, ensuring business data is trustworthy and protected at all times.

RELATED RISKS

Inadequate governance exposes organizations to security breaches, unauthorized access, and lower-quality decisions.



Privacy and compliance

BUSINESS PRIORITY

Meet evolving compliance standards, assuring that data shared and used by third parties adheres to the proper legal, regulatory, and contractual requirements.

RELATED RISKS

Limited visibility into how third parties use shared business data creates significant auditing gaps, increasing compliance risks and associated costs.

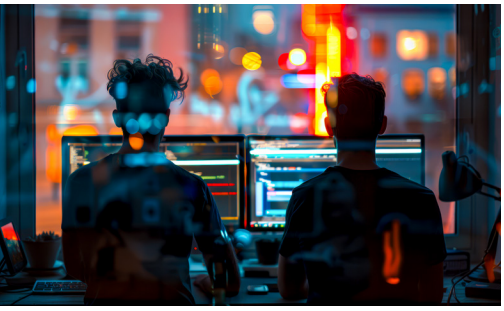
Business operations

BUSINESS PRIORITY

Ensure the business has accurate, reliable, and up-to-date information to run at its best 24/7.

RELATED RISKS

Poor-quality data disrupts everything from production schedules to on-time deliveries, customer service, and more.



Customer experience (CX)

BUSINESS PRIORITY

Deliver a seamless customer experience via secure integrations with strategic business partners, service providers, and related vendors.

RELATED RISKS

When data shared between parties isn't reliable and up to date, customers get frustrated, support teams become overwhelmed, and costs skyrocket.

Settlements and billing

BUSINESS PRIORITY

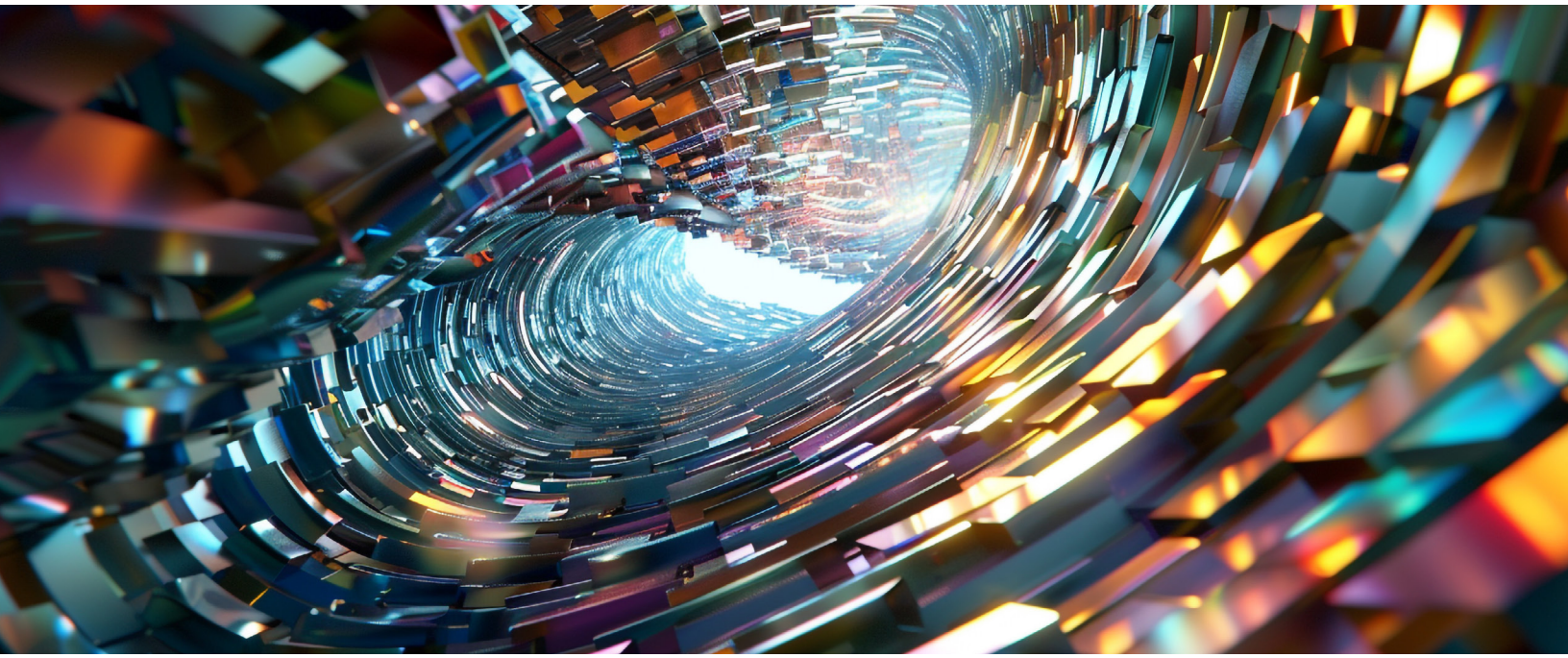
Establish, monitor, and maintain secure data exchange with third parties and ensure financial data is accurate, trustworthy, and protected.

RELATED RISKS

Any doubts over data accuracy or security bring about costly coping mechanisms like manual verification, additional auditing, and more.

#02

Guarding the gates:
Ensuring accurate, secure data flows



Effective third-party data risk management hinges on continuous oversight of two key areas: inbound and outbound data flows.

In the past, organizations relied primarily on internal data to fuel business operations and inform analytics. In today's business world, third-party data is a near-universal tool. Companies rely on it to achieve a range of benefits, such as enhancing customer experiences, preventing fraud, building tailored marketing campaigns, and much more.

But as reliance on third-party data soars, managing a continuous flow of data grows increasingly difficult—especially now that business units can easily acquire their own data sources, independent of IT. Left unnoticed or managed poorly, third-party data streams can become a backdoor for unreliable information and operational risk to sneak in.

Consequences of poorly managed outbound data

When outbound data is poorly managed, or an organization lacks visibility and control over how their data is used by external parties, the risks of security breaches and unauthorized data access go up.

EXAMPLE

Imagine selling patient data to Company A, who then resells it to Company B. The problem? You now have no control over what B does with the data.

Here's the rub: Even though you're not directly involved anymore, you (and potentially A) could still be held responsible if the data ends up misused. This can lead to hefty fines, bad press, and lost business.

Consequences of unreliable inbound data

Businesses depend on third-party data to run daily operations, but without understanding where the data came from or how it was handled, organizations risk major security and decision-making vulnerabilities.

EXAMPLE

Companies like mortgage servicers rely on financial data from multiple sources. But because these data sources change quickly, recently shared data might not reflect reality—it may be stale or incomplete.

Use of this information can snowball into a host of wrong decisions, such as incorrectly classifying a mortgage's risk level, causing big problems down the line.

Bottom line? Effectively managing third-party data risks requires that businesses continuously oversee all data shared to and from outside parties.

The data risk onion:
Peeling back the layers of third-party complexity

Even with strong internal data governance practices in place, organizations face additional layers of complexity when managing data flows with external sources.

1. Limited visibility and control

Limited visibility into how other parties collect, store, and secure data makes it difficult to enforce consistent data governance policies and standards across third-party data ecosystems.

2. Varying data practices

Further complicating matters, each third party may have its own data practices, potentially creating confusion and increasing the risk of security breaches or data misuse.

These practices often vary across countries and geographies as well. For example, data use that's acceptable in one region might be inappropriate in another (or for a business partner).

3. Lack of standardization

The lack of standardized data formats and exchange protocols across different partners and vendors adds further friction between integrated systems, potentially compromising data quality.

4. Contractual complexities

Negotiating data-usage terms and ensuring ongoing compliance is another significant hurdle. Clearly defining data ownership, usage rights, and security responsibilities within contracts with third parties is crucial but not always easy to enforce.

5. Evolving regulations

Finally, ever-evolving regulatory landscapes with data privacy regulations such as GDPR and CCPA place compliance burdens on both the organization and its partners, requiring constant vigilance and resource allocation to ensure everyone remains compliant.

#03

Why existing data infrastructure falls short

Rapid shifts in technology, regulations, social attitudes, and laws create a data governance paradox for today's organizations.

While faster data sharing is certainly a benefit of modern technology, it presents a double-edged sword: Managing third-party data flows becomes increasingly complex despite society demanding stronger data protections. Legal and regulatory frameworks—which once allowed organizations to largely ignore data outside their four walls—now hold companies wholly accountable for their data, and the data they possess, regardless of where it came from or travels to.

This growing urgency for secure, compliant external data exchange is fast-outpacing the capabilities of traditional data infrastructure, despite its many databases, data lakes, data catalogs, and ETL tools. The reason? Nearly every data tool that exists today is built for the old world—**designed around the outdated assumption that all business data is owned by a single company or entity.**

This outdated assumption crumbles in today's world, where data flows continuously between a bevy of external and internal sources. Thus, limitations of traditional data tools in managing third-party data egress and ingress introduce the following risks:

1. Data egress

Businesses readily share data with external partners without the ability to transmit crucial metadata about its integrity, source, compliance requirements, and other important details. This lack of context creates significant risks for all parties, leading to downstream problems such as partners failing to comply with GDPR requests or mishandling protected health information (PHI).

Not knowing how third parties access and use shared business data also exposes companies to big risks. In many cases, once data leaves the business, there might not be anyone who knows where it ends up or how it's being used. Blind spots inside existing tools leave business leaders grappling with unanswered questions like:

I. Who can access our data and in what systems? How is it being used?

II. How can we assure partners that data they've shared with us is secure and being used properly when passed along to a third party?

III. What partners are at risk of non compliance and how do we assess potential business impacts?

2. Data ingress

Another big mistake business leaders make is treating inbound data as inherently reliable when its origin, classification, and security are often undisclosed or unclear. They also lack the ability to effectively track and manage data (and metadata) received from third parties.

Even with ways to track external data via data catalogs, knowing what information to include in the first place is often unknown. Without this proper guidance, data catalogs become far less effective.

This lack of provenance, or data history, inside current data infrastructure brings about major security risks, with leaders struggling to answer basic questions about their data:

I. Where did this data come from?

II. How confident are we in the data's integrity? Is it complete? Accurate? Up to date?

III. How can we use this data? Are we allowed to share it with others and under what conditions? What legal, compliance, and regulatory programs is it subject to? How would using it alter our eligibility for such programs?

IV. How risky is this data? Is it subject to systematic bias? Generated by an AI? Are there broader social implications of relying on it, divulging it, or promoting it as our own?

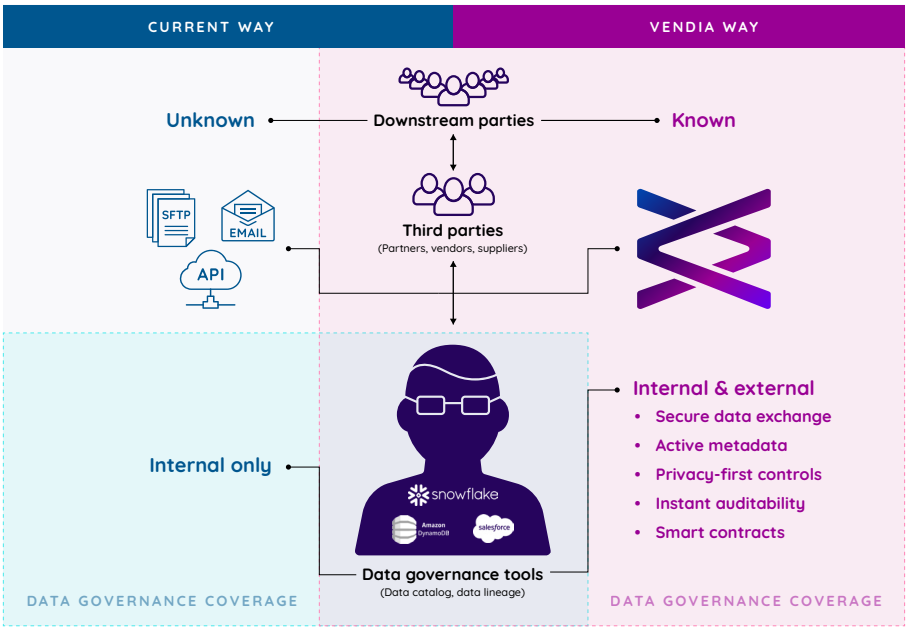
In short, current data infrastructure is ill-equipped to handle the complexities of modern data sharing—especially when dealing with continuous, multi-party data flows.

#04

A new approach to third-party data risk management

Third-party data risks demand more than traditional methods. They require 24/7 monitoring, rigorous controls, and continuous governance.

Unlike traditional data infrastructure, modern data automation platforms like Vendia are purpose-built for zero-trust, multi-party environments. The key advantage lies in its underlying distributed ledger technology foundation: an immutable, auditable transaction ledger that lets multiple parties securely exchange data (and metadata) while tracking data movement across all internal and external business tools.

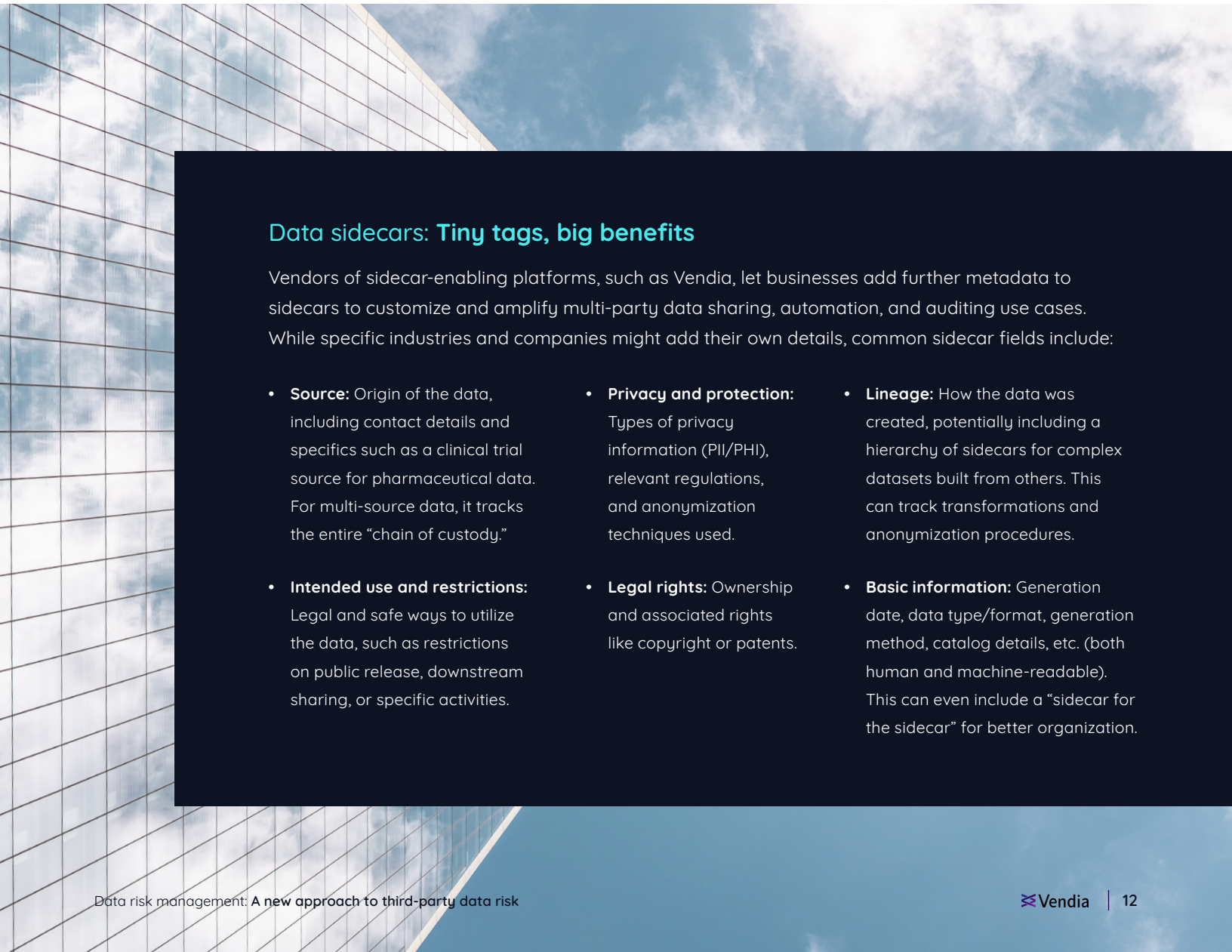


The following capabilities and benefits help businesses gain extended visibility and governance over data exchanged across third parties, reducing the risk of breaches, ensuring compliance, and streamlining risk management.

1. Secure, contextual data exchange

Collaborating securely with partners requires exchanging accurate, contextual information about the business data being shared. This is where having distributed ledger technology inside a data automation platform delivers significant advantages, providing the ability to attach critical metadata, often called "sidecars," to shared business data.

This helps ensure that data is being used responsibly, ethically, and in compliance with regulations, no matter what external system it lives in. Because this information is stored securely via an immutable distributed ledger, all parties can trust that the data being shared is both accurate and trustworthy.



Data sidecars: **Tiny tags, big benefits**

Vendors of sidecar-enabling platforms, such as Vendia, let businesses add further metadata to sidecars to customize and amplify multi-party data sharing, automation, and auditing use cases. While specific industries and companies might add their own details, common sidecar fields include:

- **Source:** Origin of the data, including contact details and specifics such as a clinical trial source for pharmaceutical data. For multi-source data, it tracks the entire "chain of custody."
- **Intended use and restrictions:** Legal and safe ways to utilize the data, such as restrictions on public release, downstream sharing, or specific activities.
- **Privacy and protection:** Types of privacy information (PII/PHI), relevant regulations, and anonymization techniques used.
- **Legal rights:** Ownership and associated rights like copyright or patents.
- **Lineage:** How the data was created, potentially including a hierarchy of sidecars for complex datasets built from others. This can track transformations and anonymization procedures.
- **Basic information:** Generation date, data type/format, generation method, catalog details, etc. (both human and machine-readable). This can even include a "sidecar for the sidecar" for better organization.

2. Always-on governance and auditability

Auditing third-party data access and usage manually is a slow, painfully ordeal. Unlike traditional governance tools, data automation platforms like Vendia deliver instant third-party auditing and continuous governance capabilities via a tamper-proof record of all data interactions across partners.

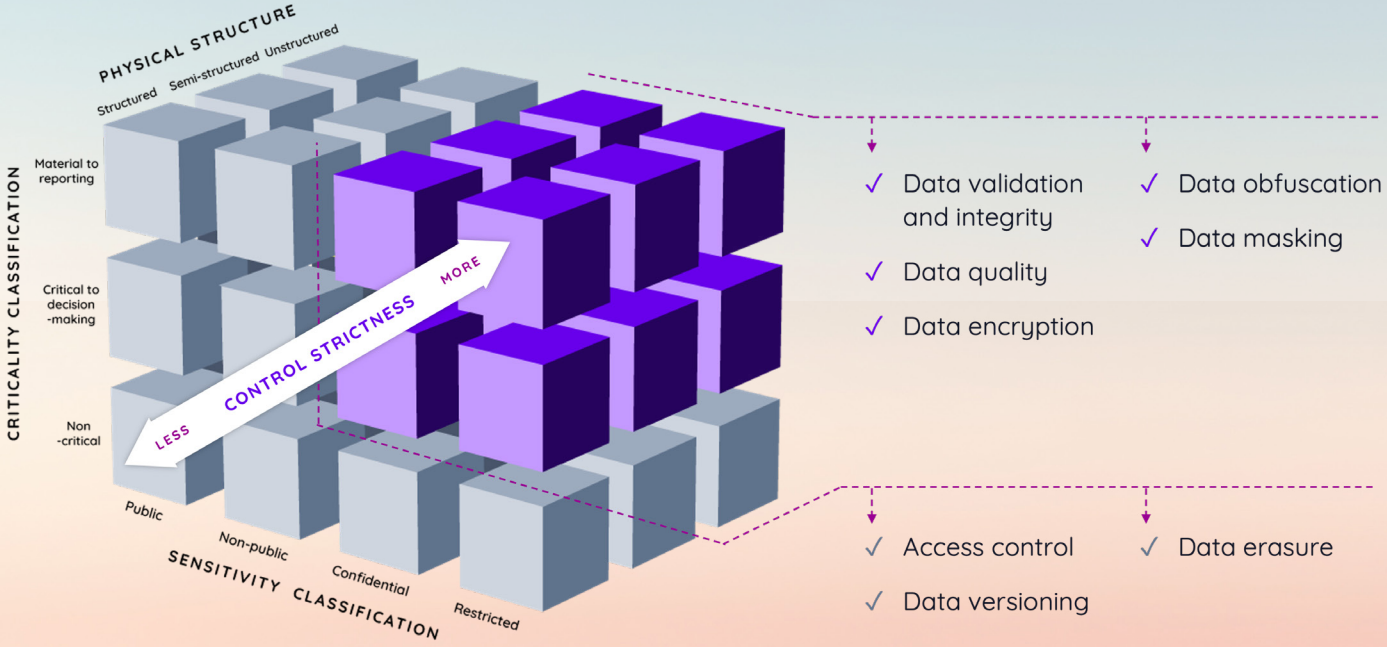
Comprehensive audit trails and data lineage provide a clear view of data movement, with features like data-access change tracking and read receipts offering a deeper, real-time look at potential and emerging third-party risks. This makes compliance audits and reports easier, builds trust with partners, and helps IT teams proactively identify and mitigate threats faster—all while saving time and resources.

3. Privacy-first data controls

New and evolving data privacy regulations like HIPAA, GDPR, and CCPA make sharing personal information (e.g., PII) with other parties increasingly complicated. Vendia's underlying foundation includes purpose-built ledgering technology to support GDPR's right to erasure. Robust data privacy features such as masking, tokenization, and erasure further simplify and streamline compliant data flows between all external parties and systems.

Businesses also retain full control over their shared data at all times, no matter what external system, cloud, or application it lives in. They can choose exactly what information to withhold or disclose to partners using granular access controls, such as permissions based on record and individual fields. They can also see who can access their data, how it's used, when it was last accessed, and so forth at any time.

Vendia simplifies secure, compliant data exchange with external parties by offering a tiered approach to data control, ensuring the right level of protection for sensitive information.



4. Streamlined risk management

Automated risk management is another big benefit of modern data automation technology. For example, Vendia instantly reconciles and standardizes all data shared across the business network, reducing data inconsistencies, errors, and other operational vulnerabilities. Companies can also score partners and vendors based on potential risks, helping them prioritize where to focus first.

Access controls, continuous monitoring, and automated workflows further streamline onboarding procedures. For example, automating data-sharing policies via Vendia lets business leaders quickly add or expand strategic partnerships while keeping tight control over the data they have access to. This not only saves time, but greatly reduces the risk of data access leakage.

5. Smart contract enforcement

Keeping constant watch over third-party data handling can also be a nightmare, especially when partners don't share the same commitment to data security or operate under different legal frameworks. These disparities often create loopholes where enforcing proper data handling becomes difficult.

Smart contracts in Vendia automate and uphold critical data governance processes in real time, freeing up valuable time and resources. These self-executing contracts automatically track and enforce data usage rules with third parties, preventing unauthorized data access and flagging any suspicious activity before it's too late.

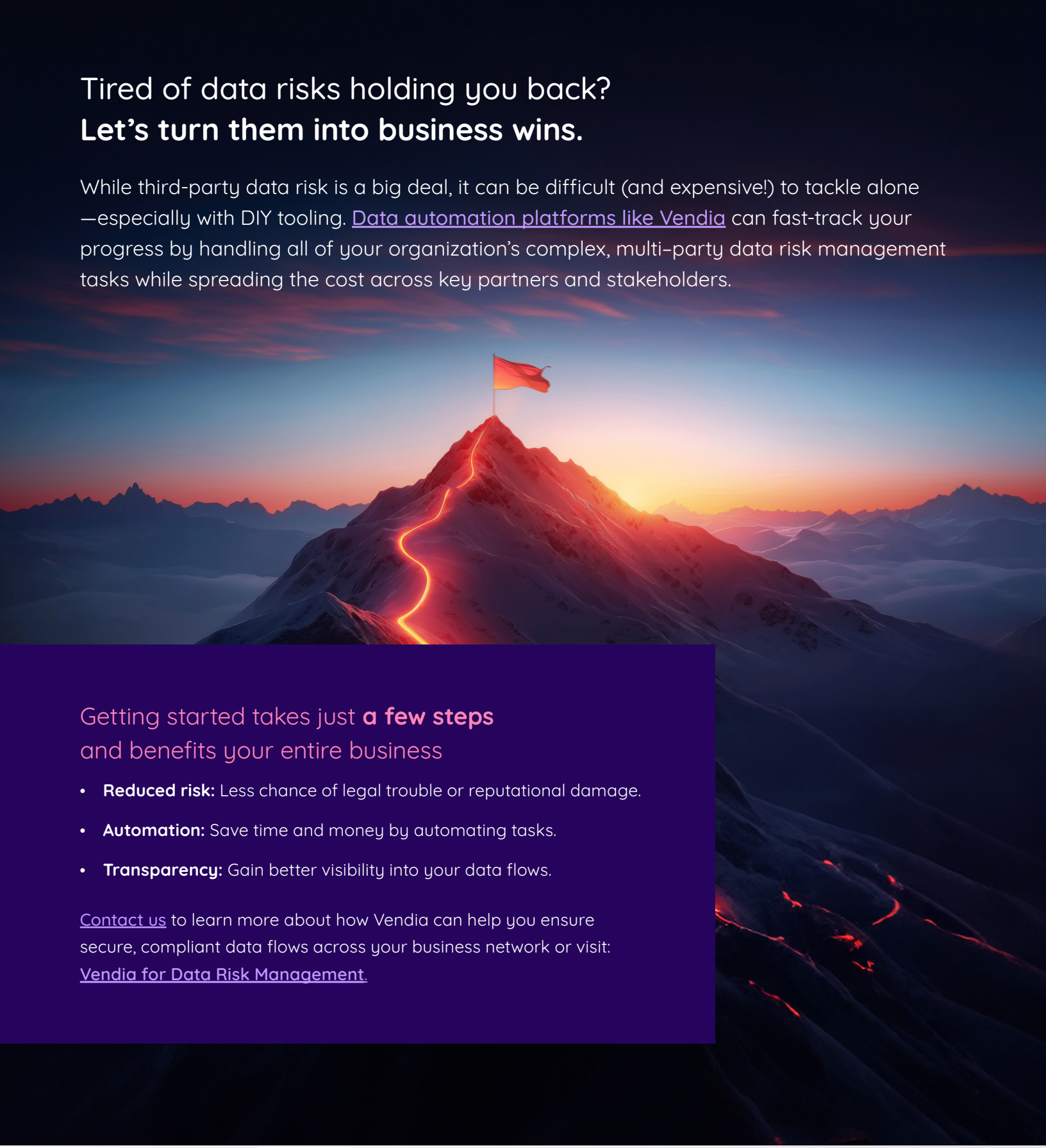
6. Interoperability at any scale

Finally, modern data automation tools work seamlessly with existing data infrastructure and governance tools. Platforms like Vendia can be leveraged alongside any system, cloud, or application to gain immediate visibility across third-party networks—without disrupting existing workflows.

Vendia is also uniquely designed to scale alongside new and evolving business needs. Businesses can start simple by using data-sharing capabilities and pre-built reports for higher-priority use cases, then expand or add on as needs change. This approach not only keeps business costs down, but helps avoid the hassle of large-scale deployments. It also ensures that companies can effectively manage third-party data risks across their entire network, regardless of scope or size.

Tired of data risks holding you back?
Let's turn them into business wins.

While third-party data risk is a big deal, it can be difficult (and expensive!) to tackle alone—especially with DIY tooling. Data automation platforms like Vendia can fast-track your progress by handling all of your organization's complex, multi-party data risk management tasks while spreading the cost across key partners and stakeholders.



Getting started takes just **a few steps** and benefits your entire business

- **Reduced risk:** Less chance of legal trouble or reputational damage.
- **Automation:** Save time and money by automating tasks.
- **Transparency:** Gain better visibility into your data flows.

Contact us to learn more about how Vendia can help you ensure secure, compliant data flows across your business network or visit: Vendia for Data Risk Management.

About Vendia

Vendia is the future of collective data intelligence, combining smart APIs, databases, and distributed ledger technology inside a single platform. Vendia's data automation cloud makes it easy to share data inside and outside of the organization in real time and with full visibility, governance, and control. Companies such as BMW, Delta Airlines, Resolution Life Insurance, and Fannie Mae use Vendia to automate contextual and compliant data flows between any-to-any systems for a harmonized, accurate view of data that unlocks speed, innovation, and cost savings. Learn more about us at Vendia.com and #UnchainYourData with Vendia.