Veridion™ AI business intelligence

Securing Third Party Risk Management with the Right Data

Data-Driven Strategies to Safeguard Your Business Against Third and even Fourth Party Risks.

Third Party Risk Management (TPRM) is one of the top concerns for a wide variety of industries and departments, as the business world is becoming more and more interconnected. The global challenges of the past few years (a pandemic, wars, supply chain disruptions, climate change, etc.) have highlighted just how linked together we are. Unfortunately, these challenges also highlighted the degree of risk to which we are all exposed to, derived from these long and sometimes hard to visualize global business chains.

In this context, third party risk management emerged as a top executive concern and has become a crucial agenda for any company large enough to be exposed to a high degree of risk from the multitude of third parties they are working with. Here's what you need to know about managing it and for defining your company's data needs for a third party risk management framework that can keep you safe.

A. The Basics of Third Party Risk Management

A1. What Is Third Party Risk Management (TPRM)?

Third Party Risk Management is the systematic process of identifying, assessing, and mitigating the risks posed by external entities - such as vendors, suppliers, partners, contractors, customers and service providers - that interact with an organization. These third parties can impact the organization's operations, data security, regulatory compliance, and reputation.

TPRM involves establishing policies and procedures to ensure that these third parties adhere to the organization's standards and regulatory requirements, thus minimizing potential threats. The scope of a solid third party risk management policy covers a wide range of risks, including cybersecurity threats, financial instability, regulatory compliance, and operational disruptions.

A2. Why Is Third Party Risk Management Important?

The importance of TPRM cannot be overstated in today's interconnected business environment. Organizations rely on third parties for various services, including IT support, supply chain logistics, and financial services. A failure or breach within any of these third parties can have severe repercussions for the organization.

For instance, a cybersecurity breach at a third-party vendor can lead to data loss, legal penalties, and damage to the organization's reputation. Moreover, regulatory bodies are increasingly holding companies accountable for the actions of their third parties, making robust TPRM practices essential for compliance and risk mitigation.

Effective third party risk management strategy helps organizations maintain operational continuity, protect sensitive information, and uphold their reputation, ultimately contributing to long-term business success.

A3. What Is the Difference Between a Third Party and a Fourth Party When It Comes to Risk

There is a lot of attention in executive business circles given to the issue of fourth parties when addressing TPRM, up to the point of questioning whether organizations actually need a fourth party risk management framework in addition to the classic 3rd party one.

Whatever the approach to a fourth party risk management framework, it all starts with the same building blocks as a good third party risk management framework: solid, reliable data.

Before we move towards the data needed for a good TPRM framework, let's first clarify the distinction between third parties and fourth parties in the context of risk management.

A third party is any external entity that has a direct relationship with the organization. This includes vendors, service providers, and contractors. Fourth parties, on the other hand, are the entities that these third parties engage with. For example, if a company outsources its IT services to a third-party provider, and that provider, in turn, uses another company for data storage, the data storage company is considered a fourth party.

The distinction between third and fourth parties is crucial in risk management because the organization has less direct control and visibility over fourth parties. **Managing fourth-party risk requires ensuring that third parties have strong TPRM practices of their own.** This involves extending the organization's risk management protocols to encompass the entire supply chain, thereby mitigating risks that could indirectly impact the organization.

A4. Who Should Care about Third Party Risk Management?

Everyone within an organization should be aware of and care about TPRM, but it is particularly crucial for certain roles:

- **Chief Risk Officers (CROs):** Responsible for the overall risk management strategy, including the risks posed by third parties.
- **Chief Information Officers (CIOs):** Concerned with the security of information systems and data, which can be compromised through third-party relationships.
- **Compliance Officers:** Ensure that third-party engagements comply with relevant laws and regulations.
- **Procurement Managers:** Oversee the acquisition of goods and services from third parties, making them pivotal in the initial risk assessment.
- **Legal Teams:** Involved in drafting and reviewing contracts with third parties to include necessary risk mitigation clauses.

There are also a few industries that stand to benefit more from having solid third party risk management protocols in place, namely those industries where working with a huge number of third parties is the norm. **IT services and procurement** are some of the top names in this category.

Incidentally, we at Veridion are specialized particularly in serving these industries with the data they need for creating good TPRM practices. Let's take a look at how third party risk is approached in IT services and in procurement, based on our direct experience with our customers and partners from these spaces.

Example #1:

Special Case Spotlight: Third Party Risk Management Service Industry

Scenario:

Company X, a leading provider of third-party risk management (TPRM) solutions, offers an advanced platform designed to help organizations manage and mitigate risks associated with their vendors and suppliers. Company X has a robust client base that spans multiple industries, including finance, healthcare, and manufacturing. However, despite their advanced technology and comprehensive risk assessment tools, they face a significant third-party risk breach.

Incident:

Company X relies on various data sources to power its TPRM platform. One of these sources, a major third-party data provider, experiences a security breach, compromising the integrity of the data supplied to Company X. As a result, the data ingested into Company X's platform includes inaccurate and outdated information, leading to flawed risk assessments for their clients.

Impact:

Several clients, unaware of the compromised data, make critical decisions based on faulty risk assessments. For example, a healthcare client, trusting the platform's assessment, engages with a new supplier that is later found to be non-compliant with industry regulations, resulting in legal repercussions and reputational damage. Another client in the finance sector unknowingly partners with a vendor involved in fraudulent activities, leading to financial losses and increased scrutiny from regulators.

How Better Data Could Have Prevented the Breach:

1. Proactive Data Quality Monitoring:

If Company X had employed more rigorous data quality monitoring mechanisms, they could have detected anomalies in the data sooner. Regular audits and validation checks would have identified discrepancies, allowing them to address the issue before it impacted their clients.

2. Diversified Data Sources:

Relying on multiple data providers instead of a single source could have mitigated the risk. By cross-referencing information from various providers, Company X could have ensured a more accurate and comprehensive risk assessment, reducing dependency on any one source and minimizing the impact of a single point of failure.

3. Real-Time Data Updates:

Implementing real-time data updates and integrations would have allowed Company X to maintain the accuracy and relevance of their data continuously. This approach ensures that any changes or new information are promptly reflected in the platform, providing clients with the most current risk assessments.

4. Enhanced Data Security Measures:

Strengthening the security measures around data ingestion and integration processes could have prevented the breach. Implementing robust encryption, access controls, and regular security audits would have safeguarded the integrity of the data, ensuring that only verified and secure information enters the platform.

Remediation and Moving Forward:

In response to the breach, Company X undertakes a comprehensive review of its data management practices. They enhance their data quality monitoring systems, diversify their data sources, and implement real-time data integration. Additionally, they bolster their data security measures to prevent future breaches. By prioritizing the quality and security of their data, Company X not only regains the trust of their clients but also sets a new standard for excellence in the TPRM service industry.

Conclusion:

This case highlights the critical importance of reliable and high-quality data in the TPRM service industry. By addressing data-related challenges and implementing robust data management practices, TPRM service providers like Company X can deliver accurate risk assessments, safeguard their clients from potential risks, and maintain their reputation as trusted partners in risk management.

Example #2:

Special Case Spotlight: Procurement Industry

Scenario:

In the procurement industry, third-party risk management focuses on ensuring the reliability and compliance of suppliers. A procurement manager might work with various suppliers for raw materials. If a key supplier fails to deliver on time or provides substandard materials, it can disrupt the entire supply chain.

Additionally, suppliers must comply with environmental and labor regulations. Effective TPRM in procurement involves thorough vetting of suppliers, regular audits, and contingency planning to mitigate supply chain disruptions. The focus is on maintaining quality, ensuring compliance, and securing a stable supply chain.

Hypothetical Case Study in the Procurement Industry:

Consider a manufacturing company, ProdMakers, that relies on a third-party supplier, PartSupply, for crucial components. PartSupply, however, fails to meet its delivery deadlines due to financial difficulties, leading to a significant disruption in ProdMakers' production line and resulting in substantial financial losses.

How the Breach Occurred:

- Inadequate Financial Assessment: ProdMakers did not thoroughly assess PartSupply's financial health before entering into the contract.
- Poor Supply Chain Visibility: There was a lack of visibility into PartSupply's supply chain, which included fourth-party suppliers experiencing their own disruptions.
- Reactive Approach: ProdMakers lacked a proactive risk management strategy, reacting only after the disruption occurred.

How Better Business Data Could Have Prevented the Breach:

- Financial Health Monitoring: Access to Veridion's business data could have provided ProdMakers with early warning signs and risk signals that could have shed light earlier on PartSupply's financial instability.
- Supply Chain Transparency: Veridion's data solutions would offer insights into PartSupply's entire supply chain, highlighting potential risks from fourth-party suppliers.
- Proactive Risk Management: With comprehensive business data, ProdMakers could have implemented a more proactive risk management strategy, including contingency plans for supplier disruptions.

Ready for a real case study from the procurement industry?

→ **Tier 1 consulting firm sees 2.5x increase in supply chain intel depth**

A5. The Main Layers of Third Party Risk Management

There are many ways to approach third party risk, and we can define them as layers, since all of these aspects need to be covered in a good TPRM plan:

- Cybersecurity
- Legal aspects
- Flow of physical goods
- Flow of digital information

A good TPRM framework also involves multiple steps to comprehensively manage risks, and these can also be defined as layers considering that there are sometimes different task forces assigned to each:

- **Identification:** Cataloging all third parties and understanding their roles within the organization. This includes gathering information on their business practices, financial stability, and any previous incidents of non-compliance or breaches.
- **Assessment:** Evaluating the risk each third party poses based on factors such as the nature of the services they provide, their access to sensitive information, and their regulatory environment. This can involve quantitative scoring models and qualitative assessments.
- **Mitigation:** Implementing measures to reduce identified risks. This could involve establishing clear contractual obligations, setting up security controls, and requiring third parties to adhere to specific compliance standards.
- **Monitoring:** Continuously tracking third-party activities and risk profiles. This involves regular audits, performance reviews, and real-time monitoring of third-party systems and processes to ensure ongoing compliance and risk management.
- **Response:** Developing and executing response plans for incidents involving third parties. This includes having clear protocols for communication, remediation, and legal action if necessary. It also involves working with third parties to address and resolve issues promptly.

What are the main areas to focus on for effective TPRM?

To build a robust Third-Party Risk Management (TPRM) framework, it is essential to focus on the following critical risk areas. Veridion's comprehensive data solutions can help you gain better control and visibility in each of these areas:

Foreign Ownership, Control, or Influence (FOCI)

Assess the extent of foreign ownership and influence on your third parties to mitigate risks related to geopolitical instability and compliance with international regulations. Veridion provides detailed corporate family linkages and ownership structures, enabling you to identify and manage FOCI risks effectively.

Regional Risk

Evaluate the regional risks associated with the geographic locations of your third parties, including political stability, regulatory environment, and regional economic conditions. Veridion's extensive global data coverage ensures you have accurate regional information, helping you make informed decisions about regional risks.

Operational Risk

Ensure comprehensive assessments of operational risks, including worker safety and compliance with occupational health standards. Understanding workman's comp and worker safety protocols can prevent significant operational disruptions and liabilities. Veridion's firmographic data includes detailed insights into operational practices, helping you identify and mitigate operational risks.

Cyber Risk

Prioritize the assessment of cybersecurity measures in place with your third parties. The increasing frequency of cyber-attacks necessitates robust cyber risk management to protect sensitive data and ensure business continuity. Veridion's data enrichment services provide up-to-date information on third-party cybersecurity practices and vulnerabilities, helping you stay ahead of potential threats.

Supply Chain Risk

Analyze the resilience and reliability of your supply chain, including risks associated with single-source dependencies, logistical challenges, and potential disruptions. Veridion's robust search functionality allows you to discover new suppliers and assess the resilience of your current supply chain, ensuring continuity and minimizing risks.

Financial Health Risk

Examine the financial stability and health of your third parties to avoid business continuity issues due to financial instability or insolvency. Veridion offers comprehensive financial data, enabling you to monitor the financial health of your partners and make informed decisions to mitigate financial risks.

Product Risk

Understand the risks associated with the products and services provided by your third parties, including quality assurance and compliance with industry standards. Veridion provides detailed product and service information, helping you assess product risks and ensure compliance with necessary standards.

Environmental, Social, and Governance (ESG) Risk

Evaluate the ESG practices of your third parties to ensure they align with your company's values and regulatory requirements. Veridion's unique operating insights include ESG data, enabling you to assess and monitor the sustainability and ethical practices of your third parties effectively.

Focusing on these areas with accurate and up-to-date data from Veridion ensures that your TPRM framework is comprehensive and effective, providing the insights needed to mitigate risks and maintain operational resilience.

A6. Mitigating Challenges from Political or Economic Sanctions with Data-Driven TPRM

In a globalized business environment, political and economic sanctions pose significant risks to supply chains and service networks. Access to reliable and comprehensive data is crucial for mitigating these risks.

Here's how a data-driven Third Party Risk Management (TPRM) framework can help:

1. **Early Detection and Monitoring**

   Comprehensive Data Sources: Integrating data from government databases, international watchlists, and real-time news feeds helps identify potential sanctions risks early.
   Continuous Monitoring: Automated tools within a TPRM framework provide ongoing surveillance of third parties, ensuring timely alerts about sanctions-related developments.

2. **Enhanced Due Diligence**

   In-Depth Investigations: Reliable business data enables thorough due diligence, including verifying ownership structures and compliance histories to ensure third parties do not pose sanctions risks.
   Screening Against Sanctions Lists: Regular screening of third parties against international sanctions lists helps identify and avoid entities subject to sanctions.

3. **Regulatory Compliance**

   Automated Compliance Checks: Automated checks ensure all third-party relationships comply with international sanctions regulations, reducing the risk of legal penalties and reputational damage.
   Documentation and Reporting: Maintaining comprehensive records of due diligence and compliance activities is essential for demonstrating adherence to regulatory requirements.

Hypothetical Examples

Example 1: Export Bans and Sanctions (Uyghur-related)

Scenario:

A technology company sources components from a supplier in a region linked to Uyghur forced labor.

Action:

Using a data-driven TPRM framework, the company identifies the supplier's risk through comprehensive data sources and continuous monitoring. Detailed due diligence reveals potential human rights violations, and the supplier is flagged for sanctions compliance risks.

Outcome:

The company swiftly replaces the high-risk supplier with an alternative, ensuring compliance with export bans and maintaining its ethical standards. Access to reliable data allows the company to act proactively, avoiding legal repercussions and protecting its reputation.

Example 2: Risk of Working with Subsidiaries of Sanctioned Companies

Scenario:

A pharmaceutical firm unknowingly collaborates with a subsidiary of a company under international sanctions.

Action:

The company's TPRM framework screens all third parties against sanctions lists and uncovers the subsidiary's connection to a sanctioned parent company. Enhanced due diligence and data analytics reveal the extent of the relationship and potential compliance issues.

Outcome:

The pharmaceutical firm terminates the relationship with the subsidiary, mitigating the risk of sanctions violations. By leveraging reliable data, the firm ensures its supply chain remains compliant and resilient against regulatory risks.

B. Creating a Third Party Risk Management Framework with Reliable Data

B1. Why Data Matters for Third Party Risk Management

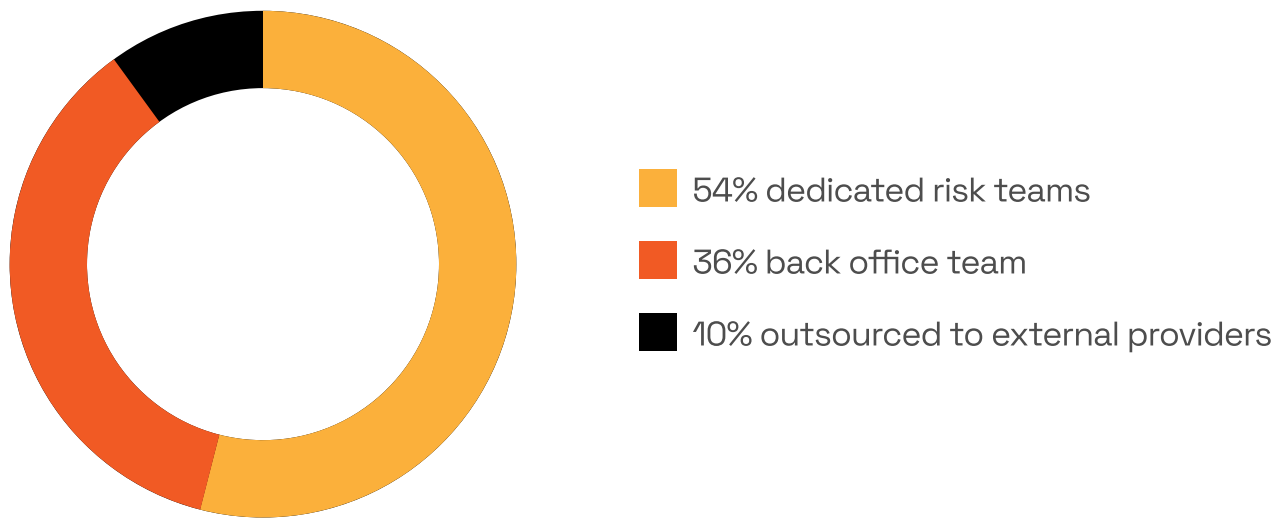
Data is the foundation of effective TPRM. Accurate and reliable data about third parties enables organizations to make informed decisions about their risk exposure. This data includes financial health metrics, compliance history, cybersecurity measures, and performance records. Without reliable data, organizations are left to make assumptions or rely on incomplete information, increasing their risk exposure.

For example, Veridion's data solutions provide comprehensive insights into third parties, helping organizations to accurately assess risks and make informed decisions. This data-driven approach ensures that risks are identified early and managed proactively, rather than reactively dealing with issues as they arise. By leveraging high-quality data, organizations can enhance their TPRM processes, ensuring they are robust, efficient, and effective.

B2. How to Start Approaching Third Party Risk Management, Hands-on

A recent survey by Panorays on third-party risk management priorities revealed the following insights into how companies approach TPRM:

- In more than half of the cases **(54%)**, dedicated IT and Risk teams, which possess specific technological expertise, are responsible for third-party cyber risk management. These teams typically include Operations and Logistics, Compliance and Privacy, Information Security, Risk Management, and Technology or IT departments.
- In **36%** of the cases, the responsibility falls to the Back Office Team, which comprises Legal, Finance, and Procurement departments. These teams often manage tasks such as handling cyber questionnaires, onboarding third parties into internal systems, and processing payments.
- A smaller portion **(10%)** of companies outsource their third-party risk management to external service providers. This approach is more common in enterprises with fewer than **5,000** employees.



Better business data can significantly enhance the effectiveness of these teams by providing comprehensive and up-to-date information on third-party vendors. Reliable data enables IT and Risk teams to perform more accurate risk assessments, ensuring that potential vulnerabilities are identified and addressed promptly.

For Back Office Teams, access to detailed vendor information facilitates smoother onboarding processes and more precise compliance checks, reducing the likelihood of overlooking critical risks.

Even for organizations that outsource these functions or who provide these outsourced services to others, **leveraging high-quality data from sources like Veridion** ensures that external providers have the necessary insights to manage risks effectively.

Lessons Learned in the Past Year Dealing with TPRM:

Increased Supply Chain Attacks and Third-Party Breaches:

The past year has seen a rise in significant digital supply chain attacks, such as those targeting MOOVEit and Citrix Netscaler, as well as third-party breaches involving companies like Okta and Dollar Tree or, even more concerning the recent breach of the UK military via third parties.

These incidents underscore the urgent need for enhanced visibility across the entire third-party ecosystem, including the identification and mapping of fourth, fifth, and subsequent parties. Access to reliable and comprehensive business data is crucial for achieving this visibility and mitigating risks.

Third Parties as Entry Points for Malicious Fourth Parties:

Third parties continue to provide avenues for cybercriminals to launch attacks. While enterprise-level companies often have the budget and resources to invest in robust cybersecurity solutions, they need to also have transparent security requirements well communicated across the third party chain.

Understanding the Criticality of Third Parties:

As supply chains grow in complexity and the number of third-party risks increases, it is imperative for organizations to assess the criticality of each vendor to their operations. This involves determining the importance of each vendor's role and the sensitivity of the data shared with them.

Organizations must then monitor these vendors regularly and maintain open communication with key third parties to address and remediate any threats or vulnerabilities as they are identified. High-quality data can significantly enhance this process, enabling more accurate assessments and proactive risk management.

B3. Defining a Third Party Risk Management Framework

Creating a TPRM framework involves several key steps.

#1. Data Collection:

Good data is the essential foundation for any risk management initiative. Nothing solid can be built in its absence. So, the first step is accessing comprehensive data on all third parties.

This includes financial information, compliance records, cybersecurity measures, and performance metrics. Reliable business data sources, such as those provided by Veridion, are crucial at this stage to ensure accuracy and completeness.

#2. Risk Assessment:

Once data is collected, the next step is to assess the risk posed by each third party. This involves analyzing the data to identify potential risks, such as financial instability, non-compliance, or cybersecurity vulnerabilities. Advanced analytical tools can help in quantifying these risks and prioritizing them based on their potential impact.

#3. Risk Mitigation Strategies:

Developing strategies to mitigate identified risks is the next step. This could involve setting up contractual safeguards, implementing specific security measures, and requiring regular compliance audits with the third parties you work with. The goal is to reduce the likelihood and impact of risks associated with third parties.

#4. Ongoing Monitoring:

Continuous monitoring of third-party performance and risk profiles is essential. This involves real-time tracking of third-party activities, periodic reviews, and audits to ensure ongoing compliance and risk management. Automated monitoring tools can provide alerts and updates on any changes in third-party risk status.

#5. Incident Response Planning:

Establishing clear protocols for responding to incidents involving third parties is crucial. This includes having predefined communication channels, remediation plans, and legal actions ready to be executed in case of a breach or failure. Regular drills and simulations can help ensure that the organization is prepared to respond effectively. You can also conduct an internal audit to evaluate readiness to deal with third party breaches.

#6. Review and Improvement:

The final step is to regularly review and update your TPRM framework. This involves assessing the effectiveness of current strategies, identifying areas for improvement, and adapting to new risks and regulatory changes. Continuous improvement ensures that the TPRM framework remains robust and effective in managing third-party risks.

By following these steps and leveraging reliable data from sources like Veridion, organizations can create a comprehensive TPRM framework that effectively manages third-party risks and enhances overall operational resilience.

B4. Common Challenges in Developing Third Party Risk Management

Whether a company is working on third party risk management measures for itself or for other parties, as a service provider or as an employer of multiple third parties, the most common challenges encountered always stem from insufficient data.

Internal Data Asset Challenges:

One of the primary obstacles in developing an effective third-party risk management (TPRM) program is the burden of building and maintaining an internal data asset. Tracking and monitoring supplier and business information requires significant resources and expertise. The complexity and resource intensity of this task can divert attention from core business activities, leading to inefficiencies and potential oversight of critical risk factors.

Difficulty Acquiring Global Data:

Effective TPRM necessitates comprehensive and accurate global business information and profiles. However, vendors often struggle to acquire such data due to variations in data availability and quality across different regions. The lack of standardized global data hampers the ability to perform thorough risk assessments and undermines the overall effectiveness of the TPRM program.

Need for Updated Information:

Continuous access to updated and recent information is vital for accurate and reliable risk assessments. The dynamic nature of business environments means that risk profiles can change rapidly. Without timely updates, risk management strategies may rely on outdated data, leading to ineffective decision-making and increased vulnerability to emerging threats.

Dependence on Existing Providers:

Many vendors rely heavily on established data providers like Dun & Bradstreet (D&B) for their risk management needs. While these providers offer extensive data, they may not always meet the specific requirements for robust TPRM. Issues such as limited data breadth, depth, or timeliness can hinder the ability to make informed risk assessments, necessitating a more diverse and comprehensive approach to data sourcing.

Downstream Processes Relying on Quality Data:

The quality and comprehensiveness of company data are critical for various downstream processes and analytics. These processes include data segmentation, adding descriptive information, and enhancing models and procedures used to generate insights for customers, such as n-tier supply chain maps. Poor-quality data can compromise these downstream activities, leading to inaccurate insights and ineffective risk management strategies.

By addressing these common challenges, organizations can develop a more effective TPRM program. Leveraging high-quality, comprehensive, and up-to-date data is essential for overcoming these obstacles and ensuring a robust approach to managing third-party risks.

As you will see if you sign up for a demo of Veridion's data (just drop us a line at contact@veridion.com), **Veridion is in a unique position to help organizations solve their data problems in order to ensure a solid foundation for TPRM.**

Why is that? Here are just a few reasons why Veridion's data can be critical to ensuring TPRM success:

- **Unparalleled Data Accuracy:** Veridion data consistently outperforms any competitor in regards to data accuracy rates, both in specific categories and overall, thanks to our proprietary AI-fueled algorithms that discern the likelihood of veracity between multiple and often conflicting data sources.
- **Encompassing Coverage of Veridion Data Universe:** Our data coverage in terms of geographical and industry criteria far surpassed any other available source of business data online. Expand your supplier business intelligence into traditionally poorly-covered areas and stay on top of business opportunities and risks.
- **Next-Gen Data Structure and Classification:** By working with our data, you'll soon discover how easy it is to accomplish your supplier enrichment goals and your general supplier discovery and supplier database management, thanks to how well structured our data is.
- **Optimal Data Freshness:** Our AI-fueled algorithms crawl the entire internet to bring you the freshest business data available in order for you to fulfill your business needs. The entire database of decision-grade data that Veridion offers is updated weekly, so you can focus on what matters most and never have to worry about data freshness.

B5. The Framework of Veridion Data for Third Party Risk Management

Here is an overview of the main data points from the Veridion Data Universe that are commonly used by our customers and partners for managing their third party risk.

Veridion Universe Data Category	Description	Relevance for Third Party Risk Management
Company Firmographic Details	Employee count and estimated revenue	Financial risk assessment
Company locations	All Locations (HQ + All Secondary Locations)	Geopolitical risk assessment
Registry information	Registered Name, Registered Country Code, Registered Country, Registered Region, Registered City, Registered Postcode, Registered Street, Registered Street Number, Registered Latitude, Registered Longitude, Registered Primary Phone, Jurisdiction, Legal Form, Company Status, Year Incorporated, Date Incorporated, LEI, EIN, VAT ID, Registry ID	General risk assessment, fraud and financial risk signals in particular.
Industry classifications	NAICS 2022 Primary Code, NAICS 2022 Primary Label, NAICS 2022 Secondary Codes, NAICS 2022 Secondary Labels, Primary NAICS Snippet, Secondary NAICS Snippet, SIC Code, SIC Label, ISIC 4 Code, ISIC 4 Label, NACE Rev2 Code, NACE Rev2 Label	Compliance and ESG risk monitoring.

Veridion Universe Data Category	Description	Relevance for Third Party Risk Management
Product data	Root Domain, Company ID, UNSPSC Class Name, Name, UNSPSC Class, UNSPSC Family Name, UNSPSC Family, UNSPSC Segment Name, UNSPSC Segment	Mapping vendor products down to catalog level to ensure manufacturer risk monitoring.
Corporate Family	Detailed corporate family linkages, connecting companies to their parent organizations	3rd and 4th party risk assessment
Sustainability News and Commitments	Content Type, Content headline, Content Relevant Text, Content Source URL, Content Pillar, Content Theme, Content Risk Criteria, Content Sentiment Value, Content Confidence Value, Content Publish Data	ESG risk assessment

View more data points →

These are just a few examples of the most popular data points in the Veridion data universe that our customers and partners are relying on for their third party risk management. Feel free to explore your own or contact us for a demo of Veridion's capabilities at sales@veridion.com.

Building the Third Party Risk Management Framework of Tomorrow

These are just a few examples of the most popular data points in the Veridion data universe that our customers and partners are relying on for their third party risk management. Feel free to explore your own or contact us for a demo of Veridion's capabilities at sales@veridion.com.

We know from the direct experience of our customers, partners and the work we do together that the right foundation for managing third party risk is good data. Come see for yourself how the Veridion Data Universe can help you solidify your third party risk management and build the framework you need for it.

Explore Veridion Data Universe →