coretelligent

Third-Party Risk Management Guide

4 Components that Reduce Risk and Strengthen Security

Third-party vendors and partners are deeply embedded in nearly every aspect of modern business operations. They enable companies to focus on core competencies – but they also dramatically increase exposure to risks from data breaches and threat actors, whose growing efficiency at launching attacks have shredded the comforting fiction that any business is too small to target.

When it comes to third-party risk management (TPRM), business leaders need to ask themselves: Are we truly protecting our organization – or are we merely going through the motions to check a box for compliance?

Even within a single industry, the answer to that question can vary widely. According to a 2023 Center for Financial Professionals survey, for example:

22% 22% of survey respondents said they conduct due diligence to evaluate IT security and risk management processes on just 25–45% of their third parties;

22% 22% said they do this on 76–100% of their vendors; and

→ the remaining cohorts of respondents bounced around from there.

And due diligence is only one part of a healthy risk management program.

With many companies still failing to implement even the most basic protective measures, raising the red flag on poor third-party risk management practices is more urgent than ever.

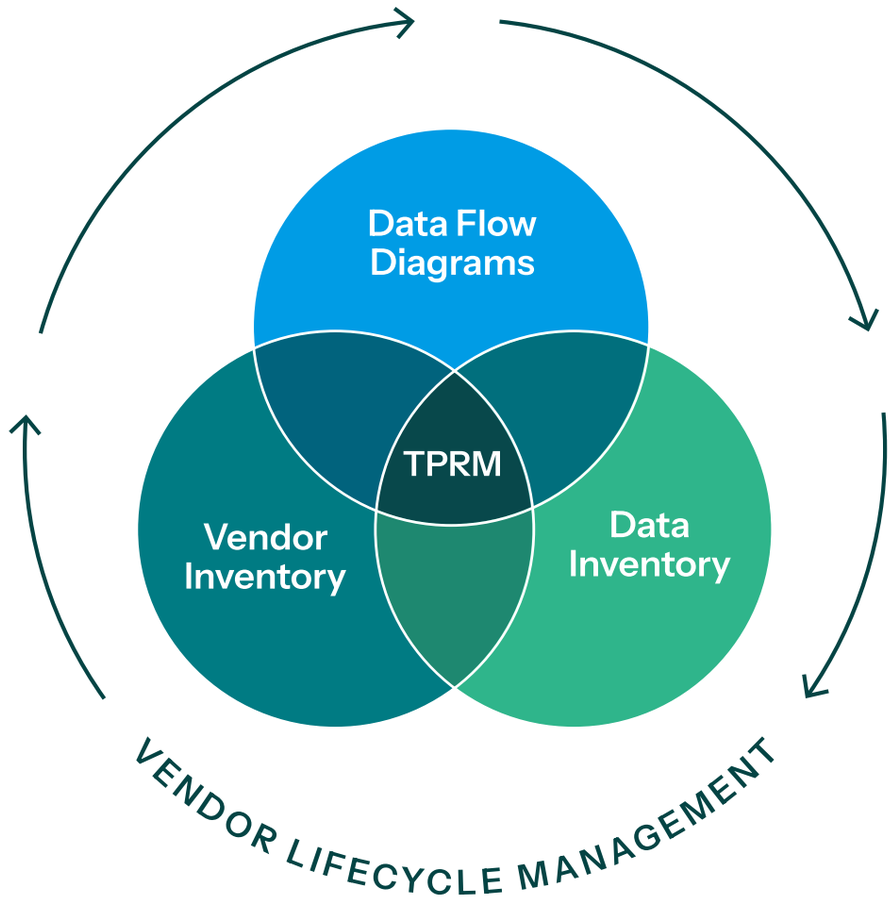
Truly effective risk management starts with asking, “How can we categorize the risk associated with our third party vendors so we can monitor and address it continuously?” This guide helps you do exactly that by walking through four essential components that enable robust, ongoing third-party risk management:

01 Vendor Lifecycle Management

02 Vendor Inventory

03 Data Inventory

04 Data Flow Diagrams



→ Review the to-do lists in each section of this guide to understand what you need to get started today.

Third-Party Risk Management

01 Vendor Lifecycle Management

What is vendor lifecycle management?

Vendor lifecycle management is the set of policies and procedures that govern how your business engages with third-party vendors. Having structured vendor lifecycle management processes in place enables you to identify, assess, and mitigate risk at every stage of the vendor relationship – from start to finish.

What risk management activities need to be conducted at each stage in a vendor lifecycle?

➜ **Stage 1: Vendor Evaluation – prior to onboarding**

- Define criteria for risk exposure evaluation.
- Conduct your initial due diligence assessments on the vendor's cybersecurity, finances, operations, and compliance.
- Review the vendor's policies, controls and incident response plans.
- Perform vendor background checks and screening for potential risks.

➜ **Stage 2: Vendor Onboarding and Contracting – after evaluation**

- Establish contractual terms aligned with your risk assessment findings.
- Define service level agreements (SLAs) and performance metrics.
- Implement security controls and access restrictions based on the vendor's risk level.
- Integrate the vendor into your third-party risk management processes and systems.

➜ **Stage 3: Continuous Monitoring and Periodic Reviews – ongoing**

- Monitor for changes that could impact the vendor's risk profile.
- Conduct periodic risk reassessments and security reviews.
- Evaluate performance against SLAs and contractual obligations.
- Monitor for any external events, threat intel, or vulnerabilities affecting the vendor.

➜ **Stage 4: Issue and Incident Management – ongoing**

- Report, triage, and escalate vendor incidents.
- Collaborate with the vendor on risk remediation.
- Plan for contingencies and exiting in case of vendor service disruptions.

➜ **Stage 5: Termination and Offboarding – for safely disengaging**

- Revoke the vendor's access to systems, data, and facilities.
- Ensure secure handling and disposal of your organization's data.
- Conduct lessons learned reviews to improve future vendor engagements.

Within vendor lifecycle management, what role do requests for proposals, inherent risk questionnaires, and due diligence questionnaires play?

Requests for proposals (RFPs), inherent risk questionnaires (IRQs), and due diligence questionnaires (DDQs) all contribute valuable data points to your third-party risk evaluations. Each one serves a different function at a different stage in the vendor relationship. Here's a quick overview:

→ **RFPs help assess technical fit –**

- **Purpose:** Shared by businesses to solicit proposals from vendors.
- **Timing:** Typically issued early on in the procurement cycle for a specific project.
- **Content:** Outline specific project requirements, scope, timelines, budgets, and evaluation criteria for vendors to respond to.

→ **IRQs help determine the level of due diligence required for a vendor –**

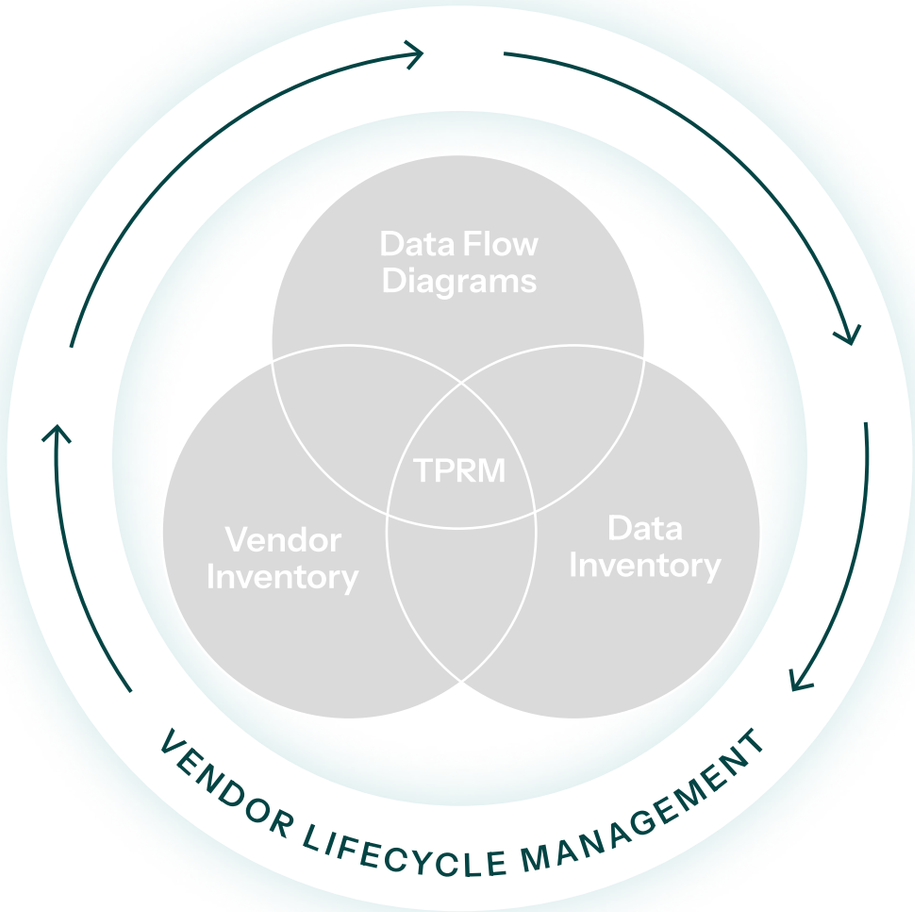
- **Purpose:** Enable businesses to calculate the inherent risk score or rating for a potential vendor.
- **Timing:** Kick off the third-party risk assessment process before a vendor is selected.
- **Content:** Gather information about a potential vendor's organization, services, data practices, security controls, etc.

→ **DDQs help ensure vendor relationship risks are understood and addressed –**

- **Purpose:** Enable businesses to evaluate a vendor's overall suitability and ability to meet compliance and security standards.
- **Timing:** Initial DDQs are issued after a vendor has been shortlisted through RFP evaluation but before finalizing any contracts. Periodic DDQs may also be issued annually or even quarterly, depending on the vendor relationship.
- **Content:** Dig into areas like a vendor's financials, legal/compliance posture, business continuity plans, and in-depth risk assessments to identify risks to be mitigated through contracts and controls.

How does vendor lifecycle management fit into your third-party risk management?

Vendor lifecycle management provides your business with a holistic framework for assessing, monitoring, and managing your third-party vendors according to their most up-to-date risk profiles. With this structure as your starting point, you're establishing a consistent standard – one that ensures all vendors are evaluated and managed with the same criteria and processes, reducing the chance of overlooking potential risks.



Vendor Lifecycle Management To-Do List

1. Establish a formal vendor lifecycle management process that covers all stages of the vendor relationship.
2. Define roles, responsibilities, and procedures for each stage of the life cycle.
3. Invest in technology solutions that help aggregate data from external sources, build comprehensive risk profiles, enable reporting and auditing, and streamline workflows.
4. Thoroughly document all due diligence activities, findings, and decisions in a centralized, easily accessible digital format – both for regulatory compliance and your own reference.
5. Don't ignore red flags or suspicious behavior you uncover. Address things like inconsistencies in information provided, reluctance to cooperate, or attempts to conceal details promptly.
7. Regularly review and update your vendor lifecycle management policies and procedures.

More on Vendor Lifecycle Mgmt.

2 Big Third-Party Risk Management Benefits You Get with Vendor Lifecycle Management

1. **Fewer surprises** — Bringing members of your procurement, legal, finance, security, and other relevant teams into vendor evaluation early on means better communication and alignment on business risks.

2. **Avoid preventable risks** — Creating an end-to-end view of vendors' potential impact on operations enables your entire third-party risk management support team – not just IT – to take informed, decisive steps that protect your business.

Third-Party Risk Management

02 Vendor Inventory

What is a vendor inventory?

A vendor inventory is a centralized repository of information about all of your organization's third-party vendors and service providers. It supports third-party risk management (TPRM) by giving you visibility, tracking, and control over who has access to your data, systems, facilities, etc., and enables you to systematically categorize the level of risk posed by each third-party in your ecosystem.
Every business – regardless of size – needs a vendor inventory.

What information should a vendor inventory include?

A tightly controlled, risk-based vendor inventory goes beyond contact information and product or service descriptions.

For each vendor, include details like:

- **Who's the internal business owner?**
  Typical internal business owner: the department or team that manages the vendor and is responsible for ensuring they meet their contractual obligations.
- **Which internal stakeholder maintains the relationship?**
  Typical relationship-maintainers: someone from procurement; the business unit leveraging the vendor's services; a dedicated vendor management team; etc.
- **How many times has this relationship been renewed?**
  Helps assess vendor "stickiness" and the criticality of their services.
- **When the contract is up, what's the cancellation period?**
  Helps you with vendor lifecycle management and transition planning.
- **What data do they process and store?**
  Helps ensure your data inventories and data flow diagrams are accurate.
  Typical data types: customer, financial, intellectual property, etc.
- **What is their impact level?**
  Typical impact levels:

  High-risk – provide critical services, have access to sensitive data, or pose significant risks if disrupted;

  Medium-risk – provide important but not critical services, have limited access to sensitive systems/data, or pose moderate operational risks; and

  Low-risk – provide non-critical services, have minimal data access, and introduce relatively low risks.
- **What are their due diligence assessment results?**
  Typical results: did not provide/not available, needs attention, acceptable, etc.
- **What is their current status?**
  Typical status levels: Approved, rejected, under review, etc.

How do you maintain a vendor inventory – and who's responsible for doing so?

- Regardless of whether your vendor inventory lives in a master spreadsheet, an internal database, or a dedicated software application, it should be updated at vendor onboarding, offboarding, and whenever a vendor's role or responsibilities change significantly.
- A complete vendor inventory audit for all third parties should be performed annually.
- Adding, removing, and modifying vendor information is most practical as a shared, cross-functional responsibility – so it's important to clearly define who owns which parts of the process. Ultimately, team members from IT, procurement, legal, and business units may each play a role.

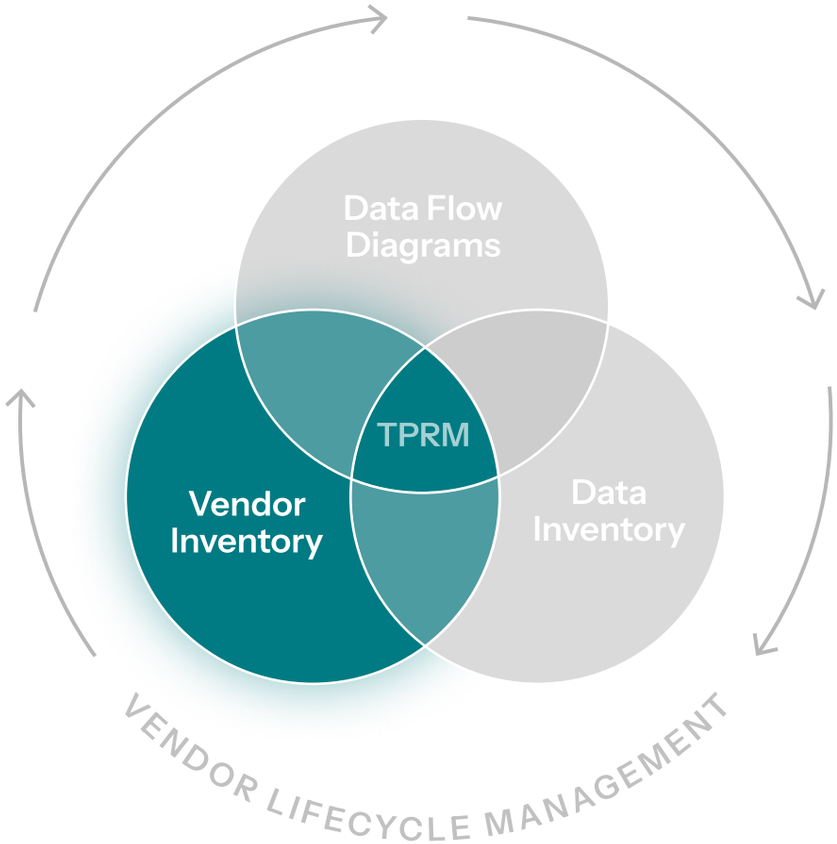
Does your company also have an approved vendors list?

Many organizations proactively maintain a list of vendors that have already undergone due diligence and meet specific security, compliance, and performance criteria. When needs arise, having a list of pre-approved vendors helps with things like:

- ensuring that all third parties are subject to the same rigorous vetting process;
- preventing introduction of unmanaged risk from rogue vendor contracts; and
- enabling periodic reviews of each vendor's risk assessment, performance, contracts, and other details to determine if they should remain approved.

How does your vendor inventory fit into third-party risk management?

A vendor inventory serves as the cornerstone in your third-party risk management (TPRM) program. It provides a complete view of your organization's third-party ecosystem, documents the criticality level of each third-party vendor, and anchors the framework that enables you to identify and address the extent to which your data is exposed to risk.



Vendor Inventory To-Do List

1. Establish and document a centralized vendor inventory if one doesn't exist.
2. Assemble an internal, cross-functional vendor inventory team, and assign ownership/roles and define processes for maintaining the inventory.
3. Ensure all departments and business units contribute their own vendor information.
4. Make your vendor inventory accessible to the owners of your other third-party risk management processes and tools.

More on Vendor Inventory

Six Vendor Buckets to Check – Because Leaks Can Happen Anywhere

It's important to remember that IT vendors aren't your only sources of third-party risk. Given the opportunity, bad actors will exploit any opportunity to access your systems and data.

One standout example of this is the 2013 compromise of millions of Target customers' payment card data. Cybercriminals used a phishing scam to trick an HVAC contractor into providing credentials to the retailer's vendor portal and launch malware onto their POS system.

Here are six third-party vendor buckets (with examples) to cover in your master vendor inventory.

1. **Software Vendors** — cloud hosting providers; SaaS (Software-as-a-Service) solutions; web content management systems; accounting software providers; etc.
2. **Service Providers** — employment/staffing agencies; delivery services; insurance brokers; investment brokers; mortgage brokers; marketing agencies; accounting firms; legal firms/lawyers; consultants; call center providers; etc.
3. **Suppliers** — raw material suppliers; component suppliers; equipment/hardware suppliers; etc.
4. **Contractors** — IT contractors; short-term/long-term contractors; maintenance contractors (HVAC, equipment repair, etc.); etc.
5. **Business Partners** — affiliates; distributors; resellers; agents; etc.
6. **Other Vendors** — cloud service providers; website hosting services; payment processing companies; debt collectors; landscapers; phone/telecom providers; etc.

More on Vendor Inventory

Multi-Vector Software Supply Chain Attacks

As software supply chains grow more complex and interconnected, threat actors have an expanding attack surface for infiltrating your data and systems.

By giving you an explicit understanding of all the players in your vendor ecosystem – and enabling you to assess, monitor, and control it – a holistic third-party risk management (TPRM) program can help ensure that things like weaknesses in code and access controls aren't your organization's undoing.

Here are six attacks cybercriminals may try against you that TPRM can help mitigate:

1. **Compromising Software Updates and Code Repositories** — injecting malicious code into legitimate software updates or compromising code repositories used by software vendors.
2. **Compromising Continuous Integration/Deployment Pipelines** — exploiting vulnerabilities in software-build tools and processes to taint code from the inside.
3. **Exploiting Vulnerabilities in Third-Party Software** — actively searching for and exploiting unpatched vulnerabilities in popular business software.
4. **Credential Theft and Access Abuse** — stealing credentials or abusing legitimate access of third-party vendors.
5. **Automated Scanning for Weaknesses** — using automated tools to rapidly exploit insecure network configurations, unprotected cloud resources, and other weaknesses across software supply chains at scale.
6. **Targeting Fourth-Party Suppliers** — compromising the sub-contractors and suppliers (fourth parties) of your own third-party vendors.

Third-Party Risk Management

03 Data Inventory

→ What is a data inventory?

A data inventory is a comprehensive listing of all the data your organization possesses, including its location, classification, ownership, and the employees, systems, and vendors that access or process it.

While your vendor inventory provides a big-picture overview of your third-party relationships, your data inventory documents the specific data elements involved in each vendor relationship.

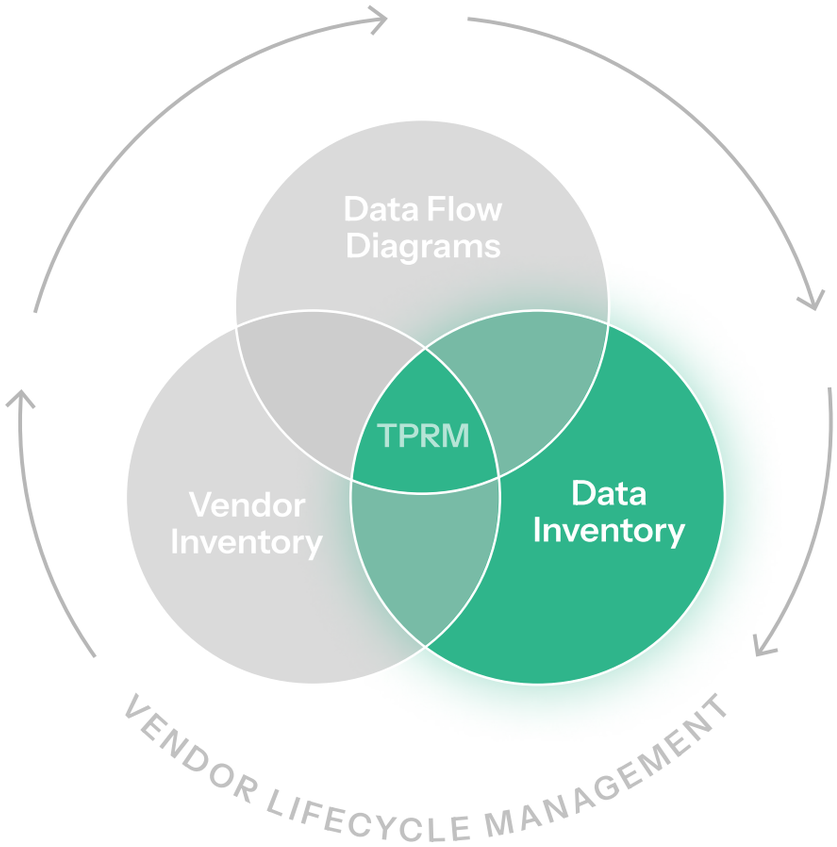
What information should a data inventory include?

A risk-aware data inventory needs to answer the following questions for each type of data you have (e.g., customer records, financial data, intellectual property, etc.) and enable you to draw connections between that data and any vendor that stores, processes, or accesses it:

- **Where is the data stored (geographically and digitally)?**
  Examples: on-premises data centers, cloud storage (AWS, Azure, etc.), employee laptops, mobile devices, etc.
- **What types of documents store it?**
  Examples: Word documents (contracts, reports), Excel spreadsheets (financial data, customer lists), PDFs (scanned documents, invoices), databases, etc.
- **How sensitive is the data (using data classifications, ideally)?**
  Examples: public (marketing materials), internal (employee directories), confidential (trade secrets, financial data), restricted (personal data, health records), etc.
- **What regulations apply to the data?**
  Examples: GDPR, HIPAA, PCI-DSS, CCPA, etc.
- **Who is ultimately responsible for the data – the "data owner"?**
  Examples: finance department (financial data), HR (employee data), marketing (customer data), product team (product specs), etc.
- **How critical is the data to your daily operations?**
  Examples: mission-critical (customer database, financial records), important (product roadmaps, marketing plans), non-critical (internal memos, old reports), etc.
- **Which third-party vendors have access to the data?**
  Examples: payment processors (customers' financial and transaction data), background screening firms (candidate names, addresses, and SSNs), cloud services providers (internal data, systems, and storage), etc.

How does your data inventory fit into third-party risk management?

Your data inventory helps establish your level of risk exposure with each party on your vendor inventory. By cross-referencing the two inventories, you can prioritize third-party risk management (TPRM) efforts based on the criticality of each vendor combined with the sensitivity of data they access. **High-risk vendor + high-risk data = highest priority for rigorous assessments.**



Data Inventory To-Do List

1. Conduct a comprehensive data discovery and classification exercise.*
2. Document data elements to the vendors that access or process them.
3. Use your data inventory to establish data governance policies and procedures (e.g., data quality management, data access and security, data lifecycle management, etc.).

**Note: Obviously, you can't protect data you don't know you have. To ensure your data inventory is accurate and complete, you may need to employ a specialized solution. Software as a Service (SaaS) management tools, for example, can assist with discovering shadow IT – e.g., systems and software that have been deployed outside the approval or control of your central IT department. If you suspect this is a concern for your organization, let's connect – we can help.*

Third-Party Risk Management

04 Data Flow Diagrams

What are data flow diagrams?

Data flow diagrams (DFDs) are visual representations that illustrate how the data involved in every business process (e.g., customer onboarding, product development, financial reporting, etc.) moves through your organization's systems, applications, and third-party vendors.

What types of information do data flow diagrams include?

- Where the data begins.
- Where the data ends.
- Where the data goes when it's no longer needed.
- Any systems or people that process the data.
- Any systems or people that transfer the data.
- Whether or not the data is encrypted, and if so, at which points and what protocol is used.
- Any authentication, authorization, or access control mechanisms that are applied to the data.

How do you create data flow diagrams – and who does it?

Most companies use popular software tools like Microsoft Visio or online diagramming applications to create their data flow diagrams (DFDs). With built-in functionalities for things like standard shape libraries, automated diagramming, linking, complex hierarchies, and file-sharing, these programs are better suited to DFDs than more manual drawing options.

Typically, IT teams, security professionals, or third-party consultants with expertise in data mapping and visualization will work with business units to create DFDs.

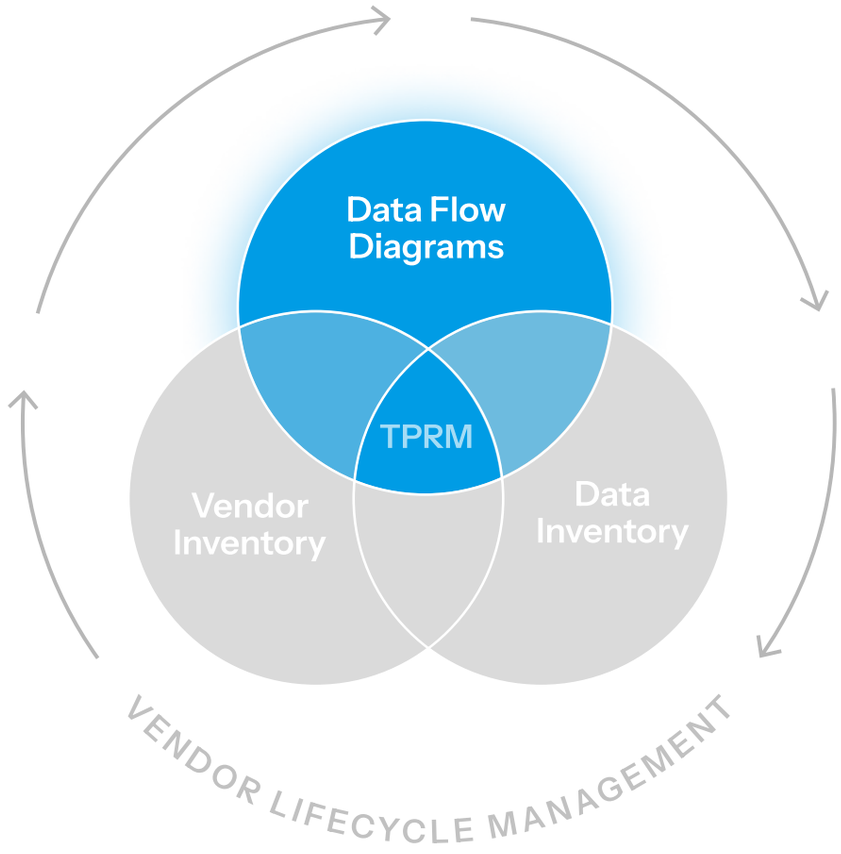
What do you do with data flow diagrams?

Data flow diagrams support third-party risk management efforts by drawing the who, where, and how connections across your data, people, and systems so you can do things like:

- Identify potential risks or vulnerabilities and design appropriate security controls.
- Identify where you need to implement access rules in order to comply with data protection regulations (e.g., GDPR, CCPA).
- Conduct impact assessments for system changes and new data processes.

How do your DFDs fit into third-party risk management?

Data flow diagrams (DFDs) provide the critical data movement context necessary to properly monitor ongoing risk exposure from each vendor based on their data access, controls, and regulatory compliance requirements.



Data Flow Diagrams To-Do List

1. Leverage your vendor and data inventories to create comprehensive DFDs.*
2. Involve relevant stakeholders (IT, security, business units) in DFD reviews to ensure accuracy and completeness.
3. Integrate DFDs into third-party risk management-related processes, such as vendor risk assessments, vulnerability monitoring, and incident response planning.

**Note: Data inventories and DFDs help with more than just managing third-party risk. Strategic executives are putting data at the center of everything they do – every system, process, and decision – and transforming their organizations from the inside out. Download "Driving Data Centricity: An Act-Now Guide for Smart Business Leaders" for more information.*

coretelligent

Because Partnering with the Right Vendor Matters: Maximize Your Third-Party Risk Management with Us

Laying a secure risk-management foundation is one part of protecting your business from bad actors. Real-time threat intelligence with 24/7 detection and response is another. We use your vendor lifecycle management framework and the information captured in your vendor inventory, data inventory, and data flow diagrams to identify and secure your areas of vulnerability.

Need help making – or making sense of – your data inventory or other third-party risk management component? Our team of cybersecurity and compliance professionals is here for you. We provide a full range of strategic risk-mitigation and data capabilities, including access control management and data mapping, vCISO services, and much more. Let's connect.

→ Visit us online at Core.tech.