MITRATECH
Prevalent

Vendor Offboarding Due Diligence Guide

Best Practices for Reducing Risk and Simplifying the Process of Terminating Vendor Relationships

Table of Contents

Using Vendor Offboarding to Reduce Risk and Avoid Exposure

Most business relationships are temporary. Your organization likely has several established contracts with third-party vendors that feed your supply chain and enable your business to operate efficiently. However, most third-party relationships will inevitably cease as product designs are updated, projects are completed, or better alternatives become available. In addition, terminations may be necessary when third parties present unacceptable levels of risk, such as security exposures, performance shortfalls, financial challenges, or reputational problems. Whatever the reason for terminating a vendor contract, it's important to have a structured offboarding process in place. Vendor offboarding is the process of removing a vendor's access to systems, data, and corporate infrastructure—and making sure other final actions are executed as stipulated in the contract.

The goals of vendor offboarding are to provide a smooth and secure transition, minimize risk and disruption to business operations, and protect sensitive information. Many organizations overlook the importance of a secure and programmatic offboarding process, which exposes them to future risks. This vendor offboarding guide:

- Provides examples of common risks associated with offboarding a vendor
- Examines challenges in managing vendor offboarding
- Discusses best practices to securely wind down business relationships
- Recommends a comprehensive vendor offboarding checklist to reduce risk and simplify the process.

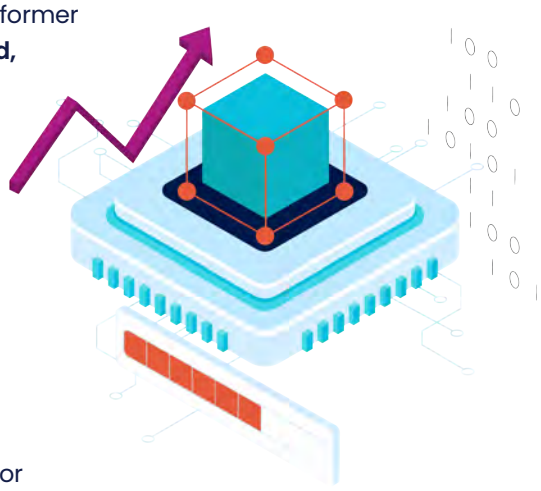
Types of Risks to Consider When Offboarding Vendors

Proper vendor offboarding is critical to managing risk, particularly since security, procurement, and vendor management teams discontinue vendor oversight when the relationship ends. An incomplete or hastily conducted offboarding process can result in financial losses, regulatory penalties, and reputational damage.

CYBER RISK

There are several examples of how incomplete third-party vendor or supplier offboarding processes have led to data breaches that damaged organizations.

- In 2023, a major telecommunications provider reported a data breach that exposed the private information of roughly 5 million customers. Rather than directly attacking the organization itself, the criminals targeted a "former third-party vendor" to access the records. **When a vendor is offboarded, the vendor should return or securely delete all your records.**
- In 2021, a major medical center suffered a breach when an unauthorized individual with a former vendor gained access to backup files on archived servers that included protected health information (ePHI). The former vendor had previously provided patient education services for the medical center. **When it is not possible to securely delete data due to record retention policies, organizations should make sure the vendor has controls to prevent unauthorized access to the data.**
- A 2018 breach cost one major hospitality enterprise over $28 million. The breach was executed by accessing the network of an outside vendor formerly used by the company.



FINANCIAL RISK

The end of a vendor relationship can trigger additional costs. For instance, the vendor may have negotiated an early termination fee. Furthermore, your organization may incur costs to identify, select, and onboard a replacement vendor, such as ramp-up and training fees. Without a smooth transition process, there can be delays in receiving parts, products, and services from new vendors — which, in turn, can disrupt your organization's ability to deliver to its clients.

LEGAL RISK

Disputes over intellectual property (IP) ownership or termination parameters can arise if your legal department does not thoroughly review the contract during negotiation and with each development throughout the course of the relationship. Legal fees can be substantial if there is a dispute about an organization's right to terminate an agreement.

REPUTATIONAL RISK

Maintaining good relationships with vendors is important, even when terminating business agreements. Other vendors may interpret poor communications or contract fulfillment with a vendor as evidence that your company is difficult to work with. This can also negatively impact your relationships with other existing vendors or potential business partners.

These examples demonstrate that organizations must assess a wide range of business risks when offboarding vendors.

Vendor Offboarding Challenges

Procurement, vendor management, and security teams often view third-party risk management (TPRM) as an exercise to be conducted prior to onboarding a new vendor. So, it's no wonder that vendor offboarding is an afterthought at many organizations. Our annual Third-Party Risk Management Study showed that only 43% of companies are tracking risks at the offboarding stage of their vendor relationship. While due diligence in vendor sourcing and selection is an important activity, measuring and managing risk extends throughout the relationship with a vendor. This includes managing the end of a relationship with thorough vendor offboarding.

LIMITED STAKEHOLDER INVOLVEMENT

As with vendor onboarding, knowledge silos can make it difficult to identify all the required tasks to offboard vendors. Procurement may notify a vendor that a contract will not be renewed, but legal must review contract terms and provide details on what steps are required for a clean termination. In some cases, engineering may need to identify intellectual property shared with the vendor. Manufacturing and operations must confirm which steps are required to avoid production stoppages. Finance must identify outstanding invoices or credits owed by the vendor. IT security must make sure data is destroyed and system access is revoked. Without coordination between these teams, offboarding is a complicated task.

LAX OFFBOARDING DUE DILIGENCE

It is easier to focus on activities with new vendors than on those being offboarded. To mitigate the risks referenced above, it is critical to be thorough when offboarding a vendor. This requires all team members who have interacted with the vendor to identify potential risks, agree to mitigation requirements, and meticulously track progress. Manual methods for performing due diligence will inevitably lead to missed tasks and unresolved risks.

INCOMPLETE VISIBILITY INTO RISK MITIGATION

Tracking tasks in spreadsheets or shared documents can make the offboarding process inconsistent and prone to errors. The completeness and accuracy of a task list is subject to the expertise of everyone involved in the offboarding process. For example, a less-experienced employee may overlook critical tasks or incorrectly mark an item complete without full documentation from a vendor. Spreadsheets that can be accessed by multiple employees also lack auditing controls.

Best Practices for Vendor Offboarding

A centralized process can help teams automate vendor offboarding, verify its completeness, and effectively mitigate risk. Here are seven best practices to follow during the offboarding process:

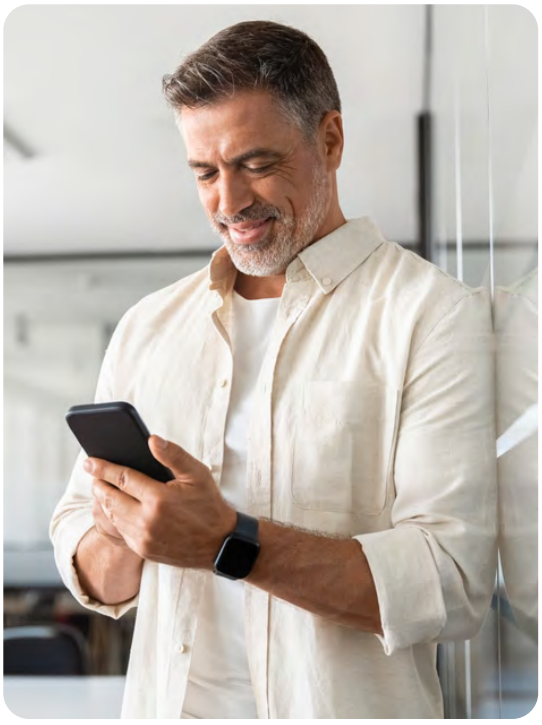
1. Keep Lines of Communications Open

Teams can mitigate risk by keeping the lines of communication open with the vendor throughout the offboarding process. This includes informing the vendor of the offboarding timeline, answering any questions, and providing clear instructions regarding what is expected during the process. A solution that centralizes interactions with the vendor, maintains tasks and timelines, and requires approval workflows will greatly reduce the manual work required to address these issues.

2. Perform a Final Review of the Contract

Review the contract's termination provisions to make sure you have the right to terminate the relationship, and if so, the proper timelines for doing so. If you are terminating due to a breach of contract terms, be sure notices have been issued and the vendor's rights to remedy shortcomings have been honored. Teams may have changed contract terms over time. A final review with legal and procurement can identify scope creep and confirm that the vendor provided all the contractually obligated goods and services.

Finally, review key performance indicators (KPIs), pending deliverables, and payments. If the vendor is supplying parts, make sure warranty and support agreements that survive termination are clear.



3. Settle Any Outstanding Invoices

After thoroughly reviewing the contract terms and identifying remaining obligations for both parties, ensure that you receive final deliverables and schedule final payments. Do not forget to include any credits or returns when calculating payments, as these may be difficult to recover after you terminate the relationship.

4. Revoke Access to IT Infrastructure, Data, and Physical Buildings

Partners and vendors may require access to your systems, such as those used for purchasing, engineering, marketing, and financial data. When offboarding a vendor, it is critical to terminate its access to your intellectual property and other sensitive data. This includes:

- Having a list of all vendor accounts and deleting login credentials.
- Providing the vendor with a complete list of all company-owned equipment it must return. When repurposing returned equipment, be mindful of data retention requirements.
- Changing all logins, including shared credentials if a vendor has elevated privileges to systems.
- Deauthorizing access to all applications, including VPNs and cloud apps for file sharing and messaging.
- Deauthorizing any access the vendor may have had through APIs, as these could be a useful attack vector if a hacker later compromises the vendor.

Some vendor employees may have required physical access to your offices or server rooms. Deactivate any keycards and badges and confirm that the vendor has returned all physical keys. In some cases, you may need to change entry codes to server rooms. Work with your physical security teams to document a clear process for managing physical vendor access.

5. Review Data Privacy and Information Security Compliance

Vendors often have access to sensitive data subject to regulatory requirements such as CCPA, GDPR, PCI DSS, and others. During offboarding, make certain that you align your vendor termination procedures with your legal obligations. Third-party risk management platforms have built-in reporting that aligns with these regulatory obligations, simplifying the compliance process. If the vendor has copies of your sensitive data, it could be exposed in a later breach. One major financial provider failed to properly oversee the decommissioning of servers by a third party. A subsequent breach of the third party exposed personal information and resulted in a $60 million fine from the Office of the Comptroller of the Currency.

Verify that all intellectual property and sensitive data are returned. Also, require an affidavit from the vendor that electronic copies on the vendor's infrastructure—including on employee devices—are securely deleted. Additionally, review with the vendor remaining obligations such as confidentiality, non-disclosure, and non-compete agreements.

6. Update Your Vendor Management Database

Not all terminations are permanent. You will want a clear record of the vendor's history with your organization, including its KPIs. To reduce legal risk, clearly document the reasons for terminating the relationship and maintain a complete accounting of the termination procedures. Make sure you have records of all communications, contracts, and other documentation between your organization and the vendor so you can quickly resolve any questions or issues moving forward.

7. Continuously Monitor Vendors for Potential Future Risks

Even though the contract has been terminated and all offboarding tasks have been successfully completed, risks to your systems and data, along with compliance or reputational risks, can still emerge long after the relationship ends. Continuously monitoring multiple risk vectors will give your team extended visibility into potential future risks.

Vendor Offboarding Checklist

Use the checklist below to determine if you have the information required to securely offboard a vendor.

NOTE: This checklist is not comprehensive. It provides a list of common sources of information and criteria to help you make more informed offboarding decisions, and it can be customized for your organization's unique needs.

Offboarding Step	Task	Complete?
STEP 1: KEEP LINES OF COMMUNICATIONS OPEN		
Centralize interactions with vendors to encourage accountability and reduce manual work.	Notify vendors of contract termination and provide instructions and a forum to answer questions.	
	Maintain a central list of contacts, tasks, ownership, and due dates with reminders triggered if dates have been exceeded.	
	Implement rules to automatically suggest actions based on tasks and route to stakeholders for review and approval.	
	Centralize the management of vendors into a single comprehensive profile available to all internal team members responsible for managing the vendor relationship.	

Offboarding Step	Task	Complete?
STEP 2: PERFORM A FINAL REVIEW OF THE CONTRACT		
Provide a central forum for managing contract provisions to make certain all requirements have been met.	Review contract provisions with legal and procurement teams.	
	Establish a schedule for final deliverables and payments. Confirm applicable warranties and ongoing support agreements are in place.	
	Track all contract attributes such as type, start and end dates, value, and status.	
	Provide customized, role-based contract views for internal stakeholders and external vendors.	
	Build customizable workflows based on user or contract type to automate reviews throughout the contract lifecycle.	
	Assign and track tasks such as automated reminders and overdue notices against contracts.	
	Centralize contract discussions, with email notifications distributed to participants—internal and/or external—when comments are added.	
	Identify relationships between the vendor and its vendors (i.e., fourth and Nth parties) to determine dependencies and visualize information paths that could further expose your organization.	
STEP 3: SETTLE ANY OUTSTANDING INVOICES		
Update vendor contact information to make sure you receive final deliverables and schedule final payments.	Validate the following contact information: ▪ Business contact (day to day) ▪ Legal contact (contracts) ▪ Remittance address (payments) Review final deliverables and make final payments.	

Offboarding Step	Task	Complete?
STEP 4: REVOKE ACCESS TO IT INFRASTRUCTURE, DATA, AND PHYSICAL BUILDINGS		
Terminate vendor access to your intellectual property and other sensitive data and facilities.	Maintain a list of all vendor accounts and delete login credentials.	
	Provide the vendor with a complete list of all company-owned equipment it must return.	
	Change all logins, including shared privileged credentials. Deauthorize access to all applications and APIs.	
	Deactivate keycards and badges; change entry codes to server rooms.	
	Assign and track tasks such as automated reminders and overdue notices against contracts.	
	Build a survey for vendors to report on system access, data destruction, and access management.	
	Design automated rules to accept or reject answers to questions, suggest actions, or kick off tasks with defined owners based on answers to offboarding assessments. Prioritize risks based on likelihood of occurrence and impact on the business.	
	Identify remediations to recommend to the vendors to minimize residual risk. Track remediations through to closure.	
	Capture and audit conversations, recording estimated completion dates for remediations for a secure audit trail.	
	Determine if compensating controls are sufficient. Establish a cadence to continuously monitor the internet and dark web for cyber exposures of your company's data and systems.	

Offboarding Step	Task	Complete?
STEP 5: REVIEW DATA PRIVACY AND INFORMATION SECURITY COMPLIANCE		
Align your vendor termination procedures with legal obligations.	Understand where the vendor shared your company's client data and determine whether additional 4th-party or Nth-party assessments are necessary.	
	Assess vendor controls against privacy regulations and identify areas for remediation.	
	Design automated rules to accept or reject answers, suggest actions, or kick off tasks (with defined owners based on answers to data privacy assessments).	
	Map risks and assessment responses to controls, calculating a percent-compliant rating for regulatory reporting.	
	Identify and recommend remediations to vendors to minimize residual risk.	
	Track remediations through to closure.	
	Determine if compensating controls are sufficient.	
	Continuously monitor for vendor data breach notifications with alerting.	
STEP 6: UPDATE YOUR VENDOR MANAGEMENT DATABASE		
Document the reasons for terminating the relationship and maintain a complete accounting of the termination procedures.	Centrally store and manage historical documents, such as non-disclosure agreements, service level agreements, statements of work, security certifications (e.g., NIST, ISO or SOC 2), and contracts.	
	Update the full primary operating address of the third party; include the location from which the third-party service was delivered.	

Offboarding Step	Task	Complete?
Document the reasons for terminating the relationship and maintain a complete accounting of the termination procedures. *(continued)*	Maintain a record of the service provided by the vendor, including KPIs.	
	Keep the name, organizational role, and contact details for the primary third-party representative updated.	
STEP 7: CONTINUOUSLY MONITOR VENDORS FOR POTENTIAL FUTURE RISKS		
Establish an ongoing process to evaluate the performance, compliance, and risk profile of all active and potential vendors.	Establish a cadence to monitor the following: ▪ **Cybersecurity information:** Criminal forums; onion pages; dark web special-access forums; threat feeds; paste sites for leaked credentials; security communities; code repositories; and vulnerability databases could be potential exposures to your company's data. ▪ **Financial and business news:** M&A, divestitures, and partnerships/alliances to ascertain changes in ownership that can impact warranties. ▪ **Sanctions and legal findings:** Bribery and corruption/ethics violations and sanctions that could impact contracts. ▪ **Reputational information:** Adverse media and negative news that could signal poor governance processes.	
	Correlate results of continuous monitoring with final assessment results to determine whether all remediations were satisfactorily applied. Escalate to vendor contacts as necessary.	
OFFBOARDING GO/NO-GO DECISION:		

How Mitratech Helps

The Mitratech Third-Party Risk Management Platform automates the vendor offboarding process to reduce your organization's risk of post-contract exposure. The Platform:

- Provides a single source of truth for vendor information, encouraging internal stakeholder and vendor collaboration in a central solution.
- Centralizes contract lifecycle management, automating tasks to ensure contractual provisions are met to protect the company.
- Automates the assessment and continuous monitoring of vendor risks—from onboarding to offboarding—centralizing results in a single risk register that enables coordinated action.
- Includes built-in remediation guidance to make certain offboarded vendors meet your company's compliance and security requirements to an acceptable level of risk.
- Delivers a prescriptive process to address final tasks and report according to compliance requirements.

Offboarding should not be a static process. By leveraging the Mitratech Third-Party Risk Management Platform, you can be certain your offboarding processes are complete and meet the requirements of all stakeholders.

Who Benefits?

Multiple enterprise teams benefit from a more programmatic and intelligent offboarding process:

PROCUREMENT

Ensures offboarded vendors do not create the potential for risk by leveraging a programmatic process for assessing third parties at contract termination.

IT SECURITY

Reduces the risk of a post-contract breach with visibility into data access, physical and virtual security controls, and built-in remediation guidance.

COMPLIANCE & RISK MANAGEMENT

Centralizes the management of risks throughout the vendor lifecycle, simplifying regulatory reporting.

Next Steps

For more on how Mitratech can help simplify and secure vendor offboarding with a comprehensive, insights-driven and programmatic process, contact us today to **schedule a demo**.

About Mitratech Third-Party Risk Management

Mitratech takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers, and other third parties across the entire vendor lifecycle. Our clients benefit from a flexible, hybrid approach to TPRM, not only gaining solutions tailored to their needs, but also realizing a rapid return on investment. Regardless of where they start, we help our clients stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.
To learn more, please visit **www.mitratech.com**.

EMPOWER. AUTOMATE. ELEVATE.