Prevalent™

Quick Start Guide:

5 Ways to Simplify and Speed Third-Party Risk Management Audits

How to Harmonize TPRM Compliance Requirements

Table of Contents

Editor's Note: The information presented in this guide should not be considered as legal recommendations or used as a substitute for auditor or regulatory guidance. Please consult your organization's legal and internal audit teams and external auditors for a full review of the requirements communicated in these and other industry frameworks and regulations.

Third-Party Risk Management Compliance

Audit.

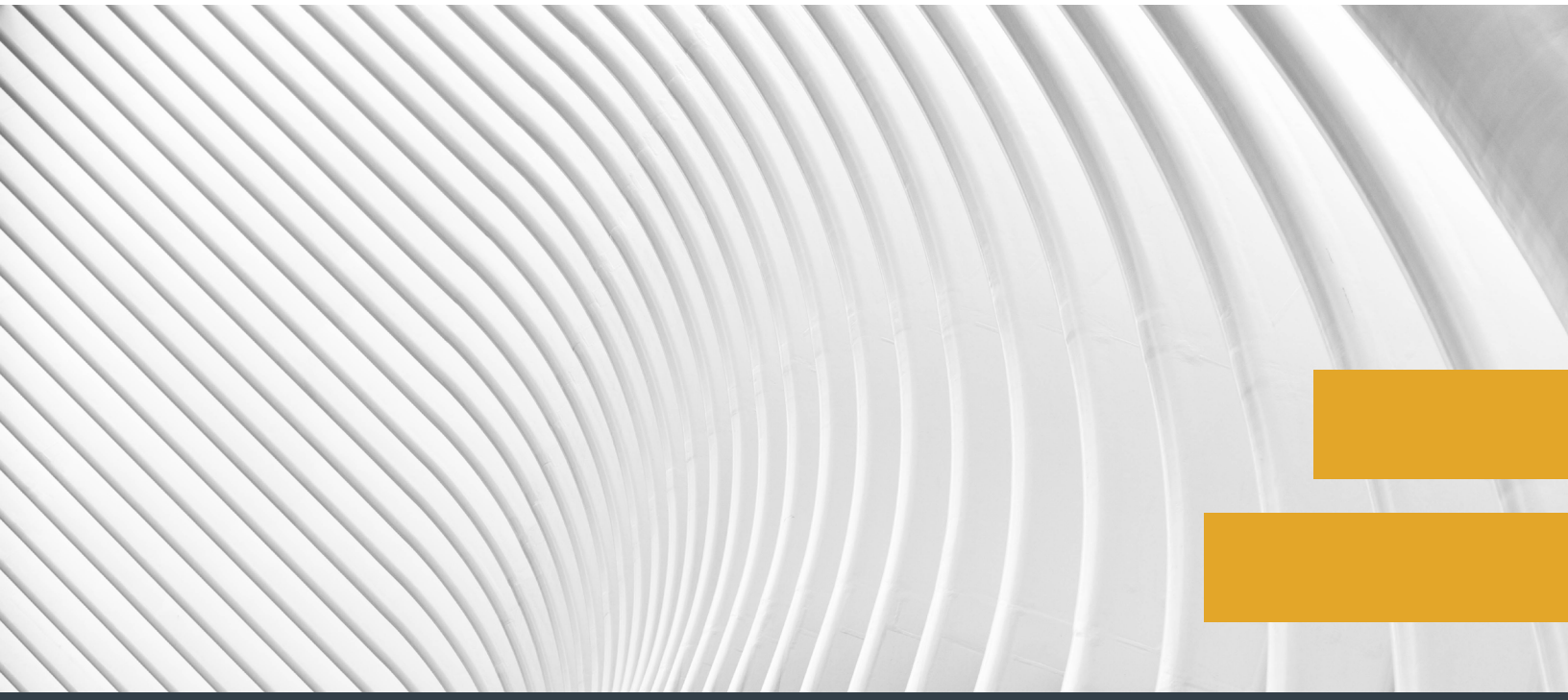
Feel that shudder? Very few words have the power to instill a sense of foreboding and professional dread in security and risk management professionals like the word "audit." It's no wonder, really. A single IT security audit often includes reviews of thousands of documents and internal controls, with dozens of stakeholders spending hundreds of hours away from their day-to-day jobs. When audits extend to examining the IT security and risk management practices of third-party vendors and suppliers, the amount of time and resources required can multiply exponentially.

The problem isn't only the time involved in gathering evidence, identifying, and reporting on control gaps, and remediating audit findings. Performing an IT security controls audit demands understanding and navigating an increasingly complex, unclear, and sometimes overlapping regulatory landscape.

So, how does a security and risk management team responsible for third-party risk management (TPRM) sift through a multitude of requirements to ensure that their vendors and suppliers are adhering to sound risk management principles – and do it without exhausting the team?

The key is recognizing the commonalities across multiple regulatory and IT security control frameworks and starting your auditing efforts with those baselines.

This guide examines five areas that many regulations and information security frameworks require and offers best practices guidance to address these common TPRM requirements as a baseline for compliance auditing. To accomplish this, the guide leverages the Interagency Guidance on Third-Party Relationships: Risk Management, a straightforward framework that U.S. federal regulators developed for the financial industry. Although the Interagency Guidance is for banking and financial services organizations, its framework represents a solid foundation of common TPRM components around which to structure your organization's compliance efforts.



Five-Step Starting Point for TPRM Compliance

To address compliance requirements, TPRM programs generally need to:

- Define and document operational processes
- Inventory third parties
- Document results
- Report on the program to multiple stakeholders
- Ensure ongoing oversight

The US Financial Interagency Guidance addresses these themes throughout each of the five steps for managing third-party relationships in a lifecycle:

1. **Planning**
   Answers questions like: What third parties do we already have? What services are needed? Who are our critical vendors?

2. **Due diligence and third-party selection**
   Requires organizations to select third parties based not only on needs but also on the organization's risk tolerance.

3. **Contract negotiation**
   Ensures that key provisions, such as the right to audit, are documented in the contract to minimize risk to the organization.

4. **Ongoing monitoring**
   Requires continuous third-party monitoring for new and emerging risks.

5. **Termination**
   Aims at protecting the organization after the contract ends.

Source: *Board, FDIC, and OCC*

Planning

Understanding your organization's risk exposure from third parties is a common thread woven throughout many regulatory and control frameworks. Two types of third parties are particularly important to focus on – third parties providing critical products or services and software that supports key business processes. Many regulatory regimes require programmatic determinations made regarding vendor criticality, and that third-party software be centrally managed and monitored.

Determine Vendor Criticality

A vendor's or supplier's criticality helps determine how frequently to assess and monitor them. Factors that inform this decision can include:

- A third party's role in supporting key business processes
- The function the vendor provides
- The classification of information that the supplier handles – is it subject to stringent data protection requirements?
- The third party's physical or logical access to organizational infrastructure
- Whether the organization has outsourced internal control functions to the vendor
- The location of the third party and whether there is a high risk of physical disruption

A third party that supports a critical business process or handles sensitive information could qualify as a critical vendor. This would require advanced due diligence, along with ongoing monitoring and periodic detailed internal controls-based assessments to ensure the supplier is adhering to business resilience practices to ensure continuity in case of a disruption.

Best Practice Recommendation: Conduct a profiling and tiering exercise to determine inherent risk and identify vendor criticality.

Inventory Third-Party Software

With software supply chain attacks increasing, it is critical to have an inventory of all software used within the organization and to tie the software inventory back to business processes and the third parties and subcontractors who develop, support, and operate it.

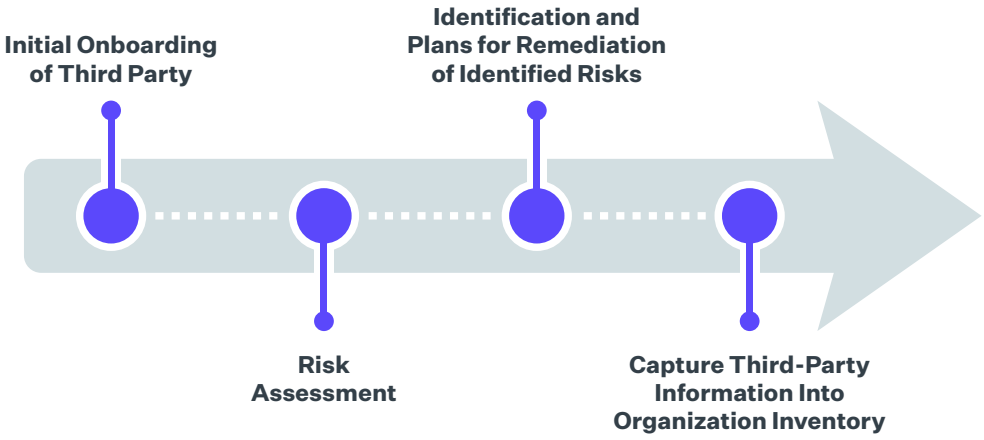
When an attack such as the MOVEit vulnerability occurs, for example, having a centralized third-party software inventory in place – and visibility into which third parties are using an impacted technology – can greatly accelerate the discovery of potential impact and reduce the time to mitigate any potential damage.

Best Practice Recommendation: Some of the most widely used cybersecurity supply chain risk management frameworks, such as the National Institute of Standards and Technology (NIST) SP 800-53 r5 and SP 800-161, include specific provisions on monitoring third-party software. Structure your third-party risk assessments around these best practice frameworks.

Due Diligence and Third-Party Selection

Once the rules for determining vendor criticality are in place and there is an inventory of existing third-party software and services, it's time to apply the principles of sound due diligence to selecting new solutions.

Choosing a solution or service based on whether it is fit for purpose is just one consideration in vendor selection. An equally important consideration is whether the vendor fits the organization's risk profile. That's where a comprehensive vendor due diligence process comes in. Vendor due diligence enables organizations to capture relevant supplier information upfront. This enables teams to build and manage a comprehensive third-party inventory, a key control in many regulatory frameworks for having an effective TPRM program.



The process to perform vendor due diligence is straightforward:

1. Once onboarding is completed, assess the third-party vendor or supplier on their cybersecurity and data privacy practices, business and operational factors, reputation, compliance status, ESG policies, and finances. Gaining visibility risks into each of these domains is essential to understanding a vendor's complex risk profile. After all, not every risk is cyber-related.

2. Centralize risks and control gaps into a single risk register that enables enterprise-wide visibility for multiple stakeholders. That will drive the development and enforcement of vendor remediation plans before signing the contract and facilitate internal discussions on whether the vendor presents an acceptable level of risk.

3. Build a central third-party inventory that enables teams to manage the vendor throughout its relationship lifecycle. This should be the same inventory built to manage third-party software, per the Planning step above, and should include attributes such as vendor company data, financial information, and location.

Best Practice Recommendation: The goal of performing regulatory-required pre-contract due diligence is to mitigate identified risks, not just to perform the assessment to "check the box." Therefore, enforce remediations to ensure third parties align with your organization's risk thresholds.

The Importance of Visibility Into Your Extended Supply Chain

To have an effective TPRM program, you need visibility into your extended supply chain. Extended supply chains represent some of the largest operational risks to your business because subcontractors and Nth parties may be tied to or provide critical business functionality. Lack of visibility into subcontractors can lead to operational failures and decreased operational resilience in the case of a cyber or physical disruption. Indeed, many large data breaches can be tied back to third-party compromises, but, when investigated, it is often found that the compromise started at the subcontractor level.

Best Practice Recommendation: To address this expanded risk surface, require third parties to identify their third parties during the due diligence process and incorporate key provisions in the vendor contract to require report and disclosures of disruptions and vulnerabilities. You can discover fourth parties through either a targeted assessment or via passive scanning.

Contract Negotiation

Organizations can be held accountable for the regulatory violations of their third parties and subcontractors. Therefore, consider adding these three critical requirements to third-party contracts:

1. The right to audit the third party for compliance with key security and data privacy protections.
2. Timely breach notification for faster response to security incidents.
3. Remediation of identified issues to mitigate the risk of control failures impacting the organization.

Best Practice Recommendation: Third parties are responsible for enforcing contractual requirements that extend to all subcontractors. Evidence of this enforcement or monitoring should be available if requested. If the vendor is using a fourth or fifth party, those terms are equally applicable to them as well and they will be held accountable if something happens in the extended supply chain.

Ongoing Monitoring

Continuously monitoring environments for potential disruptions and risks is a key requirement in multiple regulatory frameworks. For many regulations, this extends to third parties and subcontractors as well. Being able to continuously monitor third parties enables organizations to manage risks and preserve operational

resilience more effectively and efficiently. Most regulatory regimes recommend monitoring the following third-party risks:

- **Cyber:** Cyber-attacks, data breaches, data loss, threats and vulnerabilities, emerging cyber risks.
- **Operations:** Business resilience, resource management and turnover, mergers and divestitures, infrastructure capacity.
- **Compliance:** Legal (e.g., anti-money laundering, anti-bribery and corruption), regulatory findings, negative news.
- **Financial:** Revenue and expense trending, solvency/bankruptcy, credit ratings, liquidity.
- **Geopolitical:** Pandemics, natural disaster events, location risks, concentration risks.
- **ESG:** Trends with environmental, social and governance topics.

Best Practice Recommendation: Many organizations monitor their third parties inefficiently, using disparate tools in multiple departments with minimal collaboration. Instead, organizations should adopt a consolidated approach that unifies risk insights for widespread stakeholder use and enables risk management teams to leverage insights to validate due diligence assessment results. This will greatly simplify and reduce the time required for regulatory audit reporting.

Awareness Training

Many regulatory frameworks require routine security awareness training to help teams spot social engineering and phishing attacks.

Best Practice Recommendation: Extend this training to contractors, subcontractors and third-party employees to ensure all parties with access to the company's sensitive data and systems are up to date in their knowledge of these tactics. Be prepared to document training processes and results.

Board and Senior Management TPRM Program Governance

Board and senior executive oversight and governance are common requirements in TPRM compliance. Regulations generally require:

- Reporting to show key actionable trends, not just data.
- Incident management processes, including tabletop training for senior management.
- Communications with regulators when there is a material impact on operations.

Best Practice Recommendation: As part of your organization's risk governance program, have an internal audit function perform independent reviews of the TPRM program and reporting.

Triggers for Re-Assessments

Circumstances change, and the following events discovered by ongoing monitoring are important reasons to re-assess third-party relationships:

- Third-party data breach
- Change in ownership, merger or acquisition
- New potential regulatory or reputation risks
- Moving a data center to a new physical location, including offshoring
- Migrating applications or infrastructure to the cloud
- Expansion of the supplier relationship through new business functionality
- Significant changes to the volume or classification of information shared with a third-party
- Deterioration of the supplier's financial situation
- Changes in fourth or Nth party use

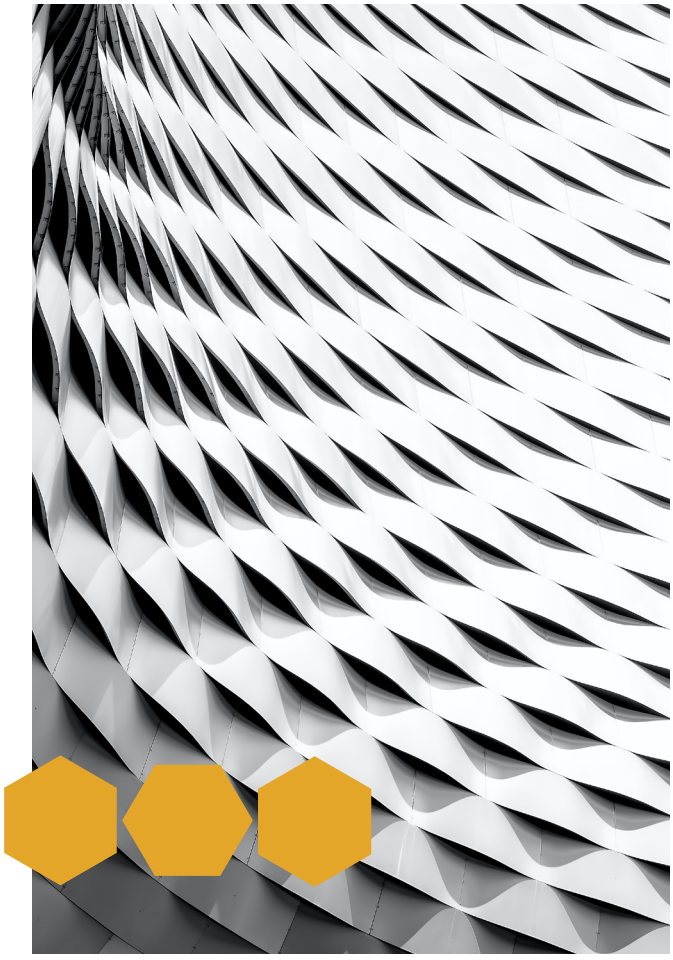
Termination

Most regulatory frameworks require that organizations have a documented exit strategy when outsourcing their critical business functions. For example, the European Banking Authority (EBA) Outsourcing Guidelines says: "Develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested (e.g., by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider)."

The exit strategy must include the following objectives:

- Return or destroy all sensitive information entrusted to the third party and subcontractors during the course of the relationship.
- Terminate all data, infrastructure and physical access for the third party and subcontractors.
- Ensure contractual clauses provide an orderly process for contract termination that prioritizes operational resilience during the transition.

Best Practice Recommendation: Leverage checklists and automated workflows to report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more. This will greatly simplify the process of offboarding third parties and demonstrate to auditors that your organization has a prospective process in place.



> **Develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested...**
>
> -European Banking Authority (EBA) Outsourcing Guidelines

Checklist: Common Compliance Requirements

Use the following checklist to get a head start on meeting TPRM compliance requirements. Remember, these tasks are just the basics. Be sure to contact your internal audit team and external auditors to expand on this list with your organization's specific compliance requirements.

Steps	Requirements	Outcomes	Best Practices
Planning	Determine criticality of existing third-party services and products.	Identify and focus on areas of greatest third-party risk.	Conduct a profiling and tiering exercise to determine inherent risk and identify vendor criticality.
	Inventory existing third-party software.	Ensure effective third-party incident response.	Structure your third-party risk assessments around cybersecurity supply chain risk management frameworks, such as the NIST SP 800-53 r5 and SP 800-161.
Due Diligence & Third-Party Selection	Onboard third parties.	Ensure third-party inventory is comprehensive and low risk, and avoids duplication of functionality, minimizing cost.	Enforce remediations to ensure third parties align with your organization's risk thresholds.
	Gain visibility into extended supply chain.	Ensure all critical suppliers and subcontractors are identified and included in the scope of the TPRM program.	Discover fourth parties through either a targeted assessment or via passive scanning.
Contract Negotiation	Build key provisions – including breach notification, right to audit and commitment to issue remediation – into contracts, including contract provisions for extended supply chain.	Provide regulatory compliance and protection from legal, reputational, financial and operational risks.	Ensure key contract provisions extend to all suppliers; focus on critical business processes.

Steps	Requirements	Outcomes	Best Practices
Ongoing Monitoring	Provide ongoing monitoring of risks to ensure operational resilience.	Use a holistic framework for addressing operational risks – compliance, cyber, financial, geopolitical, operations, ESG risks.	Take a consolidated approach that unifies risk insights for multiple stakeholder usage and enables risk management teams to use the insights to validate due diligence assessment results.
	Re-assess third parties based on specific triggers.	Provide visibility into the need to re-assess potentially critical changes with third parties.	Continuously monitor for a wide range of risks that can impact business resilience – not just cybersecurity.
	Enforce internal and external awareness training.	Improve people and process security for third parties and extended supply chain relationships.	Ensure all parties with access to the company's sensitive data and systems are up to date in their knowledge of these tactics. Be prepared to document training processes and results.
	Establish board and senior management TPRM program governance.	Ensure transparency; set proper "tone at the top" for organizations; implement incident management process and independent oversight for TPRM program.	Have an internal audit function perform independent reviews of the TPRM program and reporting.
Termination	Document third-party exit strategy.	Ensure plan for ongoing operational resilience.	Leverage checklists and automated workflows to report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more.

How Prevalent Helps

Prevalent can help your organization establish a comprehensive TPRM program in line with your broader information security, governance and enterprise risk management programs. With the Prevalent Third-Party Risk Management Platform your organization can:

- Create a centralized vendor inventory at the time of onboarding with profiles that include insights into multiple vendor risk domain areas.
- Quantify inherent risks for all third parties to automatically tier and categorize suppliers and set appropriate levels of further diligence.
- Leverage a large library of more than 200 pre-built templates for third-party due diligence backed by risk quantification, workflow and built-in remediation guidance.
- Map fourth-party vendor ecosystems through dedicated assessments and passive scanning.
- Centralize the distribution, discussion, retention and review of vendor contracts to automate the contract lifecycle and ensure key clauses are enforced.
- Continuously track and analyze external threats to third parties, including monitoring the Internet and dark web for cyber threats and vulnerabilities, as well as public and private sources of operational reputational, sanctions and financial information.
- Automate contract assessments and offboarding procedures to reduce your organization's risk of post-contract exposure.
- Simplify regulatory reporting, with built-in templates for multiple stakeholders, common internal controls frameworks and industry-specific regulations.

Distilling thousands of controls from dozens of third-party risk management regulatory requirements into five steps might seem like an unachievable task, but successfully addressing these steps will provide a solid baseline from which to build your TPRM program.

For more on how Prevalent can help simplify TPRM compliance, request a demonstration today.

About Prevalent

Prevalent 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 and suppliers throughout the third-party lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

To learn more, please visit www.prevalent.net