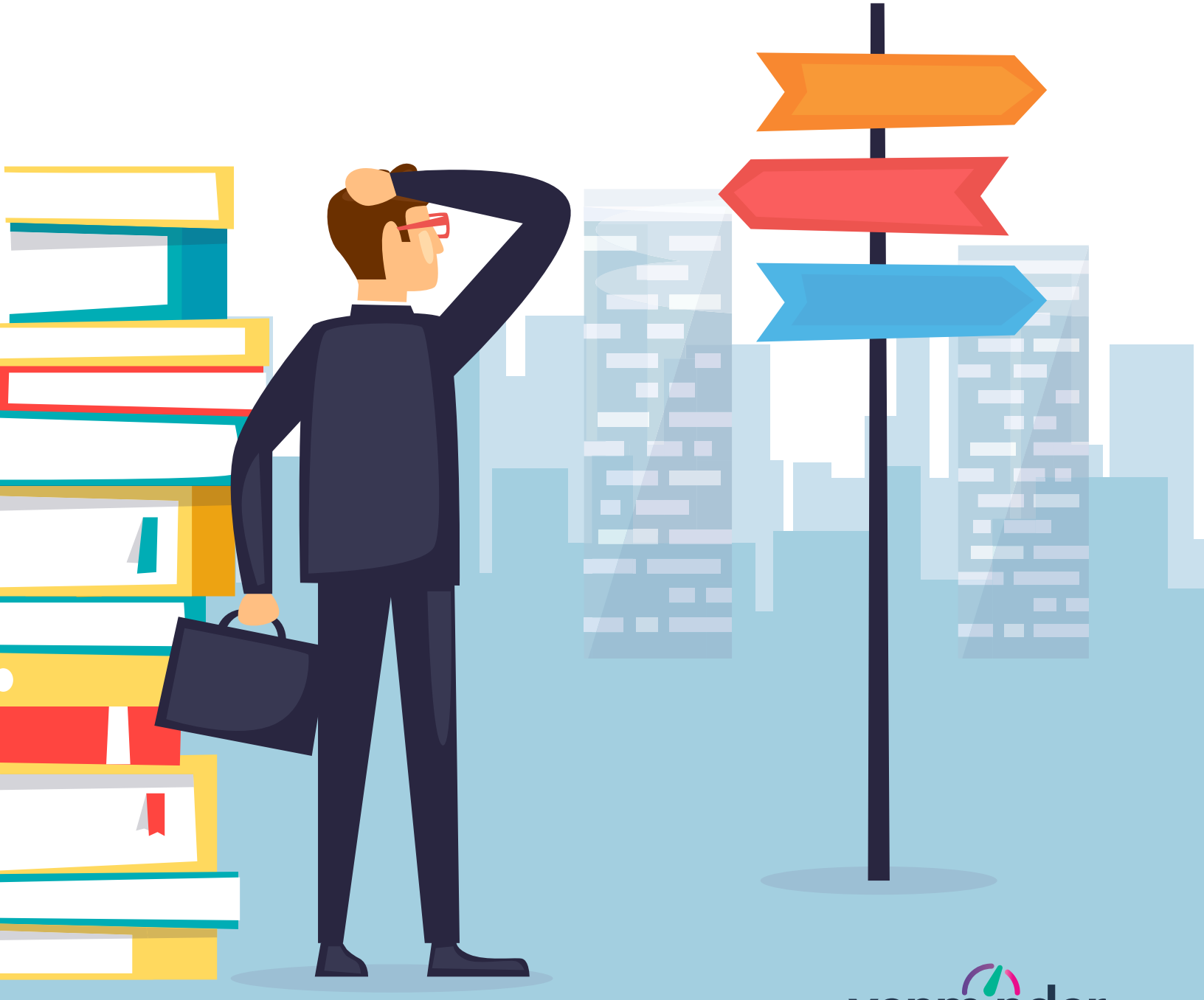
Third-Party Risk Management

GUIDANCE AND REGULATIONS



venminder

Third-Party Risk Management

GUIDANCE AND REGULATIONS

Third-party risk management (TPRM) guidance has historically been issued by financial services regulatory agencies, such as the OCC and FDIC. In recent years however, it's become clear that regulators in other industries are seeing the value of TPRM and have since published their own guidance.

Automotive, healthcare, and higher education industries are just a few examples of where regulators are looking at TPRM with more scrutiny. Even if your organization isn't regulated, it's always a good idea to note current TPRM guidance and best practices that can keep your organization safe. After all, third-party risk is something that impacts nearly every organization, regardless of industry.

Regulatory guidance and best practices can change over time, so it's worth actively reviewing new information as it becomes available. Legal analysis by a qualified expert can help determine where your practices should be changed and updated. Regulatory examinations are another opportunity to review any provided recommendations and adjust your practices as needed. The guidance listed here is not all-inclusive, as there are many other regulators such as state or local agencies that may govern your organization and industry.

This eBook contains helpful information and tips to comply with various TPRM guidelines.

Interagency Guidance on Third-Party Relationships: Risk Management

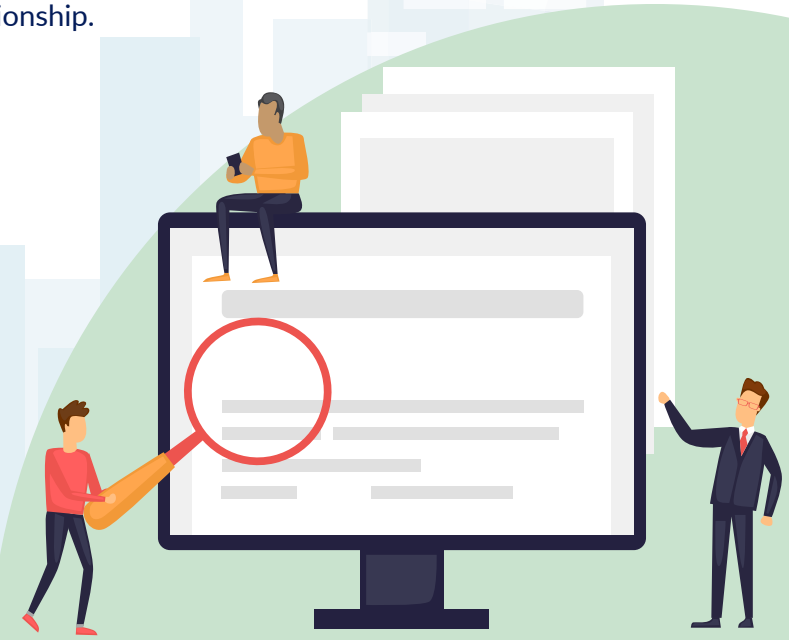
In June 2023, the **Interagency Guidance on Third-Party Relationships: Risk Management** was jointly released by the Federal Reserve Board, FDIC, and OCC. It gives unified regulatory expectations on how banking organizations should manage their third-party relationships. Each agency had issued its own third-party risk management (TPRM) guidance over the years, which has now been replaced by this final guidance.

Although this guidance is aimed towards banking organizations, many of the best practices outlined throughout are applicable for other industries. Plus, this guidance is further proof that regulators often look to each other for TPRM standards and expectations. It shouldn't be surprising to see regulators in other industries take note of this guidance for their own use.

Key takeaways from the guidance:

- **Determine criticality and inherent risk.** Regulators will expect different levels of oversight, depending on each vendor's risk level and criticality, so it's essential to have a process in place that can identify these criteria. A critical activity is generally one that will have a significant impact on your customers if it fails or doesn't meet expectations. It may also have a significant impact on your finances or operations.

- **Expand the scope of your TPRM program.** The Interagency Guidance makes it clear that all business arrangements and third-party relationships are in scope for TPRM. While this may seem like an increased burden on your program's limited resources, regulators do not expect the same level of oversight or management for every third-party relationship.



- **Understand common risks.** Examples of third-party risks include strategic, reputation, operational, transactional, credit, and compliance. Once you understand how regulators define these risks, you can identify them easier within your third-party relationships.

- **Implement a TPRM lifecycle that aligns with the guidance.** The overall goal of the lifecycle is to identify, assess, monitor, and manage third-party risk. This can be achieved by various activities throughout the onboarding, ongoing, and offboarding stages. Those activities should include inherent risk assessments, due diligence, vendor selection, contract management, documentation and reporting, ongoing monitoring of risk and performance, and contract termination.

- **Ensure proper oversight and reporting.** The guidance specifies that an organization's board of directors is responsible for overseeing the TPRM lifecycle, particularly when it involves higher-risk activities. The board of directors should oversee activities, such as reporting of ongoing monitoring and issue remediation. You should create a concise and consistent reporting format for the board and senior management.

- **Evaluate your vendor's financial performance.** A vendor's poor financial performance can lead to several negative consequences for your organization, such as unmet service level agreements (SLAs), regulatory fines, or increased cybersecurity risk. Review the financial health of your vendor to ensure that your organization won't be facing any surprises down the line.

- **Include fourth parties in your contract.** Fourth and nth parties shouldn't be overlooked just because you don't have a contractual relationship with them. When necessary, include contractual provisions defining which products or services are subcontracted to a fourth party. And include terms and conditions that obligate your third party to manage their vendors (your fourth and nth parties) to the standards your organization deems acceptable.

- **Create a regular cadence of ongoing monitoring.** The frequency and scope of your ongoing monitoring activities will vary depending on the vendor's risk and criticality, but regulators expect organizations to regularly assess different areas such as their vendors' performance, effectiveness of their controls, and any emerging issues. Ongoing monitoring is typically performed by the vendor owner or manager who can identify any changes in performance or risk. These changes should then be communicated to a qualified subject matter expert (SME) who can determine an acceptable remediation plan.

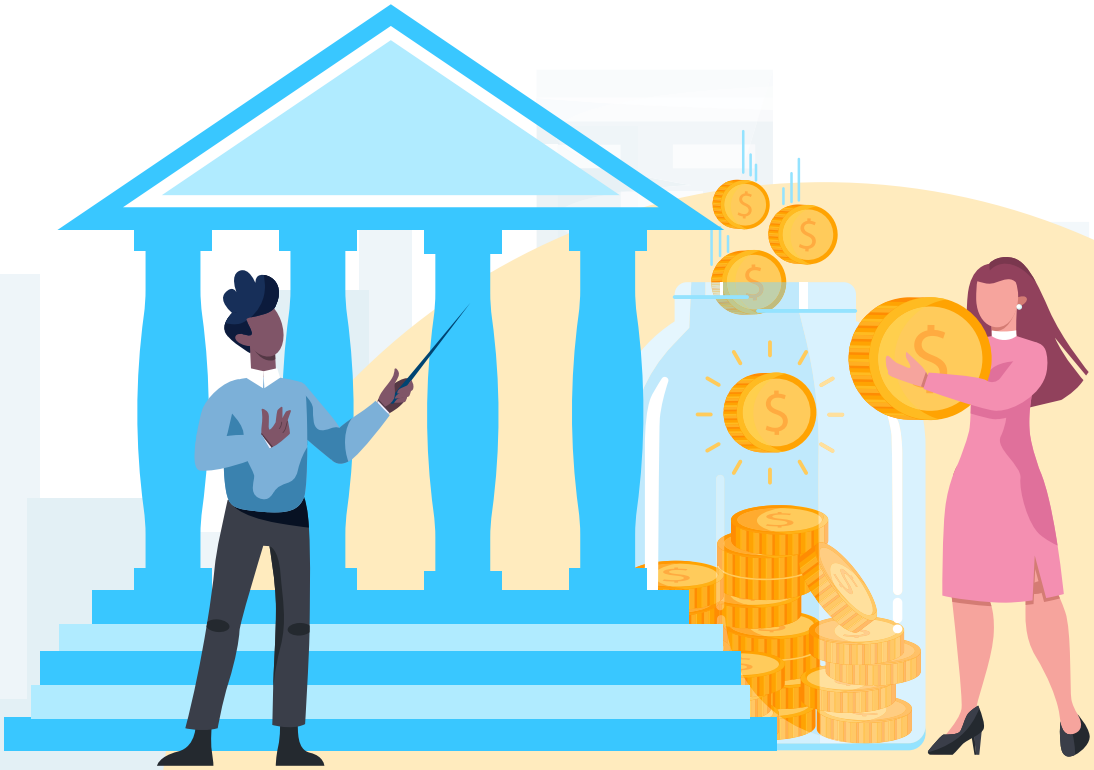
OFFICE OF THE COMPTROLLER OF THE CURRENCY (OCC)

In addition to the Interagency Guidance, the OCC covers foreign third-party service providers in **Bulletin 2002-16.** The OCC states that foreign-based third parties may require additional oversight because of their unique risks to federal savings associations and national banks.

Key takeaways from the guidance:

- **Monitor country and compliance risk.** Foreign third parties may be impacted by political, social, and economic events, so it's essential for organizations to monitor these risks and implement contingency plans and exit strategies as needed. Organizations must also ensure that their foreign third-party vendors comply with U.S. regulations.

- **Consider contract management.** The OCC gives specific guidance on managing contracts with foreign third parties, such as including choice of law covenants, privacy provisions, and assurance of confidentiality of information.



FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

The FDIC is the second regulator that helped shape third-party risk management (TPRM) standards in the Interagency Guidance. Additional TPRM guidance from the FDIC can be found in **FIL-3-2012**, **FIL-43-2013**, and **FIL-41-2014**, which relate to third-party payment processor relationships. You can find information about risk mitigation, due diligence, and ongoing monitoring expectations in these three letters.

Key takeaway from the guidance:

- **Establish robust due diligence requirements.** Vendors with elevated risk should be subject to higher levels of due diligence, which may include on-site visits and an assessment of the vendor's marketing materials. Some organizations may also need to review their vendor's due diligence procedures to determine whether their standards are adequate and meet regulatory requirements.

FEDERAL RESERVE (THE FED)

The Fed is the final regulator that took part in creating the Interagency Guidance, along with the OCC and FDIC. Although they don't have any additional guidance, third-party risk management (TPRM) is also mentioned in the Fed's semiannual Supervision and Regulation Report, which outlines their examination priorities.

Federal Financial Institutions Examination Council (FFIEC)

All primary financial regulators have a seat at the table of the FFIEC, where they compare best practices, share concerns, and promote uniformity on how to supervise financial institutions.

The FFIEC's **Information Technology Examination Handbook** is a comprehensive resource that guides examiners in assessing a financial institution's security risks. The handbook contains a wealth of information, including risk mitigation procedures, criteria for an incident response program, and an appendix of related laws, regulations, and guidelines. Also consider the handbook's **Appendix J**, which focuses on third-party resiliency, and the **Outsourcing Technology Services Booklet**, which outlines the examination procedures for managing and monitoring third-party IT relationships.

Another regulation worth considering is the **Vendor and Third-Party Management** section in the Retail Payment Systems Risk Management booklet. Like the guidance for financial institutions, this emphasizes the importance of contract provisions and due diligence processes for the retail payments systems industry.

Key takeaways from the guidance:

- **Review your business continuity plans.** Verify that they meet the FFIEC's expectations for strengthening the resilience of technology service providers (TSPs). Appendix J highlights four elements of effective business continuity (BC) planning: responsibility to control the TSP and its subcontractors' BC risks, addressing the potential impact of a significant business disruption, validating and testing BC plans, and addressing cyber resilience.

- **Establish good contract management.** Contracts should be reviewed by a legal team and qualified subject matter experts before entering a third-party relationship. This helps ensure that the contract meets the FFIEC's expectations on business resilience, such as defining service level agreements (SLAs) and including the right to audit.

- **Thoroughly document and test your third-party risk management (TPRM) program.** Proper documentation is essential for reporting third-party risk management (TPRM) activities to the board and senior management so they can stay informed of evolving third-party risks and make changes to the program as needed.

Consumer Financial Protection Bureau (CFPB)

The CFPB sets clear expectations regarding third-party oversight in **Compliance Bulletin and Policy Guidance 2016-02**. Traditional oversight guidance generally focuses on third-party risk to an organization, but this CFPB guidance offers a slightly different perspective. The CFPB's mission is to protect consumers from financial harm, so this bulletin focuses on third-party risks that can negatively impact a consumer's financial well-being.

With this perspective, organizations should look at their third-party vendors as extensions of their operations. The CFPB's guidance leans more toward reviewing a vendor's policies and procedures related to compliance management systems. Simply put, you should ask, "How can this vendor negatively impact my customer?"

Key takeaways from the guidance:

- **Prioritize compliance with your vendors.** Conduct thorough due diligence to verify your vendor is capable of understanding and applying regulatory compliance requirements.
- **Include unfair, deceptive, or abusive acts or practices (UDAAP) in your contract.** This will set the expectations of remediation and help ensure that your vendor isn't involved in any activities that may fall under unfair, deceptive, or abusive acts or practices.
- **Obtain policy and procedure documentation from your vendor.** These will offer greater insight into the overall internal operations of your vendor.
- **Incorporate ongoing monitoring.** A vendor's performance and risk can change over time, so it's essential to monitor your vendor to remediate issues as they occur.

U.S. Securities and Exchange Commission (SEC)

Third-party risk management (TPRM) guidance from the SEC is primarily found in its annual **Examination Priorities**. This publication highlights different focus areas which can help organizations better prepare for exams. Another regulation worth noting is the **SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures**. This guidance isn't heavily focused on TPRM practices but specifically mentions the need for organizations to consider third-party cybersecurity risks.

Although not yet in effect, a proposed rule on **Outsourcing by Investment Advisers** would require registered investment advisors (RIAs) to conduct due diligence and perform ongoing monitoring of their third parties.

Key takeaways from the guidance:

- **Ensure you have strong cybersecurity practices.** This includes reviewing your vendor's cybersecurity program, especially if they rely heavily on technology and have access to your organization's or customer's data. The SEC and OCIE have stated the importance of vendor cybersecurity, and an OCIE examiner may request your internal findings from your cybersecurity controls program.

- **Identify your covered functions and service providers.** These activities and vendors meet one of the following criteria:

    - Your organization deems them necessary to provide services that must comply with Federal securities laws.

    - They would have a negative material impact on your customers if they performed negligently or not at all.

The SEC provides examples of covered functions for its proposed rule, including cybersecurity, investment risk, and record keeping. Understanding which of your vendors are covered by this rule is an excellent first step to ensure compliance.

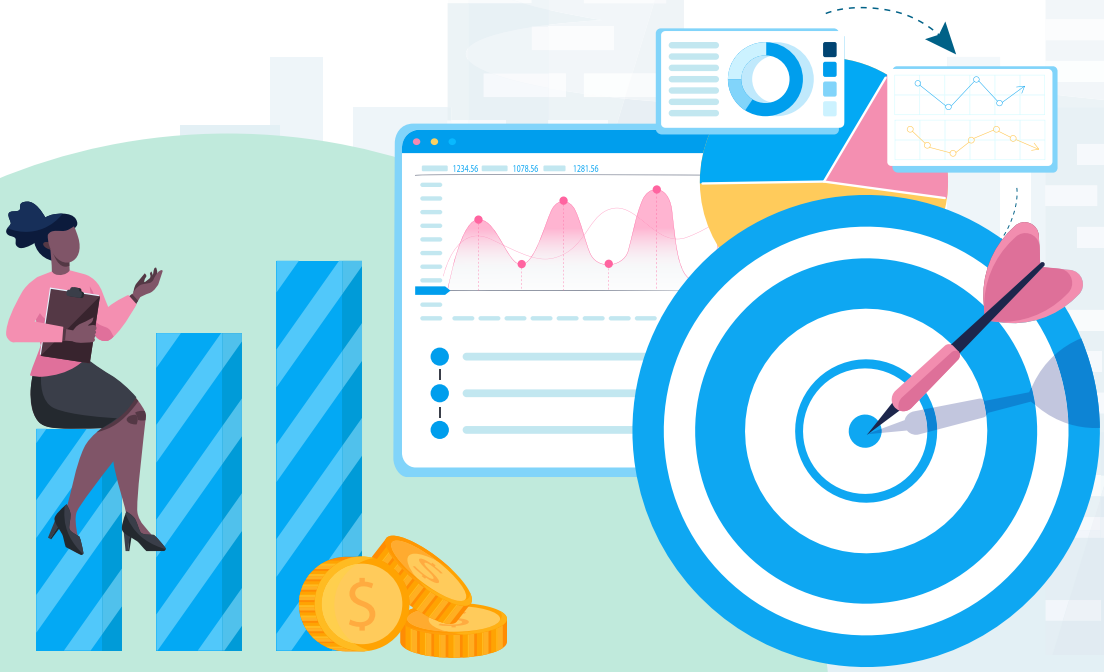
National Credit Union Administration (NCUA)

The NCUA's guidance **SL No. 07-01** is a bit older, but is still a good foundation for third-party risk management (TPRM) best practices. This Supervisory Letter for credit unions highlights the importance of risk assessments, due diligence, and contract management. A third-party relationships questionnaire can be found within the guidance **08-CU-09**, which shows how NCUA examiners will evaluate these relationships. **SL No. 17-01** provides additional guidance on compliance risk indicators and exam procedures. Technology and cybersecurity best practices have changed drastically since the initial publication of 2007's SL No. 07-07, so it's best to review this NCUA guidance alongside more current standards.

Key takeaways from the guidance:

- **Planning is essential during the onboarding stage in your TPRM lifecycle.** Even before you complete an initial risk assessment and perform due diligence, it's important to consider whether a vendor will support your strategic goals. A third-party relationship will have risks and benefits, as will the decision to keep the activity in-house.

- **Determine your vendor's criticality.** This is typically determined by the vendor's material impact on your organization or customers. A vendor would likely be critical if its failure could cause significant disruption to your organization or customers. Similarly, your organization and customers might be negatively impacted if a critical vendor requires more than 24 hours to restore service.



U.S. Department of Health and Human Services (HHS)

The healthcare industry is a prime target for cybersecurity incidents, often involving third-party vendors. The **Health Insurance Portability and Accountability Act (HIPAA)** is a comprehensive regulation that incorporates the Privacy Rule, Security Rule, and Breach Notification Rule. These rules state that HIPAA-covered entities may share protected health information (PHI) with third parties, but only if the third party can ensure that they'll safeguard the information. In certain circumstances, HIPAA also includes requirements for covered entities to notify individuals of data breaches.

Key takeaways from the guidance:

- **Include breach notification requirements in your contract.** Make sure to include details such as notification timelines, a designated person(s) of contact, and how the vendor will investigate and remediate the breach.

- **Conduct robust third-party risk assessments.** An inherent risk assessment is one of the first steps to take in any third-party relationship. This will give you more insight into the vendor's risk profile, security assurances, and the amount and type of due diligence you'll need to collect and review.

Federal Trade Commission (FTC)

In recent years, the FTC's **Safeguards Rule** has expanded in scope to higher education and the auto industry. Because these industries deal heavily with sensitive customer information, regulators expect them to implement and maintain information security programs.

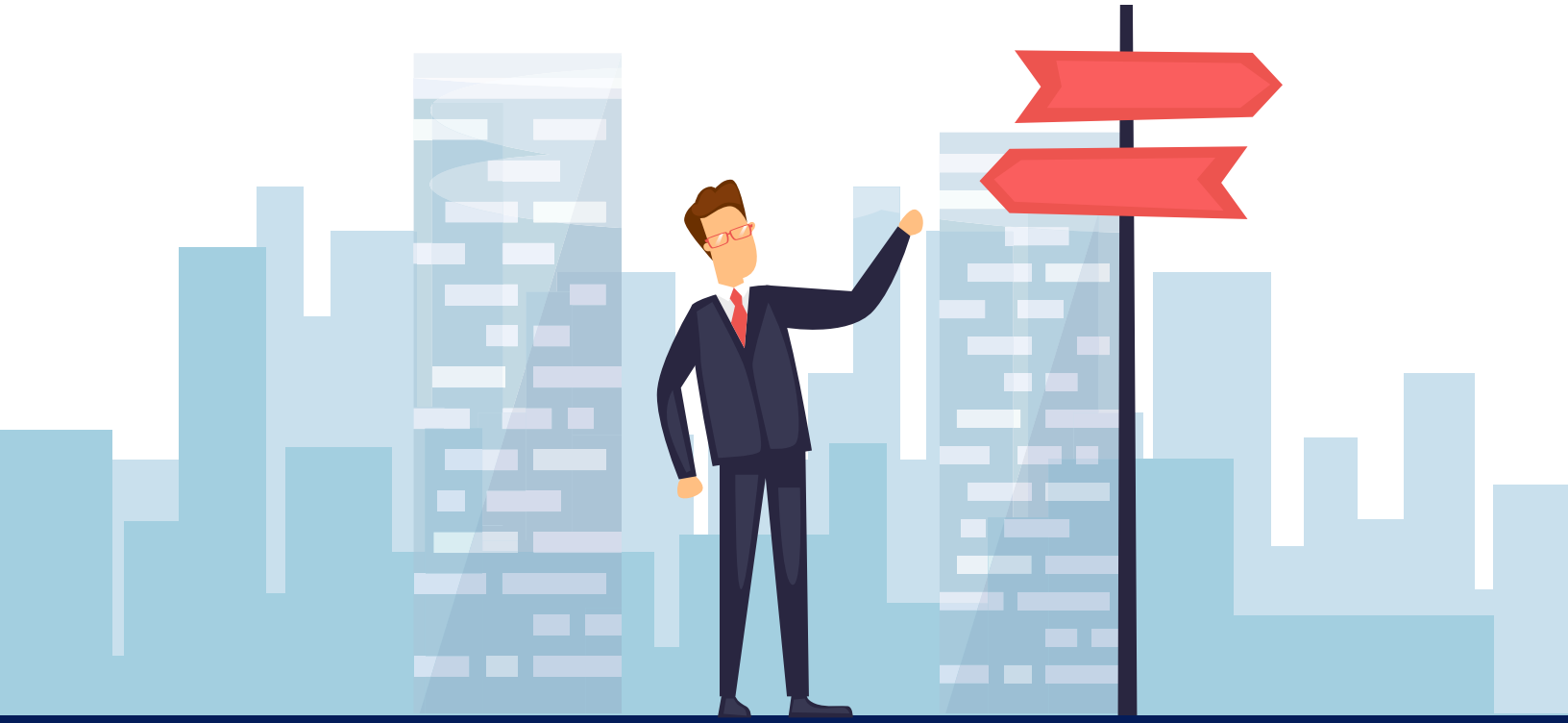
Key takeaways from the guidance:

- **Obtain a qualified subject matter expert (SME).** Whether your organization outsources this position or retains the SME in-house, it's essential to have a qualified SME who can implement and monitor your information security program.
- **Implement a schedule of regular reviews.** Access controls, user activity, and app security are just some of the safeguards that should be regularly reviewed so you can identify and resolve any issues as they occur.
- **Establish an information disposal process.** The Safeguards Rule states that customer information should be securely disposed of within two years since it was last used. There are two exceptions – you have a business need or legal requirement to save the information, or the information is maintained to prevent you from disposing of it.

It's clear that regulators across many industries are paying more attention to TPRM. As regulators look to each other for best practices and guidance, consider how your organization can implement these guidelines into your TPRM program. Taking these steps will reflect positively with regulators, your customers, the board, and senior management.

Download free samples of Venminder's vendor Control Assessments and see how they empower third-party risk professionals in mitigating risks.

Download Now



venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

+1 (888) 836-6463 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise, and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting, and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals, and more, are readily available in an online exchange library. The assessments enable customers to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance, and more.