Compliance and Third Party Risk Management Guide

A FUNCTION FOR CONTINUED SUCCESS

One PPG Place, Suite 1700
Pittsburgh, PA 15222
(412) 697-5200
www.schneiderdowns.com

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

Compliance and Third Party Risk Management Guide

A FUNCTION FOR CONTINUED SUCCESS

Third Party Risk Management (TPRM) has always been a compliance hurdle that seems to be a 9-headed monster, due to the ever-evolving headaches associated with vendor onboarding/off boarding, due diligence, the RFP process, legal obligations, contractual requirements, compliance requirements, performance requirements and continuous monitoring. Additionally, third party relationships carry numerous hidden risk factors including strategic risk, reputation risk, operational risk, transaction risk, credit risk and compliance risks, the primary focus of this paper.

Our TPRM team at Schneider Downs has developed a cheat-sheet to help you and your organization better understand the regulatory and compliance landscape, and how it fits into your third party risk management program.

Third Party Risk Management Guide: Getting Started

Understand your enterprise's compliance concerns through an enterprise risk assessment

Enterprise-wide risk assessment help you better understand the interworking third party relationships that your company relies on to perform daily business operations. A few things to consider when embarking on an enterprise risk assessment is to first identify critical/high risk suppliers/third parties. For example, if you are a company positioned in the financial sector, understanding a supplier's risk for potential bribery can be a great starting point.

Additionally, other raw attributes such as time in business, degree of marketplace activity, location, severe financial risk indicators and changes in circumstances can help fuel your risk-assessment model. In assessing risk, businesses should consider leveraging third party data, insights and proprietary predictive scores, which can greatly strengthen client controls, risk triggers and defensible position pillars. Various third party "insight" tools exist, such as BitSight, RiskRecon, SecurityScorecard and RiskLens. These insights help strengthen compliance programs by enhancing depth of due diligence and moving beyond sole reliance on self-disclosed information from a questionnaire.

Perform necessary due diligence related to the business sector and risk of the third party

A simple employee screening/background check is not enough information to comprehensively assess a potential vendor to determine whether that third party is viable to work with your organization. We recommend seeking a depth of diligence that includes leveraging global data assets on entities, including legal name, organizational structure, parent companies, names of all principals/officers/beneficial owners, and industry. This allows your company to understand the holistic structure behind a specific vendor/supplier and understand their risk at an even better level than through the enterprise risk assessment.

Establish a comprehensive Third Party Management Program

Your firm/company should leverage a third party/vendor management program that includes all the necessary steps to performing a full end-to-end third party/vendor management review. This program should include all the necessary touchpoints your firm believes are necessary to properly assess and onboard a potential vendor or supplier. Schneider Downs suggests that a third party/vendor management program should include the following requirements:

- Vendor Selection Process
- Vendor Risk Assessment Process
- Due Diligence Process
- Contractual / Regulatory Review Process
- Reporting Process
- Ongoing Monitoring Procedure

Although a third party/vendor management program should include the items listed above, a program is not limited to this list. It is helpful to note that the process' noted above are "living and breathing" meaning that these process' will need tuned in order to assist your organization in assessing third parties and vendors properly.

Create a process for company-wide monitoring and an approach to risk management

Having the right governance and internal controls in place helps companies benefit from complete visibility into third party transactions. By managing internal regulatory requirements, incoming third party compliance requirements can seem less daunting as your firm may already have a process established on how to deal with evolving compliance hurdles. Additional risks you should also consider monitoring for are financial, human rights, data privacy and cybersecurity risks.

Although the listing above provides a great summary of an efficient TPRM program, we would like to direct you to the listing below that identifies the most relevant TPRM-specific compliance requirements. The following regulatory/certification standards all include requirements that your organization (if working with third parties) must maintain the following:

- A listing of your critical third parties as it relates to your business operations (a company that provides your daily kitchen supplies is not a critical third party)
- Assess your critical third parties on an annual basis through an agreed upon methodology and determine whether your third parties are adhering to the same regulatory/certification standards
- Establish an ongoing monitoring program to ensure all your critical third parties are aligning to regulatory, legal and contractual standards.

Third Party Risk Management Guide: Regulatory and Certification Standards

System and Organization Controls (SOC)

This series of standards designed to help measure how well a given service organization conducts and regulates its information. A SOC 1 report is designed to address internal controls over financial reporting while a SOC 2 report addresses a service organization's controls that are relevant to their operations and compliance. One or both could be right for your organization. Controls in scope related to TPRM are:

- **CC2.3**: The entity communicates with external parties regarding matters affecting the functioning of internal control.
- **CC9.2**: The entity assesses and manages risks associated with vendors and business partners.

Payment Card Industry (PCI)

PCI compliance is mandated by credit card companies to help ensure the security of credit card transactions in the payments industry. The Payment Card Industry Security Standards Council was originally formed in September 2006 by American Express, Discover Financial Services, JCB International, MasterCard and Visa Inc. with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard. Controls in scope related to TPRM are:

- **8.3**: Is two-factor authentication incorporated for remote network access originating from outside the network by personnel (including users and administrators) and all third parties (including vendor access for support or maintenance)?
- **9.9.3**: Are personnel (including third party employees) trained to be aware of attempted tampering or replacement of devices?
- **12.3.9**: Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?
- **12.3.10**: For personnel accessing cardholder data via remote-access technologies, does the policy specify the prohibition of copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need?
- **12.8**: Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data?
- **12.8.1**: Is a list of service providers maintained?
- **12.8.2**: Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?
- **12.8.3**: Is there an established process for engaging service providers, including proper due diligence prior to engagement?
- **12.8.4**: Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?
- **12.8.5**: Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?

The Office of the Comptroller of the Currency (OCC)

The OCC is a federal agency that oversees the execution of laws relating to national banks. The OCC charters, regulates, and supervises all national banks and federal savings associations as well as federal branches and agencies of foreign banks. Controls in scope related to TPRM are:

- **OCC Bulletin 2013-29**
  - » A bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.
  - » A bank should ensure comprehensive risk management and oversight of third-party relationships involving critical activities.
- An effective risk management process throughout the life cycle of the relationship.
  - » Plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.
  - » Proper due diligence in selecting a third party.
  - » Written contracts that outline the rights and responsibilities of all parties.

ISO/IEC 27001

This certification specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an audit. Controls in Scope related to TPRM are:

- **15.1**: Information Security in supplier relationships
- **15.2**: Supplier service delivery management

Sarbanes-Oxley Compliance (SOX)

The United States Congress passed the Sarbanes-Oxley Act in 2002 and established rules to protect the public from fraudulent or erroneous practices by corporations and other business entities. The goal of the legislation is to increase transparency in the financial reporting by corporations and to require a formalized system of checks and balances in each company. Controls in Scope related to TPRM are:

- **APO10.01/APO10.02**: Selection of vendors for outsourced services is performed in accordance with the enterprise's vendor management policy and process.
- **APO10.03**: A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.
- **APO10.04**: Third-party service contracts address the risk, security controls and procedures for information systems and networks in the contract between the parties.

HITRUST CSF

HITRUST CSF is a security framework that aggregates relevant information security controls from the standards and regulations incorporated into HIPAA. Thus, it creates a single framework that healthcare providers and their business associates can use to meet the technology requirements embedded in HIPAA. Controls in Scope related to TPRM are:

- **5.02 External Parties**: To ensure that the security of the organization's information and information assets, are not reduced by the introduction of external party products or services.

- **05.i Identification of Risks Related to External Parties**: The risks to the organization's information and information assets from business processes involving external parties shall be identified, and appropriate controls implemented before granting access.

Federal Risk and Authorization Management Program (FedRAMP)

FEDRAMP is US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that saves cost, time, and staff required to conduct redundant Agency security assessments. Requirements to be considered related to TPRM are

3rd Party Assessment Organizations (3PAOS)

3PAOS play a critical role in the FedRAMP security assessment process, as they are the independent assessment organizations that verify cloud providers' security implementations and provide the overall risk posture of a cloud environment for a security authorization decision. These assessment organizations must demonstrate independence and the technical competence required to test security implementations and collect representative evidence. 3PAOs must:

- Plan and perform security assessments of CSP systems
- Review security package artifacts in accordance with FedRAMP requirements

Privacy Standards

Gramm-Leach-Bliley Act (GLB Act or GLBA)

Also known as the Financial Modernization Act of 1999, the GLB Act is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information. Requirements to be considered related to TPRM are:

- A financial institution must provide notice of its privacy policies and practices, and allow the consumer to opt out of the disclosure of the consumer's nonpublic personal information to a nonaffiliated third party if the disclosure is outside of the exceptions in sections 13, 14, or 15 of the regulation.

General Data Protection Regulation (GDPR)

GDPR is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas. Requirements to be considered related to TPRM are:

- Sign a data processing agreement between your organization and any third parties that process personal data on your behalf.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. Requirements to be considered related to TPRM are:

- **Privacy**: An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party.

California Consumer Privacy Act of 2018 (CCPA)

CCPA gives consumers more control over the personal information that businesses collect about them. This landmark law secures new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.

The New York SHIELD Act

This Act requires any person or business owning or licensing computerized data that includes the private information of a resident of New York ("covered business") to implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information. Requirements to be considered related to TPRM are:

- Is the organization conducting internal controls-based assessments of third-parties based on the requirements in applicable laws such as GLBA, HIPAA, or NYCRR Part 500?
- Is the organization monitoring external third-party networks and utilizing business risk intelligence such as news events, financials, layoffs, leadership changes, lawsuits, etc. that can serve as predictors of future vulnerabilities?
- Is there a defined process in place to identify, categorize, prioritize, and manage risks to an acceptable level?
- Does the organization have a defined workflow process in place to escalate identified risks for remediation?

How Can Schneider Downs Help?

Schneider Downs is a registered assessment firm with the Shared Assessments Group, the clear leader in third party risk management guidance. Our personnel are experienced in all facets of vendor risk management, and have the credentials necessary (CTPRP, CISA, CISSP, etc.) to achieve meaningful results to help your organization effectively achieve new vendor risk management heights. In addition to our third party risk management services, our team of IT audit and compliance professionals provide a growing slate of services including:

- Business Continuity and Disaster Recovery Planning
- Cybersecurity Maturity Model Certification (CMMC)
- FFIEC IT Compliance Assessment
- GDPR Compliance
- HIPAA Compliance Assessment
- HITRUST
- Information Technology Audit
- IRS Publication 1075
- ISO 27001 Compliance Assessment
- IT General Controls Audit
- The National Institute of Standards and Technology (NIST)
- Payment Card Industry DSS Compliance
- Risk Assessment Services
- Sarbanes-Oxley Compliance Audits
- SOC Reporting

CONTACT US

contactsd@schneiderdowns.com
www.schneiderdowns.com/tprm

Register to receive our bi-weekly newsletter, Focus on Cybersecurity, at www.schneiderdowns.com/subscribe.

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

www.schneiderdowns.com

© 2020 Schneider Downs & Co., Inc.

SOURCES

www.cdc.gov/phlp/publications/topic/hipaa.html
www.digitalguardian.com/blog/what-pci-compliance
www.dnb.com/perspectives/corporate-compliance/how-to-manage-third-party-risk.html
www.fdic.gov/news/financial-institution-letters/2008/fil08044a.pdf
www.fedramp.gov
www.gdpr.eu
www.investopedia.com/terms/g/glba.asp
www.oag.ca.gov/privacy/ccpa
www.occ.treas.gov/
www.prevalent.net/blog/new-york-shield-act-where-third-party-risk-management-comes-into-play/
www.securitymetrics.com/blog/what-hitrust-compliance
www.sixfifty.com/the-ccpa-and-third-parties-what-is-required/
www.varonis.com/blog/sox-compliance/
www.venminder.com/blog/what-is-a-vendor-management-program
www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html