CYBERSECURITY COLLABORATIVE

A CyberRisk Alliance Community

V2.0

Third Party Risk Management Program 2022

Implementation Guide for Addressing New Threats and Regulations

A CISO Developed Resource

Table of Contents

Acknowledgements

The Cybersecurity Collaborative would like to acknowledge the CISOs and staff of the following member organizations for their collaborative efforts which, through discussions, experience, and research, provided the content for this document.

Please direct any questions to members@cyberleadersunite.com

2U

AMERICAN FAMILY INSURANCE

CENTERS FOR MEDICARE AND MEDICAID INSURANCE (HHS)

COATS

DELTA DENTAL

DEPARTMENT OF TRANSPORTATION, NEW YORK CITY

DUCK CREEK TECHNOLOGIES

ELI LILLY

HUMANA

INTEROS

NATIONWIDE MUTUAL INSURANCE COMPANY

NISSAN

ONEMAIN FINANCIAL

ORANGE COUNTY GOVERNMENT FLORIDA

PENN NATIONAL INSURANCE

ROCKWELL AUTOMATION

Overview

Introduction

We rely on third parties for handling many business functions, such as managing computing infrastructure, providing security services, processing payroll, and developing computing applications. However, each third party poses a security risk. Third-party vulnerabilities, when exploited, could expose our confidential data or impact the availability of our services. Some of these vulnerabilities are subtle or hard to detect, but potentially devastating nonetheless, like the Target and SolarWinds breaches.

Only through the effective operation of a third-party risk management (TPRM) program, which formally and continuously assesses and treats third-party risks, do we have any hope of managing these risks.

Version 1.0 (2021) of this document (*Third-Party Risk Management Program 2021 – Implementation Guide*) established a TPRM framework and provided guidance for implementing a TPRM program. Version 2.0 (*Third-Party Risk Management Program 2022 – Implementation Guide for Addressing New Threats and Regulations*) incorporates the findings and best practices from the Third- and Fourth-Party Incident Response Task Force.

Guidance Document Purpose and Audience

Purpose and Audience. This document, and its supporting tools and templates, is a guide to help an entity, like a commercial enterprise, non-profit organization, or government organization, establish or improve a TPRM program. It is intended for CISOs or their management who do not have a TPRM program and want guidance on establishing one or desire to improve the efficiency and effectiveness of their current TPRM program.

This document is for members of the Cybersecurity Collaborative and may not be distributed to non-member organizations or individuals. The TPRM Program Workbook is an exception, as this supplemental tool is designed for members to send to third parties as part of their TPRM program.

A TPRM program is a key component of an overall cybersecurity program that protects the confidentiality, integrity, and availability of an entity's information and processes handled or managed by a third party. A third party is an independent, legal entity that provides goods and services to another legal entity, such as a company or government agency. In general, a third party is a part of a company's supply chain. Examples of third parties include companies that manage another entity's IT infrastructure, supply computing equipment, provide applications development contractors, or provide human resource applications. In the context of this document, the words supplier, vendor, and third party are used interchangeably.

Guidance Document Purpose and Audience (cont.)

A TPRM program is key to complying with many industry security standards, such as NIST CSF, ISO 27001, and PCI-DSS, in addition to security regulations like the New York State Department of Financial Services (NYSDFS) Cybersecurity Requirements for Financial Services Companies. These standards require controls and processes to assess and address information and processing risks imposed by third parties.

Document Structure. The document identifies new threats, regulatory pressures, and strategies to address them. It then delineates and describes components of a TPRM program before addressing one of the key components, the TPRM program lifecycle framework. Within this section, each lifecycle phase is described in terms of objectives, processes, and systems, including tips for improving process effectiveness. Last, this guide ends by answering frequently asked questions about TPRM programs.

Supporting Tools and Templates. In addition to this document, there are two templates and a compendium to help member organizations build or enhance their TPRM program.

1. *Third-Party Risk Management Standard*. As a modifiable template, this document will supplement organizational security policies by defining the required components and processes of a TPRM program.

2. *TPRM Program Workbook*. This Excel-based workbook contains two tabs. The first can record and document TPRM activities for each third party, while the second is a security questionnaire that third parties can complete as part of the assessment process, as described later in this document. The questionnaire automatically scores the strength of the entity's cybersecurity program. The TPRM Program Workbook includes a supplier security scorecard.

3. *TPRM Program Compendium: Strategies for Addressing New Threats and Regulations*. This guidance document summarizes task force strategic guidance recommendations for addressing new threats and regulations, like log4j and *NYSDFS Cybersecurity Requirements for Financial Services Companies*, respectively.

New Threats, Regulatory Pressures, and Strategies to Address Them

The scope of a TPRM program is rapidly changing, as its importance to an entity's cybersecurity program. As organizations increasingly rely on the uninterrupted supply of products and services from third parties, new threats are emerging along with greater regulatory scrutiny of TPRM program management.

New Threats

It is now within a TPRM program's scope to address critical, pervasive vulnerabilities, defined as highly exploitable, widespread, and usually with a high CVSS score. SolarWinds and Log4j are current examples of critical, pervasive vulnerabilities.

First discovered by FireEye, a plug-in to the SolarWinds' Orion software was compromised. This vulnerability allowed the attacker, Cozy Bear (APT 29), to communicate to third-party servers and execute commands to transfer files, run programs, reboot machines, and destroy information. Since the SolarWinds' Orion software is a widely used network and applications monitoring platform, this is an excellent example of a critical, pervasive vulnerability.

More recently, the Apache Log4j vulnerability was discovered. This vulnerability allows remote attackers to gain control over vulnerable targets. To remotely execute code, the attacker only needs to send a malicious request that contains a formatted string that the Log4j library then picks up. This vulnerability is highly pervasive in libraries, embedded code, Cloud applications (e.g., Salesforce, Success Factors), and software developed by commercial firms.

The SolarWinds and Log4j vulnerabilities prompted entities to reach out to their third parties to ensure they were addressing the vulnerabilities. This is an example of TPRM programs no longer focusing on incident response but expanding to monitor third-party management of critical, pervasive vulnerabilities.

Regulatory Pressures

Task force members in the financial services industry noted greater regulatory scrutiny of their TPRM programs by NYSDFS and the Securities and Exchange Commission (SEC). This increased scrutiny prompted them to invest in commercial TPRM and security evaluation systems to help manage the following current and anticipated regulatory audit requirements:

- Most regulators do not look at fourth parties, but the belief is that they will soon ask questions about how fourth-party risks are being addressed.
- Auditors are now examining how companies monitor processes and ensure that they are monitoring at the frequencies stated in policies.
- Auditors are asking if businesses are looking at findings, including SOC 2 exceptions, and following up on these findings.
- If there are dependencies, auditors will look at third-party business continuity plans.
- External financial auditors were examining third-party responses to SolarWinds.

- The SEC was interviewing companies on their response to SolarWinds. If a company does not respond appropriately to a third-party breach, it could negatively affect their stock and require reporting in their annual Form 10-K.

- Auditors are now examining vendor tiering and risk assessment methodologies.

- Regulatory risks cannot be passed on. Regulators hold companies accountable for a fourth-party breach, including ransomware attacks. Therefore, more oversight of fourth-party security is required.

- Timeframes for third-party incident notification requirements (e.g., 72-hour timeframe for NYSDFS) are being audited and enforced.

Strategies

To address new threats and regulatory pressures, a task force member recommended the following strategies for TPRM programs:

1. Rescope: Expand the scope of your Third-Party Risk Management (TPRM) program to include fourth-party risks, critical, pervasive vulnerability management, and continuous monitoring.

2. Redefine: Redefine the relationships with your suppliers to include fourth-party security management requirements, communications vis-à-vis incident notification and critical, pervasive vulnerabilities mitigation, and participation in incident response plans and tests.

3. Retool: Acquire a TPRM system (or leverage the third-party risk management capabilities of a GRC tool) to administer processes within TPRM program lifecycle phases.

The TPRM Program Compendium: Strategies for Addressing New Threats and Regulations provides detailed guidance on these strategies and implementing them. Additionally, all components of these strategies are reflected within the next section, titled TPRM Program Components.

Third-Party Risk Management Program Components

A holistic and effective TPRM program will consist of the following components:

1. Executive Endorsement and Oversight

Successful implementation and operation of a TPRM program requires executive endorsement and oversight. Executive endorsement increases the likelihood that the cross-functional organizations operating the program, such as the procurement, legal, or security departments, will dedicate sufficient resources for successful interdepartmental cooperation. Executive oversight, often in the form of a committee or an agenda item on a standing committee, ensures that program operations are effective while serving as a forum for resolving operational issues.

2. Cross-Functional Roles and Responsibilities

While the security department will take the lead in evaluating security risks, other parties are responsible for different aspects of the TPRM program. These include the organization's Chief Risk Officer (CRO), if one has been designated; procurement and acquisition services; the legal department, such as the Chief Legal Officer (CLO) and staff; organizational business owners; and third-party suppliers. Within the security department, a third-party risk management team should be established with a budget sufficient to ensure its responsibilities can be carried out. For more details, consult Appendix I: Cross-Functional Roles and Responsibilities.

3. A TPRM Program's Lifecycle Framework

Addressing third-party risks occurs throughout the lifecycle engagement with the third party, which often begins with a request for proposal (RFP) process and ends with the termination of the relationship. Listed below are six lifecycle phases for structuring the TPRM program:

1. **Phase I: Supplier Identification.** Identify all relevant suppliers of goods and services that meet or exceed the predefined risk threshold to the organization in preparation for supplier intake and onboarding.

2. **Phase II: Supplier Classification.** Assign risk criticality to each supplier of goods and services. Criticality is often used in a tiered fashion, where Tier 1 designates the most critical suppliers and Tier 3 contains the lowest risk.

3. **Phase III: Supplier Assessment.** Assess the risk that a supplier of goods and services introduces into the organization. Supplier assessment generally follows the organization's risk management framework and considers whether supplier controls are in place and operating as intended.

4. **Phase IV: Supplier Onboarding.** Implement processes required to onboard and manage supplier risk. These processes include supplier TPRM system registration, data inventory, risk mitigation, and contracts.

5. **Phase V: Supplier Monitoring & Management.** Monitor and manage the risk posture of suppliers in a manner that is commensurate with the level of risk introduced by the supplier and supplier criticality. Monitoring and management processes include contractual compliance; performance reviews; addressing critical, pervasive vulnerabilities; incident management; identifying and reassessing risks; addressing changes to supplier services; and performance metrics.

6. **Phase VI: Supplier Relationship Termination.** The supplier may have gone out of business, been purchased by another firm, performed unsatisfactorily, or is no longer valuable. Whatever circumstances caused the change, termination processes are essential to ensure confidentiality agreements are maintained post-relationship, company data is returned or destroyed, company equipment is returned, and access to company systems and networks is terminated.

4. Documentation

A TPRM program's lifecycle framework requires the following documentation to be created and maintained:

a) Policies and Procedures. Requirements for a TPRM program should be included within an organization's security policies. This document should affirm the company's responsibility for maintaining a program, which is often validated through internal and independent audits. Procedures should be developed to guide responsible parties through each of the six phases described above. The Third-Party Risk Management Standard, separate from this guide, is a template that identifies requirements and a procedure for each lifecycle phase.

b) Risk Evaluation Methods. Third-party risks must be evaluated so businesses can make engagement choices or impose risk-remediation requirements. Frequently, questionnaires are used to determine risks by collecting and processing information about the third party's financial health and security controls. The TPRM Program Workbook includes a questionnaire that can be completed in 30 minutes and calculates a risk score. Other risk evaluation methods include onsite interviews, independent audits, vulnerability scans of externally facing websites and infrastructure, and reviews of documentation like policies and penetration testing results.

c) Third-Party Contract Templates. Contracts bind third parties to requirements for reducing risks and maintaining security controls. Companies should have pre-established contract templates with language that requires, at minimum, supplier maintenance of a security program modeled on an industry security standard.

5. Support Systems

For entities managing the security risks of a large volume of third parties, MS Office tools, like Excel, are inefficient. Instead, implement a commercial TPRM system, like OneTrust and Panorays. These systems either have or integrate with tools that have discovery (e.g., fourth parties, breaches) and threat intelligence (e.g., notification of zero-day vulnerabilities) capabilities. These systems may also integrate with the vendor management system, which the purchasing department usually administers. See *Appendix III: TPRM Systems* for Task Force guidance on the general use of these tools and specific information about the tools used.

An Excel spreadsheet may suffice for tracking purposes for organizations engaging a small number of third parties. *The TPRM Program Workbook* includes Excel spreadsheets for tracking TPRM activities for individual third parties, though switching to a dedicated program is recommended as a company grows larger.

6. Metrics

As a TPRM program matures, measuring how specific processes perform will help improve the efficiency and effectiveness of the overall program. Efficiency metrics include the number of third parties managed per security full-time equivalent (FTE) or mean time to contract execution, like the time it takes to move a supplier from Phase I to Phase 4. Effectiveness metrics include the percent reduction of high-risk remediation items over time or the percent of contracts with all relevant security clauses, such as breach notification and remediation requirements.

A Third-Party Risk Management Program's Lifecycle Phases

This section details each lifecycle phase and includes a chart for triaging work efforts by risk class to improve process efficiency.

Phase Objectives, Processes, Systems, and Effectiveness Tips

Phase I: Supplier Identification

Objectives.

a) To identify all third-party candidates for an engagement.

b) To catalog all third parties currently engaged by the entity.

c) To pinpoint any changes to goods or services provided that may introduce new risks to the organization.

Processes.

1. RFP Process. The process of introducing third-party candidates to the TPRM program's lifecycle selection, as listed in Phase I through III.

2. Supplier Relationship Changes. The process of identifying relationship changes, including using new fourth parties, as outlined in Phase II through VI.

Criteria, Inputs, and Systems.

Typically, companies use a vendor management system or a GRC tool component to track and manage supplier relationships throughout the relationship lifecycle. Often the procurement department is the source for identifying all new third-party candidates and engagements.

Tips for Effective Processing.

• *Develop a complete inventory of third parties.* Organizations managing a TPRM program should know what third parties the entity uses. Chief Information Officers and Chief Technology Officers are also excellent at identifying third parties that provide IT goods and services. Alternatively, the accounts payable system may be used to extrapolate payables information to identify third parties or the procurement department may have a list of approved suppliers and master service agreements.

• *Ensure that departments do not engage third parties outside of the TPRM program.* Senior management can ensure this by requiring the procurement department to coordinate all evaluation and selection processes for all third parties.

• *Ensure that changes to the services or products that a supplier has traditionally provided trigger a security review.* When a new purchase order or statement of work is being submitted in the purchasing system, add a simple check box to indicate if the existing supplier will provide new products or services. This box will trigger a security assessment. One member claimed that this technique changed compliance percentages from 33% to over 80%.

Phase II. Supplier Classification

Objectives.

To determine the level of risk the third party or third-party candidate imposes on the organization to triage work efforts associated with the supplier assessment, management, monitoring, and relationship termination processes. In general, TPRM assessment, management, and monitoring work efforts should focus on high-risk suppliers.

Processes.

1. Risk Classification Process. The process of assigning third parties and third-party candidates to risk classes, based on risk criteria.

Criteria, Inputs, and Systems.

Categories of third-party risk, shown in *Appendix II: Third-Party Risks*, may be used to develop criteria for defining risk classes. Alternatively, a simpler set of criteria is shown below in Table 1:

Table 1: Criteria for Assigning a Risk Class to Third-Party Suppliers

RISK CLASS	CRITERIA

High (Tier 1)	• Direct access to or integration with the entity's network, systems, or data
	• Management of data processing systems and services
	• Providing security systems or services
	• Handling of the entity's personal information (PI) or intellectual property (IP)
	• Vendor criticality:
	  o Requiring high availability of service
	  o Having strategic or operational importance to the business
	  o Sole source vendor of a key process or service
	• Volume of business
	• Significant reliance on fourth parties for their products and services
	• History of data breaches
	• A data breach would have significant impact
	• Regulatory risks

Medium (Tier 2)	• Restricted or no access to the entity's network, systems, or data • Handling the entity's confidential information, but not PI or IP • A data breach would have moderate impact
Low (Tier 3)	• No access to the entity's network, systems, or data • No handling of confidential information since all information the third party sees is classified as public

Tips for Effective Processing.

• *Limit the number of risk classes.* Using three risk classes, high, medium, and low, improves processing speed, while creating more than three risk classes may unnecessarily complicate the risk classification process.

• *Leverage your Data Classification Policy.* If you have a Data Classification Policy, apply that criteria for defining risk classes to supplier classification risk classes. For example, if processing social security numbers is designated as a high-risk class (e.g., "restricted" or "sensitive), suppliers that process that data will be assigned to the high-risk class.

• *Leverage a risk register.* CROs should maintain a list of risks that are of most concern to the company.

Phase III: Supplier Assessment

Objectives.

To assess the risk of potentially using or continuing to use a third party. The assessment will trigger one of three decisions: accepting third-party risks, accepting third-party risks subject to third-party risk remediation, or rejecting third-party risks.

Processes.

1. Risk Assessment Process. Several assessment methods are shown in Table 2:

Table 2: Methods for Assessing Risk in Third-Party Suppliers

ASSESSMENT METHOD	CRITERIA
Questionnaires	• Develop a questionnaire that third parties can use to self-assess their risk exposure. These self-assessments vary in detail depending on the criticality of the third-party provider. • The TPRM Program Workbook includes a ready-to-use assessment questionnaire.
Onsite Reviews	Visit third-party facilities to review physical security controls, interview personnel, and collect artifacts supporting security controls.
Review of Regulatory and Audit Artifacts	Review the third-party provider regulatory and audit artifacts based on risk classification. This should include, but is not limited to, artifacts such as: • Service Organization Control 2 (SOC 2) assessment report • ISO 27001 certification statement • Internal audit reports • Sarbanes Oxley Section 404 audit reports
Commercially Available Supplier Risk Scoring Tools	Commercially available automated tools are tools that provide third-party risk information. Examples include BitSight and SecurityScorecard. Please note that risk scoring tools should only provide minimal input into the overall risk assessment and should never be used as the solitary method for assessing risk. These tools provide insight into the following risks: • Financial risk, by assessing the financial health of a third-party • Cybersecurity risks, as given by calculating the vulnerabilities and risk exposures organic to a third-party • Supply chain risk, based on factors that can affect the supply chain, such as the location of the third party, which may be affected by geopolitical disturbances
Open-Source Intelligence (OSINT)	OSINT is the process of gathering publicly available and accessible information to help paint a picture of the third-party's risk exposure. OSINT tools include, but are not limited, to: • Internet searches and queries • Dark and deep web searches • Media and online searches • Commercial suppliers of business information and information brokers • Internal incident security reports from the third party, including the nature of the incident, response activities, mitigation efforts, and a root cause analysis • Internal security operational reports from the third party, including penetration testing of networks and applications and defensive team security testing reports

2. Risk Identification. Using risk class and the results of questionnaires and independent security assessments, like BitSight or SecurityScoreCard, develop an overall risk score and identify risk remediation requirements. For example, assign a value to each risk class (e.g., High, Tier 1 = 5, Medium, Tier 2 = 3, and Low, Tier 3 = 1). Assign risk values to each question used in your questionnaire and independent security assessments. Sum the scores of the highest risk response to questions and results of independent security assessments. This summary score is the top of the risk range. The actual risk score is derived from the risk values assigned to the responses to the questions and the results of independent security assessments. Remediation requirements can be derived from high-risk responses and independent security assessments.

3. Risk Treatment. In the process of treating third-party risks, businesses may accept the risk, require the third party to remediate some or all risk, or decide that the third party poses an unacceptable risk.

Criteria, Inputs, and Systems.

Entities must develop and use a system or tool to evaluate risk and identify remediation requirements. The questionnaire used in the *TPRM Program Workbook* has automated risk scoring capabilities, showing both an overall score and red flags.

Tips for Effective Processing.

• *Avoid long, detailed questionnaires.* Long questionnaires are tedious to complete and extend the time it takes to engage a third party. Limiting questionnaires to key security controls will be more effective.

• *Ask whether the third party has a TPRM Program in place.* If they answer, "Yes," you will confirm they evaluate their third parties, which are your fourth parties. A "no" answer is a red flag.

• *Disaster Recovery and Business Continuity Planning are important requirements for critical vendors.* Recovering operations is especially important for sole-source vendors providing critical services.

• *Rely on artifacts and OSINT for evaluating large cloud service providers (CSPs).* CSPs, like Amazon Web Services and Azure, are unlikely to complete a security questionnaire. Instead, rely on audit evidence, such as a SOC 2 report. CSPs who are members of the Cloud Security Alliance's STAR Registry share information about their security program through self-assessment questionnaires or third-party audits.

• *Ask for artifacts to backup questionnaire responses.* Require high-risk third parties to submit artifacts to validate questionnaire responses. Examples include policy statements, independent audit reports, external vulnerability scans, and penetration testing results.

• *Risk scores are important management and communication methods.* Although risk is subjective, risk scores and changes to risk scores help management understand and support supplier selection decisions and risk mitigation recommendations.

• *"Right-size" the assessment process for small organizations.* Small organizations may not have formal security programs and will not know how to respond to large security questionnaires. Focus on evaluating key controls and identifying ways to reduce the security risks they pose.

Phase IV: Supplier Onboarding

Objectives.

a) To obtain sufficient security information about the supplier.

b) To contractually establish security and communications requirements to ensure the ongoing operation and effectiveness of supplier security controls.

Processes.

1. Supplier TPRM System Registration. Having registered with the entity's vendor management system, suppliers must now register with the entity's TPRM system. The registration process will identify supplier contacts and other information listed in the data inventory section below.

2. Data Inventory. The following information should be collected on each supplier:

a. Contacts and contact information (e.g., cellphone, email)

b. Names of critical fourth parties, particularly fourth parties that:

i. Process sensitive customer information;
ii. Have a significant impact on third-party security;
iii. Will significantly disrupt third-party services if breached;
iv. Access customer systems; or
v. Will physically access customer facilities.

c. Software and hardware components, to the extent feasible, to identify critical vulnerabilities like log4j and SolarWinds. This may include Software Build of Materials (SBOM) information.

3. Risk Mitigation. Third parties with associated risks that need ameliorating should be monitored using the TPRM system or a risk mitigation tracking tool. At minimum, it should identify the risk to be mitigated and the target completion date.

4. Contracts. Suppliers should be held legally responsible for the security of the entity's processes and information. Contracts for high-risk suppliers should minimally include the following requirements:

a. Maintaining a security program, including existing certifications.

b. Notifying the entity of:

i. Incidents and breaches, including response criteria, timeframes, and notifications from fourth parties;
ii. Significant changes to the business, including financial difficulties;
iii. Changes to fourth parties identified in the data inventory, including terminations and new fourth parties; and
iv. Changes to supplier or fourth-party security programs which may significantly increase or reduce security risks.

c. Implementing the remediation plans identified from the assessment phase.

d. Registering with the TPRM system.

e. Addressing communications promptly, including those relating to mitigating critical, pervasive vulnerabilities like log4j.

f. Accepting liability for fourth-party breaches of information.

g. Maintaining a SBOM, if the third-party provides software.

h. Participating in customer incident management exercises.

i. Upholding multiple clauses, including:

i. A right to audit clause;
ii. Service-level agreements (SLAs) for responding to incident response calls and other communications; and
iii. Privacy clauses, such as model contracts, for handling personal information protected by the General Data Protection Regulation.

Criteria, Inputs, and Systems.

The TPRM system is the principal system used for onboarding supplier security information and managing the security relationship going forward. However, the TPRM system should integrate with the vendor management system, sharing contact information and identifying changes to the business relationship with the supplier.

Tips for Effective Processing.

• *Append evaluation questionnaire responses and risk mitigation items to supplier contracts.* This action will reduce the likelihood of misleading assessment responses and make remediation a contractual obligation for the supplier.

• *Collect detailed inventory data on key suppliers.* It is difficult and time-consuming to gather detailed inventory data on all suppliers.

• *Focus on collecting information about critical fourth parties.* It is impractical to collect and maintain information about all fourth parties.

• *Collect fourth-party information during the data inventory process and NOT during contract negotiation.* Contracts should require suppliers to manage all their third parties, as these are an entity's fourth parties.

• *Collaborate with the legal department and supplier's business owners to enforce contract requirements and penalties.* This action is often accomplished via supplier review committees comprised of business owners and members from the security, legal, and procurement departments.

Phase V: Supplier Monitoring and Management

Objectives.

a) To manage relationships with engaged suppliers to ensure that identified risks are mitigated and the supplier maintains effective security controls.

b) To monitor the contractual compliance of suppliers, including risk mitigation efforts, maintenance of security controls, and changes to the business relationship.

Processes.

1. Monitoring Contractual Compliance. Entities should monitor third-party compliance to contract terms, including mitigating identified risks, maintaining security controls, and notifying the entity of breaches and major changes to the third-party business.

2. Performance Reviews. This process is how entities interact with supplier management to address performance issues and track risk mitigation activities.

3. Critical, Pervasive Vulnerabilities. Being notified of critical, pervasive vulnerabilities from threat intelligence sources is necessary to ensure that relevant third and fourth parties address those vulnerabilities.

4. Incident Management. Third parties should be required to notify you of any relevant incidents, including ransomware, which affect them or their third parties. If a breach has occurred, follow up to ensure they have recovered, addressed deficient controls, and are monitoring for future threats. Critical third parties should participate in incident response tests.

5. Identification and Reassessment of Risks. Regularly reassess third-party risk using assessment methods, such as questionnaires and onsite reviews. Methods to be considered are:

a. Formal onsite assessments. For Tier 1 third-party providers, schedule onsite assessments at required time intervals. The business unit receiving the goods and services should coordinate this activity with the third-party supplier.

b. Remote reviews. Companies can assess third parties in lower risk classes using remote reviews. Use self-assessments and note any deviations from previously submitted self-assessments. Consider reviewing Tier 3 third-party providers less frequently.

c. Automated TPRM tools. Entities can leverage the information from risk scoring tools, like BitSight, as used in the lifecycle assessment phase. These tools provide limited, but helpful, up-to-date information on a third-party provider's risk posture. However, keep in mind that these tools should never be used in a stand-alone fashion. Use threat intelligence tools to gain information about third-party breaches, threat targeting, and security weaknesses.

6. Address Changes to Supplier Products or Services. If the third-party goods or services change, companies should reengage the supplier classification, assessment, and management phases.

7. Performance Metrics. Supplier adherence to contractual requirements should be measured as part of the monitoring process. Metrics include on-time remediation efforts, availability of SLAs, and maintaining or lowering risk levels over time, as determined by assessment results.

Criteria, Inputs, and Systems.

The TPRM system should track monitoring activities, including contract compliance, risk reassessments, and relationship changes. Threat intelligence should identify third-party security risks, while vulnerability feeds should track critical, pervasive vulnerabilities, like log4j.

Tips for Effective Processing.

- *Validate assessment responses.* Businesses can spot-check third-party data handling processes through sampling and requesting documentation to validate responses.

- *Maintain a good relationship with the supplier.* A good relationship with suppliers is a tremendous boon when companies need to resolve contract compliance or risk remediation issues.

- *Set up regular supplier reviews.* Use reviews to examine risk mitigation status and address issues, such as performance. Maintain open and candid communications with your supplier account representative.

- *Focus on monitoring critical suppliers.* Although a TPRM system will increase efficiencies, large organizations reliant on many third parties will find it difficult to monitor all their third parties.

- *Incorporate threat intelligence and other discovery information into the TPRM.* Tools can identify the fourth parties that suppliers are using but have not reported. Threat and vulnerability feeds can determine if a supplier is being targeted, is breached, or has a critical, pervasive vulnerability to address.

- *Ensure that fourth-party security is being monitored.* When assessing third-party risks, examine the breadth and depth of third-party security monitoring of fourth parties. Require third parties to give you advanced notice 30 days before onboarding a critical fourth party.

- *Maintain a scorecard on each critical supplier to identify changes to the supplier's security posture.* As part of the scoring criteria, include the degree of supplier responsiveness to all your communications and requests. Acknowledge suppliers who improve their security scores and respond promptly to communications requests.

- *Keep contact lists up to date.* Know whom to call for any security issue, particularly incidents.

Phase VI: Supplier Relationship Termination

Objectives.

To ensure that all risks associated with using a supplier have been eliminated or significantly reduced.

Processes.

1. Data Return and Destruction. Suppliers must return or destroy all company information in their possession, whether electronic or non-electronic.

2. Equipment Return. If the entity loaned equipment to the supplier, it must be returned.

3. Access Termination. This is the systematic termination of all third-party access to the company's network, systems, and data.

4. Adherence to Confidentiality Agreements. This process requires the supplier to legally adhere to the confidentiality agreements that survive the terminated relationship.

Criteria, Inputs, and Systems.

The entity should use its identity and access management system to terminate supplier connections to the network and systems. However, not all supplier access points are administered by an access management system. These must be terminated as well. Company contracts and non-disclosure agreements will identify the confidentiality requirements the supplier will be bound post-termination.

Tips for Effective Processing.

- *Maintain a thorough inventory of data, loaned equipment, and access accounts for each supplier.* The record will serve as a checklist for completing termination processes.

- *Create a transfer-of-services plan and contractual requirements.* Contractually require the supplier to support the transfer of services in the event of contract termination.

- *Conduct an exit interview with supplier management to ensure the maintenance of confidentiality agreements.* Have a member of the legal department conduct the interview.

Efficiently Triaging Work Efforts Based on Risk Class

The efficiency of a TPRM program depends on the ability to triage effort based on the risk class assigned to various third parties. In other words, third parties that impose higher risks should be more heavily scrutinized. Table 3 makes recommendations for triaging work by risk class:

Table 3: Using Risk Class to Prioritize Risk Assessment Methods for Third-Party Suppliers

ASSESSMENT METHOD	RISK CLASS High (Tier 1)	Medium (Tier 2)	Low (Tier 3)
Assessment Methods	One or more of the following: • SOC 2 Report • ISO 27001 Certification • Assessment Questionnaire • Onsite reviews • Independent assessments and audits	One of the following: • SOC 2 Report • ISO 27001 Certification • Assessment Questionnaire	Verification that the third party is low risk.
Assessment Frequency	Quarterly/Semi-annual reviews and annual reassessments or after a change in the business relationship	Annually or after a change in the business relationship.	Every three years or after a change in the business relationship
Risk Treatment	Low-risk acceptance. Develop a risk mitigation plan for significant risks.	Moderate risk acceptance. Develop a risk mitigation plan for significant risks.	N/A
Monitoring	Monitor for business changes that alter the risk profile, including using fourth parties.	Monitor for business changes that alter the risk profile, including using fourth parties.	Monitor for business changes that alter the risk profile, including using fourth parties.

Table 3: Using Risk Class to Prioritize Risk Assessment Methods for Third-Party Suppliers (cont.)

ASSESSMENT METHOD	RISK CLASS High (Tier 1)	Medium (Tier 2)	Low (Tier 3)
Contracts	1. Require maintaining a security program, including maintaining existing certifications. 2. Incident and breach notification requirements, including response criteria, timeframes, and notifications from fourth parties. 3. Notifications of: a. Significant changes to the business, including financial difficulties; b. Changes to fourth parties identified in the data inventory, including terminations and plans to use new fourth parties; and c. Changes to the supplier or fourth-party security programs which may significantly increase or reduce security risks. 4. Remediation requirements identified from the assessment phase. 5. Requirements to register with the TPRM system. 6. Requirements to address communications promptly, including those relating to mitigating critical, pervasive vulnerabilities like log4j. 7. Supplier is liable for fourth-party breaches of information. 8. A right to audit clause. 9. Requirement for maintaining a SBOM, if providing software. 10. Requirement to participate in customer incident management exercises. 11. SLAs for responding to incident response calls and other communications. 12. Privacy clauses, such as model contracts, for handling personal information protected by the General Data Protection Regulation.	1. Require maintaining a security program, including maintaining existing certifications. 2. Incident and breach notification requirements, including response criteria, timeframes, and notifications from fourth parties. 3. Notifications of: a. Significant changes to the business, including financial difficulties; b. Changes to fourth parties identified in the data inventory, including terminations and plans to use new fourth parties; and c. Changes to the supplier or fourth-party security programs which may significantly increase or reduce security risks. 4. Remediation requirements identified from the assessment phase. 5. Requirements to register with the TPRM system. 6. Requirements to address communications promptly, including those relating to mitigating critical, pervasive vulnerabilities like log4j. 7. Supplier is liable for fourth-party breaches of information. 8. A right to audit clause. 9. Privacy clauses, such as model contracts, for handling personal information protected by the General Data Protection Regulation.	Maintain good privacy and security practices.

Guidance on FAQs

Frequently Asked Questions

Senior Management Endorsement:

What are ways of convincing senior management to endorse a TPRM program?

You can begin by describing the risks that third parties impose and describe major breaches caused by third-party vulnerabilities, including Target and SolarWinds. However, you will be unlikely to convince senior management by yourself. Partner with the risk and legal departments to understand and communicate the potential impact of breaches. Have a plan to demonstrate to senior management that you are capable and ready to implement a TPRM program.

Using Fourth Parties:

How do I address the potential risks of third parties outsourcing my processing and data to fourth parties?

The most effective way to prevent third parties from outsourcing your information or processing to fourth parties is to contractually obligate the third party not to do so. Require third parties to notify you if they intend to use fourth parties that might handle your information. Alternatively, when you contract with a third party, you may accept their existing relationship with a fourth party. However, ensure the third party has a TPRM program that evaluates the new fourth party's security before contracting with them.

Resources:

How do I determine how many staff members are needed to support a TPRM program?

When beginning a TPRM program, determining security FTE requirements will be difficult, especially since the volume and risk of third processes may be unknown. Depending upon the size of your security organization, you may need to initially assign one or two individuals on a part-time basis. Once the details are assessed, you can measure productivity. A good productivity measure is your best argument for recommending staff increases. Additionally, if the risk classification criteria and processing timeframes are accepted by other departments, such as procurement, legal, and risk, you have support for your argument.

Cloud Service Providers:

How do I effectively evaluate the security posture of CSPs?

This is difficult to do using questionnaires since large CSPs will be reluctant to complete them. However, you can ensure that their security practices are thoroughly audited by external agencies, such as a CPA firm, or in conjunction with certifications, such as SOC 2 and ISO 27001. Alternatively, many providers are members of the Cloud Security Alliance, and some will show evidence that their security practices are independently audited by presenting a STAR Certification.

However, what matters is how CSPs handle your information. While we assume from security certifications that CSPs will handle your information securely, there is no guarantee. Therefore, rely on contract language. Contracts with CSPs should delineate tenant and CSP security responsibilities and offer remediation for data breaches.

The Veracity of Third-Party Assessment Responses:

How do I assess the truthfulness of third-party assessment responses?

There are three primary ways to validate answers to self-assessments. The first is to add questionnaire responses to the contract to make them legally binding, such that false answers could be considered a breach of contract. The second way is to request documentation from the third party to support their answers. For example, if the third-party reports conducting annual penetration testing, ask to see the penetration testing results for the last two years. Last, engage a firm like BitSight or SecurityScorecard to scan websites and externally facing infrastructure for vulnerabilities and determine if the score provided aligns with the third-party responses.

Appendices

Appendix I: Cross-Functional Roles and Responsibilities

Because of the inherent risk that third-party suppliers of goods and services can introduce, TPRM programs must identify and clarify roles and responsibilities to limit risk exposure. The TPRM organization must be articulated to each role listed below, consistent with the enterprise risk management (ERM) governance framework.

Third-Party Risk Management Organization: The TPRM organization establishes, implements, maintains, and monitors the TPRM program's function. Specifically, it is the responsibility of the TPRM organization to:

- Serve as the advocate for the TPRM program and champion senior leadership buy-in and support.
- Collaborate with business owners and stakeholders in the design and implementation of the TPRM program.
- Develop the formal policies and procedures for the TPRM program.
- Ensure that the TPRM organization is incorporated into the ERM function.
- Educate business owners and stakeholders on the TPRM program.
- Manage, monitor, and provide feedback on the effectiveness of the TPRM program throughout the program's lifecycle.

Chief Risk Officer: The CRO establishes, implements, maintains, monitors, and reports on the organization's ERM posture via a formalized program. Specifically, it is the responsibility of the CRO to:

- Partner with the TPRM organization to ensure that the TPRM program is aligned with and complies with the ERM program's policies and procedures.
- Validate the effectiveness of the TPRM program and provide feedback on gaps in controls, methodologies, procedures, and policies.

Third-Party Suppliers: Third-party suppliers and vendors are individuals, companies, and organizations that supply goods and services to their customers. Third-party supplier goods and services can include staff augmentation, full lifecycle management of outsourced functions, software, hardware, and other professional services. The responsibilities of third-party suppliers include, but are not limited to:

- Formally adopting and complying with TPRM control requirements commensurate with the risk of exposure inherent to its assigned risk tier by the customer.
- Promulgating, managing, and monitoring TPRM control requirements for their own suppliers and vendors, including taking appropriate corrective action for noncompliance.
- Communicating any changes in risk to the customer in the timeframe identified in the contractual agreement between the third-party supplier and its customer.
- Responding to and providing the appropriate data and information to the customer concerning TPRM assessments, audits, reviews, or inspections in a timely fashion and the manner identified in the contractual agreement between the supplier and customer.

Appendix I: Cross-Functional Roles and Responsibilities (cont.)

- In compliance with incident response procedures, disclosing to the appropriate customer point of contact (POC) any breaches, compromises, or material incidents that affect the customer's risk exposure.

Chief Legal Officer or General Counsel: The CLO or General Counsel provides guidance and counsel and oversees the legal requirements of the TPRM program. It is their responsibility to:

- Guide the TPRM organization through developing the principles, policies, and language required to manage third-party suppliers.

- Ensure that the TPRM function conforms to the organization's requirements and legal framework.

- Serve as counsel to the TPRM organization when suppliers of goods and services are noncompliant with TPRM policies and procedures.

Organizational Business Owners: Business owners establish and manage relationships with suppliers. It is the responsibility of business owners to:

- Identify and appropriately categorize the risk tier of suppliers as defined by organizational policy and procedures.

- Ensure that suppliers understand, adopt, and maintain proper security and privacy controls as required to reduce the risk of exposure and compromise, commensurate with their tier categorization.

- Serve as the POC for suppliers for all matters related to third-party risk issues, such as noncompliance and escalation.

- Understand the risk exposure introduced by suppliers and work with them to close gaps in controls and formally accept residual risks that remain due to gaps in coverage.

- Notify the appropriate body of significant changes to their suppliers' risk posture or tier.

Procurement and Acquisition Services: Procurement and acquisition services establish, maintain, and control the procurement and acquisition process lifecycle for goods and services. It is the responsibility of procurement and acquisition services to:

- Ensure that agreements for goods and services incorporate language that describes the security and privacy requirements to be adopted by the supplier.

- Validate the supplier's tier categorization with the business owner requesting goods and services.

- Actively participate and discharge their required duties as specified in the TPRM risk assessment process, according to the organization's formal TPRM policies and procedures.

Appendix II: Third-Party Risks

• **Financial Risk.** Third parties can introduce financial risks to an organization through mismanagement of their business operations, leading to an inadequate or corrupted supply of critical goods and services. Supplier mismanagement can lead to product shortages, poor services, or supply chain disruption, any of which can have an immediate and observable impact on the customer's revenue.

• **Operational Risk.** Third parties that provide critical goods and services can cause insurmountable harm to an organization's essential operations. For example, poorly developed software provided by the supplier can lead to the compromise, degradation, disruption, or destruction of the customer's operations.

• **Regulatory and Compliance Risks.** When an organization must meet regulatory, legal, compliance, or due diligence requirements, third parties that provide critical goods and services to that organization can negatively impact the customer's compliance posture. Failure to adhere to requirements in regulated industries can result in hefty fees, sanctions, criminal liabilities, blacklisting, and delisting.

• **Strategic Risk.** Critical suppliers can severely impact the long-term strategic competitiveness of an organization. Because critical third-party suppliers are vital to an organization's success, any realized risk exposure can have a long-term impact on the organization's strategic competitiveness.

• **Reputational Risk.** Third parties that take on contracts in bad faith can cause significant reputational harm to the customer. This secondary risk manifests as one of the many primary risks listed above. While many companies rebound from reputational damage, there is almost always an immediate, short-term financial impact secondary to bad publicity when a risk is realized.

Appendix III: TPRM Systems

As a vendor-independent organization, the Cybersecurity Collaborative does not endorse specific vendors or products. However, systems like SIEMs, IPS', and EDRs, are indispensable components of the technical controls required to protect an organization from cyberattacks and breaches.

Likewise, commercial TPRM systems are invaluable for helping organizations evaluate and oversee the security programs of the many third parties they engage or are considering engaging. Commercial systems are becoming essential to managing critical, pervasive vulnerabilities and emerging TPRM requirements, such as fourth-party risks.

Below, Table 4 summarizes the task force discussions on the use of TPRM systems in general and provides insights on two tools that some task force members use.

Table 4: Methods for Assessing Risk in Third-Party Suppliers

TPRM SYSTEM	COMMENTS
Overall Task Force Comments	• Members are examining tools that identify fourth parties and provide security visibility. • RFP criteria include threat intelligence capabilities, third- and fourth-party insights, investments made in the tool, and the future roadmap. • Do not take tool security insights at face value: do more digging. • Tools can create and administer security questionnaires and provide a communication path with third parties. • Tools can track mitigations and progress against addressing critical, pervasive vulnerabilities. • Some tools create risk scores and track risk reduction over time to show executives who like to see scores. As the basis of a supplier scorecard, tracking can be an incentive for suppliers to improve. • Take the "inside out and outside in" approach. "Outside in" uses a tool like SecurityScorecard to evaluate a company's publicly facing security posture while "inside out" uses a security questionnaire. • Members either leverage the risk assessment capabilities of a commercial system or create their own risk assessment processes using inputs from these systems. • Adding fourth parties to the system may increase the number of seats and, therefore, the costs of using a tool. • It is challenging to find tools that can store information about fourth parties. • A prominent auditing firm warns that data collected by these tools is "discoverable" from a legal perspective.
OneTrust https://www.onetrust.com	• OneTrust is used for third-party risk management, including managing a variety of risks, including SarBox. • SaaS-based system. • Third parties have an account on the system (ID, password) and may need to sign a non-disclosure agreement before opening an account. • Features: o Communications capability (e.g., can look up the top 250 suppliers and send them a communication. o All risks are in a single place for each vendor. o References external reports (like 301 Trade Report) to see if the supplier presents a higher risk. o Can set up various risk criteria, including information shared, network access, physical access, and application integration. o Can create a custom dashboard. o If personally identifiable information is going to be handled, it triggers a privacy questionnaire and notifies the privacy team. o A risk score is created after the questionnaire is completed. o Questionnaire capabilities: • Easy to create • Can draw from multiple templates (e.g., CAIQ, SIG, SIG-Lite, Shared Assessments) • Can set risk values for each question response.

TPRM SYSTEM	COMMENTS
OneTrust (cont,) https://www.onetrust.com	• Vendor support: o Can pay OneTrust to do the assessments for you. o Will provide completed third-party questionnaires at an additional cost. o Monteros is used for training and will show you how to configure the system. • Takes one month to set up with a hired full-time resource. • Monthly meetings are held with the different constituents using this system
Panorays https://panorays.com	• Third parties have an account on the system for one year. • Features: o Provides a risk panel of overall third-party risk scores. o New third party: add domains, business information, the likelihood of being a target, the volume of confidential data, availability requirements, and contact information. o Determines which regulations apply (e.g., FFIEC, GDPR, HIPAA, PCI, NYDFS). o Can create a customized questionnaire by selecting specific options (e.g., file transfers, on-premises requirements, sensitive information, legal risks). o Questionnaire asks which fourth parties are used. o Continuously scans third parties for information: social media accounts, business type, number of employees, dark web, asset reputation. o Calculates ratings based on cyber posture (scan of IPs), questionnaire rating, business impact rating, and final risk rating. o Other capabilities: • Does industry comparisons. • Creates a full map of IP domains, including disclosing the owner and assets scanned. • Monitors changes to vendor security posture through continuous scanning. • Automatically identifies fourth parties, which you can add as a supplier for cyber posture ratings. • Meets NYDSF requirements for continuous monitoring; can add NYDSF requirements to the questionnaire. • Questionnaire can be drawn from SIG and other questionnaire templates. • Can customize questionnaires and send out special questionnaires (e.g., log4j). • Costs and Support: o Approximately $100k per year for 500 vendors. o Good support.
Other Systems	• Black Kite o Provides a risk score. o Includes a security business strategy. o Similar to SecurityScorecard and BitSight. o Develops and tracks action plans for mitigation items. o Uses the FAIR risk assessment framework to show potential cost impacts. • RiskRecon monitors third and fourth parties, including breaches. • BitSight o Provides a security score for several domains (SPF headers, patching cadence, etc.). o Capable of identifying fourth parties. • SecurityScorecard has similar capabilities to BitSight.