

Effective Third-Party Risk Management

Key Tactics and
Success Factors





Table of Contents

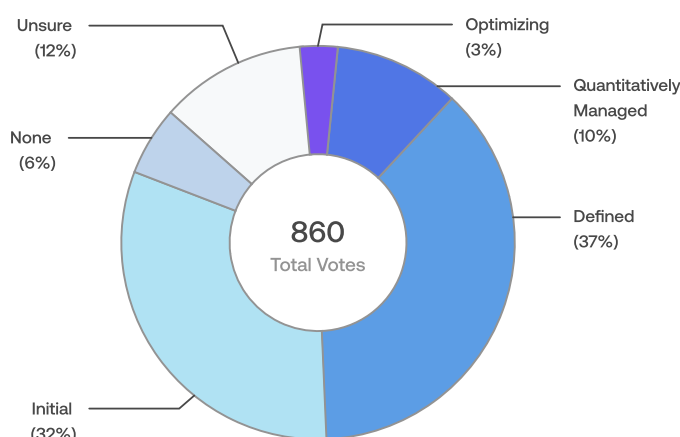
Introduction	3
Third-Party Risk Management Programs: Overview	4
– Guiding Principles	4
– Common Program Components	4
– Common Gaps and Obstacles	5
Third-Party Identification & Discovery Tactics	6
– Ensure Ongoing Visibility Between the “Where” and the “Who”	6
– Enable Smart and Proactive Resource Deployment	7
Third-Party Risk Categorization Tactics	7
– Stratify Third Parties in Proportion to Risk Level	8
– Ensure Realistic, Appropriate Distribution Across Tiers	8
Risk/Controls Assessment Tactics	9
– Security Controls Questionnaires	9
– Standardized Questionnaires	9
– Compliance Certifications and Reports	10
– Onsite Audits	11
– Contract Reviews	12
– Reputation Services	12
Continuous Monitoring Tactics	14
– Establish Periodic Reassessment Cadence Based on Risk Level	14
– Perform Rediscovery With Internal Relationship Owners	14
– Perform Targeted Assessments Following Key Events	15
Issue Management and Reporting Tactics	15
– Focus on Meaningful, Effective Reporting	15
– Build Accountability Around Regularly Updated Risk Assessments	16
– Create Reporting That Supports Effective Decision Making	16
Conclusion	17
About the Author	18
About AuditBoard	18
About AuditBoard’s Third-Party Risk Management Solution	19

Introduction

Many organizations are reemphasizing the importance of effective third-party risk management (TPRM), due to the third-party security breaches that have recently dominated the headlines. For recent examples, think SolarWinds, Kaseya, Accellion, Microsoft, and Volkswagen — the data and information security, regulatory, compliance, financial, and brand/reputational risks are increasingly clear.

Most organizations, however, are still struggling to get TPRM right. As organizations sought to control costs by outsourcing key functions throughout the COVID-19 pandemic, many learned how unprepared their TPRM programs really are. A 2021 survey of 1,170 respondents in 30 countries by [Deloitte](#) found that more than half (51%) faced one or more third-party risk incidents while responding to COVID-19, with 42% sharing concerns over inadequate cybersecurity investment. A 2021 AuditBoard survey of 800+ risk and compliance professionals across North America found similar results. Nearly 37% of respondents rated their TPRM maturity as either nonexistent or simply reactive, with activities performed on an ad hoc basis. And very few — only 3%, according to AuditBoard's survey — are at the point of optimizing.

How would you rate your vendor risk management program's maturity level?



- Optimizing — Innovative, technology enabled, automated (3%)
- Quantitatively Managed — All processes measurable and controlled (10%)
- Defined — Proactive, well-understood, established program (37%)
- Initial — Reactive or performed on an ad hoc basis (32%)
- None — We do not currently have one in place (6%)
- Unsure (12%)

How would you rate your organization's TPRM program maturity? Do policies and processes provide adequate protection against third-party risk? Or are you among the majority still struggling to mature TPRM capabilities?

Any third party can present risk to your organization. That includes not only vendors and suppliers, but also partners, customers, and third-party software providers. In this guide, you'll learn key third-party risk management principles and tactics that can go a long way toward helping you mature your organization's TPRM program.

Third-Party Risk Management Programs: Overview

Guiding Principles

TPRM programs are designed to provide discipline, structure, and oversight to guide the plans, policies, and processes by which your organization:

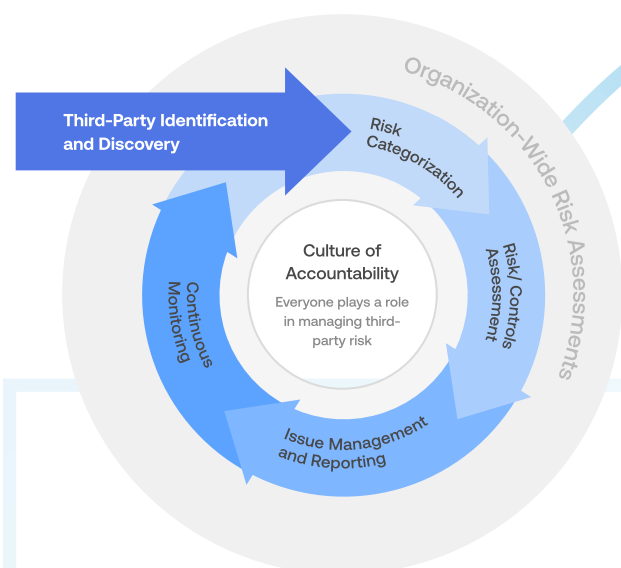
- **Identifies and categorizes the third parties you engage.** You can't manage risk effectively without a regularly updated inventory of all potential sources.
- **Understands and prioritizes the risks presented by third parties.** All third parties do not present equal risk and should not consume equal risk assessment capacity.
- **Establishes and enforces key controls for mitigating those risks.** Third-party risk/controls assessments should address and prioritize the risks that matter most to your organization. Set up contracts, expectations, and service-level agreements (SLAs) to hold third parties accountable for effectively managing those risks.
- **Performs monitoring that tracks and regularly reassesses third-party relationships and risk exposures.** Risk is dynamic, changing over time. Design TPRM policies and processes to help you catch and respond to the changes that matter.
- **Responds to real-time issues, and communicates TPRM awareness and accountability throughout the organization.** Everyone can play a role in managing third-party risk. TPRM policies, protocols, and reporting should support organization-wide awareness of key risks, ongoing engagement with third-party relationship owners, proactive TPRM practices, informed decision making, and timely, effective issue responses.

Common Program Components

TPRM programs vary based on the size, scope, resource and budget constraints, regulatory requirements, and risk profiles of the organizations for which they're built. One size does not fit all — but all programs share certain components. As depicted in the overview graphic, TPRM programs:

- **Are cyclical.** As new third parties enter the equation and existing relationships evolve over time, you should periodically revisit risk categorization, assessment, issue management, reporting, and continuous monitoring.

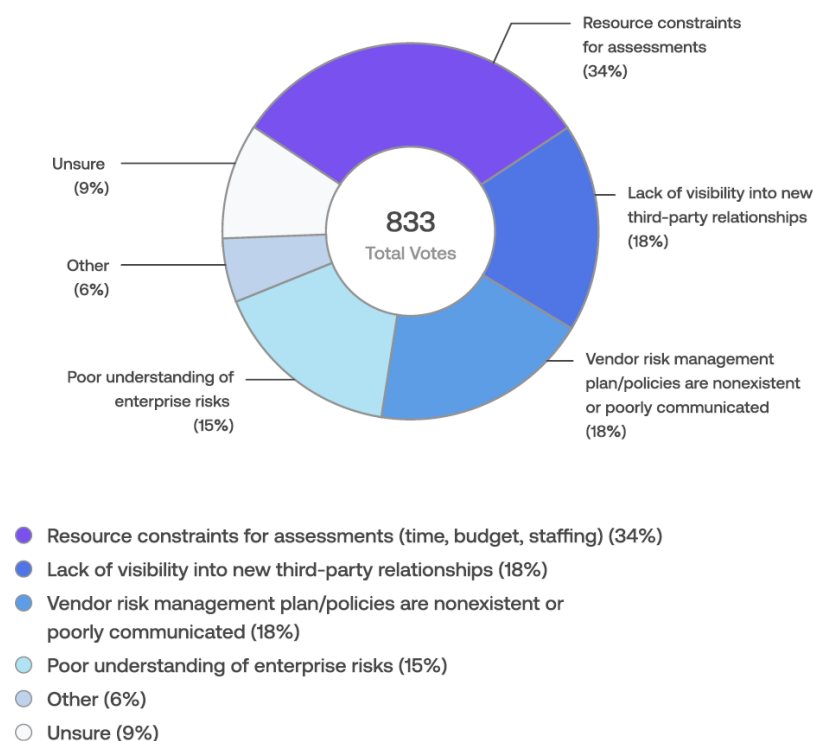
Third-Party Risk Management Program: Overview



- **Occur against the backdrop of your organization’s enterprise and cyber risk assessment(s).** As your risk profile, exposures, and prioritization evolve, so must your TPRM program.
- **Are best built around a culture of accountability.** TPRM responsibilities are often distributed across a range of functions and business units. Set the tone that everyone has an important role to play in managing the risks that are presented by the third parties they engage with.

Common Gaps and Obstacles

What is the biggest gap or obstacle to more effective vendor risk management at your organization?



All organizations face challenges in establishing effective TPRM programs. AuditBoard’s survey found that resource constraints for assessments (e.g., time, budget, staffing) was the most commonly cited challenge. Lack of visibility into new third-party relationships, nonexistent or poorly communicated vendor risk management plan/policies, and poor understanding of enterprise risks followed closely behind.

Whatever your biggest challenges, improving your understanding of key TPRM tactics and success factors can help you close gaps and overcome obstacles.

Third-Party Identification & Discovery Tactics

What's the best way to formalize your plan, policies, and processes for continually identifying the new third parties working with your organization?

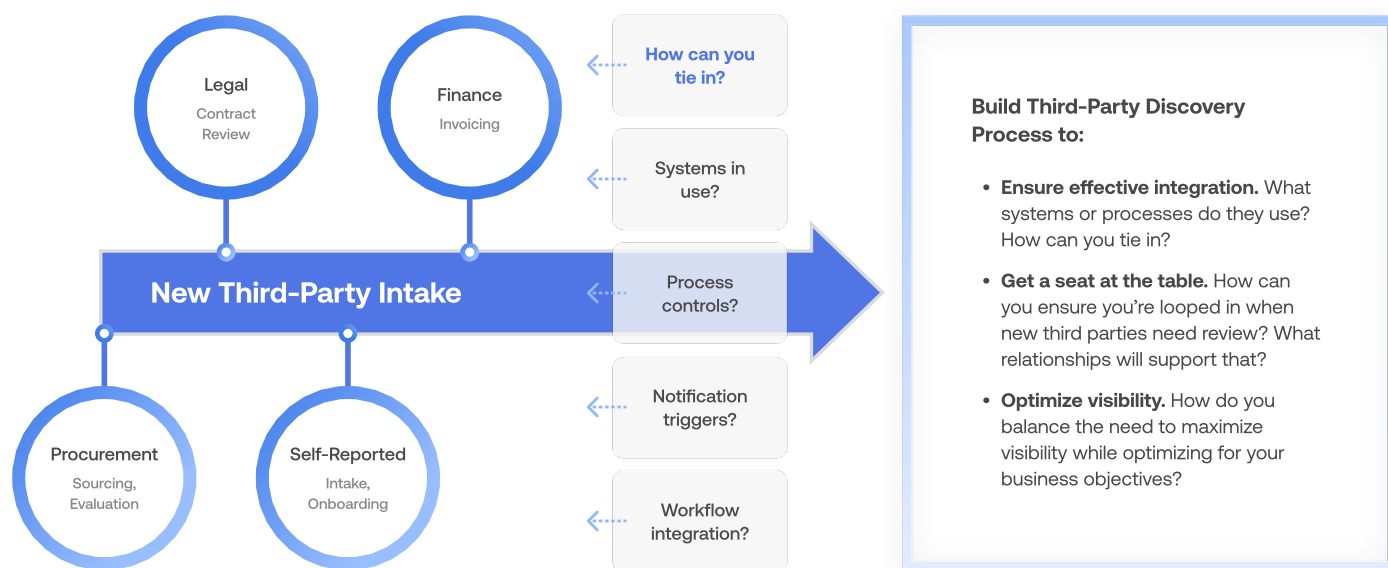
Ensure Ongoing Visibility Between the “Where” and the “Who”

The most important tactic is to:

1. Assess **WHERE** in your organization new third-party engagements are initiated.
2. Identify **WHO** is responsible for assessing and making decisions about relationship risk.
3. Build a process that ensures ongoing visibility between the **WHERE** and the **WHO**.

The graphic below further fleshes out the goals your identification and discovery process should be designed to support.

Third-Party Identification and Discovery Process



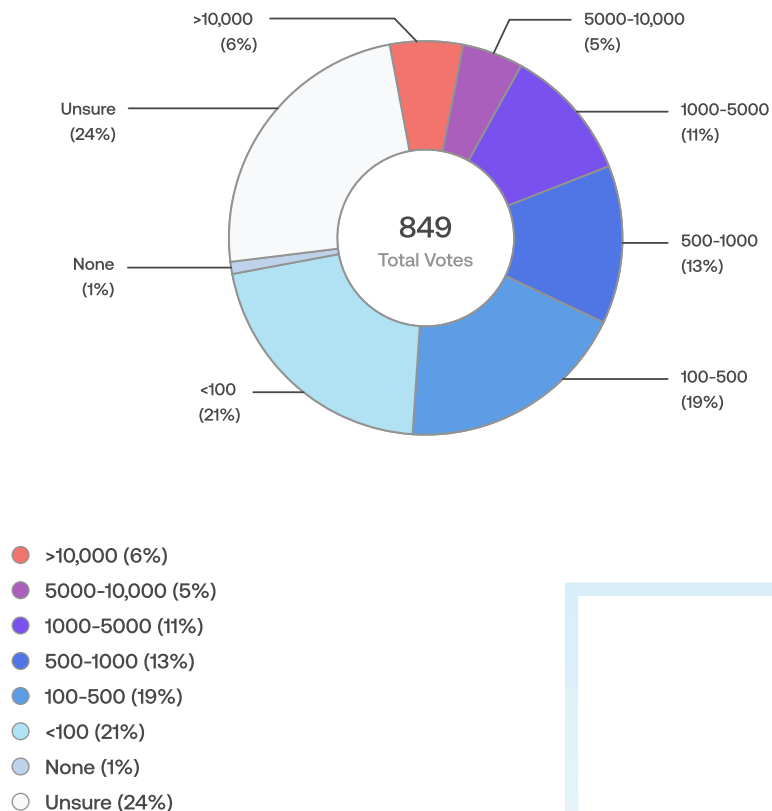
Enable Smart and Proactive Resource Deployment

- Create and promote clear, readily available TPRM policy and process guidance.
- Use simple vendor request and review forms at the point of intake.
- Establish a complete, regularly updated inventory of third parties.
- Scale assessment and remediation approach(es) as appropriate to match risk levels.
- Consider technology tools that create a safety net and offer ongoing visibility. For example, automated discovery tools that connect to payment or contracting systems (e.g., G2 Track) can be set up to provide alerts following triggers you establish.

Third-Party Risk Categorization Tactics

Whether your organization works with 10, 1,000, or 10,000 third parties, the problem is the same: You have finite resources. How can you deploy them most effectively?

How many third-party relationships does your organization have?



Stratify Third Parties in Proportion to Risk Level

Since all third parties do not present equal risk, they should not consume equal risk assessment capacity. Develop criteria to help you categorize third parties into high-, medium-, and low-risk buckets that help you better allocate your limited resources where they'll have the most impact. Creating and updating third-party risk categorization is a key success factor for any TPRM program.

Begin by referring back to your enterprise and cybersecurity risk assessments, assessing each third party based on the risks that matter most to your organization. For example, if access to confidential data is the most important consideration for your organization, you may establish the following risk tier categories.

Risk Tier Characteristic	Tier 1 – High Risk	Tier 2 – Medium Risk	Tier 3 – Low Risk
Data Access	Confidential	Proprietary	Public or None
Review Frequency	1 Year	2 Years	3 Years
Review Requirements	Onsite Audit Controls Questionnaire Certification Review	Certification Review	None

Based on the risk profile of your organization, you could also consider categorizing third parties based on questions such as:

- Is the third party a critical dependency to meet organizational objectives?
- Will the third party have access to confidential or customer data?
- Will the third party have direct access to your infrastructure, networks, or systems?
- Does the third party support the availability of customer-facing services?
- Does the third party support any critical internal business functions?
- Can the third party impact your organization’s reputation or business relationships?
- What is the estimated spend?
- How many internal users, teams, functions, or processes will rely on this third party to perform?

Ensure Realistic, Appropriate Distribution Across Tiers

Keep an eye on distribution across tiers. Most third parties should fit into Tiers 2 and 3. Be very discerning with categorizing third parties as Tier 1, since that’s where you’ll invest the most time and resources.

Risk/Controls Assessment Tactics

What tactics can you use to better understand and control third-party risks and controls? TPRM programs commonly employ a range of tactics. The most important success factor is to make sure tactics are proportional to the level of risk each third party presents to your organization.

Security Controls Questionnaires

The most common tactic is the security controls questionnaire. This extremely flexible approach allows you to customize each questionnaire based on the type of third party and the risks you are concerned with. Since you can be highly detailed and prescriptive about the controls you expect to be in place, this approach can provide confidence that third parties are appropriately controlling the risks you care about most.

Pros	Cons	Sample Use Case
<p>Customizable based on:</p> <ul style="list-style-type: none">• Vendor type• Use cases• Data classification• Level of access• Likely risk/impact area	<ul style="list-style-type: none">• Highly manual• Subjective• Time-consuming (for both your organization to create, and third party to respond to)	<p>Third party will have access to proprietary data. You tailor the questionnaire to detail the exact numbers and types of data security controls required.</p>

Standardized Questionnaires

Another common tactic is standardized questionnaires. Standardized questionnaires have been developed through the collective knowledge and experience of a range of security experts and technology organizations. Widely used options include [Shared Assessments’ Standardized Information Gathering Questionnaire \(SIG\)](#) and Cloud Security Alliance’s [Cloud Control Matrix \(CCM\) Consensus Assessment Initiative Questionnaire \(CAIQ\)](#). Third parties may be familiar with, and have ready responses to, these questionnaires.

Standardized Questionnaires Cont'd

Pros	Cons	Sample Use Case
<ul style="list-style-type: none">• Standardization, with some customization options• Easy to compare responses from different third parties• Faster turnaround time	<ul style="list-style-type: none">• Highly manual• Subjective• Time-consuming	<p>Your RFP requires third parties to complete SIG as part of initial vetting so you can screen out and make apples-to-apples comparisons.</p>

Compliance Certifications and Reports

Security frameworks are blueprints for security programs that effectively reduce and manage risk. For lower-risk third parties, you may be able to gain appropriate assurance by reviewing and confirming any regulatory or security-focused certifications and reports they have earned.

Sample Certifications and Reports

 HIPAA	 GDPR	 NIST 800-53
 SSAE-16 SOC 2	 CCM™ <small>Cloud Controls Matrix</small>	 Cloud Security Alliance STAR

Compliance Certifications and Reports Cont'd

Pros	Cons	Sample Use Case
<ul style="list-style-type: none">• Regulatory requirements met• Third-party-verified (not subjective)• Cost-effective• Time-effective, expediting review process	<ul style="list-style-type: none">• Could lack specificity or applicability to the risks you're most concerned about	Your primary concern is whether the vendor is suitable for handling regulated data, such as credit card information. You require a PCI Certification for proof they are suitable and have been reviewed by a third party.

Onsite Audits

Onsite audits allow you to take a fully customized first-hand look at how third parties address the risks you care about. You (or your third-party risk assessment provider) are able to directly verify and evaluate their internal policies against risk. But while onsite audits are the safest and most effective way to assess third-party risk, they are neither cost- nor time-effective. They should generally be reserved only for your highest-risk third parties — those that present truly critical risks to your organization.

Pros	Cons	Sample Use Case
<p>Ability to:</p> <ul style="list-style-type: none">• Interview key control owners• Validate control testing• Collect evidence	<ul style="list-style-type: none">• Very costly• Very time-consuming• Tough to negotiate in a third-party contract	A third party is deeply ingrained in your processes and networks, presenting an existential level of risk to your organization. You contractually require permission for onsite audits.

Contract Reviews

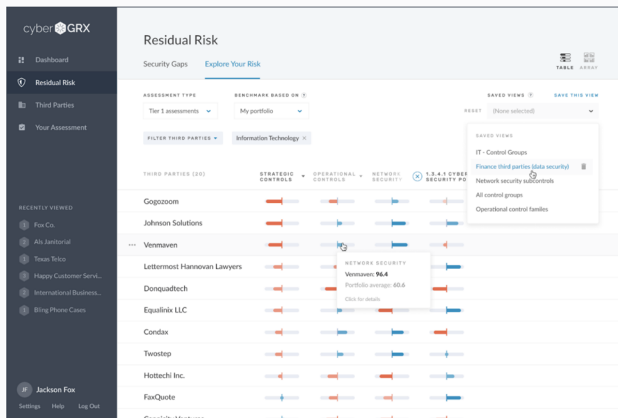
Contract reviews can be an effective way to invest resources in evaluating third-party risk and controls. While contract reviews are generally performed by your legal team, it’s ideal to embed your risk team in the process. You can embed language that helps you gain a higher level of assurance that third parties can be held accountable for meeting control obligations.

Pros	Cons	Sample Use Case
<ul style="list-style-type: none">• Higher level of assurance• Legally actionable• Ability to embed specific requirements for controls or gap remediation	<ul style="list-style-type: none">• High-effort• Tedious and time-consuming to review• Negotiation reluctance from third parties	<p>You uncover gaps in a third party’s security framework. Instead of calling off the deal, you embed a clause requiring them to remediate gaps to a certain level by a set date.</p>

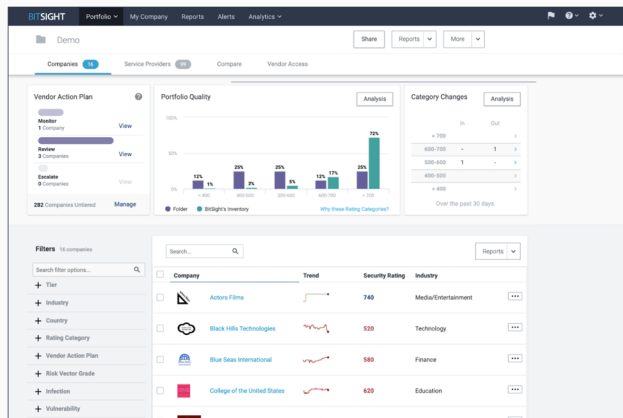
Reputation Services

Third-party reputation services are a relatively recent evolution. By crowdsourcing risk assessments ([CyberGRX](#)) or scraping websites, DNS and TLS configurations, and other publicly available data for objective, verifiable security information ([BitSight](#)), these services develop third-party risk ratings — essentially “security credit scores.”

Sample Reputation Service Reports



BitSight



Pros

- Low effort for your organization
- Third-party-verified (not subjective)
- Easy to share reports with partners

Cons

- Could lack specificity or applicability to the risks you're most concerned about
- May use only existing publicly available info

Sample Use Case

You lack TPRM resources. To save time and effort in assessing lower-risk third parties, you use a reputation service to access risk reports.

Continuous Monitoring Tactics

Given your organization's risk prioritization and TPRM categorizations, how should you tailor monitoring tactics to match?

Establish Periodic Reassessment Cadence Based on Risk Level

Again, the most important success factor is to structure and formalize continuous monitoring activities based on risk level. Higher-risk third parties should receive more attention more frequently, and lower-risk third parties should receive less attention less frequently.

Periodic Reassessment Cadence Example

Risk Tier	Contract Review	Risk Categorization	Security Review	SLA Review
Tier 1 – High Risk	Upon Renewal	Annually	Annually	Annually
Tier 2 – Medium Risk	Upon Renewal	Every 24 months	Every 24 months	Every 24 months
Tier 3 – Low Risk	Upon Renewal	Every 36 months	Not Required	Not Required

Perform Rediscovery With Internal Relationship Owners

Risk changes over time, so reassessments should involve appropriate rediscovery with your organization's third-party relationship owners. This will help ensure that TPRM approaches and categorization continue to be appropriate for each third party.

Most often, rediscovery occurs via surveys that are either sent manually or triggered within an automated technology platform. Surveys should address:

- **Relationship ownership.** Are they still the owner?
- **Risk categorization.** Have the use cases that the third party is addressing changed? Have there been changes to the third party's risk profile?
- **Contract renewals.** Should terms be restructured to better manage risk or account for new considerations?
- **SLAs.** How do they feel about the overall performance of the third party? Are SLAs being met? While SLA review isn't typically in the risk mandate, reassessment touchpoints are a great opportunity to assess SLA compliance.

Perform Targeted Assessments Following Key Events

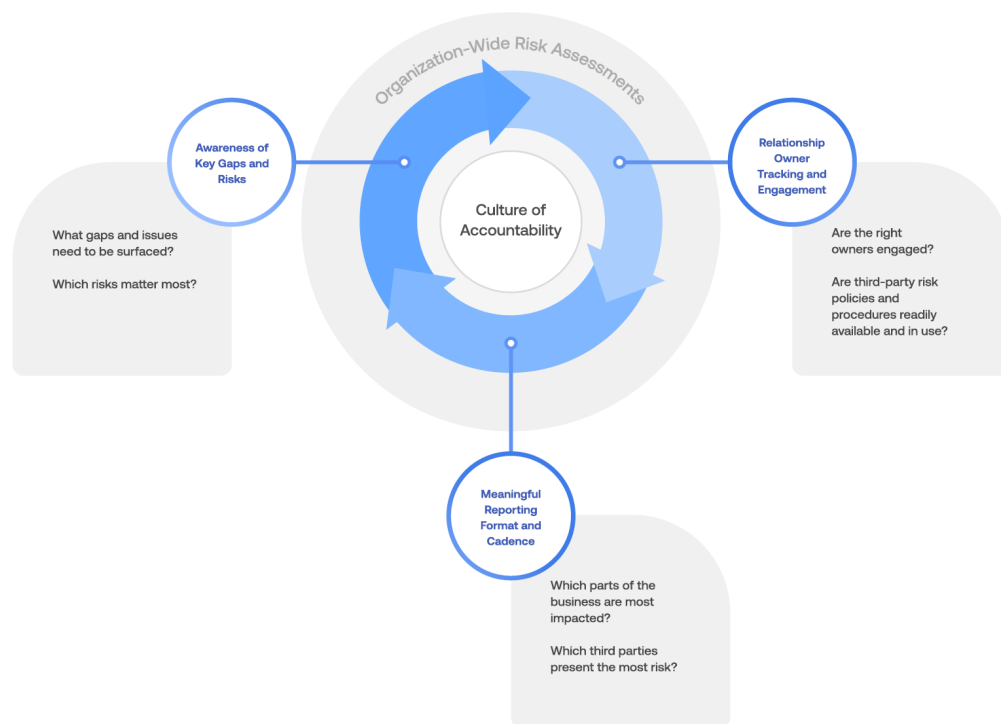
You may want to reengage third parties outside your normal cadence to either reassess or perform a targeted assessment:

- After a security incident or breach.
- After a public zero day, if it's likely the third party was impacted.
- After you've updated your internal risk assessment(s).

Issue Management and Reporting Tactics

How can you ensure that your TPRM program drives optimum value for your business?

TPRM Issue Management and Reporting Life Cycle



Focus on Meaningful, Effective Reporting

The key success factor is creating meaningful reporting that regularly communicates risk information and insight to the right people across your organization. As depicted in the graphic, effective TPRM issue management and reporting are symbiotic, benefiting and supporting each other in turn. Meaningful reporting helps to create ongoing awareness of key gaps and risks. When awareness is raised with the right people, reporting remains meaningful and accurate — and people are equipped not only to avoid issues, but to respond more effectively when they occur.

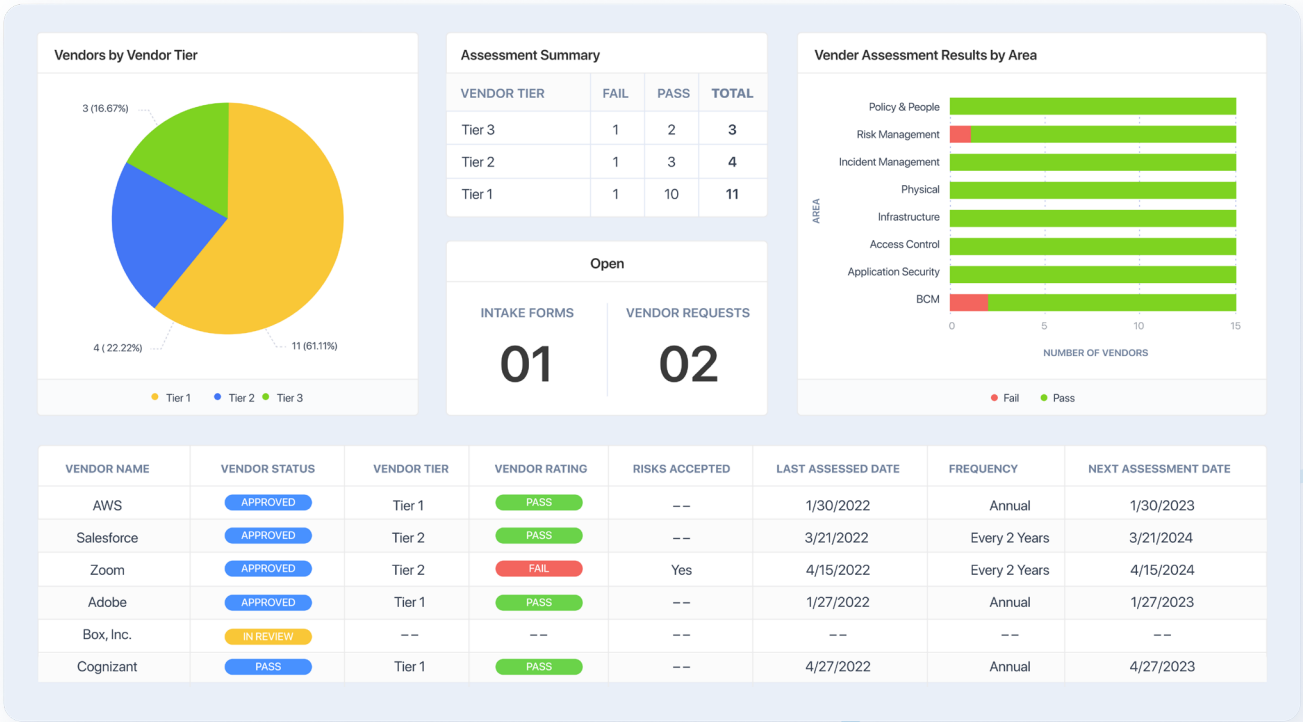
Build Accountability Around Regularly Updated Risk Assessments

Just as in the overview graphic on page 4, effective TPRM programs take place against the backdrop of regularly updated organization-wide risk assessment(s) and around an overall culture of accountability. The risks stemming from control gaps or other identified issues with third parties should be quantified and rolled up from the relationship owner, to the executives responsible for owning the overall risks for their area of the organization. As a result relationship owners can collaborate with risk owners on the tradeoffs of engaging this third party, changing how they negotiate that third party’s contract and SLAs, implementing compensating internal controls, — or causing them to engage a different third party altogether.

Create Reporting That Supports Effective Decision Making

Ensure that your TPRM reporting format and cadence are designed to help executive leadership and relationship owners to understand and use risk data to better manage and mitigate third-party risk. Reporting should help people readily understand which third parties present the most risk to the business, which areas of the business are most affected by third-party risk, and what the plans are to mitigate those risks. [AuditBoard’s Third-Party Risk Management Solution](#) allows teams to create a central third-party repository while streamlining communication with stakeholders — acting as the single source of truth from identification and assessment through monitoring, remediation, and reporting.

Third-Party Risk Reporting Dashboard Example



Conclusion

Many of the organizations that have been humbled by third-party risk incidents over the past few years are still in damage-control mode. Their valuable risk resources remain focused on responding to past impacts, rather than proactively preventing future incidents.

These organizations are still vulnerable. Will they survive the next third-party impact?

Against an ever-evolving risk landscape in which third parties present significant risk, businesses can no longer afford to treat TPRM as low-priority. Fortunately, the majority seem to have learned this lesson. As [Deloitte's 2021 TPRM survey](#) found, 71% of organizations now identify digital risk as their top-priority area, and almost half (49%) are using tech investments to update due diligence and monitoring processes to make them “intelligence-led” and real-time.

Remember, TPRM is primarily about making the smartest use of limited resources. Is your risk team focused on the third parties and risks that have the most potential impact? Which tactics will help you be more proactive in managing third-party risk? Are there opportunities to more effectively use existing or new technologies (e.g., information security and risk management software) for third-party discovery, monitoring, and reporting activities? How can you optimize your TPRM program to make better decisions for your business?

If your organization hasn't yet prioritized its TPRM program, the time to act is now. Don't let your organization become the next third-party security breach headline.

About the Author



Richard Marcus

Head of Information Security
AuditBoard

Richard Marcus. CISA, CRISC, CISM, TPECS, leads the Information Security Team at AuditBoard where he is focused on product, infrastructure, and corporate IT security. He is also responsible for leading the charge on AuditBoard's own internal compliance initiatives. In this capacity, he has become an AuditBoard product power user, leveraging the platform's robust feature set to satisfy compliance, risk assessment, and audit use cases.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management. More than 35% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2 and Gartner Peer Insights, and was recently ranked for the third year in a row as one of the fastest-growing technology companies in North America by Deloitte.

To learn more, visit: [AuditBoard.com](https://auditboard.com).

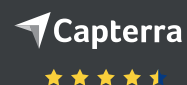


Third-Party Risk, Uncovered.

The biggest threat isn't always visible at a glance. Take a strategic approach to your third-party risk management program and surface the risks that matter.



AuditBoard is Top-Rated by Customers



Your TPRM Program, Centralized.



Streamline Vendor Evaluation and Onboarding

- **Automate workflows** for requesting, submitting, and reviewing vendor questionnaires.
- Aggregate details to create a **central vendor inventory**.
- Leverage auto-inherent risk scores to **prioritize** your vendor inventory.

Vendor Intake Form

1. Products & Services

☐ Services (Professional, Consulting, etc.)

☐ Software as a Service (SaaS)

☐ Software (Custom)

☐ Software (Off the Shelf)

☐ Hardware (Physical devices)

☐ Other (please enter in next field)

2. Functionality

Briefly, what functionality does this service provide (i.e. what is the business use case)?

3. Vendor Access Requirements

Will Vendor employees require access to AuditBoard assets, applications, systems, or data?

☐ Yes

☐ No

☐ Maybe

4. AuditBoard Data Access

Will vendor employees have access to sensitive AuditBoard data (including, but not limited to, user information, audit logs, and system configuration)?

☐ Yes

☐ No

Submit Vendor

Vendor Name

AWS

Vendor First Name

James

Vendor Last Name

Clarke

Vendor Contact Email

james.clarke@aws.com

Business Contact

Select contact

Cancel Submit

Vendors				Vendor Criticality	Risk Score
Name	Vendor Type(s)	Owners	Description		
Oracle	Software As A Service (SAAS)	Amelia Clarke	Financial Accounting	Tier 3	Established
Paylocity	Software As A Service (SAAS)	Vincent Ray	Payroll Processing S	Tier 3	--
Zoom	Software As A Service (SAAS)	Amelia Clarke	Virtual Meeting Serv	Tier 1	Standard
DocuSign	Software As A Service (SAAS)	Andrew Johnson	Document Signatur	Tier 3	Established
Clarizon	Software As A Service (SAAS)	Tiffany Byrd	Project & Resource	--	--
Salesforce	Software As A Service (SAAS)	Landon Matthews	Sales Lifecycle Man	Tier 3	Established
Box, Inc.	Software As A Service (SAAS)	Eugene Kim	Document Sharing f	Tier 3	Established
Adobe	Services	Mary Lim	PDF Read Write and	Tier 3	Standard

Conduct Vendor Risk Assessments With Ease


- Create **custom assessments** or utilize out-of-the-box **templates** to perform vendor assessments.
- Simplify decision-making with **auto-risk scoring**.
- **Track mitigation efforts** to demonstrate program improvement.

Manage Your Mitigation Plans

- Document and track issues identified via **risk assessments**.
- **Assign** mitigation owners, view the status of action plans, and send reminders.
- **Gain visibility** into top third-party risks so they can be proactively remediated from a centralized dashboard.

AP#8 – Andrew Johnson

COMPLETE



REMIEDIATION OWNER
Andrew Johnson

+ Workstream Task

REMIEDIATION DATE
2022-04-30


DUE DATE
2022-05-15

REMIEDIATION ACTION
Obtain 2022 SOC report and review for deficiencies.


MANAGEMENT RESPONSE
Vendor stated that the report should be available by 5/5/2

WORKSTREAM TASKS
There are no WorkStream Tasks associated to this Action Plan.

FILES

 [Remediation Workpaper.xlsx](#)
15 hours ago by Amelia Clarke

Action Plan 1



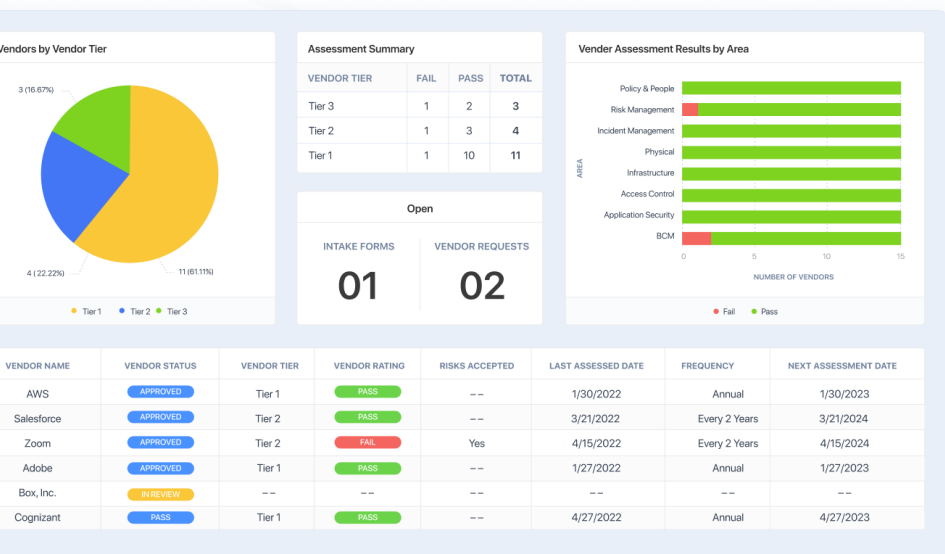
Andrew Johnson
Due: 2022-05-15

COMPLETE



“ We were doing control testing, third-party risk assessments, corporate risk management, policy management, issue management, and a SOC 1 — all within AuditBoard, and all within one year of buying the tool.

MYLES GOLD | OPEN DEALER EXCHANGE
GRC Manager




Stay Ahead With Vendor Monitoring

- Leverage **dashboards** to monitor performance and proactively identify potential failures.
- Enable periodic **monitoring processes** and send out risk assessment **questionnaires**.
- **Identify any changes** to the vendor's control environment or follow up on newly identified vulnerabilities and request evidence.

To get more info, schedule a demo or contact us:

 [auditboard.com](#)

 1 (877) 769-5444