Prevalent™

Best Practices Guide

# Six Steps to Complete Third-Party Risk Management

A Guide to Build, Mature or Optimize Your TPRM Program

# Table of Contents

**Table of Contents** ..... 2

**Today's Reality: Balancing Business Growth vs. Business Risks** ..... 4

**The Goal: A More Mature and Optimized Third-Party Risk Management Program** ..... 5

**Level 1: Automation-Centric TPRM** ..... 5

**Level 2: Compliance-Centric TPRM** ..... 5

**Level 3: Risk-Centric TPRM** ..... 5

**What to Look for: Six Steps to a More Mature Third-Party Risk Management Program** ..... 7

**Step 1: Define/Build/Optimize – Basic Program Decisions** ..... 8

Factors to consider in making tiering decisions ..... 8

Which questionnaire to use? Industry-standard or proprietary? ..... 9

Top 5 capabilities to look for as you build your program: ..... 9

**Step 2: Monitor for Vendor Cyber and Business Risks** ..... 10

What cyber/data to monitor ..... 10

Business risks are important, too! ..... 11

Top 6 continuous monitoring capabilities: ..... 12

**Step 3: Collect Evidence and Perform Due Diligence** ..... 13

Choosing the right collection and due diligence review method – do-it-yourself, shared, or outsourced? ..... 13

Top 6 evidence collection and review capabilities: ..... 14

Case Study: Global Pharmaceutical Company Achieves Tangible ROI ..... 15

**Step 4: Analyze and Score Results** ..... 15

The value of a central risk register ..... 15

The importance of an inside-out/outside-in score ..... 16

Top 5 analysis and scoring capabilities: ..... 17

Case Study: Cancer Research UK Reduces Risk to Accelerate Life-Saving Research Through Partners ..... 17

**Step 5: Remediate Findings** ..... 17

The importance of a vendor portal ..... 18

Top 5 remediation capabilities: ..... 18

**Step 6: Report to Internal and External Stakeholders** ..... 18

The importance of regulatory-specific reporting ..... 18

But it's about more than just compliance ..... 19

Top 5 reporting capabilities: ..... 20

Case Study: Allianz UK Achieves 50% Time Savings ..... 20

**The Prevalent Difference ..... 21**

**The Prevalent Platform Delivers 360-Degree Third-Party Risk Management .....21**

**Depth of Features for Maximum Risk Visibility .....21**

**Fully Integrated Sharing Networks Accelerate Time-to-Value.....21**

**Unmatched Industry Expertise & a Defined Process for TPRM Program Maturity .....21**

**Conclusion: Delivering Business Value..... 22**

**Appendix: Solution Provider Comparison Checklist ..... 23**

**About Prevalent..... 25**

## Today's Reality: Balancing Business Growth vs. Business Risks

All organizations rely on partners and suppliers on some level to deliver products and services to their customers, with these third parties often receiving and handling sensitive information. So, with an ever-increasing number of cyber-attacks originating from third parties, and growing data privacy concerns driving increased regulatory activity, ensuring that those partners and suppliers manage information securely is paramount.

Whether manual or ad hoc, assessing third-party risk can be enormously time-consuming, prone to errors and omissions, and leaves decision makers to rely on outdated and incomplete information. An effective risk management process throughout the vendor relationship life cycle includes:

- Identifying and prioritizing vendors based on their inherent risk
- Designing the right questionnaire content and surveying each third party's internal controls according to their inherent risk
- Performing due diligence by reviewing the answers and evidence partners submit, and then using that information to determine a residual risk level
- Remediating to minimize risks to an acceptable level
- Providing reports to auditors to prove compliance with regulatory frameworks

Manually overseeing this continuous loop is costly, inefficient, and more importantly, not scalable across an entire partner ecosystem. Yet the risks of not doing it right are painfully apparent: fines, failed audits, non-compliance, and worst of all, the dreaded data breach and its (very) public disclosure.

The critical question you must answer is this: How can you automate your processes to quickly and efficiently ensure that your third parties do not create an unacceptable potential for business disruption in your supply chain?

This best practices guide will help you answer just that by illustrating where to begin a third-party risk management (TPRM) program; how to mature it into a scalable, agile program that's adaptable to business changes; and what business outcomes to expect along your journey. To set the stage, we'll first define levels of program maturity and map attributes of a TPRM program into those levels. Then, we'll walk through the six steps required to complete TPRM optimization.

Throughout this guide, you'll see various signposts to help guide you along. Watch for these!

**It's a Trap!**
Pitfalls to avoid

**Tips & Best Practices**
What we've learned along the way

**Technical Attributes**
*Key capabilities*

**Case Study**
What real customers are doing to solve this problem

# The Goal: A More Mature and Optimized Third-Party Risk Management Program

Although Gartner makes it very clear that the primary driver for TPRM is compliance, TPRM programs can be borne out of any one of a number of organizational demands – from automation, to compliance, to risk management. Based on our experience, we've defined three levels of TPRM program maturity.

## Level 1: Automation-Centric TPRM

Programs that start out as a reaction to personal pains (e.g., workload or complexity) tend to be the least mature. They usually aren't driven by risk management or compliance concerns, but rather by an individual, perhaps in procurement, looking to expedite the vendor onboarding process. Level 1 organizations lack the oversight of more mature programs that are tied to a governance, risk and compliance (GRC) effort. The goal here is to automate as much of the process of collection and analysis of vendor evidence as possible to reduce the incessant back-and-forth between the enterprise and the vendors. There's nothing wrong with starting your TPRM program here. After all, you have to start somewhere, and you can successfully make the business case for funding for such a project by tying inconsistent, manual processes to the risk of errors that can lead to data breaches.

## Level 2: Compliance-Centric TPRM

Moving up the maturity scale, Level 2 programs are primarily compliance-driven in that the organization has to address one or more regulatory requirements. Organizations at this maturity level realize they need a *program,* not a *project,* to risk-rate their top-tier vendors. However, they often have limited visibility with too many spreadsheets and too much email interaction with their suppliers. If your organization is at this maturity level, take heart that most other companies are here, too.

## Level 3: Risk-Centric TPRM

The most mature TPRM programs are driven from the top-down by risk management programs – and compliance is a byproduct of this effort. Organizations at Level 3 maturity know the number of vendors and can quantify the risk of those vendors, albeit with less-than-ideal levels of automation. Their TPRM and GRC/IRM programs are intertwined; they enjoy executive sponsorship; and they likely secure the services of one of the Big 5 audit firms for outsourcing or program management. This level of maturity is rare outside of large, highly regulated organizations with sufficient resources, vision and scale.

Take a look at the table on the next page to assess where your program is currently and where you would like to see it evolve.

*Table 1: Example TPRM maturity levels*

| Maturity | Driver | Attributes |
|---|---|---|
| Level 1 | Automation | • Bottom-up approach<br>• Manual process-driven<br>• Need simple, custom questionnaires without overkill<br>• A project (versus a program)<br>• Starts small with a limited number of suppliers<br>• Limited awareness/visibility of risk<br>• Business not directing risk reduction or compliance efforts |
| Level 2 | Compliance | • Middle-out approach<br>• Has a specific compliance mandate<br>• Manual processes to assess a subset of suppliers<br>• Suppliers tiered by critical service or spend<br>• Understands lack of visibility over risk<br>• Is looking to create a TPRM program but needs help to define it |
| Level 3 | Risk Management | • Top-down approach<br>• Understands the bigger picture<br>• Part of a larger risk management program<br>• Knows total number of suppliers and is able to quantify risk<br>• Currently assesses a percentage of the total number of vendors using manual processes<br>• C-Level sponsorship and budget allocated<br>• Understands this is a program, not a project |

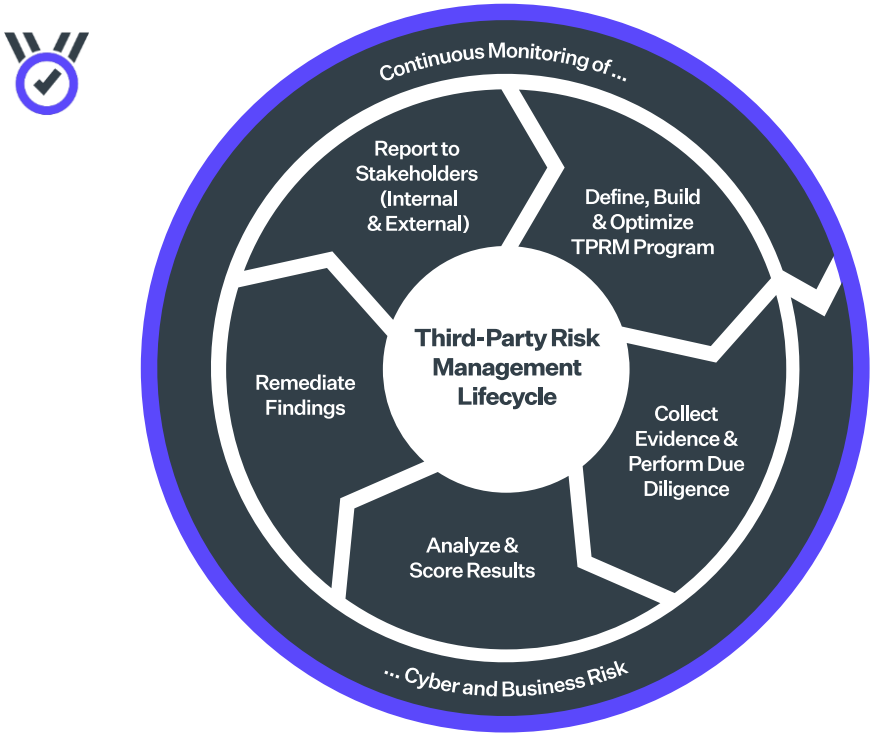
The path to maturity is not easy. And it's not fast. There are no shortcuts. However, by investing in the right people, processes and technology, you can achieve greater levels of automation that will ultimately increase your risk management team's productivity. This will help you align your efforts with your priorities. The next section of this guide discusses a six-step approach to achieving a more mature and effective third-party risk management program.

# What to Look for: Six Steps to a More Mature Third-Party Risk Management Program

A programmatic process is the fastest path to optimizing and maturing your third-party risk management program. Implementing an end-to-end TPRM program should follow a defined process to minimize costs and distractions while speeding results. This section of the guide identifies a six-step deployment plan for TPRM and identifies key capabilities to look for in a solution provider. See figure 1 below for a representation of the process.

The result of this process is greater visibility into vendor risks, more automation to speed your vendor assessments, and the ability to scale your program to meet future demands.

*Figure 1: A closed-loop process for maturing a TPRM program*




Throughout the process of evolving your third-party risk management program, keep in mind these business requirements, as they'll help you be an effective advocate for this program with your colleagues:

- Minimize total cost of ownership
- Provide a fast time-to-value
- Deliver information to make the best risk-based decisions

## Step 1: Define/Build/Optimize – Basic Program Decisions

There are several decisions that must be made prior to kicking off a third-party risk management program. Expert advisory services can help define the parameters of the program; ensure you're assessing the right vendors according to inherent risk and criticality to the business; and define the right content to collect from vendors based on regulatory frameworks or industry standards.

Key decisions to make at this step include:

- What factors will you consider in making vendor tiering decisions?
- Which questionnaire will be used to gather information about your vendor's controls? Will you use industry-standard or proprietary surveys?
- What collection method(s) will be used? Will you manage the collection yourself? Will you take advantage of repositories of pre-completed questionnaires? Will you outsource collection to a partner? Some combination of each method?*

  **This decision is so important that this guide dedicates Step 3 to it!*

### Factors to consider in making tiering decisions

You can use any criteria to tier or categorize vendors, from annual spend and inherent risk, to criticality of services and sensitivity of access. However, tiering decisions should be influenced primarily by the regulatory environment in which you operate. For example, if GDPR is a significant driver for your organization, then tiering vendors based on their access to your customer's personal data should be a primary consideration in the process. A typical process to tier vendors could follow this logic:

#### *Define key attributes*

- Type of content required to inform controls reporting
- Criticality to business performance
- Supplier location and whether this location raises any legal or regulatory obligations such as GDPR
- Determining if the supplier's services rely on fourth parties

#### *Supplier criticality considerations*

It's important to fully understand the impact a supplier could have on your business if it was to fail in terms of delivery or performance of services. Accordingly, you should leverage a scoring system that determines the supplier tier group. This could include the following criteria:

- Operational or client facing processes
- Interaction with personal data
- Financial status and implications
- Legal and regulatory obligations
- Reputation

Once you determine your supplier tiers, you should have a clear breakdown of which suppliers are most critical. For example, you should be able to run a report on all suppliers that are US-based, handle personal data, and are top tier.

## Which questionnaire to use? Industry-standard or proprietary?

There are cases to be made for both. Utilizing industry-standard questionnaires (e.g., the Standard Information Gathering – or SIG – questionnaire, or the H-ISAC questionnaire for healthcare organizations) can get you started faster by providing an accepted pool of content that your vendors are likely already familiar with. Assessing all vendors using the same industry-standard content also provides consistency. You gain a more like-for-like comparison of similar services, while enabling your vendors to eventually share their responses with other partners if they choose to do so. Answering a questionnaire once and sharing it with many partners has a tangible benefit (more on that in Step 3).

On the other hand, creating proprietary content by drawing from multiple questions or questionnaires is valuable for organizations that have fewer vendors to assess (i.e., where consistency is less important), or for those that need a survey instrument specific to the needs of their business.

Utilizing a repository of pre-defined assessments – including industry-standard questionnaires like SIG Core, SIG Lite, and H-ISAC, and compliance and security framework-specific questionnaires like GDPR, FCA, PCI-DSS, ISO 27001, NIST and more – simplifies and automates the survey collection and management process. Look for the capability to import or create items to be reviewed during the assessment process, with customization capabilities for combining questions to meet unique needs.

Regardless of standardized or proprietary, as you begin to engage TPRM providers, make sure they have the flexibility to deliver both types of questionnaires, so you aren't locked into a single, rigid questionnaire.

### Top 5 capabilities to look for as you build your program:

1. Thorough, multi-variate process for determining vendor criticality that can adapt to business changes
2. Multiple questionnaire options – industry-standard, pre-built, customizable – with the ability to weight the answers and evidence submitted per question according to business importance
3. Multiple collection and analysis options, including doing it yourself, leveraging a network of completed questions and submitted vendor evidence, and the ability to outsource it to a trusted partner
4. A disciplined, rigorous consulting and advisory process geared to progressively maturing your program
5. Relationships with systems integrators and other partners that can accelerate the time to realize value

Prevalent's Strategic Advisory and Professional Services organization works with you and your partners to deliver best practices and ongoing optimization to meet your business requirements, with multiple professional services package options available to fit your project scope. From consulting, to implementation, to optimization, Prevalent provides the complete spectrum of services to mature your third-party risk management program.

## Step 2: Monitor for Vendor Cyber and Business Risks

Once you've decided how to tier your vendors and selected questionnaire content, the next step to comprehensive third-party risk management is to begin monitoring the cyber and business risks of those vendors. Although periodic assessments are essential to gaining an understanding of how vendors govern their information security and data privacy programs at a point in time, it's a lengthy process for surveys to be communicated out to vendors – and for vendors to begin submitting completed content and evidence. Plus, you're likely only assessing vendors yearly, and a lot can happen to a vendor in a year between assessments! Monitoring your vendors at this early stage in the process has several benefits, including:

- **Immediacy** – Gaining an instant view of the risks that hackers exploit can inform your vendor tiering and prioritization logic
- **Validation** – Validating vendor responses to surveys when they start coming in
- **Frequency** – Obtaining more frequent, unbiased insights into your vendor's potential cyber vulnerabilities or relevant business risks that can negatively impact your business

Take a step back to consider whether a "score" or "security rating" will solve what ails you. Those tools only provide an external network scan showing basic cyber risks. With no vendor assurance, no context, and limited information boundaries based on relevance to your company, scoring and rating vendors provide a limited view of vendor risk – meaning there is no real assessment happening. Remember back in Step 1 where we said most TPRM programs are driven by compliance? Consider this:

- What about measuring a vendor's internal adherence to compliance mandates? Can an external scan reveal that?
- Can a security score tell you how a vendor handles your data?
- How can security ratings automate the collection of vendor evidence and due diligence?

While outside-in risk scoring or ranking can deliver risk insights, it will not meet compliance requirements when used as the only mechanism to evaluate vendor risk. Best practices for TPRM as published by Shared Assessments, Gartner, Forrester and others include vendor questionnaire assessments *plus* continuous monitoring for a complete view of vendor risks.

### What cyber/data to monitor

Monitoring your vendor's networks is more than just vulnerability management, although vulnerability management is an important part of it. Combine it with multiple external sources of cyber threat intelligence – including from internet sensor networks, global threat databases, collaborating security partners, and anti-virus users – to return intelligence on:

- **Data breaches** – Historical data breach records including total records affected, plus overviews and locations of breaches

- **Threat events** – IP threats, phishing attacks, and domain reputation information
- **Secure Sockets Layer (SSL) risks** – SSL/TLS (Transport Layer Security) Certificates, SSL/TLS versions supported, Supported cipher suites, Packet headers, and Online Certificate Status Protocol (OCSP) adherence
- **Domain Name System (DNS) risks** – Sender Policy Framework (SPF) record presence, State of Name Servers (responsive, non-responsive, open recursion and zone transfer allowed), and DMARC (Domain-based Message Authentication, Reporting & Conformance) record presence
- **Application security** – Web application security risks informed by OWASP's Top 10 list, including Broken Authentication and Session Management, Sensitive Data Exposure, Security Misconfigurations, and Potential for Cross-Site Scripting (XSS)
- **Deep/Dark Web** – Threat intelligence gathered before, during and after cyberattacks.

This information is exactly what is visible to hackers. The intelligence can be used to help vendors clean up their open-source footprint or change internal processes to reduce risk by way of closing the disconnects and gaps of anomalies – similar to cleaning up your credit report prior to applying for a home loan.

## Business risks are important, too!

Understanding the cyber risks in your vendor's public-facing internet assets is only one half of the continuous monitoring equation. The other half is understanding qualitative business information that can indicate possible future risks. Business risk indicators include the following:

- **Operational** – M&A activity, layoffs, leadership changes, partnership changes, customer relationships, and geographic expansions
- **Brand** – Data breaches, product recalls, and brand changes
- **Regulatory/Legal** – Probes, fines, economic sanctions/blacklists, and major lawsuits and settlements.
- **Financial** – Bankruptcy, capital transactions (debt, equity, etc.), and data breach impact on financial viability

Together, cyber and business risk monitoring provide a much more comprehensive view of a vendor. This "outside-in" view gives you an edge in interpreting the potential impact of vendor risk while augmenting your "inside-out" assessments to gain a more informed and accurate risk score.

## Top 6 continuous monitoring capabilities:

1. A view into business risks that can augment cyber security scanning, providing a more holistic view into a vendor's potential risks
2. Industry-standard scanning and third-party sources, providing a comprehensive, trusted and transparent scoring methodology
3. Prescriptive guidance and remediation recommendations on vendor risks
4. Clear reporting on risk status, helping internal teams to focus and prioritize what's most important
5. A flexible scoring framework that can incorporates business context and quantifies risks to enable objective and comparative decision making
6. Native integration with detailed vendor assessments, providing a single view of all vendor risks in one place

Delivered as part of the industry's only purpose-built, unified platform for third-party risk management, the cloud-based Prevalent Cyber & Business Monitoring Service provides both snapshot and continuous vendor monitoring with immediate notification of high-risk issues, prioritization and remediation recommendations. Data security and business risk monitoring enables you to look beyond tactical vendor health and gain the strategic business view of a vendor's overall information security risk. These insights inform overall vendor risk management, augmenting scoring based on internal, controls-based assessments.

### Case Study: Large U.S. Energy/Utility Company Gains Immediate Visibility into Previously Unknown Risks

A large U.S. energy/utility company was challenged to assess thousands of vendors. With limited staff, the organization was constantly reacting to vendor-based threats, with a lack of confidence and proper validation in vendor security policies and procedures. They implemented the Prevalent Cyber & Business Monitoring Service to gain broader context of vendor risk events. In less than a week, the Prevalent solution identified a risk event concerning an active, highly insecure web service on one vendor's website. The site exposed logins and critical information in clear text and Prevalent identified the associated website vulnerability. The utility notified the vendor, which immediately remediated the vulnerability – avoiding exposure of the client's (and others'). By combining monitoring with Prevalent's assessment capabilities, the utility has achieved 360-degree protection and vendor assurance.

## Step 3: Collect Evidence and Perform Due Diligence

The next step toward third-party risk management program maturity is evidence collection and due diligence review on submitted answers. As mentioned in Step 1, collection and due diligence review can take many forms – managing the process yourself, utilizing a repository of pre-completed questionnaires, outsourcing to a partner, or some combination thereof.

### Choosing the right collection and due diligence review method – do-it-yourself, shared, or outsourced?

#### *Do-It-Yourself*

Once you define your questionnaire, you can internally manage vendor data collection and analysis – but make sure you have the backing of a solution to manage workflow, vendor communications, and document/evidence management to centralize, track and simplify the due diligence process. The solution should include an easy-to-use vendor-facing portal that clearly displays status of survey completion and suggested remediations, while maintaining a complete audit trail for future validation. Remember, the easier you make it for vendors to complete and submit required information, the faster you can identify and remediate risks.

#### *Shared*

Third-party risk management processes can be taxing on under-resourced teams. Data collection processes and vendor back-and-forth communications account for the largest share of time needed to reduce risk and complete assessment assurance. Compounding this issue is the ever-shifting regulatory landscape, which requires expertise to understand compliance reporting obligations. Achieving compliance and meeting vendor risk management requirements while maximizing your team's skillsets is a balancing act for sure.

To accommodate resource constraints, many organizations – especially those with a solid vendor tiering plan – choose to leverage completed content already submitted and shared within an industry exchange. These vendor exchanges are self-fulfilling prophesies – the more vendors participate in them, the greater the overlap is with other enterprises, which speeds up the risk identification and mitigation process and minimizes the time required to spend collecting the data.

Prevalent runs two (2) industry-specific vendor evidence exchange networks: the Legal Vendor Network (LVN) and the Healthcare Vendor Network (HVN) through H-ISAC. We also offer a "network of networks" called Prevalent Exchange. Each network is built on industry-standard questionnaire content accepted by the relevant members or governing body, simplifying and speeding risk analysis and mitigation. If your organization is a law firm or in a healthcare-related industry (e.g., pharmaceutical, insurance, etc.), be sure to investigate the Prevalent networks. Customers report that approximately 40% of their vendors are already part of the network. That delivers immediate time and cost savings.

*Outsourced*

A final option is to outsource the collection and analysis of evidence to a TPRM vendor, audit firm, or systems integrator. Your solution provider or systems integrator can offer remediation and analysis capabilities without tying up your inhouse resources. This enables your team to focus on risk management efforts (e.g. identification and remediation), rather than on collecting vendor evidence and ensuring its accuracy. This delivers a faster time-to-value for risk reduction efforts and is a solid option for extremely resource-constrained teams – or those with limited internal skillsets.

As with questionnaire selection, TPRM providers that offer flexibility in collection methods will enable your team to stay agile.

## Top 6 evidence collection and review capabilities:

1. Survey section/creation – draw from a large library of pre-built questionnaires or build your own
2. Survey scheduling assistant – define assessment schedules and chasing reminders with a dashboard for a real-time view into survey completion status
3. Flexible collection and analysis options, including doing it yourself, leveraging a network of completed questions and submitted vendor evidence, and the ability to outsource it to a trusted partner
4. A flexible scoring framework that quantifies risk and incorporates the necessary business and regulatory context to promote vendor communications and emphasize the importance of remediation
5. Bi-directional document and evidence management with tasks, acceptance, and mandatory upload features to obtain proof of controls
6. User dashboard – a centralized overview of tasks, schedules, risk activities, survey completion status, agreements and documents

The Prevalent Network enables risk and IT/OT teams to focus on remediating risk and addressing compliance by leveraging a repository of completed vendor questionnaires backed by continuous monitoring. With outsourced collection of due diligence and monitoring, organizations save time and resources, enabling them to quickly scale their third-party risk management program. At Prevalent, this is driven by Risk Operations Centers, teams of third-party risk management experts who collect vendor evidence, review it for completeness, and provide remediation guidance for top risks.

### Case Study: Global Pharmaceutical Company Achieves Tangible ROI

A global pharmaceutical company was behind in completing its 250-550 annual third-party risk assessments and at risk of missing important compliance deadlines due to ongoing complexity issues with their existing TPRM tool. By implementing the Prevalent TPRM Platform, they have since removed 18 manual steps from their process, equating to one person-hour reduction of time per assessment. As a result, the company saves between 250 and 550 person-hours (i.e., 31-68 days) to complete their vendor risk assessments. This also eliminated the need for outsourced contract resources, freeing resources for other risk management projects in the organization.

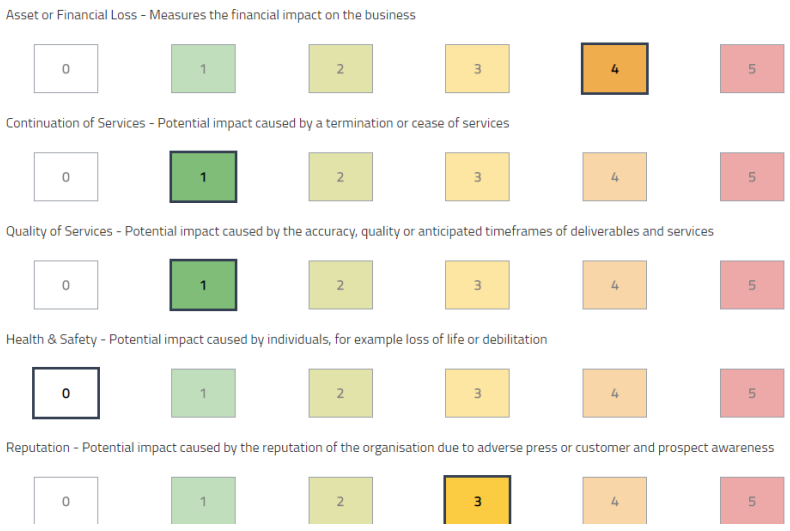
## Step 4: Analyze and Score Results

You're halfway through! So far, this guide has identified criteria to consider as you build your program, what to monitor in your vendor's networks, and how to collect and review evidence. You're at the point where you have completed (and perhaps validated) questionnaires and evidence – and now need to analyze and score all evidence so you can prioritize risk migration activity (discussed in the next step). Analysis tends to be a resource-draining exercise – namely performing tasks such as checking red flags in documentation, contextual comments, and considering variations in services vs. risks.

### The value of a central risk register

The best approach to analyzing and scoring is to first centralize results into a risk and compliance register. Automatically generating a risk register once a survey or scan has been completed filters out unnecessary noise and helps your team zero-in on areas of possible concern.

Since not all risks are created equal, it's important to have flexibility in how you weight risks. For example, if a vendor responds to a question indicating a lack of an employee security awareness training program, but that is not important to your organization, then it should be weighted so your team can laser-in on what the real risks are. This is illustrated below:



When vendors answer questions in an assessment, you should be able to create risks based on how the question was answered. Typically, your reviewers or vendor managers will then research the submitted evidence to identify false positives or negatives as part of the submission process. As they review the possible deficiencies, they could raise flags requiring further attention. The reviewer would validate the evidence and then create the risk if the evidence warranted it. Flagging points of concern in vendor responses ensures that the right risks are investigated, helping to reduce your organization's overall vendor risk profile.

A successfully implemented TPRM practice will categorize risks according to likelihood and impact. Like a heat map, this capability can help teams focus on the most important risks.

A sample of this capability is illustrated at right.


## The importance of an inside-out/outside-in score

As we mentioned in our warning back in Step 2, scoring and security ratings delivered from an external network scan will tell only half the TPRM story. That's why it's important to combine those results with what you get from your questionnaire-based assessment. This combination yields a true representation of your vendor's compliance and risk status, with much more thorough guidance on remediating those risks.

### Top 5 analysis and scoring capabilities:

1. Automatic generation of a risk register for centralized risk analysis and faster risk mitigation
2. Flexible risk weightings that granularly define the importance of specific risks to the business
3. Flagging and categorizing – either automatic or manual – to escalate a risk and route it to the appropriate contact for remediation
4. A matrix that dynamically enables risk analysis based on likelihood of an incident and its potential impact on the business
5. Integration with a cyber and business monitoring system to provide a single risk score per vendor that includes the results of an internal, controls-based assessment and an external network scan

The Prevalent Assessment Service delivers inside-out assessments of vendor compliance with IT data security, regulatory and privacy requirements. With a library of over 50 standardized assessments, content customization capabilities, and built-in workflow, the solution automates everything from survey collection and analysis to risk identification and reporting.

### Case Study: Cancer Research UK Reduces Risk to Accelerate Life-Saving Research Through Partners

Cancer Research UK is one of the world's leading cancer charities dedicated to saving lives through research. The organization was struggling with a manual approach to supplier risk management that was time consuming and not scalable. This made it difficult to produce the reports needed for internal stakeholders and effectively remediate risks – potentially hampering their ability to conduct life-saving research with their vendor partners. With the Prevalent Third-Party Risk Management (TPRM) Platform, Cancer Research UK realized time savings from survey scheduling and automated reassessments. They were able to automatically generate risk registers and leverage built-in discussion tools to simplify partner communication and speed risk remediation.

## Step 5: Remediate Findings

At this point, you've likely gone back-and-forth with your vendors to get questionnaires completed and evidence submitted. Perhaps you've even conducted some remote or onsite validation of that evidence. Unfortunately, the back-and-forth isn't over yet. Now comes the hard part – remediating the findings.

Remember the vendor tiering we discussed in Step 1 (plus how it's informed by scanning in Step 2) and the risk register we covered in Step 4? Those attributes will be extremely important during this step and will help you dynamically categorize vendors based on risk levels and criticality to the business. They will also enable bi-directional remediation workflow and document management on the risk register.

Projecting future levels of risk can be tricky, so look for capabilities that demonstrate how risk levels can change over time once recommended remediations are applied.

### The importance of a vendor portal

Working with your vendors to address control deficiencies or identified risks should be as transparent as possible, which is why a centralized vendor portal (or user dashboard) is recommended.

### Top 5 remediation capabilities:

1. A risk register for centralized analysis of risks
2. Built-in workflows that make it easy to bi-directionally manage and mitigate risks
3. A full audit trail that captures and audits conversations; records completion dates; and assigns tasks based on risks, documents or entities
4. Document/evidence management
5. Remediation guidance and recommendations to reduce risk

The Prevalent Assessment Service delivers inside-out assessments of vendor compliance with IT data security, regulatory and privacy requirements. With a library of over 50 standardized assessments, content customization capabilities, and built-in workflow, the solution automates everything from survey collection and analysis to risk identification and reporting.

## Step 6: Report to Internal and External Stakeholders

You have now collected and reviewed vendor-submitted questionnaires and supporting evidence; analyzed and scored risks based on the answers; and worked with your vendors to remediate findings. But the process isn't complete until the auditors say so, and that's why comprehensive reporting is necessary to close the loop on your third-party risks.

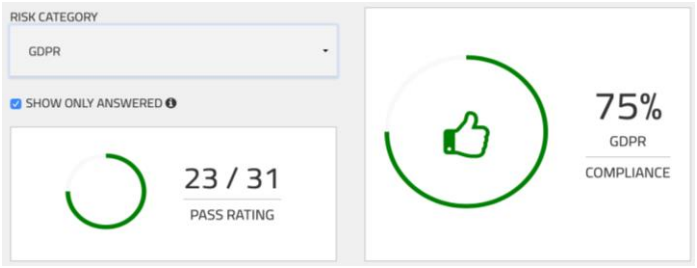
### The importance of regulatory-specific reporting

Since third-party risk management is a key control focus in most regulatory regimes and industry frameworks, it's important to show progress toward achieving compliance with those requirements – for auditors outside and inside your organization. However, compliance reporting can be complex and time-consuming with many risk management tools. Built-in reporting for common regulations and industry frameworks is therefore key to speeding and simplifying the compliance process.

Prevalent has a detailed white paper that extracts the specific third-party risk management requirements set forth in in multiple regulations and industry frameworks; explains what those requirements mean; and then maps key solution capabilities into the requirements to demonstrate how a complete TPRM platform can help ease the burden of compliance. Save your sanity and download that paper!

One of the ways to speed compliance reporting is to gain visibility into each vendor's level of compliance. Start by establishing a compliance "pass" percentage threshold against a risk category (e.g., X% compliant against a particular framework or guideline). All reporting will tie back to that percent-compliant rating and your team can focus on subareas where compliance pass rates are low. This should also be conducted at the macro level across all vendors; not just at the vendor-level. Macro-level reporting will be important for the board as they seek to determine how compliant the organization is against the "flavor of the month" regulation.

"Percent-compliant" should be part of every auditor report, which should also indicate specific areas requiring additional remediation. See GDPR example at right.




## But it's about more than just compliance

Although compliance is a critical driver behind third-party risk management, you still have specific cybersecurity requirements to report on. A complete TPRM solution should feature rich reporting for areas including:

- Average risk by score and status
- Risks by likelihood
- Highest risks by vendor
- Risks by impact
- Common identified risks
- Risks per business impact area
- Trending of risk over time by score/impact/likelihood
- Projection of risk score/impact/likelihood over time

Visualizing compliance and risk status across the vendor landscape with built-in executive views provide specific and overall visibility into the third-party risk profile for more confident reporting to the board.

## Top 5 reporting capabilities:

1. A unified reporting framework that enables you to take the answers from any question and map them to any regulatory or industry standard framework, guideline or methodology
2. Regulatory compliance, framework and guideline-specific reports such as for ISO 27001, NIST, GDPR, CoBiT 5, SSAE 18, SIG, SIG Lite, and NYDFS
3. Ability to show percent-compliant to demonstrate progress on risk mitigation efforts
4. Deep reporting by vendor and across all vendors
5. Projection of risk scoring over time after remediations are conducted and risks are mitigated

The Prevalent Assessment Service delivers inside-out assessments of vendor compliance with IT data security, regulatory and privacy requirements. With a library of over 50 standardized assessments, content customization capabilities, and built-in workflow, the solution automates everything from survey collection and analysis to risk identification and reporting. Deep reporting capabilities include filters and click-through interactive charts. The solution includes a complete repository of all documentation collected and reviewed during the diligence process.

## Case Study: Allianz UK Achieves 50% Time Savings

Allianz Insurance plc is one of the largest general insurers in the UK and part of the Allianz SE Group, the largest property and casualty insurer worldwide. The company was challenged to meet its Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) compliance and risk management objectives. This was largely due to a lack of consistency in reporting, plus a time-consuming vendor assessment process that leveraged spreadsheets and onsite visits. Once deployed, the Prevalent Third-Party Risk Management (TPRM) Platform simplified the whole process, enabling Allianz to perform assessments and onboard vendors twice as fast as before. Allianz has since extended their use of the Prevalent Platform to managing the organization's request for information (RFI) and request for proposal (RFP) processes.

# The Prevalent Difference

Why select a single vendor to address all aspects of third-party risk management? Why Prevalent?

Prevalent delivers the industry's only purpose-built, unified platform for third-party risk management. Delivered in the simplicity of the cloud, the Prevalent platform combines automated vendor assessments, continuous threat monitoring, assessment workflow, and remediation management across the entire vendor life cycle, with expert advisory and consulting services to optimize your risk management program. With Prevalent, organizations gain a 360-degree view of vendors to simplify compliance, reduce risks, and improve efficiency for a scalable third-party risk management program.

Our differentiation in the third-party risk management market lies in the integrated platform, the depth of our solution offering, network and outsourced options, and the value you gain with our industry experience.

## The Prevalent Platform Delivers 360-Degree Third-Party Risk Management

Prevalent delivers what industry experts, customers and analysts such as Gartner and Forrester consider to be the complete spectrum of third-party risk management capabilities. From automating the cumbersome process of collecting, analyzing, and remediating vendor due diligence, to continuously monitoring vendor cyber and business risks, Prevalent unifies these best-of-breed capabilities into a single, integrated platform. This comprehensive model delivers maximum visibility, simplifies management, and lowers total cost of ownership.

## Depth of Features for Maximum Risk Visibility

Prevalent goes beyond traditional vendor risk management solutions by leveraging integrated, continuous cyber and business risk monitoring to provide a more complete picture of vendor risk. This includes intelligence on financial disclosures, layoffs and other events that can raise red flags. This zero-gap coverage delivers deep, holistic insights into potential vendor risks for faster, more proactive risk reduction.

## Fully Integrated Sharing Networks Accelerate Time-to-Value

Prevalent is the only vendor to combine assessment and threat monitoring capabilities with a fully integrated vendor risk network, providing options for organizations to leverage shared assessment content and evidence to accelerate risk reduction efforts. Reducing the effort required to collect or complete surveys means that you and your vendors can spend less time gathering information and more time on what's important: working together to eliminate security control gaps and reduce overall risk.

## Unmatched Industry Expertise & a Defined Process for TPRM Program Maturity

Prevalent employs experts in the third-party risk management space who help to define widely adopted industry standards for data collection and risk mitigation. The company also offers an end-to-end outsourced service for managing risk audits with continuous tracking and monitoring. Prevalent has the global resources, plus a well thought-out approach to programmatically maturing your third-party risk management program.


Prevalent unifies inside-out, automated risk assessment with outside-in, continuous monitoring to provide you with more comprehensive, better informed vendor risk visibility.

## Conclusion: Delivering Business Value

This best practices guide explained what an enterprise TPRM deployment looks like and described key features to look for in the solution evaluation process. Prevalent is the epitome of a complete third-party risk management solution, offering a holistic, automated TPRM program unified by a single, easy-to-use platform. With Prevalent, you gain:

- **Greater visibility** with a centralized platform that eliminates coverage gaps; enables better risk-based decisions to inform compliance, prioritize resources, and remediate risks; and delivers a single repository for effective reporting to satisfy audit requirements.
- A **faster time to value** through reduced complexity and greater automation; accelerating vendor onboarding and re-certification; and minimizing time spent managing operational processes.
- A **scalable program** that simplifies and unifies the end-to-end process of third-party risk management for greater consistency, predictability and agility.

Contact Prevalent today for a strategy session on maturing your TPRM program and solving your third-party risk challenges.

# Appendix: Solution Provider Comparison Checklist

Use this table to evaluate your third-party risk management program and compare solution providers.

| Step | Attribute | Options | Achieved |
|---|---|---|---|
| Define/Build/ Optimize – Basic Program Decisions | Thorough, multi-variate process for determining vendor criticality that can adapt to business changes | | |
| | Multiple questionnaire options – industry-standard, pre-built, customizable – with the ability to weight the answers and evidence submitted per question according to business importance | Industry-standard | |
| | | Customizable | |
| | Multiple collection and analysis options, including doing it yourself, leveraging a network of completed questions and submitted vendor evidence, and the ability to outsource it to a trusted partner | Platform | |
| | | Network | |
| | | Outsourced | |
| | A disciplined, rigorous consulting and advisory process geared to progressively maturing your program | | |
| | Relationships with systems integrators and other partners that can accelerate the time to realize value | | |
| Monitor for Vendor Cyber and Business Risks | A view into business risks that can augment cyber security scanning, providing a more holistic view into a vendor's potential risks | | |
| | Industry-standard scanning and third-party sources, providing a comprehensive, trusted and transparent scoring methodology | | |
| | A flexible scoring framework that can incorporates business context and quantifies risks to enable objective and comparative decision making. | | |
| | Prescriptive guidance and remediation recommendations on vendor risks | | |
| | Clear reporting on risk status, helping internal teams to focus and prioritize what's most important | | |
| | Native integration with detailed vendor assessments, providing a single view of all vendor risks in one place | | |

| Step | Attribute | Options | Achieved |
|---|---|---|---|
| Collect Evidence and Perform Due Diligence | Survey section/creation – draw from a library of prepared questionnaires or build your own | | |
| | Survey scheduling assistant – define assessment schedules and chasing reminders with a dashboard for a real-time view into survey completion status | | |
| | Flexible collection and analysis options, including doing it yourself, leveraging a network of completed questions and submitted vendor evidence, and the ability to outsource it to a trusted partner | Platform | |
| | | Network | |
| | | Outsourced | |
| | A flexible scoring framework that quantifies risk and incorporates the necessary business and regulatory context to promote vendor communications and emphasize the importance of remediation | | |
| | Bi-directional document and evidence management with tasks, acceptance, and mandatory upload features to obtain proof of controls | | |
| | User dashboard – a centralized overview of tasks, schedules, risk activities, survey completion status, agreements and documents | | |
| Analyze and Score Results | Automatic generation of a risk register for centralized risk analysis and faster risk mitigation | | |
| | Flexible risk weightings that granularly define the importance of specific risks to the business | | |
| | Flagging and categorizing – either automatic or manual – to escalate a risk and route it to the appropriate contact for remediation | | |
| | A matrix that dynamically enables risk analysis based on likelihood of an incident and its potential impact on the business | | |
| | Integration with a cyber and business monitoring system to provide a single risk score per vendor that includes the results of an internal, controls-based assessment and an external network scan | | |

| Step | Attribute | Options | Achieved |
|---|---|---|---|
| Remediate Findings | A risk register for centralized analysis of risks | | |
| | Built-in workflows that make it easy to bi-directionally manage and mitigate risks | | |
| | A full audit trail that captures and audits conversations; records completion dates; and assigns tasks based on risks, documents or entities | | |
| | Document/evidence management. | | |
| | Remediation guidance and recommendations to reduce risk | | |
| Report to Internal and External Stakeholders | A unified reporting framework that enables you to take the answers from any question and map them to any regulatory or industry standard framework, guideline or methodology | | |
| | Regulatory compliance, framework and guideline-specific reports such as for ISO 27001, NIST, GDPR, CoBiT 5, SSAE 18, SIG, SIG Lite, and NYDFS | | |
| | Ability to show percent-compliant to demonstrate progress on risk mitigation efforts | | |
| | Deep reporting by vendor and across all vendors | | |
| | Projection of risk scoring over time after remediations are conducted and risks are mitigated | | |

## About Prevalent

Prevalent helps enterprises manage risk in third-party business relationships. It is the industry's only purpose-built, unified platform that integrates a powerful combination of automated assessments, continuous monitoring, and evidence sharing for collaboration between enterprises and vendors. No other product on the market combines all three components, providing the best solution for a highly functioning, effective third-party risk program.

To learn more, please visit www.prevalent.net.