MITRATECH
Prevalent

Best Practices Guide

Navigating the Vendor Risk Lifecycle

Keys to Success at Every Stage

Table of Contents

Every Stage of a Third-Party Relationship Introduces Risk

If you're reading this, then your organization probably entrusts sensitive information to vendors and suppliers. While third parties are crucial to doing business, they also bring the risk of data breaches and operational disruptions—any of which can lead to customer problems, lost revenue, lawsuits, reputational issues, and regulatory penalties. Ensuring that suppliers have proper security, compliance, and operational controls can be a moving target, but it's a critical one to hit.

THERE'S MORE TO TPRM THAN YOU THINK

It's a common mistake to see third-party risk management (TPRM) as a one-time vendor risk assessment followed by risk remediation. Experience shows that there is much more to TPRM. Organizations need to address distinct risks at every stage of the vendor lifecycle, including:

- Sourcing and onboarding vendors that meet acceptable risk thresholds
- Measuring performance and watching for changes that affect risk
- Securely offboarding third parties when business relationships end

However, manually overseeing continuous assessments is costly, inefficient, and not scalable across third-party ecosystems. So, how can you automate your processes to quickly and efficiently ensure that third parties don't present unacceptable risks to your organization?

MATURING YOUR TPRM PROGRAM

This guide illustrates the challenges, capabilities, and business outcomes to expect at every stage of the vendor risk lifecycle. We'll start by mapping third-party risk management program attributes to a best-practice maturity model and then walk through seven critical stages of program optimization.

To uncover the benefits of a mature TPRM program, Mitratech surveyed hundreds of customers to understand how they leverage the **Mitratech Third-Party Risk Management Platform** to address and manage vendor risk. The results, several of which are shared below, provide helpful guidance for increasing visibility and reducing risk throughout the third-party lifecycle.

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

CASE STUDY

What real customers are doing to solve this problem

TIPS & BEST PRACTICES

What we've learned along the way

TECHNICAL ATTRIBUTES

Key capabilities

IT'S A TRAP!

Pitfalls to avoid

The Goal: A Smarter, More Unified, and Prescriptive Approach to Third-Party Risk Management

Third-party risk management programs are typically driven by mandates for regulatory compliance, data security and privacy, supply chain resilience, or a combination of all three. With that in mind, Mitratech defined five levels of TPRM program maturity based on the Capability Maturity Model developed by **Watts Humphries** and others at the Carnegie Mellon University Software Engineering Institute in the late 1980s. The Model examines five key pillars:

1. **Entity Coverage:** Most organizations begin their TPRM programs by assessing their most critical vendors. This is a logical approach, but risk can come from any entity. More mature organizations will have a consistent method for tiering or risk-ranking vendors to ensure that all are included in the program, including 4th-and Nth-party vendors.
2. **Content:** Risk assessment questionnaires often begin as ad hoc initiatives. Questions are submitted to vendors and free-form answers are received and evaluated. More mature programs will regularly review assessment questions to understand what each question is trying to find in terms of risk to the organization and then weight it appropriately. More mature programs will also be diligent in ensuring that vendors supply requested evidence of compliance.
3. **Roles and Responsibilities:** Less mature programs may follow guidelines but lack documentation of procedures and clear roles and responsibilities. Mature programs will train assessment participants and publish and follow an operational manual to ensure that processes are standardized. More mature programs will have documented RACI charts establishing responsible, accountable, consulted, and informed individuals throughout the organization.
4. **Remediation:** Remediation metrics are focused on the efficiencies, standardization, and quality of the risk management approach following the identification of risks. Less mature programs will identify risks and request remediation from vendors. More mature programs implement scoring mechanisms to weight risks and remediations and prescribe standardized remediation guidelines to vendors.
5. **Governance:** Governance includes how the program is measured and success is proven. Less mature programs lack sufficient assessment reporting and third-party program audits. More mature programs aggregate third-party assessment data to provide teams with the intelligence necessary to measure risk and steer decision-making. They also measure third-party vendors and suppliers against key performance indicators (KPIs) and key risk indicators (KRIs).

Levels of TPRM Program Maturity

LEVEL 1: IMMATURE

Organizations in the first level of the Maturity Model do not prioritize TPRM. Risk management is siloed. Activity is ad hoc and reactive, occurring only when a problem arises or when red flags are obvious, because processes are undocumented and poorly defined, a successful assessment for a single vendor is unlikely to be repeatable.

TPRM in Level 1 is a manual process for a limited number of vendors. Vendor questionnaires are inconsistent and distributed as discrete spreadsheets. Responses may be in narrative form and difficult to assess for risk. Standards for risk mitigation controls do not exist. Teams do not monitor vendors for ongoing compliance or new risks.

LEVEL 2: DEVELOPING

In Level 2, some (but not all) teams have defined and documented processes that allow for repeatable results. For example, security teams may have standardized questionnaires and penetration testing requirements, or finance may have standardized financial disclosure parameters. Other teams, however, remain ad hoc. This siloed approach leads to inconsistent assessments and prevents programs from scaling.

Without a standardized approach, vendors cannot be tiered according to their risk levels. This leads to higher risk if critical vendors are lightly assessed and inefficiencies if low-risk vendors are over-scrutinized. Level 2 organizations continue to use spreadsheets and shared documents, making reliable, auditable, and thorough TPRM unattainable.

LEVEL 3: SCALABLE

At Level 3, TPRM has been properly resourced and processes are consistent within individual functions in an organization. Most silos have been dismantled and teams have standardized, documented, and

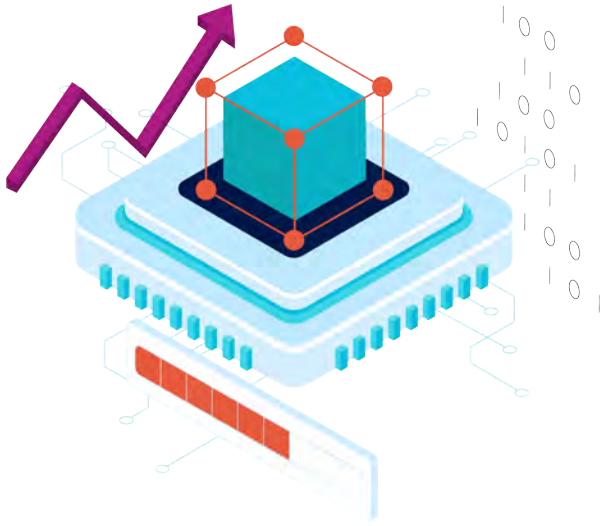
integrated activities for identifying and evaluating risk. Risk monitoring has expanded beyond business and IT risk to include corporate governance, compliance, and reputational risk. Risk tiering is standardized, and organizations begin to institute contract lifecycle management and formal offboarding procedures.

Processes in Level 3 are semi-automated. For example, onboarding may leverage automated questionnaires, while monitoring for remediation and ongoing compliance with requirements remains manual. This enables teams to moderately scale TPRM, but it can still leave gaps in visibility.

LEVEL 4: OPTIMIZED

Level 4 organizations view TPRM as a strategic requirement and have standardized policies and procedures across all departments. TPRM teams conduct automated, standardized vendor risk assessment with vendor risk monitoring, have structured assessment workflows, and manage the remediation process across the entire vendor life cycle. Risk mitigation controls are formalized and vendor monitoring is fully implemented. Automation also enables the program to be fully auditable.

Level 4 organizations can scale TPRM to all vendors across the entire vendor lifecycle. Reporting on KPIs and KRIs is automated and continuous improvement initiatives are data-driven. Communications with third parties focus on mutual benefits of a TPRM program.



LEVEL 5: VISIONARY

Level 5 is an aspirational level of maturity achievable by few organizations. It represents a fully automated TPRM program that anticipates risks, assigns effective controls, and monitors vendors for cyber, operational, financial, environmental, compliance, reputational, ESG, and performance risks. A visionary organization works with vendors proactively to improve the vendor's business while lowering risk.

At level 5, residual risk remains but can be addressed quickly through formal, tested procedures, and then accepted by the business as necessary.

TIPS & BEST PRACTICES

Review the table below to assess the status of your current TPRM program and determine where you would like to see it evolve.

	Entity Coverage	Content	Roles & Responsibilities	Remediation	Governance
Level 5: Visionary	All third, fourth, and Nth tier partners & vendors	Fully automated & weighted templates	Interdisciplinary & interchangeable teams	Standardized remediation and validation with ongoing monitoring	Third-party attestation and quarterly publication
Level 4: Optimized	Fourth and Nth tier vendors	Category templates	Trained teams, RACI, and operational manuals	Scoring and weighted risks	Annual, independent auditing
Level 3: Scalable	Risk ranking of vendors	Weighted risk criteria	Documented cross-functional teams	Validation of remediation	Program weaknesses tracked over time
Level 2: Developing	Most vendors	Standardized questionnaire	Organized silos	Standardized guidelines	Defined KPI and internal reporting to senior management
Level 1: Immature	Most critical vendors	Ad hoc assessment criteria	Individual effort	Vendor driven	None

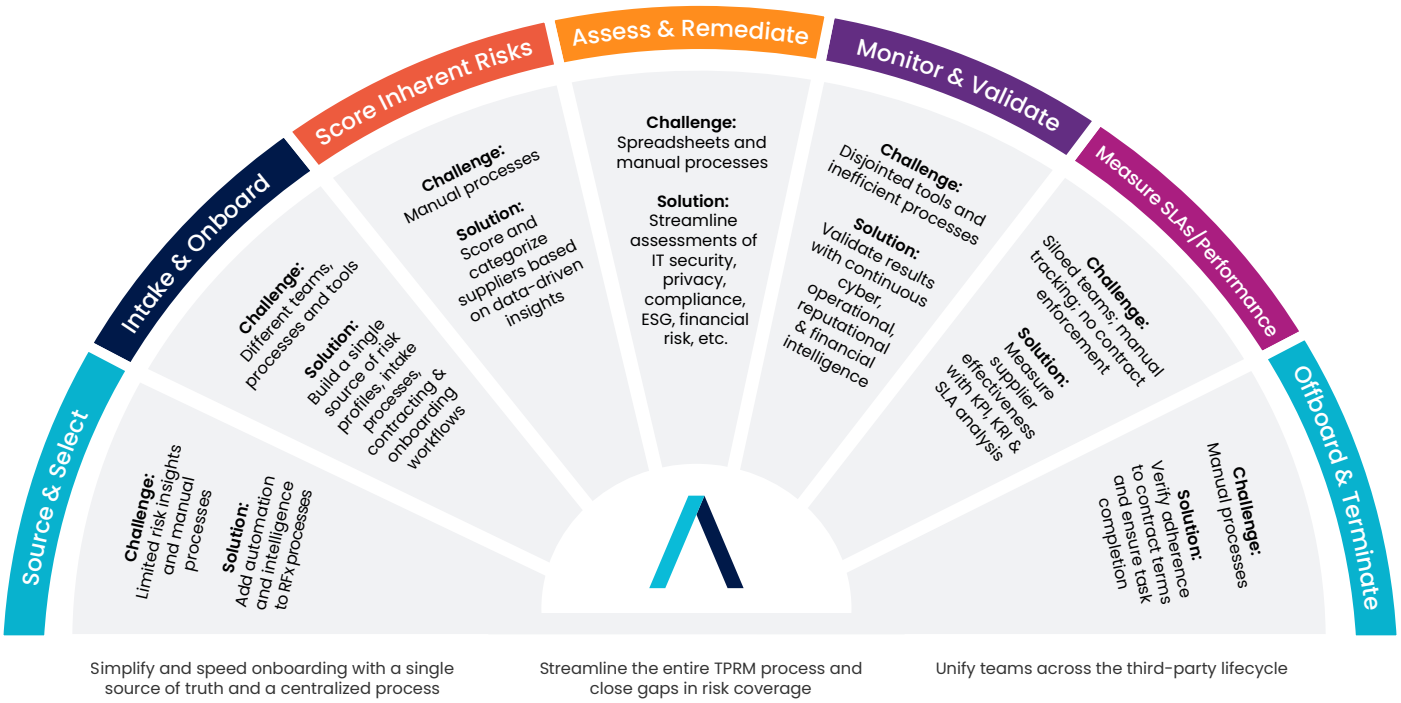
Navigating the path to TPRM maturity is not easy. However, by investing in the right people, processes, and technology, you can achieve greater levels of automation and productivity. The next section of this guide presents a seven-stage approach to achieving a more mature, proactive, and effective third-party risk management program.

What to look for:

Seven Stages to a More Mature and Proactive Third-Party Risk Management Program

A programmatic process is the fastest path to stopping the pain of third-party risk management, making informed risk-based decisions, and adapting and growing your program over time. This section of the guide outlines a seven-stage deployment plan for TPRM and identifies key capabilities to look for in a solution provider.

See the figure below for a representation of the process. The result is a simpler, faster process to onboard and manage vendors; a streamlined process to assess and monitor vendors; and the unification of all teams under a single solution.



Simplify and speed onboarding with a single source of truth and a centralized process

Streamline the entire TPRM process and close gaps in risk coverage

Unify teams across the third-party lifecycle

Consider these TPRM criteria as you advocate for evolving your program within your organization:

- **Smart:** An approach that is data-driven, comprehensive, and contextual. Vendor intelligence should be gathered and correlated from a wide range of public and private sources—and presented in a quantifiable and contextual way for more informed decision-making.
- **Unified:** Risk monitoring and assessment must go hand in hand. Break down silos between internal departments (e.g., IT, procurement, security, risk management) and enable better collaboration with vendors to prioritize and reduce risk.
- **Prescriptive:** Provide remediation recommendations and playbooks that automate the remediation process. Back it up with customer success and services teams that can help navigate every step.

Stage 1: Sourcing and Selection

When considering vendor risk management, it is natural to think first about vendor selection. In many cases, multiple teams are involved in the vendor selection process—each with different priorities. For instance, engineering may focus on a prospective vendor's ability to meet specifications; procurement on their business viability; security on controls to protect sensitive systems and data; and compliance on reporting and audits.

However, understanding the quality, reliability, and security of a new vendor can be challenging when internal teams lack a single source of vendor profiles and risk ratings. This can slow purchasing cycles and delay important organizational projects and initiatives. To adapt, organizations publish requirements and accept competitive bids, then evaluate each vendor for its ability to meet a baseline set of security, privacy, operational, reputational, and financial requirements.

Manual spreadsheets listing requirements and each vendor's responses are a typical approach used to evaluate potential vendors. However, a manual approach presents challenges:

- **Inconsistent answers** are common, making comparisons between vendors difficult. Vendors may obscure unmet requirements or simply skip related questions hoping they will be ignored.
- **Limited risk insights** into a potential vendor's cyber posture, financial health, or operational history may obscure potential problems.
- **Extensive effort** is required even before contracts are executed, wasting time for vendors and TPRM teams.

Centralizing supplier demographic information, fourth-party technologies, ESG scores, and data breach history—along with operational, reputational, and financial performance insights—enables teams to make risk-based decisions from the earliest stages of the third-party lifecycle. Replacing scattered, siloed supplier information sources with a single supplier profile backed by industry-standard risk scoring will not only aid in supplier selection but also provide a foundation for more advanced and efficient due diligence.

HOW MITRATECH HELPS

Mitratech RFx Essentials centralizes and automates the distribution, comparison, and management of requests for proposals (RFPs) and requests for information (RFIs), while centralizing disparate vendor information sources. RFx Essentials makes it easy for your procurement team to not only select vendors that meet your organization's functionality and risk requirements, but also take a critical first step in managing risk throughout the third-party lifecycle.

CASE STUDY: A U.S. BROKER-DEALER SAVES 50% OF TIME ON VENDOR SOURCING AND SELECTION

A **U.S.-based broker-dealer** was spending too much time scouring disconnected sources of information to make sound, risk-based vendor selection decisions. With the **Mitratech Third-Party Risk Management Platform**, they streamlined the whole process and reduced the time normally required to source third parties by 50%.

Stage 2: Intake and Onboarding

Negotiating, reviewing, and managing vendor contracts can be a time-consuming version control nightmare —– especially when using manual processes or when internal stakeholders do not follow established protocols. Without an automated approach to vendor contract management, procurement teams might not know when a new service is being contracted, and legal teams might not have the visibility into contracts to ensure the company is protected. This results in unnecessary costs and risks to the business.

Complicating matters, vendor information is often siloed between departments. Engineering may have specifications based on their requirements and vendor technical capabilities; operations teams may have production forecasts; procurement manages contracts and pricing; and compliance may have requirements on how the vendor meets its PCI or General Data Protection Regulation (GDPR) regulatory obligations. When information is splintered, it is difficult to gain a holistic picture of vendor risk.

OPTIONS FOR VENDOR ONBOARDING

The process for onboarding vendors typically involves a manual or bulk upload. Connecting a pre-configured spreadsheet or API to an existing vendor management or procurement solution is a more efficient way to create a central repository of vendors. Leverage role-based access to enable different teams to populate data from vendors and invite other employees to contribute.

HOW MITRATECH HELPS

Mitratech Contract Essentials is a SaaS solution that centralizes the distribution, discussion, retention, and review of vendor contracts. It also includes workflow capabilities to automate the contract lifecycle from onboarding to offboarding. With Contract Essentials, procurement and legal teams have a single solution to manage vendor contracts, simplify contract reviews, and reduce cost and risk.

Mitratech provides procurement, security, and risk management teams with a single source of supplier risk profiles, **intake processes, and onboarding workflows**. Onboarding vendors doesn't have to be a manual data entry process. Mitratech integrates with existing solutions to upload vendor lists and others to build a comprehensive supplier profile. Plus, the Mitratech Platform enables a simple spreadsheet upload of vendor information and extends a straightforward intake form to anyone in the organization to jump-start the onboarding process. This reduces the time and cost required to assess suppliers, enabling faster onboarding and due diligence.

CASE STUDY: U.S.-BASED HEAVY EQUIPMENT MANUFACTURER

A **U.S.-based manufacturer of heavy equipment** for the construction and transportation industries. Prior to using Mitratech, the company was spending too much time manually onboarding new vendors. Once deployed, the **Mitratech Third-Party Risk Management Platform** made assessing vendors infinitely easier than any manual method.

Stage 3: Scoring Inherent Risks

Not every vendor requires the same scrutiny. For example, an office supply vendor presents lower organizational risk than one providing critical parts or legal services. An organization located in a politically volatile location, with a history of breaches, or with poor credit history presents more risk and warrants increased due diligence.

To properly understand the risk posed by a vendor, you must be able to calculate **inherent risk**. This is the vendor's risk level before accounting for any specific controls required by your organization. A comprehensive view of inherent risks provides a baseline and helps you decide what type of further due diligence is required. Once inherent risk is baselined, it is much more straightforward to calculate **residual risk**, which is the risk level that remains after controls are applied.

Inherent risk can also inform vendor profiling, tiering, and categorization decisions. This accelerates risk assessments by ensuring vendors are assessed against the risks and standards that matter most to a business, its customers, and regulators or standards bodies.

EXAMPLE TIERING ATTRIBUTES

- Type of content required to validate controls
- Criticality to business performance
- Location(s) and related legal or regulatory considerations
- Level of reliance on fourth parties

SUPPLIER CRITICALITY FACTORS

It's important to understand the potential ramifications of a supplier's failure to deliver products or services to your organization.

Accordingly, you should leverage a scoring system to determine each supplier's tier. This could include the following criteria:

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

Once you define supplier tiers, it should be easy to understand which suppliers are most critical. For example, you should be able to run a report on all suppliers that are U.S.-based, handle personal data, and are top-tier.

Having vetted information earlier in the process and in an easily accessible location enables you to "right-size" due diligence initiatives, focus on vendors with the highest risk, and speed up the overall process.

When starting your third-party profiling and tiering exercise, there are some considerations to make that will help ensure success:

- **Start small and scale up:** Initial assessments will be a learning experience. Start with issuing a small number of surveys until your team is ramped up.
- **Set realistic timeframes:** Remember that each survey needs to be completed by a person, so set achievable response deadlines.
- **Consider capacity:** When scheduling profiling and tiering activities, consider how many surveys each responder can manage within a given time frame.
- **Support responders:** Prepare a frequently asked questions (FAQ) document with guidance for responders.
- **Plan communication:** Create a plan that covers objectives, emphasizes the value of assessments, and details an escalation procedures and contacts.

HOW MITRATECH HELPS

Mitratech provides comprehensive vendor profiles that include **inherent risk** scores based on the likelihood and potential impact of security, compliance, and operational incidents. By tiering (aka "risk ranking") each vendor, TPRM teams gain insight on where to focus due diligence.

Mitratech further accelerates this process by providing a library of workflow rules to trigger automated playbooks. It also offers prescriptive recommendations in line with the level and scope of due diligence for each tier.

MITRATECH CUSTOMERS AGREE

Right-sizing due diligence enables organizations to focus on the factors that matter most to their supply chain security and operational integrity.

95%

of surveyed IT organizations would agree that Mitratech provides the inherent risk visibility they need to focus on specific areas of their vendors' risk.

—TechValidate Survey of 36 users of Mitratech

Stage 4: Assessing Vendors and Remediating Risks

The level of risk posed by different third parties will vary according to their criticality to your business and other inherent risk factors. Likewise, the criteria for each tier of third parties will also vary. For instance, the criteria for a parts supplier will be different from that used for evaluating cloud hosting services.

Organizations with immature TPRM programs may address different vendor tiers by creating individual, spreadsheet-based surveys for each new project; constantly "reinventing the wheel." Responses to these surveys can vary in level of detail and completeness, making it difficult to evaluate overall risk and required controls. Tracking open items that require remediation and ensuring that remediation controls are consistent and adequate can be difficult, putting unnecessary demands on scarce security, risk, and compliance resources.

Automated assessment response collection and due diligence review can take many forms, including managing the process yourself; utilizing a repository of completed questionnaires; outsourcing to a partner; or some combination thereof. In all cases, you'll first need to determine which questionnaire to use.

Key decisions to make at this step include:

- Which questionnaire will be used to gather information about your vendor's controls? Will you use industry-standard or proprietary surveys?
- Which 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?

WHICH QUESTIONNAIRE TO USE? INDUSTRY-STANDARD OR PROPRIETARY?

There are cases to be made for both industry-standard and proprietary questionnaires. Utilizing industry-standard questionnaires (e.g., the Standard Information Gathering (SIG) questionnaire, the Health-Information Sharing and Analysis Center (H-ISAC) questionnaire for healthcare organizations, etc.) 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 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 tangible efficiencies.

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 tailored to specific business needs.

Whether you use a standardized or proprietary approach, make sure potential TPRM providers have the flexibility to deliver both types of questionnaires so that, so you aren't locked into a single, rigid questionnaire.

Choosing the Right Collection and Due Diligence Review Method—Do-It-Yourself, Shared Library, or Outsourced?

DO-IT-YOURSELF

Once you define your questionnaire, you can internally manage vendor data collection and analysis. However, make sure you have a solution to manage workflow and, 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 the 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 LIBRARY

Third-party risk management processes can be taxing for 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 prophecies—the more vendors that participate, the greater the overlap with other enterprises. This speeds up the risk identification and mitigation processes and minimizes the time required to collect data.

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 in-house 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 collection method flexibility will enable your team to stay agile. Also, consider flexibility of services in evaluating outsourced TPRM providers. Oftentimes, the collection and analysis of content and evidence is just the starting point—many companies lean on their managed services provider to perform everything from vendor onboarding and administration to performance management and reporting.

REMEDIATION

Remember the vendor tiering we discussed in Stage 2? 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 in a centralized risk register for each vendor.

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 Regulatory-Specific Reporting

Third-party risk management is a key control focus in most regulatory regimes and industry frameworks. So, it's important for auditors both outside and inside your organization to show progress toward achieving compliance. However, many risk management tools make compliance reporting overly complex and time-consuming. Built-in reporting for common regulations and industry frameworks is therefore key to speeding up and simplifying the compliance process.

Mitratech offers detailed white papers that extract the specific third-party risk management requirements set forth in **cybersecurity frameworks** and **data privacy**, **ESG**, and **industry regulations**. Each paper explains what the requirements mean and maps key solution capabilities to demonstrate how a complete TPRM platform can ease the burden of compliance. Save your sanity and download these papers!

Be sure to consider the value that artificial intelligence (AI) introduces to risk analysis and reporting. Although **artificial intelligence** isn't a new concept, the recent mainstream introduction of generative AI technologies is enabling organizations to solve business problems at an unprecedented scale. Conversational AIs trained on billions of events and years of experience can deliver expert risk management insights in the context of industry guidelines such as the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), SOC 2, and others.

One way to speed up compliance reporting is to gain visibility into each vendor's level of compliance. Start by working with your auditor to establish 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 areas where compliance pass rates are low. This should be conducted at the macro level across all vendors,; not just for individual vendors. Macro-level reporting will be important for the board as they seek to evaluate the organization's compliance level with key regulations.

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

See GDPR example at right.

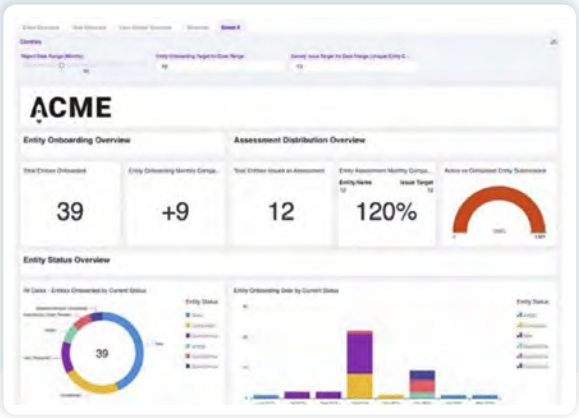
But It's About More Than Just Compliance

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

By visualizing compliance and risk status across the vendor landscape, you can better understand your organization's third-party risk profile for more confident reporting to the board.

Analytics identifies exceptions in common behavior (e.g., outliers across assessments, tasks, risks, etc.) that could warrant further investigation. Be sure to investigate if your selected TPRM solution features machine learning analytics to correlate complex datasets and see potentially hidden trends.



HOW MITRATECH HELPS

Mitratech **automates vendor risk assessments** through a centralized platform, from survey collection and analysis to risk rating, remediation, and reporting. Rather than creating a custom survey for each new project or using an inappropriate survey, Mitratech provides a library of over 600 standardized assessments, survey customization capabilities, and built-in workflow and remediation guidance. Mitratech tracks vendor controls, including IT security, compliance, performance, contract adherence, business continuity, financial position, reputation, ethics, anti-bribery and corruption, and environmental, social, and governance (ESG) criteria.

CASE STUDY: ITV

ITV is a free-to-air television network in the United Kingdom. Prior to using Mitratech, ITV was challenged with a manual, spreadsheet-based risk assessment process that was complex and time-consuming. Once deployed, the **Mitratech Third-Party Risk Management** (TPRM) Platform narrowed ITV's risk assessment process from weeks to no more than a couple of hours of effort per third party.

Stage 5: Continuous Monitoring for Security, Operational, Reputational, and Financial Risks

Although periodic assessments are essential to understanding how vendors govern their information security and data privacy programs, a typical risk assessment will only provide a snapshot of an organization's risk profile at a single point in time. This profile can change overnight as threats evolve, new breaches and bankruptcies are disclosed, or other adverse conditions arise. It's therefore important to constantly monitor each third party's cybersecurity posture and track any emerging financial, compliance, or supply chain challenges.

Unfortunately, this data is rarely available in a way that enables security and risk teams to be notified quickly, and it is often not integrated into a central register for decision-making. Instead, many organizations rely on manual processes, disparate tools, vendor notifications, and news reports.

Monitoring your vendors has several benefits, including:

- **Immediacy:** Gaining an instant view of the vulnerabilities that hackers exploit can inform your vendor tiering and prioritization logic
- **Validation:** Validating vendor responses to surveys upon receipt
- **Frequency:** Obtaining frequent, unbiased insights into your vendor's potential cyber vulnerabilities or business risks that can impact your organization

Take a step back to consider whether a "score" or "security rating" will solve what ails you. Typical scoring and rating 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 provides a limited view of vendor risk—meaning there is no real assessment happening.

It's helpful to ask a few questions when considering if scoring and rating tools are enough for your TPRM program:

- Can an external scan measure a vendor's internal adherence to compliance mandates?
- 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?
- Can an external scan deliver financial, reputational, or operational insights that can impact their ability to meet contractual expectations?

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, IDC, and others include vendor questionnaire assessments plus continuous monitoring for a complete view of vendor risks.

WHAT CYBER DATA TO MONITOR

Monitoring vendor networks is about more than just vulnerability management. It's important to combine results from vulnerability scans with multiple external sources of cyber threat intelligence—including from internet sensor networks, global threat databases, collaborating security partners, and anti-virus users—to gain intelligence on:

- **Breach events:** A large volume of breaches indicates vulnerabilities in a vendor's security program and could lead to regulatory pressures.
- **Dark Web chatter:** Recent, frequent mentions of a company on the Dark Web often correlate with more threat activity against the company, increasing the likelihood of attack. Attention on Dark Web markets may indicate illicit sale of company assets or accounts, or fraud schemes.
- **Domain abuse/typosquatting:** New domain registrations with typosquatting-style similarity to existing corporate domains are potential indications of domain abuse (such as phishing), defensive registration to prevent or mitigate domain abuse, or both.
- **Web application security:** SSL/TLS certificates and configurations.
- **Email security:** Sender policy framework (SPF) policy configurations; domain keys identified mail (DKIM); and domain-based message authentication, reporting, and conformance (DMARC).
- **Leaked credentials:** Exposed credentials and emails indicates potential password or corporate email address reuse by company employees, raising the risk of credential stuffing attacks and targeting by threat actors.
- **Incidents:** Security breach disclosures and validated cyber-attack reports signal when a company has likely experienced a recent cyber-attack, breach, or event that jeopardized the company's information assets.
- **Infrastructure exposures:** These include IT policy violations, abuse of company infrastructure, infections in company infrastructure, malware, misconfigurations, vulnerabilities, infected hosts, and unsupported software.

Remember that criminals also refer to the same sources of intelligence when identifying targets and planning attacks. By implementing a continuous monitoring solution, you can stay a step ahead of attackers and help your vendors address potential exposures. You can also monitor your own organization to strengthen internal processes, cover security gaps, and troubleshoot anomalies—similar to cleaning up your credit report prior to applying for a home loan.

OPERATIONAL, REPUTATIONAL, AND FINANCIAL RISKS ARE IMPORTANT, TOO!

Revealing cyber risks in a vendor's public-facing internet assets is only one part of the continuous monitoring equation. The other part is understanding qualitative business information that can signal future risks.

Risk indicators include the following:

- **Operational:** M&A activity, business, news, management and leadership changes, competitive news, new offerings, and operational updates
- **Regulatory/Legal/Reputational:** Adverse media and negative news; presence on regulatory, legal sanctions, or politically exposed persons (PEPs) lists; or doing business with a state-owned or government-linked enterprise might spur conflicts of interest
- **Financial:** Financial performance data, including turnover, profit and loss, shareholder funds, credit ratings, payment history, bankruptcies, and investments

Together, cyber, operational, reputational, and financial 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.

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 when a survey or scan is completed filters out unnecessary noise and helps your team zero-in on areas of possible concern.

Not all risks are created equal, so 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 focus on risks with greater potential impact on your business.

This is illustrated below:

You should be able to create risks based on answers to specific assessment questions. Typically, your reviewers or vendor managers will research the responses and submitted evidence to identify false positives or negatives as part of the submission process. As they review the possible deficiencies, they can raise flags requiring further attention.

The reviewer can also first validate the evidence and then document any applicable risk. Flagging points of concern in vendor responses ensures that the right risks are investigated, reducing your organization's overall risk profile.

A successfully implemented TPRM practice will categorize risks according to the 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.

Key: Low Medium High Critical None

THE IMPORTANCE OF AN INSIDE-OUT/ OUTSIDE-IN SCORE

As we warned above, scoring and security ratings from an external network scan will tell only half of the TPRM story. That's why it's important to combine monitoring results with those from questionnaire-based assessments. This combination yields a more accurate and complete representation of each vendor's compliance and risk status, plus more thorough remediation guidance.

HOW MITRATECH HELPS

Third-party security incidents, financial issues, and other damaging events often require quick action. **Mitratech Vendor Threat Monitor** continuously tracks hundreds of sources for new risks. The solution examines and analyzes the Internet and Dark Web for cyber threats and vulnerabilities, as well as public and private sources for adverse operational and reputational changes and financial information.

Mitratech's comprehensive threat intelligence is integrated into a unified risk register for each vendor, providing a single view of organizational risks for faster decision-making. With early notification and Mitratech response playbooks and remediation recommendations, organizations can respond quickly and effectively to risk events. Mitratech Vendor Threat Monitor includes:

- **Cyber Intelligence:** Leaked credential scanning across over 1,500 criminal forums, including thousands of onion pages, 80+ Dark Web special access forums, 65+ threat feeds, and 50+ paste sites
- **Business Updates:** Qualitative insights from over 550,000 public and private sources of reputational information, including M&A activity, business news, negative news, regulatory and legal information, and operational updates
- **Financial Insights:** A global network of 365 million businesses comprised of five years of organizational changes and financial performance, including turnover, profit and loss, and shareholder equity
- **Adverse Media Screening:** A database of profiles linked to illicit activities from over 30,000 global news sources
- **Global Sanctions List:** Sanctions lists from OFAC, EU, UN, BOE, FBI, and BIS plus over 1,000 global enforcement lists and court filings from the FDA, US HHS, UK FSA, SEC, and other regulatory bodies
- **State-Owned Enterprise Screening:** A proprietary list of government-owned and government-linked enterprises
- **Politically Exposed Persons (PEP) Screening:** 1.8 million politically exposed person profiles, including their families and associates
- **Breach Event Notification Monitoring:** A database with over 10 years of data breach history for thousands of companies globally, including types and quantities of stolen data, compliance and regulatory issues, and real-time vendor data breach notifications

CASE STUDY: GLOBAL INSURANCE COMPANY

One of the largest **insurance companies** in the world had an inconsistent, manual approach to assessing supply chain partners, which restricted visibility and increased security risks. By implementing the **Mitratech Third-Party Risk Management Platform** and leveraging **Mitratech Vendor Risk Assessment Services**, this under-resourced team exceeded its goals and achieved a measurable return on investment.

Intelligence from Every Corner

VENDOR RISK INTELLIGENCE

Continuous, comprehensive, relevant:

- Global research
- Assessments
- Partner feeds

VENDOR COMMUNITY

- Proactive assessments
- Vendor Initiated Events
- Certifications
- Docs & agreements

PRIVATE SOURCES

- Extended Profile
- Cyber Monitoring
- Credit reports
- Risk scores
- Financials
- Payments
- Legal Actions
- Certifications Cyber Monitoring
- 65+ threat feeds
- 50+ paste sites
- Blogs & social media
- Code repositories
- 1.5k+ hacker forums
- Dark web (80+ forums)

TECHNOLOGY INTEGRATIONS

- ServiceNow
- BitSight
- SourceDefense
- SecZetta

INDUSTRY PARTNERSHIPS

- H-ISAC
- LVN
- Shared Assessments
- Legal Theorem

REGULATORY MONITORING

Coverage across 30+ regulations and frameworks:

- CCPA
- NYDFS
- GDPR
- ISO
- NIST
- CMMC
- HIPAA
- PCI
- CAIQ
- And more

PUBLIC SOURCES

Financial, business & breach monitoring
across > 2 million companies

- Public Sources
- Data breach sites
- Corporate sites
- Regulatory portals
- Review websites
- Job boards
- PEP screening
- Data breach events
- Trade publications
- Industry sites
- News feeds
- Adverse media
- Sanctions monitoring
- State-owned enterprises

COMPLETED ASSESSMENTS

- 10,000+ verified records
- Sig-Lite/Sig-Core
- Prevalent Compliance Framework (PCF)
- Cybersecurity Maturity Model Compliance (CMMC)
- Cybersecurity, privacy, compliance, procurement
- ABAC, ESG, Modern Slavery

Mitratech risk scoring includes a comprehensive set of inputs.

Stage 6: Managing Ongoing Performance and SLAs

Managing risk is a continuous process. Even reliable partners can experience disruptions, and incentives to implement promised controls can wane once an agreement is signed. As with continuous monitoring for a changing risk environment, organizations also need ongoing visibility into vendor performance obligations. Some vendors may require scrutiny to ensure remediation commitments are met, and all should be measured against their service level agreements (SLAs). Doing so with discrete spreadsheets and poorly defined internal roles and responsibilities increases the likelihood of missed SLAs and associated business disruptions.

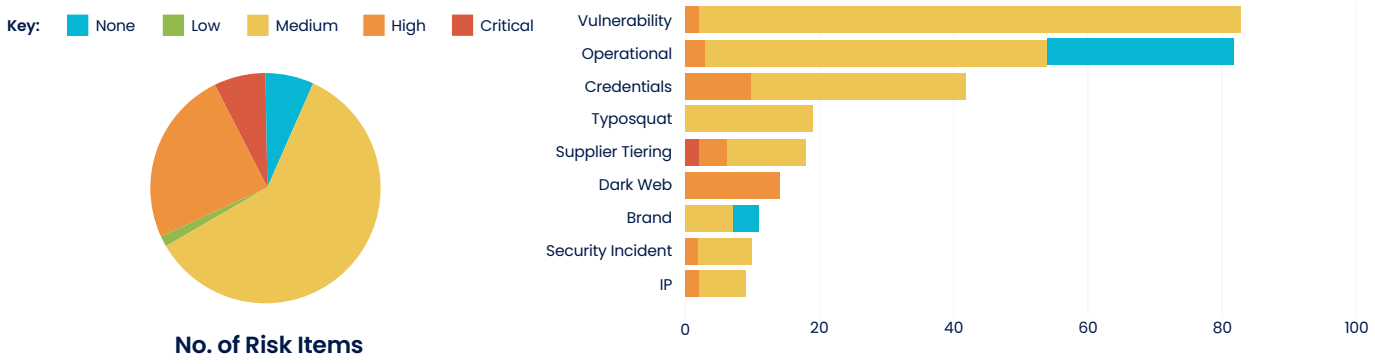
Tracking the right key performance indicators (KPIs) and key risk indicators (KRI) is a sign of a more mature TPRM program, but what do you measure? Mitratech has assembled a scorecard of the 25 most important KPIs and KRIs for third-party risk management. **Download the scorecard** and the accompanying e-book to get a head start on managing the right TPRM metrics for your organization!

HOW MITRATECH HELPS

Mitratech provides a centralized platform to **measure and report on program effectiveness** and vendor performance. Whether third parties need to meet SLAs, apply required remediations, or adhere to compliance mandates, Mitratech reduces risk by automating contract and performance assessments. Continuous vendor performance monitoring enables TPRM teams to identify potential disruptions before they adversely impact the organization.

Vendor analysis and reporting supports better-informed negotiations, contract updates, and more competitive renewals.

RISK ITEM SEVERITY OVERVIEW



Mitratech delivers a clear analysis to determine vendor performance against objectives.

CASE STUDY: NS&I

National Savings and Investments (NS&I) is one of the largest savings organizations in the UK with 25 million customers and more than £179 billion invested. NS&I was challenged with a manual assessment process that made it more difficult for a small team to assess suppliers and report on compliance. Once deployed, the **Mitratech Third-Party Risk Management Platform** smoothed their annual re-assessment and renewal processes.

Stage 7: Offboarding and Termination

When a vendor relationship ends, risk can persist. A vendor holding sensitive data must return and/or securely destroy that data; support obligations may outlive a purchase agreement; and organizations must ensure that any third-party access to internal systems is terminated. While this is easily understood, **Mitratech research** found that 39 percent of companies neither track nor remediate third-party risks during offboarding. This presents ongoing business, security, and IP risks.

More departments than ever are involved in assessing third parties. However, without prescriptive guidance and insights to evaluate potential vendors and wind down expiring supplier relationships, teams could miss key tasks that expose the organization to data breaches, disruptions, and compliance violations. Download the **Ultimate Third-Party Onboarding & Offboarding Checklist** to understand the essential insights and top 100 tasks required to securely onboard and offboard vendors and suppliers.

HOW MITRATECH HELPS

Mitratech provides a **programmatic process for securely offboarding third parties**. It provides centralized contract assessments, an offboarding workflow, document management, and real-time status reporting to ensure that data access is terminated and physical and virtual security controls are enforced.

CASE STUDY: IRISH FINANCIAL SERVICES COMPANY

One of the largest **life insurance companies in Ireland** was challenged with complex, manual processes that introduced risk into their workflows. Once deployed, the **Mitratech Third-Party Risk Management Platform** provided a programmatic process to offboard vendors that reduced risk.

A Holistic, Automated Approach to Third-Party Risk Management

It's clear that manual processes can't scale to handle thousands of vendor, supplier, partner, reseller, and service provider relationships. Modern organizations require a more holistic, structured, and consistent approach to third-party risk management—one that addresses the entire lifespan of each business relationship. With the Mitratech Third-Party Risk Management Platform, you can automate and accelerate every step of the third-party risk management lifecycle for unmatched visibility, efficiency, and scale.

GET STARTED FOR FREE

Starting or improving a TPRM program requires organizations to understand their current vendor risk posture. To get started, sign up for a free maturity assessment at: **www.mitratech.net/tprm-maturity-assessment/**.

Appendix

CRITICAL THIRD-PARTY RISK MANAGEMENT CAPABILITIES

As your organization navigates each stage of the vendor lifecycle, consider this set of capabilities as a starting point for comparing Mitratech against alternatives:

Lifecycle Stage	Attribute	Mitratech	Vendor B	Vendor C
Sourcing & Selection	Automated RFX evaluation and risk intelligence for sourcing and selection.	✓		
	Consolidated risk insights into data breaches, operational updates, financial results, and reputational concerns to measure risk prior to selection.	✓		
	Automate contract onboarding and lifecycle management to simplify and speed up review, redlining, and approvals.	✓		
Intake & Onboarding	Spreadsheet template or API connection to an existing procurement solution.	✓		
	Centralized and customizable intake form and associated workflow.	✓		
	Comprehensive profile that includes industry and business insights, including 4th-party relationships and beneficial ownership.	✓		
	Automatically suggest triage actions based on vendor attributes.	✓		
	Invite other employees to contribute to vendor onboarding initiatives.	✓		
	Service to onboard vendors on your behalf.	✓		
Inherent Risk Scoring	Simple assessment with clear scoring to track and quantify inherent risks for all suppliers.	✓		
	Tier suppliers according to their inherent risk scores, set appropriate levels of diligence, and determine the scope of ongoing assessments.	✓		
	Rule-based logic to categorize vendors based on a range of data interaction, financial, regulatory, and reputational considerations.	✓		

Lifecycle Stage	Attribute	Mitratech	Vendor B	Vendor C
(continued) Inherent Risk Scoring	Embedded machine learning insights to identify outliers warranting further investigation or score changes.	✓		
	Library of workflow rules to trigger automated playbooks.	✓		
Assessment	Conduct ad-hoc or scheduled assessments, monitor questionnaire completion progress, and set automated chasing reminders.	✓		
	600+ assessment templates, including industry-standard questionnaires and customizable questionnaires.	✓		
	Normalize, correlate, and analyze information across assessment results and continuous monitoring findings for unified reporting and remediation.	✓		
	Leverage a conversational AI trained on billions of events and more than 20 years of experience to deliver expert risk management and remediation insights in the context of industry guidelines such as NIST, ISO, SOC 2, and others.	✓		
	Communicate with suppliers and coordinate remediation efforts.	✓		
	Store and distribute documents for dialog and attestation—including nondisclosure agreements (NDAs), SLAs, statements of work (SOWs), and agreements and contracts—with version control, built-in tasks, and an auto-review cadence.	✓		
	Guidance from built-in remediation recommendations to reduce residual risk	✓		
	Identify relationships between the organization and third parties to discover dependencies and visualize information paths.	✓		
	Services to manage the assessment, analysis, and remediation process for you.	✓		
	Connector marketplace to enable an easy, no-code approach to integrating applications with the TPRM solution.	✓		

Lifecycle Stage	Attribute	Mitratech	Vendor B	Vendor C
Continuous Monitoring	Monitor for leaked credentials across 1,500+ criminal forums; thousands of onion pages; 80+ Dark Web special access forums; 65+ threat feeds; and 50+ paste sites. Gather intelligence from security communities, code repositories, and vulnerability databases.	✓		
	Qualitative insights from over 550,000 public and private sources of reputational information, including M&A activity, business news, negative news, regulatory and legal information, operational updates, and more.	✓		
	Financial information from a network of millions of businesses across 160+ countries. Five years of organizational changes and financial performance, including turnover, profit and loss, shareholder funds, etc.	✓		
	Screen vendors against an extensive database of profiles from 30,000 global news sources.	✓		
	Screen against important sanctions lists (e.g., OFAC, EU, UN, BOE, FBI, BIS, etc.), plus over 1,000 global enforcement lists and court filings (e.g., FDA, US HHS, UK FSA, SEC, etc.).	✓		
	Check companies against a proprietary list of government-owned and government-linked enterprises.	✓		
	Screen against a global PEP database. With access to over 1.8 million politically exposed person profiles, including their families and associates.	✓		
	Access a database containing 10+ years of data breach history for thousands of companies around the world. Includes types and quantities of stolen data; compliance and regulatory issues; and real-time vendor data breach notifications.	✓		

Lifecycle Stage	Attribute	Mitratech	Vendor B	Vendor C
SLA & Performance Management	Dedicated and custom contract assessment questionnaires identify potential breaches of contract and other risks.			
	Visualize all contract attributes, and track SLA requirements to manage performance to contractual obligations at renewal.			
	Customizable surveys and a central dashboard to track performance, SLAs, and contract data in a single risk register.			
	Manage all documents throughout the vendor lifecycle in centralized vendor profiles.			
Offboarding & Termination	Leverage customizable surveys and workflows to report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more.			
	Schedule tasks to review contracts to ensure all obligations have been met.			
	Centrally store and manage documents and certifications, such as NDAs, SLAs, SOWs, and contracts.			

About Mitratech

Mitratech is a proven global technology partner for corporate legal, risk, compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening organizational alignment, increasing visibility, and spurring collaboration across an enterprise. Mitratech serves over 24,000 organizations worldwide, spanning more than 160 countries.

For more info, **visit: www.mitratech.com.**