SFA SINGAPORE FINTECH ASSOCIATION | Cyber Sierra

A REPORT ON THIRD-PARTY RISK MANAGEMENT

AN INITIATIVE BY THE SFA CYBER RISK SUBCOMMITTEE, LED BY CYBER SIERRA

Cyber Sierra

Cyber Sierra, founded in 2021 by Pramodh Rai and Subhajit Mandal, stems from a vision to make security compliance easy for enterprises. Designed for mid-to-large organizations, Cyber Sierra's technology digitizes and automates cyber compliance, governance, and risk management.

Our intelligent platform catalyzes use cases that include Third Party Risk Management (TPRM), Continuous Control Monitoring (CCM), and Governance, Risk & Compliance (GRC).

Trusted by Fortune 500 companies and global banks, Cyber Sierra is also recognized within the industry as a Representative Vendor in Gartner's Hype Cycle for Cyber Risk Management 2024
in two categories: Cyber GRC and CCM.

SFA SINGAPORE FINTECH ASSOCIATION

The Singapore FinTech Association (SFA) is a non-profit organization uniting stakeholders across the fintech industry to drive innovation, collaboration, and regulatory support. As a platform for cross-industry collaboration, SFA promotes engagement through events, membership programs, and knowledge sharing. By fostering a resilient ecosystem, SFA strengthens Singapore's role as a global fintech hub.

EXECUTIVE SUMMARY

A Report on Third-Party Risk Management

An Initiative by the SFA Cyber Risk Subcommittee, led by Cyber Sierra

Recent high-profile incidents at companies like SolarWinds, Target, and Volkswagen underscore a critical reality: third-party risk management (TPRM) is no longer just a compliance requirement—it's a strategic imperative for business survival and success.

The industry's reliance on conventional tools—detailed security questionnaires and certifications—though foundational, is no longer sufficient. These static assessments fail to capture the dynamic nature of security postures, making continuous, real-time monitoring not just advantageous, but imperative for preventing the escalation of threats into costly incidents.

While most organizations acknowledge the inherent vulnerabilities in our vendor-dependent landscape, the critical question remains: What truly constitutes adequate risk management in this rapidly evolving threat environment?

This report examines the evolving TPRM landscape through multiple lenses:

- The current state and emerging challenges of third-party risk management
- The intricate regulatory framework shaping TPRM requirements
- The critical intersection of technological solutions and human expertise in light of the cybersecurity talent gap
- The imperative shift from periodic assessments to continuous security posture monitoring as the new paradigm in vendor risk management

It also offers a comprehensive three-pronged strategy encompassing vendor selection criteria, risk management solutions, and strategic investment considerations.

Success in modern TPRM demands a dual focus: investing in cutting-edge continuous monitoring solutions while cultivating security talent through robust professional development programs. Only through this balanced approach can organizations build truly resilient third-party relationships in an increasingly complex business environment.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

CHAPTER ONE

The Global Business Landscape: New Opportunities and Newer Risks

Modern businesses are global businesses, not constrained by geographical boundaries or language barriers. The rapid advancement of digital technologies, improvements in global logistics and the increasing integration of international markets have opened up unprecedented opportunities for growth and expansion.

Companies now enjoy access to diverse talent pools across the globe, new consumer markets, and cost efficiencies in different regions, allowing them to tap into and rely on a network of external entities to support various aspects of their operations.

As a result, most businesses extend their operations through a network of international third parties, including suppliers, distributors, partners, and service providers.

This global reach offers immense potential for:

- Rapid scalability
- Diversification of products and services
- Enhanced competitiveness in global markets
- Increased resilience through geographical diversification

The unbridled growth landscape, however, also introduces a complex set of challenges. Businesses have to grapple with diverse regulatory environments, manage cross-cultural communication and business practices, ensure consistent quality and ethical standards across supply chains, mitigate geopolitical risk, and most importantly, address cybersecurity threats in a globally distributed network.

Modern Businesses, Modern Challenges

As businesses expand globally, the need to manage third-party complexities effectively becomes more important. A strong third-party risk management system, solid corporate governance, and a commitment to ethical practices across borders are now more crucial than ever.

Success isn't anymore about seizing global opportunities, but also about responsibly managing the associated risks and challenges. Only companies that can strike this balance are well-positioned to thrive in the modern, borderless business world.

What is Third Party Risk Management for Modern Businesses?

Third-Party Risk Management (TPRM) is a crucial business process that focuses on managing the risks associated with an organization's external relationships.

Modern businesses are global businesses, and rarely operate in isolation. Instead, they rely on a network of external entities to support various aspects of their operations. These external entities are collectively referred to as “third parties.”

Let's break down the types of third parties mentioned:

SUPPLIERS

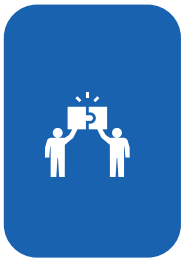
Companies that provide raw materials, components, or products that your organization uses or resells

VENDORS

They provide services or finished goods directly to your organization

AGENTS

These are individuals or entities that act on behalf of your organization, often in sales or negotiations

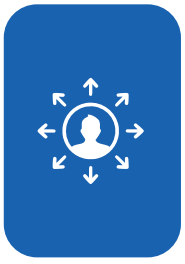


PARTNERS

These are businesses with which your organization has a collaborative relationship, often for mutual benefit

CONTRACTORS

These are individuals or companies hired to perform specific tasks or projects for your organization



DISTRIBUTORS

They help in getting your products or services to end customers

Each of these relationships can introduce various risks to your organization. For example, a supplier might use unethical labor practices, a vendor might have poor cybersecurity measures, or a distributor might engage in corrupt practices. These risks, if not managed properly, can lead to financial losses, reputational damage, legal issues, or operational disruptions for your organization.

This is where TPRM comes in. It's a systematic approach to managing these risks, which involves four key steps:

1. Identifying potential risks: This involves thoroughly examining each third-party relationship to understand what could go wrong. For instance, you might identify data security risks with a cloud service provider or compliance risks with a distributor operating in a different country.

2. Assessing the likelihood and potential impact of these risks: Once risks are identified, you need to evaluate how likely they are to occur and how severe the consequences would be if they did. This helps in prioritizing which risks need the most attention.

3. Implementing strategies to mitigate or manage these risks: Based on the risk assessment, you then develop and implement strategies to reduce or control the risks. This could involve actions like requiring certain security certifications from vendors, including specific clauses in contracts, or providing training to third parties.

4. Continuously monitoring third-party relationships: Risk management isn't a one-time activity. It requires ongoing vigilance. This step involves regularly checking that third parties are complying with your requirements and that the risk landscape hasn't changed. It might include activities like periodic audits, real-time monitoring of certain metrics, or regular relationship reviews.

By following this process, organizations can proactively manage the risks associated with their third-party relationships, helping to protect themselves from potential negative impacts while still benefiting from these essential business partnerships.

Why is Third Party Risk Management Critical for Modern Businesses?

What do Volkswagen, SolarWinds, and Target have in common?

At first glance, not much. They operate in vastly different sectors—automobile manufacturing, IT management software, and retail, respectively. But dig a little deeper into major corporate scandals of the past decade, and you'll uncover the thread that ties them together:

They all faced severe reputational damage and financial losses due to issues with their third-party relationships.

Volkswagen's emissions scandal involved software from a third-party supplier. SolarWinds' massive cybersecurity breach affected thousands of its clients through a compromised software update.

Target's notorious data breach occurred through an HVAC vendor with access to their network.

These high-profile cases underscore a critical reality of modern business: Third Party Risk Management (TPRM) is no longer just a compliance checkbox—it's a strategic imperative.

Here's why TPRM has become indispensable in today's business landscape:

- **Expanding Third-Party Ecosystems:** Companies increasingly rely on a complex network of suppliers, vendors, and partners to operate efficiently. This expansion amplifies potential risks.

- **Data Privacy Regulations:** With laws like GDPR and CCPA in force, organizations are accountable not just for their own data practices, but also for those of their third parties.

- **Cybersecurity Threats:** As the SolarWinds case demonstrated,

cybercriminals often target companies through their less-secure vendors or suppliers.

- **Reputational Risks:** In the age of social media, a third party's unethical practices can quickly become your PR nightmare, as many fashion brands have learned through supply chain controversies.
- **Operational Resilience:** The COVID-19 pandemic and recent geopolitical events have highlighted the importance of understanding and managing risks in global supply chains.
- **Financial Implications:** The costs of a third-party incident can be staggering. Target's data breach, for instance, cost the company $18.5 million in settlements, not to mention the hit to its stock price and customer trust.
- **Regulatory Scrutiny:** Regulators across industries are increasingly holding companies accountable for their third parties' actions, making due diligence no longer optional.

SIDEBAR

98%

of Organizations Exposed: The Growing Threat of Third-Party Breaches

A recent report by Security Scorecard reveals that the exploitation of trusted third parties continues to be a prevalent security concern.

The findings reveal that **98%** of organizations are linked to a third party that has experienced a breach.

These third-party incidents are responsible for **29%** of all data breaches.

The healthcare sector leads in the number of third-party breaches, followed closely by the finance sector.

Here's Why Third-Party Risk Management is Non-Negotiable Today

In an interconnected global economy, your company's risk exposure extends far beyond your own operations.

It encompasses every entity you do business with, from the cloud service provider hosting your data to the janitorial service cleaning your offices.

Effective TPRM, therefore, isn't just about avoiding disasters—it's about building resilience, ensuring compliance, and fostering trust with customers and partners.

In a world where a single third-party failure can lead to headlines you don't want to make, robust TPRM might just be your most important business strategy.

The Multifaceted Value of TPRM: Cost, Risk, and Strategic Gains

COST SAVINGS	**Reduced Contract Termination Fees:** Mitigate the risk of costly contract cancellations by ensuring third-party compliance. **Avoided Litigation Costs and Fines:** Proactive risk management helps prevent legal disputes and associated costs. **Reduced Cost of Vendor Management:** Streamline vendor processes to lower overall management expenses. **Lower Operational Costs:** Efficient TPRM reduces the operational burden and associated costs.
RETURN ON INVESTMENT	**Improved Productivity of Third-Party Buyer Users:** Optimize buyer productivity by ensuring third-party efficiency. **Minimized Business Disruptions and Lost Revenue:** Protect against disruptions that could impact revenue streams. **Improved Productivity of Third-Party Program Users:** Enhance the effectiveness of users interacting with third-party systems. **Increased Revenue by Reducing Time to Market of New Products:** Speed up product launches by ensuring third-party readiness.

OPERATIONAL EFFICIENCY	**Streamlined Vendor Onboarding and Offboarding:** Reduce the time and cost associated with managing vendor lifecycles. **Reduced Inefficiency in Third-Party Workflows:** Identify and eliminate bottlenecks in third-party operations. **Efficient Compliance Monitoring and Reporting:** Simplify compliance processes to ensure timely and accurate reporting. **Faster Incident Response:** Improve response times to incidents involving third-party vendors, minimizing impact.
RISK MITIGATION	**Mitigated Risk of Activating High-Risk Vendors:** Ensure thorough vetting of vendors to avoid potential risks. **Mitigated Risk of Regulatory Noncompliance Penalties:** Avoid fines and penalties by ensuring vendor compliance with regulations. **Mitigated Risk of Supply Chain Disruptions:** Protect against disruptions that could impact the supply chain.
STRATEGIC IMPACT	**Improved Investor Confidence:** Strong TPRM processes build trust with investors by demonstrating effective risk management.

CHAPTER TWO

Navigating the Global Maze of Third-Party Risk Management Regulations

Imagine you're playing a high-stakes game of regulatory chess. The board? The entire world. The pieces?

Your company's third-party relationships. The rules? They change depending on which square you're on.

From the stringent data protection laws of the European Union to the anti-corruption focus of the United States, and the emerging guidelines in Asia, navigating the global regulatory landscape is anything but straightforward.

Take, for instance, the contrasting approaches in **Hong Kong** and Singapore:

- In Hong Kong, the Hong Kong Monetary Authority (HKMA) has issued guidelines specifically targeting third-party risk management in the banking sector.

  Their Supervisory Policy Manual section SA-2 on "Outsourcing" provides detailed expectations for risk assessment, due diligence, and ongoing monitoring of third-party relationships.

- Meanwhile, just a short flight away in Singapore, the Monetary Authority of Singapore (MAS) takes a broader approach. Their Outsourcing Guidelines are a cornerstone of Singapore's approach to TPRM in the financial sector.

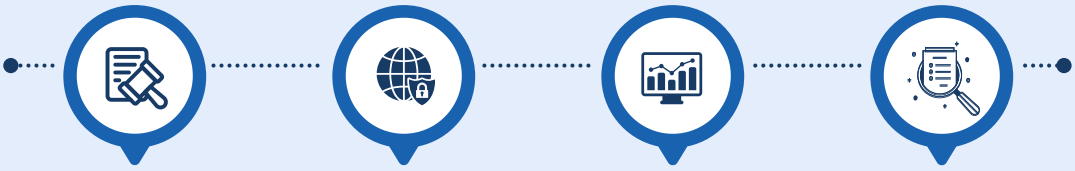
They require financial institutions to:

- Establish a robust framework for managing outsourcing arrangements
- Conduct thorough due diligence on service providers
- Ensure that outsourcing arrangements do not impede the institution's ability to manage risks and comply with regulations
- Maintain the confidentiality and security of customer information
- Implement strong business continuity management for outsourced services

The MAS outsourcing guidelines are particularly noteworthy as they apply to a wide range of services, including cloud computing.

As you expand your view to include other geographies, the complexity multiplies exponentially, creating a challenging environment for global businesses. A practice that's compliant in one jurisdiction might fall short in another. A third-party relationship that poses minimal risk under one regulatory regime could be a major liability under another.

Key Regulatory Requirements for Effective Third-Party Risk Management



Interpreting complex regulations	Managing global compliance across jurisdictions	Resource-intensive monitoring and reporting	Keeping up with evolving regulatory landscapes

As we delve into the key regulations shaping the TPRM landscape, remember: in this global game of regulatory chess, understanding the rules in each square of the board isn't just good practice—it's essential for staying in the game.

Regional Variations in TPRM Regulations

Here’s a look at some of the key TPRM regulations across the globe:

1. North America: A Plethora of Federal and State Laws

- Health Insurance Portability and Accountability Act (HIPAA) mandates healthcare organizations to ensure third-party service providers protect patient data by adhering to stringent cybersecurity practices.
- California Consumer Privacy Act (CCPA) requires companies to ensure that third parties handling personal data maintain appropriate cybersecurity measures to protect that data.
- Federal Information Security Modernization Act (FISMA) requires federal agencies to manage and secure information systems, including those operated by third parties.
- Department of Defense Cybersecurity Maturity Model Certification (CMMC) requires defense contractors and their third-party suppliers to meet specific cybersecurity standards to protect sensitive information within the defense supply chain.
- New York Department of Financial Services (NYDFS) Cybersecurity Regulation mandates financial services companies to assess and manage cybersecurity risks related to third-party service providers, including implementing policies and procedures for third-party risk management.
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) governs data protection.

2. Europe: The Gold Standard of Data Protection

- The GDPR has become the global benchmark for data privacy regulations.
- EU’s Digital Operational Resilience Act (DORA) covers 20 different types of financial entities and their ICT third-party service providers
- The Network and Information Security Directive 2 (NIS-2) includes supply chain security, focusing on the security aspects of relationships between entities and their direct suppliers or service providers.

- The UK Bribery Act goes beyond the FCPA, covering both public and private sector bribery.

3. Asia-Pacific: A Diverse Regulatory Landscape

- Japan's Act on the Protection of Personal Information (APPI) mirrors many GDPR principles.
- China's Cybersecurity Law and Data Security Law have far-reaching implications for businesses operating in the country.
- Australia's Privacy Act and its recent amendments strengthen data protection requirements.
- Monetary Authority of Singapore (MAS) Outsourcing Guidelines requires financial institutions to implement robust risk management frameworks, including cybersecurity measures, for managing third-party service providers.
- Hong Kong Monetary Authority (HKMA) mandates that banks assess and manage cybersecurity risks in outsourcing arrangements, ensuring third parties uphold strong security standards.

4. Middle East and Africa: Emerging Frameworks

- Saudi Arabian Monetary Authority (SAMA) Cybersecurity Framework mandates that organizations implement cybersecurity measures to manage and monitor risks associated with third-party vendors and service providers.
- Central Bank of the UAE (CBUAE) Information Security Regulation: Requires financial institutions to ensure that third-party service providers adhere to stringent cybersecurity controls, protecting the confidentiality and integrity of customer data
- South Africa's Protection of Personal Information Act (POPIA) requires companies to ensure that third parties processing personal data implement adequate cybersecurity safeguards to protect against data breaches and unauthorized access

Geographical Diversity in Regulations: When it comes to TPRM, one size definitely does not fit all

Authority	Regulation	Assessment Required
CA	California Consumer Privacy Act (CCPA) Transparency in Supply Chains Act	✓
EBA	Guidelines on Outsourcing Arrangements	✓
EU	European Corporate Due Diligence Act GDPR	✓
FCA	FG 16/5	✓
HHS	HIPAA Security Rule	✓
NERC	CIP-013-1 R1 & R2	✓
NY	23 NYCRR 500 SHIELD Act	✓
OCC	Bulletin 2013-29 Bulletin 2017-21	✓
SEC	Foreign Corrupt Practices Act	✓
UK	Anti-Bribery Act Modern Slavery Act	✓
US DoD	Cybersecurity Maturity Model Certification (CMMC)	✓
SINGAPORE	Monetary Authority of Singapore	✓
HONG KONG	Hong Kong Monetary Authority	✓
AUSTRALIA	Australian Prudential Regulation Authority Act	✓
UAE	Decretal Federal Law No. (14) of 2018 (Central Bank of the UAE)	✓

CHAPTER THREE

Vendor Selection Criteria: The Cornerstone of Robust TPRM

Whether enterprises juggle spreadsheets and emails to manage third-party data or have a sophisticated, bespoke third party risk governance framework, they **must** place **security risk mitigation** at the forefront of their business strategies.

This shift in focus necessitates a proactive approach, one that begins at the very inception of a vendor relationship - the due diligence stage. Due diligence, a comprehensive investigative process, serves as the foundation for assessing a third party's suitability for a given task. However, it's crucial to understand that due diligence is not a one-time event but an ongoing process that spans the entire vendor lifecycle, encompassing continuous review, monitoring, and management communication.

The overarching goal of a robust TPRM program, therefore, extends beyond mere compliance. It aims to significantly reduce the likelihood of data breaches, prevent costly operational failures, mitigate the risk of vendor bankruptcy, and ensure adherence to ever-evolving regulatory requirements.

While the concept of managing third-party risk is not new, the scale and nature of risks faced by organizations today are unprecedented. From the threat of high-profile business failures to the potential attribution of illegal third-party actions to the organization, and the looming specter of regulatory enforcement for third-party actions, the stakes have never been higher.

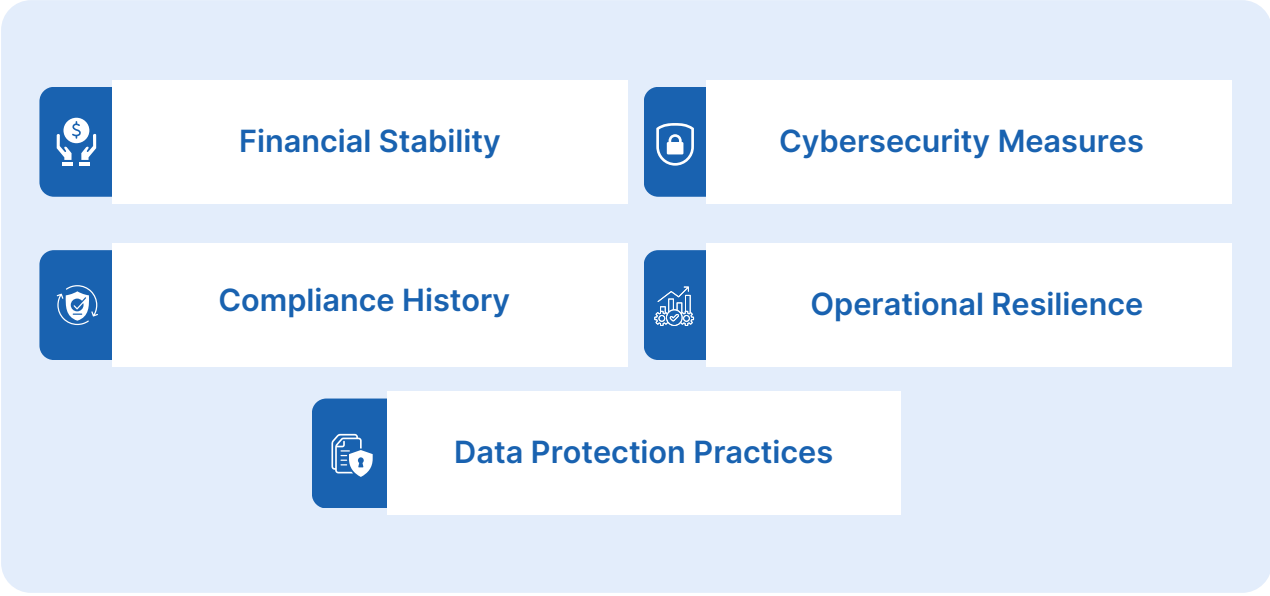
Implementing a Comprehensive Vendor Evaluation Process

In light of these challenges, establishing clear and effective vendor selection criteria and processes is paramount.

A rigorous vendor evaluation process forms the cornerstone of a strong TPRM program. It guides organizations in forging partnerships that not only drive business value but also align with their risk appetite and security standards.

Organizations should assess vendors against internal policies before entering any business relationships. This assessment must cover financial health, cybersecurity posture, adherence to labor laws, and data handling practices. The priority given to each aspect should reflect industry-specific concerns.

Key vendor selection criteria for organizations to consider include:



1. Financial Stability

Assessing a vendor's financial health is crucial for ensuring their long-term viability and ability to maintain robust cybersecurity measures. A vendor's financial instability can lead to supply chain disruptions and potentially compromise their ability to invest in necessary security infrastructure.

Key indicators to review include financial statements, credit ratings, and cash flow consistency.

Understanding these financial metrics not only protects your organization from unexpected disruptions but also ensures the vendor can sustain investments in critical cybersecurity measures.

2. Cybersecurity Measures

When selecting a vendor, their cybersecurity posture should be a top priority. A vendor with weak security practices can expose your organization to data breaches, compliance issues, and reputational damage. Assess their security policies, incident response plans, and track record with data breaches. Look for certifications like ISO 27001 or SOC 2 Type II as indicators of their commitment to information security.

Regular vulnerability assessments, penetration testing, and robust patch management are non-negotiable for maintaining strong defenses. Evaluate their use of encryption, multi-factor authentication, and network segmentation. By thoroughly examining these factors, you can significantly reduce the risk of cyber threats that could jeopardize sensitive data and harm your organization's reputation.

3. Compliance History

It's essential to know if a vendor adheres to relevant cybersecurity regulations and standards—because if they don't, your organization could face severe consequences. Take a close look at their compliance history: Have they ever been fined for security breaches or data protection violations?

Do they meet standards like GDPR, HIPAA, PCI DSS, or NIST Cybersecurity Framework? Asking for proof of compliance isn't just due diligence; it's a way to protect your organization from unexpected legal and security repercussions. When a vendor complies with cybersecurity regulations, it helps keep your business protected from potential cyber threats and regulatory penalties.

4. Operational Resilience

Operational resilience measures a vendor's ability to maintain critical functions during cybersecurity incidents and other disruptions.

Assessing their business continuity plans and disaster recovery strategies is essential for ensuring uninterrupted service and data protection.

Understanding how a vendor prepares for, responds to, and recovers from cybersecurity events is essential for the continuity of your operations.

This resilience is crucial in protecting your organization from potential data losses and service interruptions due to cyber attacks.

5. Data Protection Practices

A vendor's approach to data protection is a critical factor in safeguarding your organization's sensitive information from cyber threats. Assess their encryption methods for data at rest and in transit, data retention policies, and access controls. Evaluate their processes for secure data disposal and their ability to comply with data subject rights under privacy regulations.

These elements are key to preventing unauthorized access and mitigating the impact of potential breaches. A vendor that prioritizes data protection not only strengthens overall security but also reinforces trust in your partnership.

Ensuring that your vendors have strong data security measures in place helps mitigate the risk of data breaches, ensures compliance with data protection regulations, and protects your organization's valuable information assets.

By incorporating these cybersecurity-focused criteria into your vendor selection process, you can significantly enhance your organization's resilience against third-party cyber risks and build partnerships that support a robust security posture.

Visualizing Risk: How to Create an Effective Vendor Risk Matrix

1. Catalog and Rank Vendors

To start, compile a comprehensive inventory of all your current vendors, classifying them according to the services they offer and their significance to your operations. By understanding the role each vendor plays within your organization, you can effectively prioritize your risk assessment efforts.

The more access to your organization's critical cloud and network environments a vendor has, the more they are likely to increase your risk surface area. The same goes for vendors who will rely on other vendors (4th parties) to fulfill their duties to your company.
But it doesn't end there.

The type of solution a 3rd party brings to your company and their geographic location also matters. For instance, companies located in jurisdictions with weak compliance regulations are less likely to have security measures in place. This creates the need to categorize and prioritize vendors that your team must pay constant attention to.

Vendors deemed critical—those whose failure could significantly impact your operations—should undergo a more stringent evaluation. This process is essential to ensure that no vendor is overlooked and that your most vital partnerships receive the attention they warrant.

2. Understand Risk Types, Tolerance, and Criteria

Not all risks carry the same weight. Vendors expose your organization to a range of risks—cybersecurity, compliance, operational, and reputational, to name a few. Establishing your organization's risk tolerance and setting

clear assessment criteria for each type of risk is key to maintaining a consistent and objective evaluation process.

These criteria should align with your organization's overall risk management strategy and objectives. Understanding your risk appetite will help you discern which risks are acceptable and which demand immediate mitigation.

Types of Third-Party Risks	Description
Operational Risks	Disruptions in service delivery, failure to meet SLAs, inefficiencies in outsourced processes.
Cyber Risks	Unauthorized access to data, breaches in vendor systems, data breaches affecting company information.
Compliance Risks	Non-compliance with regulations, legal and financial penalties, violations of privacy laws.
Strategic Risks	Misalignment with organizational goals, vendor instability or changes, failure to adapt to market changes.
Legal Risks	Contractual breaches, regulatory violations, legal disputes with vendors.
Financial Risks	Vendor financial instability, service interruptions, financial losses due to vendor bankruptcy.
Reputational Risks	Lack of commitment to ethical standards, loss of customer trust, damage to brand reputation.

3. Conduct Risk Assessments

Deploy standardized questionnaires, tailored to address the specific risks associated with each of your vendor categories, to gather comprehensive information on each vendor's internal controls, financial stability, compliance history, cybersecurity protocols, and other relevant practices.

It's imperative to validate the accuracy of the information provided by vendors through independent audits or certifications.

Conducting thorough risk assessments will uncover potential vulnerabilities, enabling you to address them proactively.

4. Score Vendor Risks

Implement a scoring system to quantify the risks associated with each vendor, considering both the likelihood of occurrence and the potential impact on your organization. This scoring system offers a measurable and consistent method for evaluating vendor risks.

For example, a vendor with a high likelihood of experiencing a cyber incident but a low impact on your operations would be scored differently from a vendor with a low likelihood but high impact.

This nuanced approach to risk scoring ensures that you focus on the most significant threats.

5. Create a Vendor Risk Matrix

Create a vendor risk matrix, a visual tool that plots vendors according to their risk scores.

This matrix is instrumental in identifying which vendors pose the greatest risk to your organization.

By mapping the likelihood of a risk event against its potential impact, you can easily pinpoint high-risk vendors that require immediate attention.

Additionally, the matrix enhances communication with stakeholders by clearly illustrating where the highest risks are and providing a rationale for necessary mitigation strategies.

SIDEBAR

Vendor Risk Scoring Methodology

Organizations often quantify vendor risks using the following formula: Risk = Likelihood × Impact

This calculation evaluates potential risk based on two key factors:

Likelihood: The probability that a risk event will occur, rated on a scale from 1 to 5 (with 1 being low and 5 being high).

Impact: The potential severity of the consequences if the risk event occurs, also rated on a scale from 1 to 5.

This straight forward method allows organizations to assess and prioritize risks in a consistent and measurable way.

Example of a Risk Scoring Table:

Probability	Risk Assessment Matrix			
	Severity			
	Catastrophic-4	Critical - 3	Marginal -2	Negligible - 1
Frequent - 4	High (20)	High (14)	Serious (8)	Medium (4)
Probable - 3	High (18)	Serious (7)	Serious (9)	Medium (3)
Remote - 2	Serious (10)	Serious (5)	Medium (4)	Low (3)
Improbable-1	Medium (6)	Medium (2)	Low (2)	Low (1)

This approach aids in prioritizing vendors based on their risk levels and selecting partners that align with your security and compliance standards.

It ensures that vendor evaluation extends beyond their immediate offerings to encompass their long-term reliability and security.

6. Continuous Monitoring and Review

Vendor risk management is an ongoing process. Establish a framework for the continuous monitoring of vendor performance and risk exposure.

This involves regularly updating your vendor risk assessments to account for changes in the vendor's environment or shifts in your organization's needs. Automated tools can facilitate real-time monitoring of vendor compliance, financial health, and cybersecurity posture.

Regular reviews ensure that your vendor risk management strategy adapts alongside your organization and that emerging risks are addressed promptly.

SIDEBAR

One-Time Assessments Don’t Mitigate Vendor Risks
And it makes sense.

You can create a well-detailed security questionnaire that properly assesses vendors before joining your organization’s supply chain network. But detailed as your questionnaire might be, they don’t guarantee the detection and prompt mitigation of new risks after vendors get the nod.

In short, they don’t guarantee that vendors who went the extra mile to pass your initial checks and win your company’s business are honest.

Comprehensive Vendor Evaluation Checklist: Securing Your Third-Party Relationships

Enterprises can leverage this detailed Vendor Evaluation Checklist to conduct a thorough assessment of their third-party vendors. Designed to uncover potential vulnerabilities, the checklist ensures vendors adhere to stringent security standards across critical areas:

- **Information Security & Privacy:** Review policies and data protection measures
- **Physical & Environmental Security:** Assess facility and equipment security
- **Web Application Security:** Evaluate application security practices
- **Infrastructure Security:** Check network and server security
- **Access Control:** Ensure proper management of user access
- **Human Resources:** Confirm screening and training of personnel
- **Communications & Operations:** Review data processing and network security
- **Incident Management:** Assess incident response procedures
- **Cyber Resilience & Threat Intelligence:** Evaluate threat management and response
- **Information Systems Environment: C**heck documentation and disaster recovery plans

- **Certifications and Independent Audit Reports:** Verify security review procedures and certifications
- **Security Management in Operations:** Check configuration change procedures and monitoring mechanisms
- **Malware Infection:** Confirm comprehensive malware protection measures
- **Backup Management:** Ensure regular backups, testing, and secure storage
- **Disaster Recovery:** Confirm disaster recovery systems, including counter measures for natural disasters and fire protection
- **Log Management:** Review log generation, storage, retention, and analysis processes

Strengthen your third-party partnerships using our detailed evaluation checklist—see page [54]

SIDEBAR

Strategic Exit: Key Considerations for Third-Party Relationship Termination

The decision to terminate a third-party relationship requires careful analysis of various factors to ensure a smooth transition and minimize potential risks. Key considerations include:

Operational and Compliance Impact: Assess how termination will affect enterprise operations and regulatory compliance. Identify any high-risk or critical activities that may be disrupted.
Financial Implications: Evaluate the costs associated with terminating the relationship, including potential penalties, transition expenses, and impact on revenue streams.
Alternative Solutions: Explore available third-party alternatives or the feasibility of bringing the activity in-house. Consider the readiness of internal staff, systems, and control environments to manage the transition.
Intellectual Property Management: Determine how to handle shared intellectual property, ensuring proper protection and transfer of rights.
Access Control: Review and revoke the third party's access to enterprise systems and information. Establish a clear timeline and process for access removal.
Data Security: For third parties with access to customer data, implement protocols to confirm data return or destruction, maintaining compliance with data protection regulations.
Risk Mitigation: Develop strategies to manage risks associated with termination or migration, particularly focusing on potential customer impact.
Transition Controls: Implement additional controls and processes during the transition period to maintain operational integrity and security.

Thorough consideration of these factors will help enterprises navigate the complexities of third-party relationship termination, ensuring business continuity and compliance while mitigating potential risks.

CHAPTER FOUR

Solutions for Effective Third-Party Risk Management

Not limited by geographical boundaries, and driven by an expanding network of international suppliers, distributors, partners, and service providers, a new generation of TPRM solutions has emerged.

These advanced tools and platforms represent not just incremental improvements, but a fundamental reimagining of risk management strategies, revolutionizing how organizations identify, assess, and mitigate risks throughout the lifecycle of their third-party engagements.

Here's a look at some of the key components of modern TPRM solutions.

A. Risk Assessment Tools

At the forefront of modern TPRM are sophisticated risk assessment tools that leverage the power of artificial intelligence (AI) and machine learning (ML) to provide unprecedented insights into vendor risk profiles.

These platforms offer real-time risk analytics, automated scoring mechanisms, and highly customizable dashboards that enable organizations to prioritize high-risk vendors and allocate resources effectively.

Unlike traditional checkbox assessments, these advanced tools conduct deep, multifaceted analyses of vendor risk factors:

1. Cybersecurity Vulnerabilities: Advanced scanning tools relentlessly probe vendor systems, unearthing potential weaknesses that

conventional assessments might overlook. For instance, these tools might detect outdated software versions or misconfigured security settings in a vendor's infrastructure, allowing for immediate remediation before these vulnerabilities can be exploited.

2. Regulatory Compliance: The ceaseless evolution of worldwide regulatory frameworks renders compliance into a perpetual and complex challenge. Modern risk assessment tools incorporate up-to-date regulatory databases and use natural language processing to analyze vendor documentation, flagging potential compliance issues automatically. For example, the tool might identify discrepancies between a vendor's data retention practices and the stringent requirements of GDPR, prompting proactive measures to ensure compliance.

B. Continuous Control Monitoring Systems

The shift from periodic assessments to continuous control monitoring (CCM) represents a paradigm shift in TPRM. Unlike traditional point-in-time assessments, CCM provides near real-time insights into the vendors' emerging vulnerabilities, compliance gaps, and overall cybersecurity measures, enabling a proactive rather than reactive approach to risk management.
Key features of continuous monitoring systems include:

1. Near Real-time Data Feeds: By integrating with various data sources, including threat intelligence platforms, these tools can provide a constant stream of relevant information about vendor risk profiles.

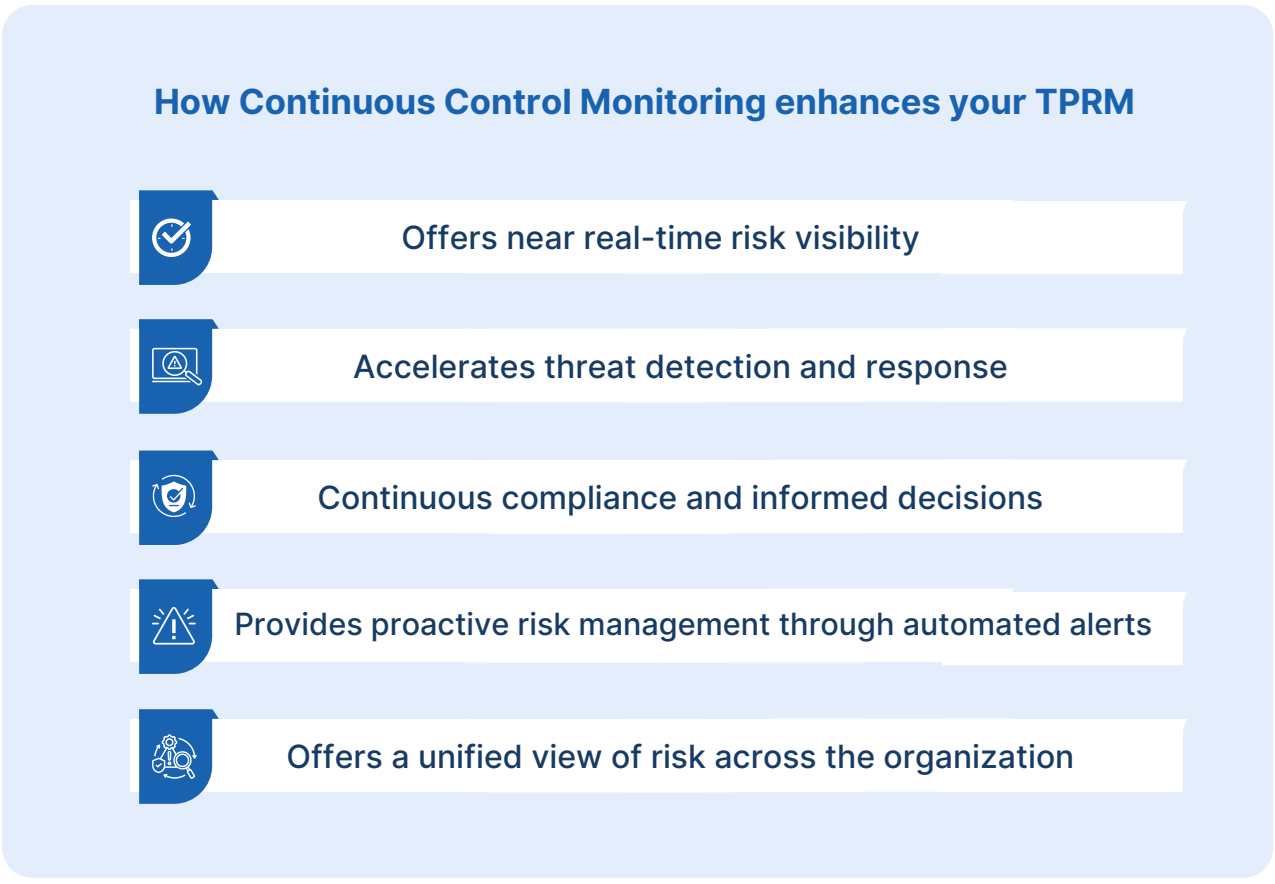
2. Automated Alerts: Sophisticated algorithms analyze incoming data and trigger alerts based on predefined risk thresholds. For example, if a vendor experiences a data breach, the system could immediately notify relevant stakeholders and initiate predefined incident response protocols.

3. Behavioral Analysis: Machine learning algorithms can detect subtle changes in vendor behavior that might indicate increased risk. For instance, unusual patterns in data access or sudden changes in financial transactions could trigger further investigation.

4. Predictive Analytics: By analyzing historical data and current trends, these systems can forecast potential future risks.

This might include predicting the likelihood of a vendor facing financial difficulties or the probability of cyber attacks in specific sectors.

5. Integration with Security Information and Event Management (SIEM): This integration allows for correlation of vendor-related data with internal security events, providing a more comprehensive view of potential risks.



C. Collaboration Platforms

Effective TPRM requires seamless communication and coordination between various stakeholders, both internal and external. Modern TPRM tools create a unified workspace that facilitates this complex interplay:

1. Secure Information Sharing: Provide a secure environment for sharing sensitive information between organizations and their vendors.

For example, vendors can securely submit compliance documentation, which can then be automatically analyzed and scored by the risk assessment tools.

2. Near Real-time Risk Assessments: Stakeholders can collaboratively conduct risk assessments, with each party contributing their expertise. For instance, IT security teams might assess technical risks while legal teams evaluate compliance aspects, all within the same platform.

3. Transparent Remediation Tracking: When risks are identified, these platforms allow for transparent tracking of remediation efforts. Vendors can provide updates on their progress, which can be verified and approved by the organization in near real-time.

4. Scenario Planning: Collaborative tools enable joint scenario planning and simulations. Organizations and their critical vendors can work together to model potential risk scenarios and develop coordinated response strategies.

5. Knowledge Management: These platforms serve as centralized repositories for risk-related information, fostering organizational learning and enabling more informed decision-making over time.

Breaking Silos: How Collaboration Elevates TPRM

D. Automated Due Diligence Processes

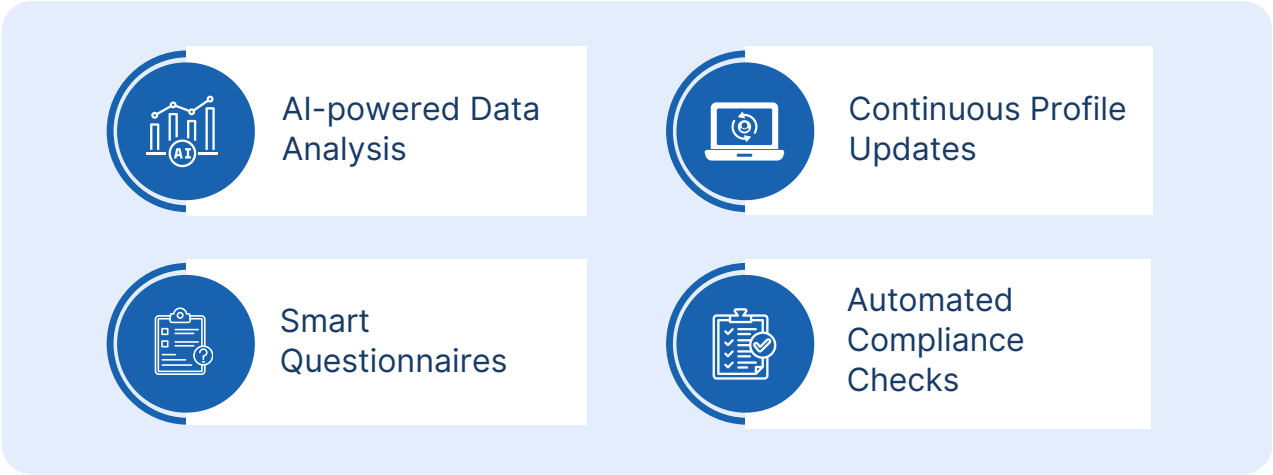
Automation is revolutionizing the due diligence landscape, dramatically improving efficiency, accuracy, and scalability:

1. AI-powered Data Analysis: Machine learning algorithms can rapidly process vast amounts of structured and unstructured data, extracting relevant information for vendor evaluations. This might include analyzing financial reports, legal documents, and public records to build comprehensive vendor profiles.

2. Continuous Profile Updates: Unlike traditional point-in-time assessments, automated systems continuously update vendor profiles based on new information. For example, if a vendor acquires a new company, the system could automatically reassess the vendor's risk profile in light of this change.

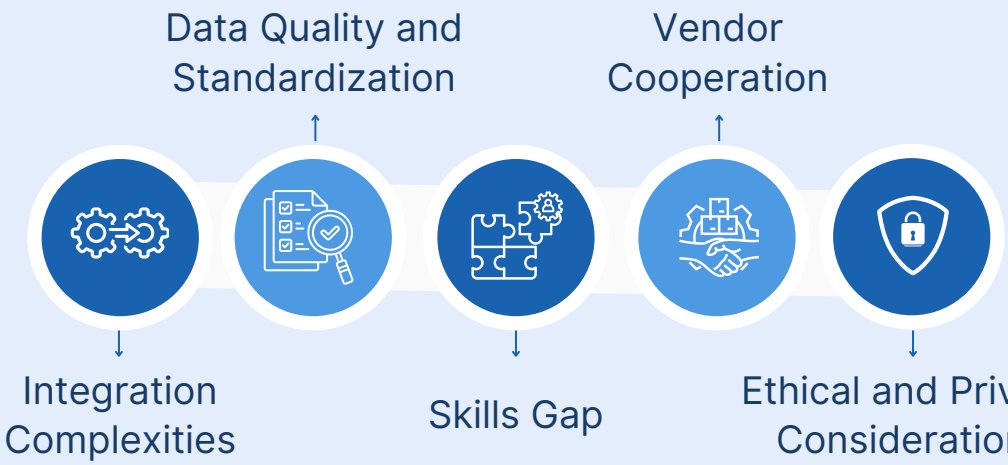
3. Smart Questionnaires: AI-driven systems can generate tailored due diligence questionnaires and help answer them too based on vendor characteristics and risk profiles. The questions evolve based on previous responses, ensuring a more targeted and efficient assessment process.

4. Automated Compliance Checks: These systems can automatically cross-reference vendor information against various compliance databases, sanctions lists, and regulatory requirements. Any red flags are immediately highlighted for further investigation.



From Vision to Reality: Addressing TPRM Adoption Obstacles

While the benefits are significant, organizations must navigate several challenges when adopting advanced TPRM solutions:



- **Integration Complexities:** Seamlessly integrating new solutions with existing systems and processes requires significant IT resources and careful change management.
- **Data Quality and Standardization:** The effectiveness of these tools relies heavily on high-quality, standardized data. Organizations may need to invest in data cleansing and standardization efforts.
- **Skills Gap:** The sophisticated nature of these tools may require new skill sets. Investment in training or recruitment of specialized talent may be necessary.
- **Vendor Cooperation:** Fully leveraging these tools often requires vendor participation in data sharing and risk management processes. Organizations may need to address potential resistance or concerns from their vendor ecosystem.

- **Ethical and Privacy Considerations:** The extensive data collection and analysis capabilities of these tools raise important ethical and privacy concerns. Organizations must carefully balance risk management needs with privacy protection and regulatory compliance.

SIDEBAR

The future of TPRM isn't just about managing risks.

TPRM solutions, aside from managing risks, offer a strategic advantage, enabling organizations to build more resilient, efficient, and trusted business ecosystems.

This transformation offers several key benefits:

- **Enhanced Risk Visibility:** Organizations can gain unprecedented insights into their vendor ecosystem, enabling data-driven decision-making and proactive risk management.
- **Improved Regulatory Compliance:** Automated monitoring and analysis can significantly reduce non-compliance risks, potentially saving organizations from costly penalties and reputational damage.
- **Increased Operational Efficiency:** Automation of TPRM processes can allow organizations to reallocate resources to more strategic initiatives.
- **Strengthened Cyber Resilience:** Continuous monitoring and rapid alert systems can enhance an organization's ability to detect and respond to cyber threats originating from the vendor ecosystem.
- **Strategic Vendor Management:** Deeper insights into vendor performance and risks. This transformation offers several key benefits, enabling more informed decisions about vendor relationships, potentially leading to cost savings and improved service quality.

CHAPTER FIVE

Bridging the Cybersecurity Skills Gap with Modern TPRM Solutions

The cybersecurity industry faces a critical challenge: a widening skills and staffing shortages that threatens organizations' ability to protect against evolving threats. With millions of cybersecurity positions unfilled globally and the complexity of third-party risks increasing daily, enterprises need innovative solutions to maintain robust security postures despite talent shortages.

And modern TPRM solutions backed by advanced technologies promise to assuage these concerns to a great extent.

Understanding the Cybersecurity Skills Crisis

The Scale of the Problem

The cybersecurity skills shortage has reached unprecedented levels, with a global workforce gap exceeding 4.8 million professionals (source: Cybersecurity Workforce Study from ISC2). This shortage has created significant operational challenges, with seven out of ten organizations reporting direct impacts from cybersecurity staffing shortages. The crisis is further compounded by rising costs associated with recruiting and retaining qualified security professionals, leading to increased workload on existing security teams and contributing to burnout.

Impact on Third-Party Risk Management

The skills gap has particularly severe implications for TPRM programs. As organizations manage increasingly complex vendor ecosystems, they

require specialized expertise to assess and monitor a growing number of third-party relationships. This challenge is further complicated by evolving regulatory requirements that demand deep compliance expertise and the need for rapid risk assessment and response capabilities. Security teams find themselves stretched thin, trying to maintain comprehensive vendor oversight while keeping pace with emerging threats.

How Modern TPRM Solutions Bridge the Gap

Technology-driven TPRM platforms are revolutionizing how organizations manage vendor risk by significantly reducing manual workload.

Automation of Routine Tasks

These solutions automate crucial but time-consuming processes such as vendor onboarding and assessments. By leveraging pre-populated security questionnaires and templates, teams can streamline their evaluation processes. The automation extends to risk scoring and categorization, while also managing scheduled assessment renewals and follow-ups, freeing security professionals to focus on more strategic initiatives.

Enhanced Efficiency Through AI and Machine Learning

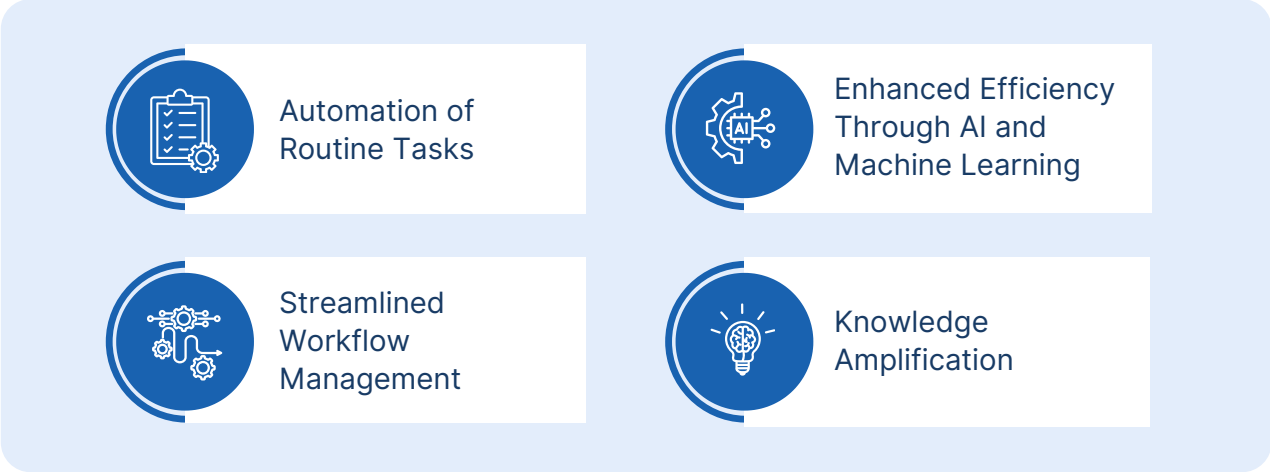
Advanced TPRM solutions harness the power of artificial intelligence to transform vendor risk management. These systems excel at identifying patterns in vendor risk profiles that might escape human notice and can predict potential security incidents before they occur. By analyzing historical data, AI-driven systems prioritize risks more effectively and provide targeted recommendations for mitigation strategies, essentially acting as a force multiplier for security teams.

Streamlined Workflow Management

Modern platforms have revolutionized team productivity through centralized information management and automated workflows. These systems create a single source of truth for vendor information and communications, automatically assign tasks, and provide clear visibility into process status. This streamlined approach enables seamless collaboration across teams and departments, ensuring that nothing falls through the cracks despite resource constraints.

Knowledge Amplification

TPRM solutions serve as powerful knowledge amplifiers, embedding industry best practices directly into daily workflows. These platforms come equipped with built-in assessment frameworks aligned with standards like NIST and ISO, providing contextual guidance for risk assessment processes. They maintain updated compliance requirements and automatically adapt to regulatory changes, reducing the need for specialized expertise in every aspect of vendor risk management.



Real-World Impact

Resource Optimization

Organizations implementing modern TPRM solutions report transformative results in their operations. Many have achieved significant reduction in the time spent on routine tasks, enabling their teams to manage larger vendor portfolios without additional staffing. This efficiency gain has decreased reliance on specialized expertise for routine assessments, allowing organizations to redirect their skilled professionals toward strategic security initiatives.

Quality Enhancement

Technology-driven approaches have significantly improved the quality of vendor risk management programs. By implementing consistent assessment methodologies and reducing human error in risk evaluation, organizations can maintain more comprehensive vendor monitoring programs. The automated systems excel at quickly identifying potential

risks, ensuring that no critical issues go unnoticed despite resource constraints.

Cost Benefits

The financial impact of modern TPRM solutions extends beyond immediate operational efficiencies. Organizations have seen substantial returns on investment through reduced hiring needs and lower training costs. The solutions help minimize the impact of staff turnover by preserving institutional knowledge within the system. Perhaps most importantly, they help prevent costly security incidents through more reliable and consistent vendor oversight.

What Lies Ahead?

The future of vendor risk management lies not in choosing between human expertise and technological solutions, but in finding the optimal balance between the two. As TPRM platforms continue to evolve, they will increasingly serve as essential tools for organizations striving to maintain effective security programs in an environment of persistent talent shortages.

CHAPTER SIX

How to Choose the Right Third Party Risk Management Solution?

Irrespective of your organization's unique situation, there are must-haves to look out for in an enterprise TPRM platform given today's precarious threat landscape. This section of the report explores those crucial features, so you can make a more informed decision as you embark on buying and adopting an enterprise TPRM solution.

A. Identifying Business Needs

The first step in the vendor selection process is to clearly define your business needs. This involves understanding the specific requirements your organization has in terms of products, services, or solutions. Consider factors such as scalability, integration with existing systems, and long-term strategic goals.

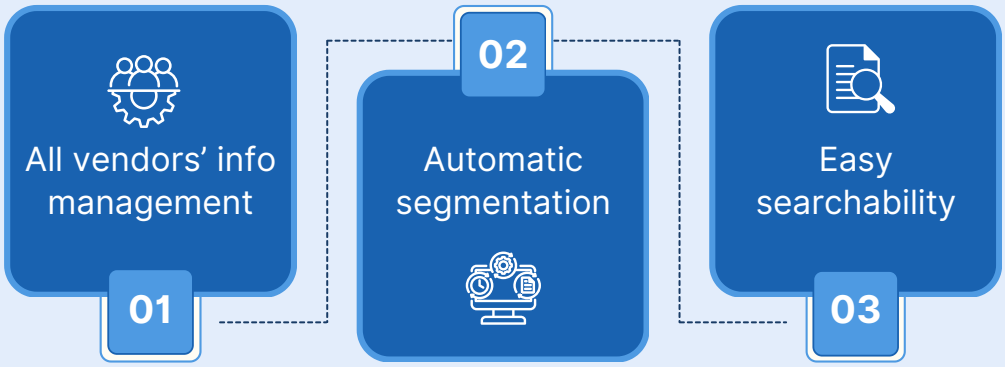
This stage sets the foundation for identifying vendors who can meet your organization's unique needs.

B. Must-have Feature Sets

1.Holistic Vendor Directory

Imagine waking up to the news that a severe cyberattack has breached the data of many tech companies located in Singapore. Knowing your company partners with third-party vendors located in Singapore, you'd want to ensure they aren't among those affected.

Doing that would be a stretch without a TPRM platform with holistic vendor directory capabilities. If the tool you choose lacks this feature, your vendor risk management team will rely on a mishmash of spreadsheets — with disconnected and disorganized pieces of information about the vendors your company is working with. It'd be difficult for you, the security leader or tech executive, to quickly filter and find specific lists of vendors whenever the need arises. A holistic vendor directory solves this in three ways:



- **All vendors' info management:** From documents, to risk profiles, and policies in a centralized cloud-based platform.
- **Automatic segmentation:** Leverages attributes like vendor location, vendor tiers, and others to automatically segment third-parties in your overall vendor ecosystem.
- **Easy searchability:** Ability to quickly filter and find vendors that match whatever criteria relevant to you at any given time.

Based on what's itemized above, here's how to view a holistic vendor directory. It is a central place where all details of past and existing third-party vendors working with your organization can be easily filtered and retrieved by authorized persons.

Each time a new 3rd party is allowed into your vendor ecosystem, varying degrees of new cyber risks are introduced.

The extent to which your team can know which vendors are likely to introduce more risks depends so much on how well you select and onboard them.

2.Selection & Onboarding

Vendor categorization, risk assessment and due diligence helps security teams tier vendors to be prioritized for ongoing risk monitoring. So vendor selection and onboarding capabilities a TPRM platform should have are:

- **Pre-onboarding risk analysis:** Streamline the risk-profiling process for new vendors through security assessment surveys.
- **Customizing assessments:** Enable leveraging standard vendor assessment templates like NIST and ISO, and the ability to customize them per your organization and vendor needs.
- **Pre-contract due diligence:** Automate the cybersecurity due diligence processes before vendor contracts are approved.
- **Multiple vendor tiering:** Automatically segmenting vendors into multiple tiers such as those with inherent or critical risks.

3.Risk Management & Remediation

To win your company's business, third-party vendors will do everything within their power to pass initial security assessments. But once most are in, they become lackluster about security. This is why you shouldn't rely on the first, positive impressions of vendors.

It's also why your cybersecurity team needs processes in place for managing and remediating vendor risks should they emerge. So after guiding vendors through onboarding and performing due diligence, a smart TPRM platform must also help you:

- **Track security assessment progress:** Streamline the process of tracking the due dates and review statuses of sent security assessment questionnaires across all vendors.
- **Re-populate questionnaires:** Use answers previously submitted by vendors to re-populate questionnaires for what has changed.
- **Auto-score assessment responses:** Automatically score responses and evidence provided by vendors to security assessment questions to understand possible risks.

4.Continuous Vendors' Monitoring

As the cyber threat landscape evolves, the third parties must also evolve to comply with changing regulatory requirements.

But the onus is on enterprises to ensure their vendors are staying compliant with those changing compliance regulations.

Failure to do this can result in collateral data breach damages and the hefty regulatory fines that come with them.

Avoiding such requires continuous vendor monitoring. First to ensure adherence to evolving compliance requirements. And second to reap the added advantage of identifying and proactively remediating risks from all vendor relationships before it's too late.

SIDEBAR

How Should Vendor Risk Assessments Be Done?

It should be ongoing. And the reasons are simple. First, CISOs can no longer afford to assess vendors once, no matter how detailed the security questionnaires used are, and go to sleep. Second, a BlueVoyant survey of top executives globally responsible for cybersecurity in their organizations supports this.

The study saw a **whopping 93% of respondents** say they suffered breaches due to weaknesses in their supply chains. Considering breaches in supply chains are usually from third-party vendors, the study uncovered even more troubling data.

What to look for in TPRM platforms

REAL-TIME VENDOR MONITORING

Track vendors' posture against compliance failures and cybersecurity risks in real-time.

CONTINUOUS RISK TRENDS' VISIBILITY

Gain comprehensive, continuous visibility into vendors' statuses against evolving risk trends and regulatory compliance requirements

AUTO-RISK FLAGGING AND SCORING

Flag all risks and automatically assign scores to each, enabling your team to prioritize.

ACTIONABLE REMEDIATION INSIGHTS

Provide useful insights your team can use to prevent data breaches and compliance failures.

C. Evaluating Solution Fit: Is it Aligned with Your TPRM Metrics?

The chosen TPRM platform should help you improve on key TPRM metrics when deployed. This would help your security team know what to improve and succeed.

1. Number of Identified Vendor Risks

This metric measures how many third party risks your security team identifies over time. The objective of this metric, relevant to most enterprise TPRM programs, is to identify as many risks as possible.

As organizations add new vendors, they need to identify all risks and security threats brought into their ecosystems. So the more risks identified over time, the more your security team can demonstrate its understanding of third party risks.

2. Number of Reduced Risks

Identifying an appreciable number of risks over time is good. But demonstrating that they are reducing relative to when your program went into effect is more important.

Say your organization hasn't added new vendors in the last three months. This metric tracks changes in third-party risks within that period. Less risk means your security team is effective.

3. Cost of Managing Third-Party Risks

Security teams should track this in twofold:

- Articulate all direct and indirect costs associated with managing vendor risks before implementing your TPRM program.
- Show how these costs have reduced over time relative to the negative business impact mitigated.

Reporting this metric is critical because it's a great way for board members to see your TPRM program as a value, and not a cost center.

4. Time to Detect Vendor Risks

As the name suggests, this metric helps you track how long it takes your team to detect vendor risks on average. A shorter risk detection time shows that your security team is efficient.

Board members would want to see risks being detected as soon as possible. This is why third-party security managers track and report on how their team has reduced their average risk detection time.

5. Time to Mitigate Risks

How long does your team take to mitigate vendor risks?

This metric measures the answer to that question. Once your team detects risks, they must immediately mitigate them. The faster they do this, the more financial and reputational damage your vendor risk management program will save your company. By tracking it, you can set objectives for improving your time to mitigate risks over time.

SIDEBAR

Achieving Vendor Risk Management KPIs & KRIs

Tracking the metrics above is good.

But without context, metrics on a dashboard won't show how effective your TPRM program is. Worse, they are not so helpful if you can't tie them to noticeable business objective indicators.

Here are three TPRM metrics, tied to business objectives, that you should prioritize.

- **Resource Efficiency:** Resource efficiency is using just the right amount of time, tools, people, and budget to implement an effective TPRM program. It indicates to management that your security team is doing a great job while saving time and money.

- **Throughput:** Throughput gives management an overview of how quickly your security team is able to address a specific number of vendor risks over a given time period.

  This KPI helps identify and minimize bottlenecks in the vendor risk management processes, enabling security teams to do more in less time.

- **Process Efficiency:** Process efficiency can be defined as striking the right balance between operational effectiveness and risk mitigation.

  It helps track the speed at which the security team assesses, manages, and mitigates third-party risks. While the first two required having the right strategy, this one is about streamlining core elements of third-party risk management.

  With these critical assessment frameworks in one place, your team can assess, onboard, manage, and mitigate vendor risks much faster.

6. Time to Complete Risk Assessments

It is important to track how long it takes to completely assess vendors. Security managers should strive to reduce the time it takes to assess vendors for two reasons:

1. Give vendors a smooth assessment experience
2. Demonstrate to management how efficiently they are risk-assessing and onboarding third parties into their ecosystem.

You can achieve these with software that streamlines the process of initiating and completing vendor risk assessments.

Choosing the Right TPRM Tool

Even with everything above checked, are there other things to consider before choosing an enterprise TPRM platform?

There are, so let's discuss them.

1. Adaptability

This one goes both ways.

As much as vendors need your organization's business, your organization also needs vendors to stay competitive. The implication of this is that a TPRM platform must be adaptable to both parties.

On the one hand, it should streamline your team's processes of managing risks posed by vendors. On the other hand, it should also streamline the steps

vendors need to answer security assessment questions and provide necessary compliance evidence.
No party should feel like it's extra work.

2. Interoperability

Third-party risk management is crucial. But it is one piece of risk management in the overall enterprise governance, risk management, and regulatory compliance (GRC) pie:

The Place of Vendor Risk Management in Enterprise GRC

Consider this when choosing a TPRM solution. Because if you choose a point TPRM tool, you'd also need to spend hard-earned resources on other tools for cybersecurity governance and compliance.

In addition to wasted spend, point cybersecurity solutions have other downsides.

To avoid these issues, seek a platform where your team can tackle vendor risks in the context of your company's security governance, overall risk management, and regulatory compliance, all in one place.

This is why interoperability is crucial and should be prioritized.

3. Value

While price is a major consideration with any enterprise software purchase, what you really want to focus on is the value you'd get. And staying with the need for interoperability over a point tool, it makes sense to prioritize a TPRM solution with full-fledged capabilities for tackling interrelated, enterprise cybersecurity needs.

Some things to look out for are:

- Beyond TPRM, does it provide a centralized solution suite for addressing other cybersecurity concerns from one place?
- Is there unlimited access, so your core security team and employees can collaborate in tackling cybersecurity?
- Can you integrate all tools and services across your organization for continuous scanning for threats and cyber risks?
- Can you customize the platform, per your organization's specific cybersecurity needs?
- Is the platform enterprise-ready and built to scale as teams across your organization, cybersecurity, regulatory compliance, and vendor risk management needs grow?

The correct answers to these questions vary from one company to another and will ultimately depend on a company's unique needs. So to get the most value out of a TPRM solution, it's best to reach out and see if it can be tailored to your needs before talking about pricing.

Step-by-step Vendor Evaluation Checklist

Criteria	Question	Comments
Certifications and Independent Audit Reports	Do you have established security review procedures with regular reviews to ensure compliance with information security requirements, agreed-upon standards, and your own policies?	
Information Security and Processing Policies	Is there an up-to-date Information Security policy in place that demonstrates management commitment, outlines principles, and has been reviewed and approved by responsible management in the past twelve (12) months?	
Information Security and Processing Policies	Is our data stored and processed in a secure, access-controlled environment, with access limited to those on a need-to-know basis? Where possible, is data encrypted to prevent unauthorized access?	
Organization of Information Security	Is there a designated Information Security Manager with the required expertise and knowledge to fulfill the obligations under our Information Security Requirements?	
Organization of Information Security	Are roles and responsibilities segregated to prevent conflicts of interest, specifically regarding permission granting, network/application administration, and system development/testing/operation?	

Criteria	Question	Comments
Risk Management	Does your organization have a structured risk management process that identifies and classifies risks related to handling our data, including scenarios for personal data and relevant key controls? Are risks, remediation plans, and status communicated to us regularly?	
Human Resources	Are screening, background checks, and monitoring of personnel involved in processing our data conducted according to our standards?	
Human Resources	Have all personnel completed periodic awareness training on Information Security and understand the requirements?	
Human Resources	Is appropriate training provided to ensure personnel understand data protection and banking secrecy requirements?	
Human Resources	Is there a maintained list of key personnel involved in processing or supporting our data? Is this list available to us upon request?	
Physical and Environmental Security	Is physical and environmental security considered in risk assessments for data centers, server rooms, and other controlled areas housing our sensitive information?	

Criteria	Question	Comments
Physical and Environmental Security	Are procedures in place to protect equipment necessary for supporting or providing access to the serviced environment, preventing unauthorized access?	
Physical and Environmental Security	Are procedures in place to protect equipment necessary for supporting or providing access to the serviced environment, preventing unauthorized access?	
Communications and Operations Management	Are procedures based on the 4-eye principle or log files in place when processing our data, with responsible units for Information Security or Data Protection informed accordingly?	
Communications and Operations Management	Are security components (e.g., firewalls, anti-virus) installed, maintained, and updated on all devices, with network security infrastructures managed using encrypted connections?	
Communications and Operations Management	Are firewalls and proxies configured to permit connections with documented business justification, and are network connections bypassing your network blocked? Are backup, archiving, and retention processes formally documented?	

Criteria	Question	Comments
Incident Management	Are management responsibilities and procedures established for a quick, effective response to information security incidents or breaches? Are escalation and resolution protocols documented, and are we notified of any actual or suspected security incidents or breaches as per contractual agreements?	
Cyber Resilience & Threat Intelligence	Is a Cyber Incident Management organization (e.g., CSIRT, CERT) in place with defined roles, responsibilities, processes, and playbooks for common attack scenarios (e.g., ransomware), and is it tested regularly? Are we notified on a timely basis (not exceeding 48 hours) of relevant incidents?	
Cyber Resilience & Threat Intelligence	Is there a threat intelligence process to stay updated with current threats? What are the threat intelligence sources, and are indicators of compromise (IOCs) checked against log data automatically?	
Cyber Resilience & Threat Intelligence	Is there a security monitoring function (SOC) or equivalent (in-house or outsourced/hybrid) to detect cyber attacks? How is this setup, and is there appropriate governance?	

Criteria	Question	Comments
Access Control	Are systems and equipment used to access our systems password-protected following industry best practices and our standards? Are shared or generic accounts avoided?	
Access Control	Is two-factor authentication (2FA) implemented for privileged accounts, with logging/recording, export control, and periodic review of user access ensured?	
Access Control	Are procedures in place for managing and controlling privileged user accounts, ensuring unique user IDs, maintaining an uninterrupted audit trail, and disabling or deleting inactive accounts appropriately?	
Access Control	Is there a process for regular review of user access, ensuring that access privileges are periodically audited and adjusted based on role changes or departures? Is the principle of least privilege strictly followed, ensuring that users only have the minimum access necessary for their roles, and that access is granted only for the duration required?	

Criteria	Question	Comments
Information Systems Environment	Is an up-to-date inventory maintained of applications and infrastructure used for processing, transferring, and storing our data, including legal entities, locations, and jurisdictions?	
Information Systems Environment	Are all operational processes for transferring our data documented in a security concept, and are changes to applications and infrastructure managed to ensure appropriate protection?	
Information Systems Environment	Are Business Continuity Planning (BCP) and Disaster Recovery (DR) procedures defined, implemented, and tested at least annually to meet agreed service level agreements and ensure data protection?	
Security Management in Operations	Are there established procedures for configuration changes to prevent unauthorized changes and errors, including obtaining administrator approval and performing double-checks?	
Security Management in Operations	Are mechanisms in place to regularly and automatically monitor settings using cloud service provider functions, with a process to analyze logs if automatic notifications are unavailable?	

Criteria	Question	Comments
Malware Infection	Do you have comprehensive malware protection measures, including anti-virus software for all platforms, behavior monitoring for suspicious activities, and anti-virus gateways for email, web traffic, and file transfers?	
Backup Management	Are backups performed regularly for all critical systems and data, tested for restoration, and securely stored offsite or in the cloud with encryption and access controls?	
Disaster Recovery	Are disaster recovery systems in place, including countermeasures for natural disasters, such as reviewing hazard maps, installing backup power supplies, and conducting periodic sufficiency reviews?	
Disaster Recovery	Have comprehensive fire protection and fireproofing measures been implemented in data centers, including fireproof materials, automatic fire alarms, sprinklers, and designated disaster prevention teams with regular training and simulations?	
Log Management	Are logs generated for critical security events, stored securely, retained according to compliance requirements, and aggregated by a centralized log management system for analysis and incident response?	

CONCLUSION

Mastering Third-Party Risk in a Connected World

The landscape of Third-Party Risk Management has fundamentally transformed in the last few years. What was once a checkbox compliance exercise has now evolved into a strategic imperative for modern businesses. And with enterprises increasingly relying on complex networks of global vendors, partners, and service providers, the stakes have never been higher. And, it is only expected to skyrocket from here on.

Key Strategic Imperatives

Proactive Risk Management is Non-Negotiable

Modern enterprises, no matter their size and geography can no longer afford to take a reactive approach to third-party risks, especially given the potential for cascading failures across interconnected business networks. With an increasing number of organizations reporting supply chain breaches, continuous monitoring and assessment have become essential rather than optional.

Technology is Reshaping TPRM Capabilities

Advanced solutions leveraging AI, machine learning, and continuous monitoring are enabling organizations to spot and address risks before they materialize into crises. Modern TPRM platforms must offer:

- Streamlined remediation workflows
- Real-time control monitoring and alert systems

- Automated risk assessment and scoring capabilities
- Vendor directories for centralized information management

Compliance Requirements are Growing More Complex

With regulations varying across regions and industries, enterprises need robust security frameworks to navigate it while maintaining operational efficiency. Success requires:

- Adaptable assessment frameworks
- Customizable compliance templates
- Automated compliance monitoring and reporting
- Integrated governance, risk, and compliance capabilities

Measuring Success

To ensure TPRM program effectiveness, organizations must focus on key metrics:

- Process throughput in addressing risks
- Comprehensive risk reduction over time
- Time to detect and mitigate potential threats
- Cost effectiveness of risk management initiatives
- Resource efficiency in managing vendor relationships

Looking Ahead

As we look to the future, successful organizations will be those that view TPRM not as a burden, but as a strategic advantage – one that enables them to:

- Drive sustainable growth
- Build resilient partnerships
- Achieve operational excellence
- Maintain regulatory compliance
- Enable innovation through trusted collaboration

The future of business is collaborative, but it must also be secure. In this context, effective Third-Party Risk Management isn't just about protecting against downside risks – it's about enabling responsible growth and innovation through trusted partnerships. Organizations that master this balance, supported by the right technology solutions and frameworks, will be best positioned to thrive in our increasingly interconnected business world.

Acknowledgments

The development of comprehensive frameworks for third-party risk management requires diverse expertise and multiple analytical perspectives.

This Report on Third-Party Risk Management – An Initiative by the SFA Cyber Risk Subcommittee, led by Cyber Sierra, represents the culmination of collaborative efforts by leading organizations in the cybersecurity and risk management spheres.

We acknowledge the strategic contributions of Bitdefender and the Cyber Risk Subcommittee of the Singapore FinTech Association. Their collective insights were instrumental in examining both the technical and operational dimensions of TPRM in today's complex and evolving threat landscape.

The synthesis of their perspectives has enabled a thorough examination of TPRM challenges and solutions—from tactical implementation considerations to strategic organizational imperatives.

This collaboration underscores a fundamental truth: effective third-party risk management requires not just technological solutions, but also the combined expertise of industry leaders dedicated to advancing the field.

SFA SINGAPORE FINTECH ASSOCIATION | Bitdefender Global Leader In Cybersecurity

CONTACT:

Swati Sodhani
Program Lead, Subcommittees
Singapore Fintech Association
swati.sodhani@singaporefintech.org

Pramodh Rai
Co- Founder,
Cyber Sierra
pramodh@cybersierra.co

Cyber Sierra