The Third-Party Risk Screening Guide

A Practical Framework for Screening Businesses, Vendors & Partners for Sanctions and Reputational Risk

sanctions.io

2026 Edition | Powered by sanctions.io

Table of Contents

Part 1 - The Expansion of Third Party Risk

1. Why businesses must screen businesses

The compliance landscape has fundamentally shifted. For years, the burden of rigorous screening fell almost exclusively on financial institutions. Today, that is no longer the case. The expansion of global supply chains, the rise of digital marketplaces, and the increasing sophistication of illicit actors have transformed third-party risk into a universal business challenge. Screening the businesses you work with, including vendors, distributors, and partners, is now a critical operational necessity.

Regulatory expectations beyond banks

Regulators worldwide are extending their reach beyond traditional banking. Authorities now expect companies across all sectors to understand exactly who they are doing business with. The Office of Foreign Assets Control (OFAC) in the United States, the Office of Financial Sanctions Implementation (OFSI) in the UK, and the European Union have all made it clear that strict liability applies to sanctions violations, regardless of industry[1] [2]. If your manufacturing firm or software company inadvertently engages with a sanctioned vendor, the regulatory penalties and reputational damage can be severe. The expectation is proactive due diligence, not reactive scrambling.

Third-party liability risk

When you onboard a vendor or partner, you are inheriting a portion of their risk profile. This concept of third-party liability means that if your supplier is involved in corrupt practices, human rights violations, or sanctions evasion, your organization can be held accountable and may be affected by reputational harm caused by third parties. In a highly connected global economy, ignorance is not a defense. The failure to adequately screen third parties exposes businesses to significant financial penalties, loss of market access, and catastrophic damage to brand trust.

Marketplace & SaaS Exposure

Digital platforms face unique vulnerabilities. Marketplaces and Software-as-a-Service (SaaS) providers process thousands of B2B relationships at high speed. As detailed in The SaaS Compliance Playbook, these platforms can easily become unwitting conduits for illicit activity if proper controls are not embedded directly into the onboarding flow [3]. The rapid scale of digital business models requires automated, high-volume screening capabilities to ensure that speed to market does not compromise compliance integrity.

Sanctions evasion via intermediaries

Bad actors rarely operate in the open. Sanctions evasion is increasingly conducted through complex networks of intermediaries, shell companies, and seemingly legitimate third-party vendors. These entities are designed to obscure the true beneficial owners and bypass basic checks [4]. Businesses must recognize that screening direct partners is only the first step; understanding the broader network and identifying potential evasion tactics is essential for maintaining a secure supply chain.

2. Where Traditional KYB Falls Short

Know Your Business (KYB) processes have traditionally been viewed as administrative hurdles, largely focused on collecting registration documents and verifying corporate existence. In the modern risk environment, however, this baseline approach is dangerously inadequate.

Company registry checks do not equal risk screening

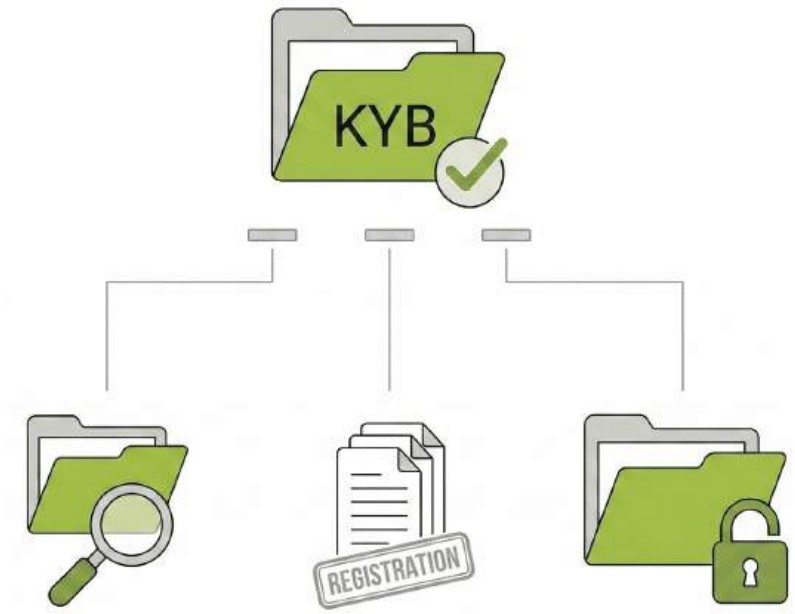
Confirming that a company is legally registered in a specific jurisdiction only proves that the entity exists. It provides little insight into the entity's operational integrity or broader risk profile. A company registry check will not reveal whether the business is secretly funneling funds to a sanctioned regime or whether it has been repeatedly cited for severe regulatory violations [5]. Treating registry verification as the entirety of a KYB process leaves major vulnerabilities unaddressed.

Ownership data does not equal sanctions risk coverage

Identifying the owners of a business is a crucial part of due diligence, but a list of names is not, on its own, a measure of risk. Ownership data only becomes meaningful once those names are run against the right watchlists and sanctions sources, and once the resulting matches are reviewed and acted on within your compliance program. Ownership structures also shift over time through acquisitions, restructurings, and changes in beneficial control, so a snapshot taken at onboarding has a short shelf life. Ownership data is best treated as an input into your broader screening and review processes, not a standalone control.

Why sanctions & adverse media must sit alongside verification

True risk mitigation requires a multi-layered approach. Basic verification should be augmented with comprehensive sanctions screening, PEP and adverse media monitoring [6]. Adverse media often serves as an early warning system, highlighting allegations of fraud, corruption, or unethical behavior long before an entity appears on an official government watchlist. By integrating these checks into the standard KYB workflow, businesses can move from administrative verification to proactive risk management.



Part 2 - What You Should Be Screening

3. Core risk checks for businesses

Building a robust third-party screening program requires a clear understanding of the specific risks that need to be monitored. A comprehensive approach must cover multiple dimensions of potential exposure.

Entity-level sanctions screening

The foundational element of any program is entity-level sanctions screening. Every vendor, supplier, and partner should be checked against local jurisdictional and global sanctions and watchlists, including those maintained by OFAC, the UN, the EU and HM Treasury[1] [2]. This screening must be continuous, as these lists are updated frequently and an entity that is compliant today may be designated tomorrow.

PEP Exposure (directorship-level where applicable)

Politically Exposed Persons (PEPs) are individuals who hold, or have held, prominent public positions and therefore may present a higher risk of exposure to bribery or corruption[7]. Screening the named directors and key decision-makers of a partner organization for PEP status is a practical step that helps compliance teams apply appropriate enhanced due diligence and reduce the risk of entering into relationships that could create regulatory or reputational exposure.

Adverse Media Risk

As emphasized earlier, adverse media screening is essential for identifying reputational risks that have not yet resulted in formal regulatory action. Monitoring global news sources for allegations of financial crime, environmental violations, or severe labor abuses provides crucial context that standard watchlists cannot offer[6]. This proactive monitoring protects the organization's brand and helps prevent association with high-risk entities.

Jurisdiction risk flags

Not all locations carry the same level of risk. Businesses should implement jurisdiction risk flags to identify counterparties operating in regions known for high levels of corruption, weak regulatory frameworks, or active conflict. Engaging with a vendor in a high-risk jurisdiction inherently requires a higher level of scrutiny and more rigorous ongoing monitoring and may sometimes be disallowed completely if the country and its specific industry is designated.

Watchlist & enforcement lists

Not all businesses need to screen against Interpol Red List or FBI Most Wanted. For example, a SaaS company may not have to do this because they don't fall under traditional KYC/AML requirements. This is especially applicable for businesses that are legally subject to AML, KYC or CTF regulations and mandates. Beyond primary sanctions lists, businesses that are subject to AML, KYC or CTF regulations should also consider screening against broader regulatory enforcement lists and criminal watchlists, such as Interpol's Red List or FBI's Most Wanted. These databases track entities that have been penalized by environmental agencies, financial regulators, or law enforcement bodies. Screening against these lists provides a more complete view of a third party's compliance history and operational integrity.

4. Screening Directors & Key Individuals (High level)

A practical third-party screening program should include the named directors and key decision-makers who control or influence the relationship. Screening these individuals for sanctions, PEP exposure, and adverse media helps organizations identify meaningful risk signals without expanding into a broader ownership analysis that may sit outside the immediate scope of the screening workflow.

Part 3 - Building a Practical Third Party Screening Program

5. Risk based segmentation

Not all third parties present the same level of risk, and applying a one-size-fits-all screening approach is both inefficient and ineffective. A practical program relies on risk-based segmentation so that compliance resources are concentrated where they are needed most.

Risk segmentation in practice

Counterparty type	Risk level	Recommended approach
Low-risk vendors	Low	Baseline onboarding screening with periodic review.
High-risk distributors	High	Enhanced due diligence (EDD) with deeper adverse media, PEP checks, and frequent monitoring..
Cross-border partners	Medium to high	Jurisdiction-sensitive screening with closer scrutiny of ownership, routes, and counterparties.
Regulated counterparties	Medium	Standard screening plus regulatory status verification and proportionate monitoring.
Non-regulated counterparties	High	Stronger onboarding checks, tighter approval thresholds, trigger-based re-screening and ongoing monitoring for any high risk entities

Low risk vendors

Standard suppliers of non-critical goods or services operating in well-regulated, low-risk jurisdictions generally require a baseline level of screening. For these entities, automated checks at onboarding and periodic reviews may be sufficient, allowing compliance teams to direct greater attention elsewhere.

High-risk distributors

Distributors, agents, and intermediaries often act on behalf of the company in foreign markets, significantly increasing the risk of bribery or sanctions violations. These high-risk entities require enhanced due diligence, including deeper adverse media screening and frequent ongoing monitoring, to ensure they are operating within legal and ethical boundaries.

Cross-border partners

Engaging with partners across international borders introduces complexities related to varying regulatory frameworks and geopolitical instability. Cross-border relationships should be evaluated based on the specific jurisdictions involved, with screening protocols adjusted to account for heightened risk of sanctions evasion or exposure to restricted markets.

Regulated vs non-regulated counterparties

The regulatory status of a third party is a key factor in risk segmentation. A vendor that is itself subject to strict financial regulations may present a lower inherent risk than an unregulated entity operating in a high-risk sector. At the same time, if a company is regulated heavily, it means that breaches of compliance are likely to be more severe and that the specific industry that partner operates in is liable to breaches of compliance regulations. Understanding the regulatory environment of your counterparties helps refine the screening approach and justify proportional controls.

6. Onboarding vs ongoing monitoring

A common vulnerability in third-party risk management is treating screening as a singular event rather than a continuous process.

One time screening pitfalls

Screening a vendor only at the point of onboarding provides a snapshot of their risk profile at that specific moment. Risk is dynamic. A vendor that is clean today could be added to a sanctions list next week or become the subject of a major corruption scandal next month. Relying solely on one-time checks leaves the organization exposed to emerging threats.

Periodic re-screening

Aside from trigger events and continuous monitoring, there is also an in-between: periodic re-screening (for example weekly, monthly or quarterly) which may be done manually. However, there is a risk of human error with this approach.

Trigger events

To mitigate this, organizations should define trigger events that automatically prompt a re-screening of a third party. These events might include a change in the vendor's leadership, a significant shift in operating jurisdictions, or the emergence of new adverse media. Trigger events ensure that the risk profile is updated in response to material changes in the business relationship.

Continuous monitoring best practices

The gold standard for third-party risk management is continuous monitoring. By leveraging automated systems to screen vendors continuously against updated watchlists and media feeds, organizations can detect risks in real time [8]. Continuous monitoring shifts the compliance function from a reactive administrative task to a proactive risk management strategy.

7. Reducing False Positives at Scale

As screening volumes increase, managing false positives becomes a critical operational challenge. A false positive occurs when a screening system incorrectly flags an entity as a match against a watchlist, whereas a false negative occurs when a true risk is missed entirely. High false positive rates consume valuable analyst time and can obscure genuine risks.

Entity name matching

Effective screening requires sophisticated entity name matching algorithms. These systems should account for variations in corporate naming conventions, abbreviations such as "Ltd" versus "Limited," and transliteration differences

across languages, for example, when the same name appears with different Latin spellings after being converted from Arabic, Cyrillic, or Chinese. Advanced matching logic, including the use of ML or AI, significantly reduces the noise generated by simple keyword searches and helps reduce false positives.

Common-name handling

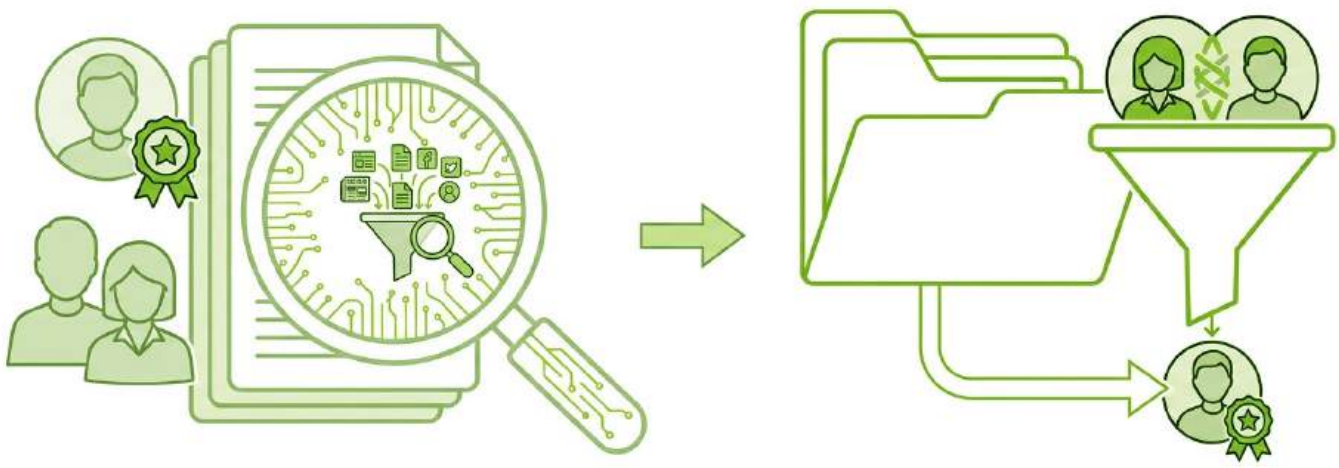
When screening individuals, common names create a substantial hurdle. A basic search for a common name can return many irrelevant hits. To address this, screening systems should use secondary identifiers such as dates of birth, geographic locations, or known associates to filter out incorrect matches and isolate the true subject of interest, or use Machine Learning capabilities to understand various contexts in order to identify the correct individual based on a contextual analysis.

Jurisdiction filtering

Applying jurisdiction filters is another effective method for reducing false positives. If a business is screening a local vendor operating exclusively in Canada, the system can be configured to deprioritize or filter out alerts related to similarly named entities operating in unrelated regions.

Review workflows

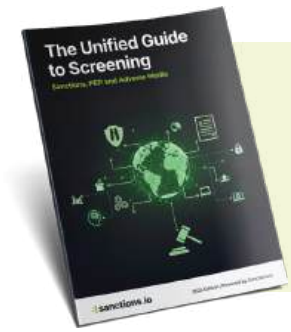
Technology must be supported by efficient human review workflows. When a potential match is flagged, analysts need a clear, standardized process for investigating and resolving the alert. Providing analysts with consolidated data and intuitive workflows allows them to determine quickly whether an alert is a true positive, ensuring that resources remain focused on genuine threats.



Part 4 - Operational & Commercial Execution

8. Integrating Screening Into procurement & platforms

For third-party risk management to be truly effective, it should be seamlessly integrated into the organization's existing operational workflows with minimal tool fragmentation - because tool fragmentation also increases operational and data privacy risk. Siloed compliance processes create friction and delay business operations, and also create risk in data integrity and increase the chances of data leaks.



See our Unified Guide to Screening to learn how to create a unified screening workflow across sanctions pep and adverse media screening with minimal tool fragmentation

Procurement workflows

Screening should be embedded directly into the procurement lifecycle. Before a contract is signed or a vendor is approved in the ERP system, necessary checks should already have been completed. By integrating screening into procurement, organizations ensure that compliance is a prerequisite for doing business rather than an afterthought.

Marketplace onboarding

For digital marketplaces, speed is critical. Integrating API-based screening directly into the onboarding flow allows platforms to vet new merchants or partners in milliseconds. This frictionless approach supports compliance without degrading the user experience, enabling the platform to scale securely.

API based screening and CRM based screening

Modern compliance relies on connectivity. API-based screening solutions allow organizations to connect risk screening directly to proprietary systems. Integrating screening into Customer Relationship Management (CRM) platforms such as Salesforce or HubSpot also ensures that sales and partnership teams have immediate visibility into the risk status of potential counterparties, aligning commercial goals with compliance requirements[9].

9. Demonstrating Compliance to Regulators & Auditors

A strong screening program helps organizations reduce risk, support safer business decisions, and maintain a clear record of the controls applied to third-party relationships. Regulators and auditors expect transparency, consistency, and accountability, so businesses should be able to show how screening is performed, how alerts are reviewed, and how decisions are documented over time.

Audit trail best practices

Every action taken within the screening program should be meticulously documented. Where automated systems are in place, they should generate comprehensive audit trails that record when a check was performed, which parameters were used, which results were obtained, and which subsequent actions were taken by analysts. Where screening is handled manually, organizations should still capture the same information through a clear and consistent review process. This record is essential for supporting internal oversight and demonstrating compliance during an audit or regulatory review.

Policy documentation

Organizations should maintain clear, current policy documentation that outlines their risk appetite, screening methodologies, and escalation procedures. This documentation serves as the blueprint for the compliance program and gives regulators a clear understanding of how third-party risk is managed.

Proportionality justification

Regulators expect compliance efforts to be proportional to the level of risk. Organizations should therefore be able to justify their screening approach, explaining why certain vendors are subject to enhanced due diligence while others require only standard checks. A well-documented risk segmentation strategy provides the necessary rationale for these decisions.

10. Third-Party Screening Checklist

To ensure your organization is prepared for the evolving risk landscape, use the following framework to evaluate current capabilities and identify priorities for improvement.

Maturity model

Maturity level	Characteristics
Basic	Manual checks at onboarding with no continuous monitoring
Developing	Automated onboarding checks, but high false positive rates and limited workflow maturity
Advanced	Risk-based segmentation with integration into procurement systems
Advanced	Continuous monitoring, stronger entity resolution, and comprehensive audit trails
Leading	Predictive risk analytics and seamless integration across business units

Internal self-assessment

Organizations should consider whether they have a documented risk appetite for third-party relationships, whether they screen for adverse media and PEP exposure alongside standard watchlists, whether the screening process is integrated into procurement or onboarding workflows, and whether there is a clear and auditable process for resolving alerts.

Implementation roadmap

The implementation journey typically begins with an assessment of current vendor data and identification of gaps in screening coverage. Organizations can use our sanctions.io Vendor Selection Guide to select the right vendor features aligned with their business risk profile. The next phase is design, where the organization develops a risk-based segmentation strategy and defines trigger events. Integration should then connect screening APIs to procurement, CRM, and ERP systems. Automation should follow for high-risk third parties through continuous monitoring, and optimization should refine matching logic to reduce false positives and improve analyst efficiency.

Conclusion

11. Why sanctions.io Is Your Ideal Partner

Building a strong third-party screening program requires more than basic verification. It requires a platform that can help your team identify sanctions exposure, assess reputational risk, reduce false positives, and operationalize screening across onboarding, procurement, and ongoing monitoring workflows.

Comprehensive Risk Coverage: sanctions.io helps businesses screen third parties against global sanctions lists, PEP data, criminal watchlists, and adverse media sources, giving compliance teams a broader and more actionable view of external risk.

Built for Operational Workflows: Whether you are screening vendors for procurement or evaluating distributors in higher-risk markets, sanctions.io seamlessly fits into your workflow with a 350ms response time API, Salesfoce/ HubSpot integration, SAP integration or simply use our portal.

Smarter Matching, Fewer Bottlenecks: Effective third-party screening depends on accuracy as much as coverage. sanctions.io is designed to handle entity name variation, transliteration issues, and common false-positive scenarios, using Machine Learning for contextual analysis to reduce false positives, so analysts can focus attention on the alerts that matter most.

Monitoring That Keeps Pace With Risk: Third-party risk does not stop at onboarding. With continuous monitoring and real-time alerts, sanctions.io helps organizations stay informed when a vendor's risk profile changes after the relationship has already begun.

Scalable for Growth: From lean compliance teams to large international operations, sanctions.io helps organizations build screening processes that are proportionate, auditable, and ready to scale as third-party ecosystems become more complex.

With sanctions.io, third-party screening becomes a practical control that supports both compliance and commercial growth.

12. Your Next Steps

1. Assess Your Current State. Use the checklist in Chapter 10 to evaluate how your organization currently screens vendors, suppliers, distributors, and partners. Identify where you rely on one-time checks, where monitoring gaps exist, and where false positives are slowing down decision-making.

Use our risk calculator to assess your current global risk exposure in just 3 minutes, for free. You receive a calibrated personal score from 0 to 100, an explanation of that score, and an overview of mandatory and recommended watchlists for your business.

2. Prioritize Your Highest-Risk Third Parties. Start by reviewing the counterparties that create the greatest exposure, such as cross-border partners, intermediaries, and suppliers operating in higher-risk jurisdictions. Apply stronger screening, clearer escalation rules, and ongoing monitoring where the risk is most material.

3. Assessing vendors. Access our Vendor Selection Guide to understand the features that matter most when choosing a screening partner and find the right fit for your business.

With sanctions.io, you can build a third-party screening program that is faster, more consistent, and better aligned to today's sanctions and reputational risk environment.

Prefer to chat to someone about how your compliance process can be transformed from inefficient to simple, scalable and unified? Talk to one of our experts today.

Book a call

Sources

[1] Office of Foreign Assets Control (OFAC). Sanctions Compliance Guidance. (2024).

[2] European Commission. Restrictive measures (sanctions). (2024).

[3] sanctions.io. The SaaS Compliance Playbook. (2025).

[4] Financial Action Task Force (FATF). Concealment of Beneficial Ownership. (2024).

[5] Stripe. Know Your Business (KYB): A Guide for Businesses. (2026).

[6] sanctions.io. What Is Adverse Media Screening? (2025).

[7] Financial Action Task Force (FATF). Politically Exposed Persons (Recommendations 12 and 22). (2013).

[8] sanctions.io. Screening vs Monitoring in Sanctions, PEP, and Adverse Media. (2026)

[9] sanctions.io. Streamlining Compliance: The Complete Guide to Our Salesforce Integration. (2025).