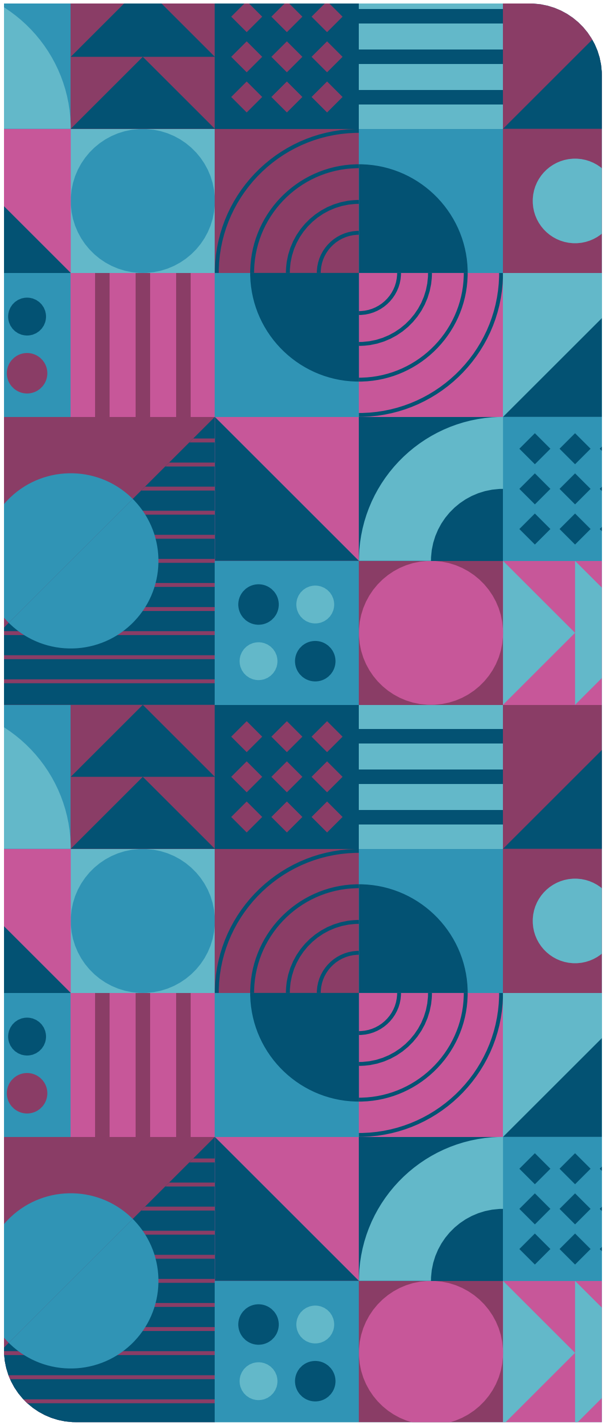
dun & bradstreet

EBOOK

How to Create an Effective Third-Party Risk Management Policy



Contents

PART I

PART II

PART III

PART I

What Is a Third-Party Risk Policy, and Why Do I Need It?

"No man is an island" — we've all heard that famous line of 17th-century poetry. The same is true for businesses and other organizations. It's virtually impossible for today's organizations to operate as "islands," without connections to third parties, if they intend to function on a basic level much less grow and thrive. Whether you're a financial institution, a CPG company, or a nonprofit, working with third parties such as vendors and suppliers is essential to meet strategic objectives.

That said, doing business with third parties carries inherent risks that could potentially outweigh the benefits of these relationships — and these risks are continuing to intensify in the current business climate of increasing complexity, regulatory expansion, and cyber and fraud threats.

To guard against these risks, mature organizations develop and utilize a third-party risk management policy. This policy provides standardized guidance for evaluating specified risk factors and determining whether the third party is an acceptable partner — one that will contribute to the business's growth and operational efficiency without causing damage to its reputation or profitability.

What is a third-party risk policy?

This policy serves as the basis for a third-party risk management framework that ideally applies to the whole business — not just the compliance department. Since it's likely that every part of the business will, at one time or another, want to work with a third party to obtain needed goods or services, this framework needs to be part of the infrastructure that supports and safeguards the entire business against external risks.

At the same time, the policy is a necessary component of an active due diligence process in which third parties are screened, assessed, and evaluated to gain an understanding of the risks they may present to the business. Those risks may be driven by regulatory requirements, or by the need to avoid relationships with entities that have been sanctioned or are involved in corruption, such as bribery or money laundering. Or they may be driven by escalating risks from cybercrime, business-to-business fraud, and emerging technologies, such as generative artificial intelligence (AI).

Simplistically, the policy functions like a handbook that sets defined thresholds of risk that dictate who a company should and shouldn't work with. It helps the business answer the foundational questions: What risks are we concerned about? Why are we concerned about them? And the policy then provides direction on which aspects of third parties to examine to see if those risks are present.

Why does compliance need this?

A third-party risk policy isn't something that exists just for the benefit of the compliance team. Third-party risk is a larger business risk that spans all teams that work with external companies and individuals. There are many risks that could have a disruptive impact on the company if not detected and mitigated. For example, companies that fail to comply with critical laws and regulations have been required to pay the U.S. Securities and Exchange Commission (SEC) billions of dollars in penalties to resolve Foreign Corrupt Practices Act (FCPA) violations that originated with third parties. Similar enforcement oversight exists in other markets across a broad range of regulations, including data protection regulations. And that's just the money; the cost to a business's reputation from the resulting press coverage and loss of public trust can be the final blow that shuts the business down permanently.

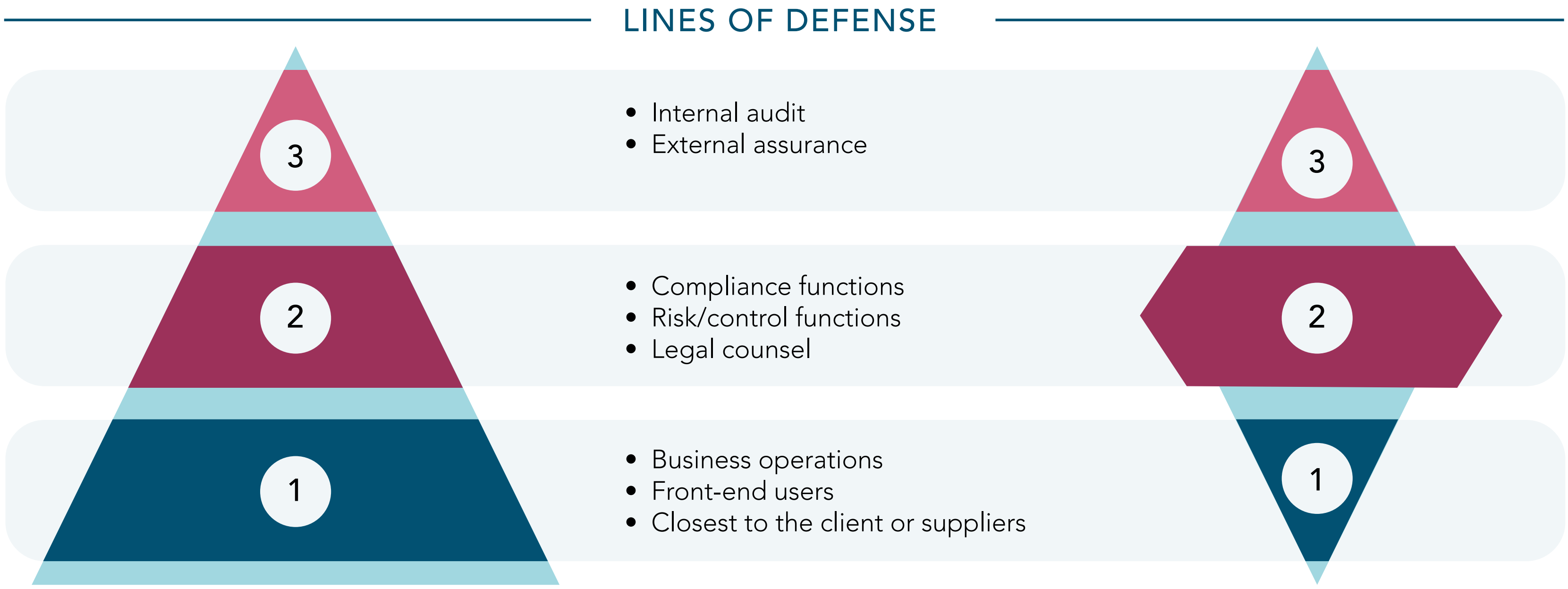
What does it mean to "have" a third-party risk policy?

There's a surprising degree of variation in how companies create and use these policies. In some organizations they may not even be written down. Or they may exist as a set of slides or in a Word document that's used only by a specific group of professionals within and adjacent to the compliance team. But this is not a best practice and can actually escalate the degree of risk the company faces from relationships with third parties.

Where the compliance team is specifically concerned, the third-party risk policy can help address a common structural problem with a business's "lines of defense" (LOD) — the people or teams that interface with external parties and (should) play a primary role in assessing the risks those parties might pose to the business.

This diagram shows how the lines of defense should ideally be organized:

But often the lines of defense function more like this:



LINES OF DEFENSE

- Internal audit
- External assurance

- Compliance functions
- Risk/control functions
- Legal counsel

- Business operations
- Front-end users
- Closest to the client or suppliers

This is what the third-party risk management process can look like in a business that's operating without a formal policy. The functions that are closest to the vendors, suppliers, and other third parties are not equipped with the knowledge or the guidance — or the technology solutions, but we'll get to that shortly — to perform risk assessment or mitigation processes. So for lack of a better alternative, this responsibility ends up being passed over to the second LOD and spread across different second-line functions, each focused on its own silo of responsibility. **Each and every time, for potentially hundreds or even thousands of third-party engagements**.

Creating and operationalizing a third-party risk policy can reduce that bulge at the second level and redistribute responsibility so that the second LOD can focus on the cases where its specialized expertise has the most value — the gray areas or edge cases that can't be easily adjudicated within the parameters of the policy. Meanwhile, the first LOD gains clarity around the business's risk appetite with a set of guidelines and procedures that enable those teams to make sound decisions about relationships and interactions with external parties.

Another significant benefit of a third-party risk policy is that it's an important requirement for automating the third-party risk management process. The policy enables you to implement technology solutions that allow users to monitor third-party compliance risk according to a defined set of standards for your organization. These solutions typically enable automated screening workflows configurable to your policies and your definition of material risk. So if you're seriously interested in improving operational efficiency and compliance defensibility through increased automation, you need to make sure that you've got a third-party risk policy as a necessary first step.

> If you're seriously interested in improving operational efficiency and compliance defensibility through increased automation, you need to make sure that you've got a third-party risk policy as a necessary first step.

Who else uses the policy?

Technically, all business units, lines, and departments are involved in third-party risk management, working with risk subject matter experts (SMEs) during the due diligence and risk assessment phase. But those risk SMEs are the primary stakeholders for the risk policy itself. They are mainly responsible for creating the policy by determining which risks are most material to the business; designing the process by which entities are screened and assessed; and selecting, implementing, and using the technology solutions and systems that will support screening, onboarding, and monitoring those entities.

What are the risks of not having a third-party risk policy?

Besides all the third-party risks that might slip through the cracks and cause damage to your business, there are more than a few downsides to not operating with a formal policy. We already mentioned one: creating a roadblock to compliance automation. Having a third-party risk policy is a prerequisite for implementing intelligent compliance solutions with policy-led workflows that analyze third-party data to perform risk assessments.

Another internal risk involves the need to standardize third-party risk management throughout the business. A formal third-party risk policy establishes a consistent set of procedures, assessment criteria, and risk evaluation methodologies. This helps to prevent an ad hoc approach for each vendor or partner as well as silos, duplication, and inconsistencies across functions. Without the policy, you can't really put a consistent third-party risk management framework in place. This would heighten the risk of ambiguity and inefficiency in assessing and monitoring third parties.

Disparities in risk evaluation, where different stakeholders are applying different levels of scrutiny than others to different third parties, may result in errors and missed opportunities that ultimately do harm to the business. The awareness that this could happen, or is actively happening, often contributes to the bulge we saw earlier at the second LOD where every aspect of third-party assessment comes to compliance and its close associates.

In addition to compliance, procurement, and legal, these functions may also be active users of the third-party risk policy:

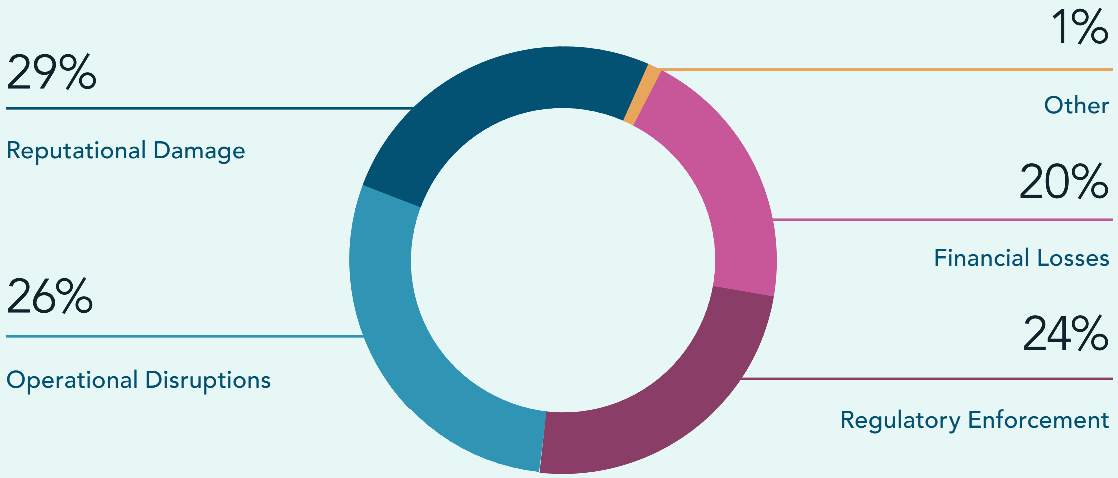
INFORMATION SECURITY
to ensure that third parties have adequate policies and processes in place addressing cybersecurity and improper use of systems and data

BUSINESS CONTINUITY
to ensure that third parties have systems and processes in place to continue providing goods or services even if they experience a critical risk event

FINANCE
to ensure that third parties can fulfill financial obligations that will allow them to continue operating and providing goods or services to customers

INSURANCE
to ensure that third parties have adequate protection from adverse events that could pose a variety of risks (operational, reputational, financial) to their customers

WHAT ARE YOU MOST CONCERNED ABOUT IF YOUR COMPLIANCE TEAM IS NOT EFFECTIVELY MANAGING RISK?

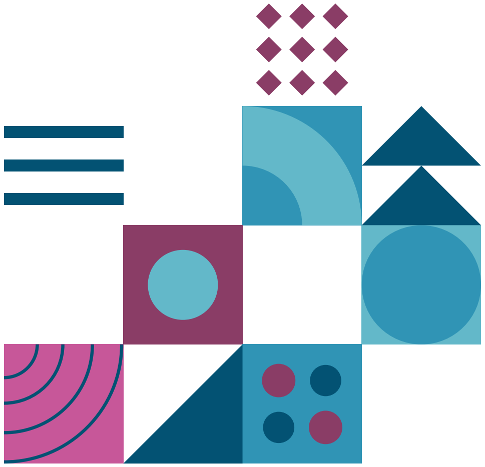


Source: "Top TPRM Priorities in 2023," a *Compliance Week* eBook sponsored by Dun & Bradstreet

And then there's the issue of how the compliance function is viewed by the rest of the business — in particular, by the organization's leadership. A well-structured third-party risk policy helps compliance to be regarded as a value creator rather than a cost center. It's true that it can be hard to demonstrate the concept that various risks have been avoided because the policy is in place; the procurement team often runs into a similar challenge trying to get credit for cost avoidance in contrast to cost savings, which are tangible and measurable.

Ultimately, however, a robust third-party risk policy can gain the compliance team recognition for achievements that are both tangible and intangible:

- The company forms relationships only with reliable, trustworthy partners, which elevates the trust the company itself receives from customers and external stakeholders.
- Adverse legal and financial impacts resulting from undetected third-party risks are minimized — thus, fewer lawsuits, regulatory penalties, and unexpected expenses.
- The process of screening, onboarding, and monitoring third parties — particularly when a compliance automation solution is utilized — becomes more streamlined and efficient, reducing administrative overhead and freeing up resources for more strategic activities.



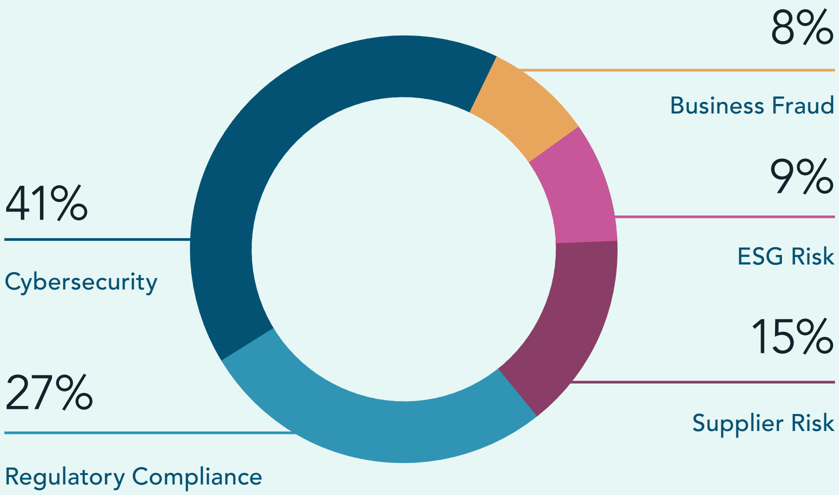
PART II

Creating the Policy: How Do I Get Started?

Determining pertinent risks and proportionate risk levels

The first step toward putting a third-party risk policy in place is assessing different types of risk and determining which ones are the most pertinent.

WHAT ARE YOUR TOP THIRD-PARTY RISK PRIORITIES TODAY?



Source: "Top TPRM Priorities in 2023," a *Compliance Week* eBook sponsored by Dun & Bradstreet

Some definitions and examples of the most prevalent third-party risk types:

Risk Type	Definition	Examples		
Cyber Risk	Potential harm or loss that can result from a breach or compromise of an organization's digital assets, information systems, or networks	• Data breaches • Ransomware attacks • Phishing	• Zero-day exploits (targeted vulnerabilities in software or hardware)	
Regulatory Compliance Risk	Potential exposure an organization faces due to its failure to adhere to relevant laws, regulations, and industry standards that govern its operations and activities	• EU and UK General Data Protection Regulations (EU GDPR and UK GDPR) and China Personal Information Protection Law (PIPL) • Anti-money laundering (AML) regulations, such as the EU AML Directive	• Foreign Account Tax Compliance Act (FATCA) • Sarbanes-Oxley Act (SOX) • U.S. Foreign Corrupt Practices Act (FCPA) and UK Bribery Act	• Trade sanctions and export control laws • ESG regulations such as the UK Modern Slavery Act and Norway Transparency Act
Supplier Risk	Potential disruptions, problems, or challenges that can arise from using external suppliers and vendors to provide goods, services, or components necessary for operations	• Supply chain disruptions • Quality and performance risk	• Geopolitical risk • Production capacity constraints	• Single-source dependency
Sustainability Risk	Potential adverse impacts on a company's performance, reputation, or long-term sustainability related to its environmental, social, and governance (ESG) practices	**ENVIRONMENTAL RISKS** • Climate change • Resource scarcity • Environmental regulations	**SOCIAL RISKS** • Labor practices • Human rights violations • Diversity and inclusion	**GOVERNANCE RISKS** • Director conflicts of interest • Executive compensation • Ethical (mis)conduct (including fraud, corruption, and insider trading)
Financial Risk	Potential adverse consequences or losses due to financial instability or mismanagement	• Insolvency • Defaults on financial obligations	• Contractual violations • Insurance liability claims • Market fluctuations	
Fraud Risk	Potential threats or vulnerabilities that a business faces from deceptive and illegal practices carried out by individuals or external entities with the goal of financial gain or causing harm to the business	• Vendor fraud — kickbacks, overbilling • Asset misappropriation	• Online payment/credit card fraud • Identity theft and synthetic identity fraud	• Contract and procurement fraud — bid rigging, unfulfilled contracts

This is not an exhaustive list of different risk types. In a business climate of heightened risk, risk prioritization should start with consideration of your business's specific objectives and the adverse events that could jeopardize them. Additional areas of risk may need to be explicitly covered in your risk policy — such as geopolitical risk, operational risk, or reputational risk.

The next stage of the process involves defining your risk appetite — the level of risk your organization or business is willing to accept or tolerate in the context of its third-party relationships. Risk appetite is typically determined through a combination of factors, including:

- The organization's goals and objectives
- Its willingness to take on risk to achieve those objectives
- Its capacity to absorb losses
- Applicable regulatory requirements
- Expectations from stakeholders, including shareholders, customers, and employees

Risk appetite is not a one-size-fits-all concept — it has to be tailored and *proportionate* to the business. Proportionality is largely influenced by the type of business you have; businesses in different industries will have different risk factors and regulations that will be more or less material to its risk tolerance. For example:

Type of Business	Financial Institution	Manufacturer/Exporter	Importer/Retailer
Higher Likelihood of Proportionality	• AML • Counterterrorist Financing (CTF) • Know-Your-Customer (KYC) • Fraud • Sanctions	• Bribery and Corruption • Sanctions • Embargoes • Sustainability	• Modern Slavery • Human Trafficking • Data Protection • Sustainability • Supply Chain

> *Risk appetite is not a one-size-fits-all concept — it has to be tailored and proportionate to the business.*

Entity assessment fundamentals

Once you have established which types of risk are most material to your business, and what levels of tolerance the business will have for various risk factors, the next step is to capture the standardized process that will be used to evaluate third parties. The goal is to be able to build a risk profile of the entity that will ultimately be used to make decisions about whether and how to establish a relationship with that entity.

The policy should contain an assessment framework that operates on a foundation of comprehensive firmographic, operational, and financial third-party data. The final framework your business adopts will be influenced by your business's specific capabilities, goals, and priorities. But here is a good general checklist to use as a starting point for your policy:

Is the entity LEGITIMATE?

- Confirm its identity
- Check business registrations
- Establish directors/managers
- Understand its corporate structure
- Determine ownership and Ultimate Beneficial Owners (UBO)

Is the entity STABLE?

- Look at financial health factors
- Look at the management team's track record
- Look at exposure — industry/sector risk, country/location risk, association-with-government risk
- Look at potential vulnerabilities — size/age of the business, governance programs, cybersecurity, data protection incidents and breaches

Is the entity HONEST?

- Screen management and beneficial owners
- Probe into connections to PEPs (politically exposed persons) or watchlists
- Check for regulatory enforcement actions
- Research adverse media, accreditations, certifications, and licenses

Incorporating these three assessment pillars into the risk policy helps ensure that all stakeholders that use the policy — particularly those in the first and second LOD — will follow a uniform and, importantly, *objective* process that is both thorough and balanced. It's important to note that the policy may also include exceptions based on the level of criticality associated with the entity and the goods or services it provides. They may also be extended to certain entities where the nature or duration of the entity's relationship with your business creates a presumption of minimal risk.

Documenting exceptions within the policy helps eliminate ambiguity, especially in the inevitable case of staff turnover. It also contributes to acceptance and adoption by communicating a practical and reasonable risk culture that promotes business growth, rather than constrains it.

PART III

Now that I Have a Third-Party Risk Policy, What Happens Next?

Operationalizing the policy

As with any other type of new policy impacting business processes and goals, the third-party risk policy has to be formally rolled out if you want your colleagues to comply with it. A structured approach will help ensure that it is effectively communicated, implemented, and integrated into day-to-day operations.

LEADERSHIP BUY-IN AND SUPPORT

Ensure that senior leadership understands and supports the importance of the new policy. Obtain their commitment through approvals initiated through your organization's policy governance process. You'll need their commitment to allocate necessary resources and provide guidance on implementation.

CROSS-FUNCTIONAL TEAM

Establish a dedicated team with representatives from, but not limited to, the first and second LODs, including compliance, legal, procurement, IT, and enterprise risk management (ERM) to oversee implementation and ongoing management. Consider formalizing the role of this team through your compliance and/or risk governance processes.

COMMUNICATION AND TRAINING

Develop a communication plan to inform employees, third parties, and key stakeholders about the new policy and its requirements. Create a training program for employees involved in third-party relationships to help them understand their role and responsibilities in following the policy. The human resources team should be consulted for guidance and assistance.

DATA, TECHNOLOGY, AND TOOLS

Research technology solutions that will help you fully realize the benefits of a third-party risk policy. Learn about newer options that leverage third-party data and automation, layering in artificial intelligence (AI) and machine learning algorithms to identify patterns, anomalies, and potential risks more effectively.

More about automated, policy-led compliance solutions

Many compliance and risk management teams use automation to maximize their resources and minimize the manual labor involved in screening and monitoring third parties. In a global business environment of persistent uncertainty, compliance teams are hearing that they have to "do more with less" and step up the critical due diligence processes that protect the business. Automated solutions help to turn these traditionally lengthy and tedious processes into a modern, streamlined, and proactive method of ongoing risk mitigation.

All elements of your third-party risk policy — the definitions of material risk, levels of tolerance of specific risk factors, the prescribed steps for entity screening and assessment — can be configured in the workflows of these solutions. The workflows can perform tasks such as matching thresholds, risk categorization, risk scoring, and scheduling of screening frequency. Here's how they typically work:

01 Data Gathering

Data is aggregated from various sources including public records, regulatory lists, and government databases. Third-party data providers can help ensure that the data used for risk assessment is clean, comprehensive, standardized, and current. The data should encompass lists of sanctioned individuals and entities, politically exposed persons (PEPs), adverse media mentions, terrorist watchlists, and other relevant information.

02 Screening

A screening request is initiated. The system applies the configured policies and rules to the data and conducts real-time or batch screening, obtaining the requested information to help verify details such as date of incorporation, corporate linkages, beneficial ownership, and applicable sanctions or watchlists.

03 Matching & Approvals

The system looks for potential matches or hits. Matches are assigned a risk score based on severity and relevance of the match to the third-party risk policy. The system applies rules to automatically approve or reject entities, or refer them to team members for further investigation and adjudication if necessary.

04 Monitoring

Entities that have previously been approved can be continuously monitored according to the frequency specified in the policy to identify any relevant changes in their risk profile. Changes can then trigger alerts for any factors that exceed the configured thresholds or risk scores.

05 Reporting

The system can include reporting capabilities that follow the requirements of the risk policy, such as documenting screening results, actions taken, and audit trails. It can maintain detailed audit logs and records of screening activities, investigations, and resolutions.

06 Policy Updates

Users of the solution can customize and update risk and compliance policies and rules as regulations change or business requirements evolve (see next section).

Maintaining the policy

We've provided an extensive definition of what a third-party risk policy is, but one thing that it's not is a document that you create once, put on the shelf, and never revisit again.

Regulations change frequently, and third-party risks are continuously evolving; new ones emerge while existing ones may recede. As an example, the onset of the Russia-Ukraine war triggered revisions of many organizations' policies because of the new sanctions that were enacted. Another example: Germany's new Supply Chain Due Diligence Act, which is imposing extensive regulations related to protection of human rights throughout supply chains. And another: the obligations under data-related laws to ensure that you've assessed your third parties' ability to uphold regulatory requirements that apply to any data processing they do for you.

So it's advisable for the policy to include standard review periods for all of its components — risk materiality, risk tolerances, the entity screening and assessment process steps — to ensure the continuity of effective risk mitigation. It's important to involve the subject matter experts for each relevant area, such as privacy and data protection, anti-bribery/anti-corruption (ABAC), and economic sanctions, to provide standards for handling and escalation of the reviews of the parts of the policy they know best.

Many organizations conduct workshops that bring these SMEs together to revisit the current landscape of risk and regulation, and to agree on needed changes to the policy or the processes it encompasses. Additional stakeholders in other areas of the business can, and usually should, be consulted for feedback on areas that they see as needing improvement. The third LOD — the internal and external auditors and providers of independent assurance of the first and second LODs — also plays an important role in highlighting possible deficiencies in the policy. They assess whether the policy is being implemented correctly throughout the business and may conduct testing to gauge its effectiveness.

FINAL THOUGHTS

Shaping an organizational risk culture

An effective third-party risk policy serves as the touchstone of an organization's risk culture. By clearly outlining expectations and procedures for managing external relationships, it sets the precedent for accountability, awareness, and proactive risk management across all functions. It encourages employees at all levels to take ownership of third-party risks, promoting a sense of collective responsibility for safeguarding the organization's interests.

This elevated risk consciousness not only strengthens risk identification and mitigation efforts but also aligns the entire workforce with the company's risk management objectives. Ultimately, an effective third-party risk policy instills a culture of vigilance and risk awareness, which is fundamental for long-term resilience and success.

Dun & Bradstreet provides industry-leading data and tools to enable compliance teams to increase efficiency, manage complexity, and modernize third-party risk management.

To learn more, visit:
dnb.com/compliance

ABOUT DUN & BRADSTREET®

Dun & Bradstreet, a leading global provider of B2B data, insights and AI-driven platforms, helps organizations around the world grow and thrive. Dun & Bradstreet's Data Cloud fuels solutions and delivers insights that empower customers to grow revenue, increase margins, manage risk, and help stay compliant — even in changing times. Since 1841, companies of every size have relied on Dun & Bradstreet. Dun & Bradstreet is publicly traded on the New York Stock Exchange (NYSE: DNB).

The information provided is for suggestion purposes only and is based on best practices. Dun & Bradstreet is not liable for the outcome or results of specific programs or tactics undertaken based on your use of the information. Please contact an attorney or tax professional if you are in need of legal or tax advice.

dnb.com