TPRM

From Third Party Assessment to Third Party Risk Management

White paper by the Strategic Compliance Studies Committee of the French Compliance Society

FRENCH COMPLIANCE SOCIETY

TPRM

From Third Party Assessment to Third Party Risk Management

White paper by the Strategic Compliance Studies Committee of the French Compliance Society

FRENCH COMPLIANCE SOCIETY

IN PARTNERSHIP WITH

AFJE Les Juristes d'Entreprise

Forward

ÉVAL TIERS www.evaltiers.eu

VERDUN VERNIOLE AVOCATS

WARNING

This white paper was produced by compliance professionals based on their experience and reflections on the implementation of legal obligations to assess third parties and, more generally, on a Third Party Risk Management approach to meet these obligations. The analysis presented in this document does not prejudge the position of the legislator, regulator, or judge, nor that of Aramis Group and Hertz Corporation on this subject. This white paper should not be interpreted as legal advice and does not bind its authors or their respective companies or organizations.

AUTHORS

Stéphanie Corbière

Head of Legal and Compliance & Secretary of the Board, Aramis Group, Co-Head of the Legal Managers Commission and Co-Pilot of the AFJE AI Scientific Group, member of the Strategic Compliance Studies Committee

Camélia Gardot

Director of Compliance, Hertz Corporation, member of the Strategic Compliance Studies Committee

Franck Verdun

Attorney at Law, founder of Verdun Verniole avocats and Eval'tiers, member of the French Compliance Society

WITH THE PARTICIPATION OF

Carmen Briceno, Group Legal & Compliance Director at Raja, Head of the AFJE Compliance Commission

Catherine Delhaye-Kulich, Chief Ethics, Compliance and Data Protection Officer at Valeo Group

Isabelle Cadet, Senior Lecturer at IAE Paris-Sorbonne, Paris 1 Panthéon-Sorbonne University

Makeda Cardenas, Compliance Officer, La Poste Group

Ling Ho, Partner at Forward Global

Stéphanie Dominguez, Director, Actuo

Summary

Introduction

Third-party assessment is the process of gathering information about a partner in order to determine whether it is appropriate to enter into or continue a relationship with them.

The importance of the relationship between a company and its value chain and the third parties that comprise it (suppliers, service providers, customers) cannot be overstated. This relationship determines the company's ability to produce and sell its products and services. It therefore contributes to the company's ultimate goal of creating value. Therefore, managing value chain risks, including assessing third parties with whom the company plans to enter into a contractual relationship, is considered good management practice.

However, the very characteristics of the value chain make managing its risks complex:

- Large number of stakeholders: on the upstream side (suppliers, service providers), this volume can quickly become considerable. The third-party assessment process therefore requires the involvement of numerous contacts within the company, who are tasked with gathering information that is perceived as time-consuming and of little value. This is why third-party assessment obligations in compliance programs are often identified as the most difficult measure to implement. In the "*National Diagnosis of Anti-Corruption Measures in Companies 2024*," the French Anti-Corruption Agency (*AFA*) notes that "*companies encounter difficulties with the volume and diversity of third parties to be assessed, requiring significant resources. Companies do not always find the right tools for this procedure, particularly for gathering information that may be purely declarative and unreliable*[1]".

1. French Anti-Corruption Agency (AFA), *National Assessment of Anti-Corruption Measures in Companies,* 2024, available at diagnostic national entreprises 2024_AFA.pdf.

Value chain risk management must therefore focus on determining which third parties to assess and what due diligence procedures to follow in order to avoid excessive consumption of resources. The regulator, and in particular the *AFA*, clarifies this point in its recommendations: "*The nature and depth of the assessments to be carried out and the information to be collected are determined on the basis of the different homogeneous groups of third parties with comparable risk profiles, as identified by risk mapping. Thus, groups of third parties deemed to be low or no risk may not be subject to assessment or may be subject to a simplified assessment, while the highest-risk groups will require an in-depth assessment*[2]".

- Multiple internal interactions with third parties without centralized governance: within the company itself, employees may be in contact with the same third parties in the course of their respective duties without having an overall view of the third party and the risks associated with it. Value chain risk management must therefore provide comprehensive information on third parties identified as risky, regardless of the reason for entering into a relationship with them.

Value chain risk management must therefore focus on identifying risks arising from relationships with third parties that could have serious consequences for the company.

Two main categories of risk can impact the value chain. Firstly, **operational risks**, such as:

- lack of sufficient skills and resources, particularly financial, on the part of the third party to meet its contractual obligations;
- economic dependence on the third party that could lead to a reclassification of the contractual relationship, or conversely, strategic dependence on the servicesor resources provided by the third party;

2. AFA, *Recommendations of the French Anti-Corruption Agency to help legal entities prevent and detect corruption, influence peddling, conspiracy, illegal taking of interest, embezzlement of public funds, and favoritism* [online], Dec. 4, 2020, § 207.

- cyber risk linked to the technical non-compliance of the third-party service provider;
- reputational risk linked to ethical shortcomings, human rights' violations, or serious environmental damage caused by the third party that could impact theprincipal.

Secondly, **legal risks** resulting from failure to comply with legal obligations to assess third parties under various laws, in particular those relating to integrity, anti-money laundering, terrorist financing, human rights' violations, and those resulting from the outsourcing of personal data, may have an impact.

The multiplicity of risks associated with third-party relationships in the value chain requires the implementation of a comprehensive risk management approach known as third-party risk management (TPRM). Based on a risk-based approach, TPRM should enable companies to identify and assess both their major operational risks in the value chain and to meet the legal obligations to assess third parties to which they are subject. The purpose of TPRM is therefore to preserve and optimize value creation by the company, beyond simply ensuring legal compliance with the obligation to assess its third parties (I).

The TPRM approach facilitates the definition of a third-party assessment policy for the company. Based on a comprehensive mapping of risks in the value chain, this policy should enable the identification and assessment of risks associated with the categories of third parties to be assessed, and the definition of assessment procedures according to the risks identified. This holistic approach avoids redundant and time-consuming third-party assessment processes and thus prevents a lack of information sharing about third parties within the company itself.

The purpose of the third-party assessment policy is to make decisions about the relationship with the third party: approval of the relationship without restriction, approval with implementation of a treatment plan, or rejection of the third party, which may be permanent or temporary (II).

The third-party assessment policy must be effectively implemented within the company, which requires action and involvement on the part of company employees who deal with third parties. In addition, the process must be verifiable in order to ensure that the third-party assessment policy is being followed (III).

The process calls for digitization given the large number of internal stakeholders involved in third-party assessment (operational staff, compliance, management), the information to be collected from the third party or external databases, and then processed in order to make a decision to reject or approve (IV).

In July 2025, the *AFA* published for consultation a draft set of practical information sheets (hereinafter "*Practical Information Sheets*") on the implementation of a system for assessing third parties with regard to the risk of corruption within companies. (https://www.agence-francaise-anticorruption.gouv.fr/fr/lafa-lance-consultation-publique-jusquau-30-septembre-2025-sur-projet-fiches-pratiques-relatives)[3].

This publication specifically addresses the third-party assessment procedure provided for in Article 17 4° of the Sapin 2 law, and we will refer to it throughout this White Paper. The practical information sheets address topics common to a TPRM approach, such as governance of the procedure, assessment of the risks of the third party and the category to which it belongs, and the nature of the assessment procedures to be carried out.

3. *3. Draft Practical Information Sheets,* [online], July 2025.

I. Third Party Risk Management, an approach resulting from value chain risk management

The objective of Third Party Risk Management is to provide a process for assessing third parties in relation to overall value chain risk management. By identifying the vulnerabilities of stakeholders in the value chain, the company can implement measures to sustain and improve its value creation process (1). These risks may be inherent to the company and its stakeholders (2). They may also result from legal obligations requiring companies to implement specific *due diligence* measures (3).

1.1 The concept of the value chain and third parties

The concept of the value chain originated in strategic business management and the work carried out by Michael Porter in the 1980s[4]. The purpose of the value chain was to identify the different "*links*" in the company's activity in order to assess their contribution to the creation of final value in the company's offering. This exercise makes it possible to identify the activities that are crucial to value creation in order to optimize them and thus enable the company to provide an offering that is likely to create a competitive advantage (i.e., the offering that creates the most value for the customer compared to the competition).

4. PORTER, Michael E., *Competitive Advantage: Creating and Sustaining Superior Performance*, Free Press, New York, 1985, 557 p.

The concept of value chain is now used more broadly, particularly thanks to CSR. The Corporate Sustainability Reporting Directive (CSRD) defines the value chain as all "*activities, resources, and relationships related to the undertaking's business model and the external environment in which it operates (...) The value chain includes actors upstream and downstream from the undertaking. Actors upstream from the undertaking (e.g., suppliers) provide products or services that are used in the development of the undertaking's products or services. Entities downstream of the undertaking (e.g., distributors and customers) receive products or services from the undertaking (...)*" [5].

This concept is also similar to the concept of the supply chain, which is defined as "*The full range of activities or operations carried out by entities upstream of the undertaking, which provide products or services that are used in the development and production of the undertaking's own products or services. This includes upstream entities with which the undertaking has a direct relationship (often referred to as a first-tier supplier) and entities with which the undertaking has an indirect business relationship*" [6].

Thus, the definition of the value chain formulated by the CSRD enables the company to define the scope within which its risk management, including third party risk management, can operate.

- **The concept of third parties:**

The *AFA* defines a third party as any person outside the company with whom it has, or wishes to have, a relationship [7]. The *AFA*'s concept of a third party covers persons with whom the company has contractual relations, but also all those with whom it plans to establish a relationship, regardless of its legal nature. A third party may therefore be a natural person or a legal entity governed by private or public law.

5. Annex 2, *Commission Delegated Regulation (EU) 2023/2772 of July 31, 2023 supplementing Directive (EU) 2022/2464 of the European Parliament and of the Council as regards sustainability reporting standards,* Official Journal of the European Union, October 22, 2023, pp. 1-46.

6. *Ibid.* and Regulation (EU) 2023/1115 on the making available on the Union market and the export from the Union of certain commodities and products associated with deforestation and forest degradation.

7. AFA, *Practical Information Sheets,* July 2025.

The *AFA* does not define legal or economic criteria for defining or identifying third parties to the company.

This broad definition of third parties encourages companies to identify all persons who interact with them in order to apply a risk-based approach to defining the third parties to be assessed, based on the risk mapping of the anti-corruption compliance program.

Financial risk	The third party does not have (or no longer has, during the commitment period) the financial resources to meet its contractual obligations. This dimension also incorporates credit management into the customer relationship.
Risk of dependency	The principal may be dependent on its co-contractor because the latter is the only party capable of providing rare skills or resources that are essential to the performance of its offer. A co-contractor may be economically dependent on the principal, which may lead to a risk of legal reclassification of the relationship or compensation for abuse of economic dependence.
Risk related to geographical/ political factors	The geographical area where the counterparty is located may give rise to specific risks: absence, instability, or inconsistency of applicable regulations, social or political events making it impossible to perform obligations, etc. It should be noted that the liability of subsidiaries operating in these areas may engage that of their parent company under specific legislation: duty of care, UK Bribery Act* etc.
Reputational risk associated with subcontracting	The co-contractor may use a chain of subcontractors that are not properly identified, which could give rise to reputational risk. This is known as "*fourth party*," i.e., the supplier of the first-tier subcontractor.
Risk linked to the low compliance/ legal maturity of the third party	The co-contractor may have low legal maturity/compliance, which could give rise to reputational or legal risks for the principal.

* UK Bribery Act 2010, Law of April 8, 2010, United Kingdom, Section 7 "*Failure to Prevent Bribery*," available at Bribery Act 2010.

Risk associated with outsourcing personal data processing operations	The company must ensure that any third party with access to the personal data it processes complies with its obligations as a data processor in terms of transparency, data limitation and traceability, data protection, and customer advice and assistance. These obligations are implemented through a contractual mechanism, but the data controller may also use a questionnaire to ask the processor about the technical and organizational measures implemented to meet them.
IT or cyber risks related to the relationship between the company and third parties	The concept of value chain as defined by the CSRD reflects the concept "*extended enterprise*," which translates into the integration of third parties through a digital channel. While this integration is a source of value creation (speed of information exchange and processing), it can also be a source of operational risks linked to a lack of IT or cyber maturity on the part of third parties. The ISO/IEC 27001 standard is a reference framework for information security management systems (ISMS) that measures the level of maturity of the information system of the third party that will be interacting with that of the company's system*. A gap analysis between the ISO recommendations 27001 and the existing third-party IS will enable risks to be identified and addressed.

* CNIL, *Practical Guide to the GDPR, Personal Data Security, 2024;* ENISA, *Technical Implementation Guidance on Cybersecurity Risk Management Measures* [online], June 2025, pp. 21-3.

1.2 Risks inherent in the value chain

The risk management process applied to the value chain therefore makes it possible to identify sensitive categories of third parties based on their position and contribution to the value chain (strategic suppliers, etc.) and, through an appropriate assessment process within these categories, to identify the vulnerability of the third parties that comprise it.

1.3 Legal obligations to assess third parties

The assessment of third parties makes it possible to identify risks that may impact the value chain and the company and that may also have negative consequences on public order itself.

Thus, public authorities have gradually implemented legislation aimed at compelling companies to assess their third parties in order to identify risks of violations that could seriously disrupt public order and to comply with state policies on international sanctions.
A distinction can be made between general obligations (applying to all companies above a certain threshold in terms of workforce or turnover) and obligations related to the nature of the operations carried out, which are therefore sector-specific.

1.3.1 General third-party assessment obligations

1.3.1.1 **Anti-corruption obligations**

- Article 17 4° of the French law known as Sapin 2 requires the implementation of third party assessment procedures in connection with a corruption risk exposure map in order to assess the integrity and reputation of third parties before entering into a commercial relationship. These procedures may include checks on their history, ownership structure, compliance with anti-corruption laws, and reputation in the sector. The French Anti-Corruption Authority (*AFA*) has published draft Practical Information Sheets to help companies implement this obligation [8].

- The UK Bribery Act 2010 [9] is British legislation that aims to combat corruption in the United Kingdom and abroad. The text calls on companies to implement adequate measures to combat corruption, which involves a process of assessing risks related to third parties. This law has now been strengthened by the creation of a "f*ailure to prevent fraud*" offense under the Economic Crime and Corporate Transparency Act (ECCTA). Companies are required to assess their third parties and exercise reasonable diligence to prevent fraud and malpractice committed by their third parties [10].

8. AFA, *op. cit.*
9. UK Bribery Act, *op. cit.*
10. The offense of "f*ailure to prevent fraud*" established by the Economic Crime and Corporate Transparency Act 2023 came into force on September 1, 2025 (United Kingdom, *Commencement Regulations 2025*, S.I. 2025/100).

• The Foreign Corrupt Practices Act[11] (FCPA) is a US law that prohibits companies and individuals from engaging in acts of corruption vis-à-vis foreign officials for the purpose of obtaining or retaining business. The U.S. Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) have provided guidance on best practices for complying with the FCPA, including assessing third-party risks[12].

• The Brazilian Anti-Corruption Law[13] (Law No. 12,846/2013 or *Lei Anti-corrupção*) imposes responsibilities on companies in terms of corruption prevention, which implicitly includes assessing risks related to third parties. Companies are thus encouraged to conduct *due diligence* on third parties with whom they do business, particularly those that present an increased risk of corruption. This may include checks on the reputation, background, and business practices of third parties.

It should be noted that certain laws (e.g., the FCPA and UK Bribery Act) have extraterritorial reach. They may apply to foreign companies based on criteria such as the location of the acts, the nationality of the executives, or, in the case of the FCPA, listing on a US stock exchange or payment in US dollars.

1.3.1.2 Obligations regarding vigilance in the protection of the environment and human rights

• The French Duty of Vigilance Act[14], enacted in 2017, requires large companies to implement a vigilance plan to identify and prevent risks of human rights' and fundamental freedoms' violations, serious environmental damage, and corruption resulting from their activities and those of their subsidiaries, subcontractors, and suppliers.

11. Foreign Corrupt Practices Act of 1977.
12. U.S. Department of Justice et Securities and Exchange Commission. *A Resource Guide to the U.S. Foreign Corrupt Practices Act,* 2nd ed., 2020.
13. *Lei Anticorrupçao,* August 1, 2013.
14. Law No. 2017-399 of March 27, 2017 on the duty of care of parent companies and contracting companies.

In this context, companies must implement procedures to assess the situation of suppliers and subcontractors with regard to respect for human rights and the environment. This may include audits, questionnaires, and on-site checks.

- The German Supply Chain Act[15], known as the *Lieferkettengesetz*, imposes specific obligations on companies regarding the assessment of human rights and environmental risks in their supply chains. The text includes provisions that require companies to examine and manage the risks associated with their business partners, including suppliers and subcontractors.

- Norwegian law, in the Norwegian Transparency Act or *Åpenhetsloven*, stipulates a *due diligence* obligation to identify, prevent, and mitigate actual or potential violations of human rights and working conditions in the value chain. This obligation applies to all of the company's partners, including indirect suppliers. Companies are therefore required to publish an annual report to demonstrate their compliance.

- Dutch law, in *the Wet Zorgplicht Kinderarbeid* or Child Labor Due Diligence Act[16], requires companies to prevent the use of child labor in their supply chains. They are required to check whether there is a risk of child labor. When a risk is identified, they must draw up an action plan and publish a statement on the measures taken. These obligations apply to all companies registered in the Netherlands, as well as to all companies operating in the Dutch market, at least twice a year, unless they are expressly excluded by law. However, although adopted in 2019, the law is not yet applicable and its date of entry into force is not known. A bill inspired by the Corporate Sustainability Due Diligence Directive, called *Wet zorgplicht mensenrechten en milieu*[17],plans to broaden its scope by introducing an environmental *due diligence* obligation.

15. Supply Chain Due Diligence Act, July 22, 2021.
16. *Child Labor Duty of Care Act,* Parliamentary Document 34506-A, May 14, 2019.
17. Human Rights and Environment Duty of Care Act, 2024.

• The Corporate Sustainability Due Diligence Directive (CSDDD)[18] is a European directive whose scope and obligations are currently being discussed as part of the European Omnibus process. The CSDDD imposes due diligence obligations on companies, depending on their thresholds, with regard to the human rights and environmental impacts of actors in their supply chains. These due diligence measures aim to identify, prevent, mitigate, and report on negative impacts on human rights and the environment in their value chains, including those related to the activities of their third parties (suppliers, subcontractors, etc.).

1.3.1.3 Identification and monitoring of international sanctions

International sanctions are coercive measures taken by one or more countries, or by international organizations such as the United Nations or the European Union, to compel a state, entity, or individuals to change their behavior or policy. It should be noted that the *AFJE* compliance committee has published a video on international sanctions[19].

With regard to companies, the existence of sanctions must be verified for the legal entity, its shareholders (excluding listed companies) and its beneficial owners. (See the definition of the concept in: EU Best Practices for the effective implementation of restrictive measures. https://www.skadden.com/-/media/files/publications/2024/07/ eus-14th-sanctions-package/best-practices1.pdf). Continuous monitoring must be carried out to check for any changes in status during the course of the business relationship. The existence of sanctions can generally be verified in registers such as the asset freeze register[20] for sanctions measures taken

18. *Directive (EU) 2024/1760 of the European Parliament and of the Council of June 13, 2024 on corporate sustainability due diligence.*

19. https://www.afje.org/ressources/compliance-video-sur-les-questions-relatives-aux-sanctions-internationales--494.

20. https://gels-avoirs.dgtresor.gouv.fr/List

by France, the EU, and the UN, and on the OFAC website for those taken by the United States [21]. The law firm NOVLAW also provides a website offering free access to international sanctions taken by France, the EU, the United Kingdom, and the United States [22].

1.3.1.4 The duty of vigilance with regard to undeclared work

In France, the duty of care of the principal provided for in Article L. 8222-1 et seq. of the Labor Code [23] requires companies that use subcontractors for contracts worth more than €5,000 excluding VAT to collect documents proving that their subcontractors have complied with their reporting obligations, namely:

- a *Kbis* extract;
- a certificate of compliance issued by the Union for the Collection of Social Security Contributions and Family Allowances (*URSSAF*) or by the Agricultural Social Mutual Fund (*MSA*), where applicable;
- a certificate of tax compliance;
- a list of foreign workers.

Checks must be carried out every six months until the end of the contract.

In the event of failure to comply with this obligation, the principal may be held jointly and severally liable for the undeclared work alleged against its subcontractor and may then be ordered to repay its tax and social security debts, pay fines, and be permanently excluded from participating in public procurement contracts.

21. https://sanctionssearch.ofac.treas.gov/
22. https://sanctions.fr/
23. Article L.8222-1 et seq. of the *Labor Code*.

1.3.1.5 Assessment of measures designed to ensure the protection of personal data

The General Data Protection Regulation (GDPR)[24] requires data controllers processing data belonging to EU residents to ensure that subcontractors involved in their processing operations comply with personal data protection standards[25].

The checks to be carried out include, in particular, checking the third party's certifications, analyzing its information security policy and incident management procedure, and auditing its data management practices to verify its compliance with the provisions of the GDPR (data retention period[26], processing register[27], etc.). The data controller must also check that the processor does not use other processors and ensure that this is done in accordance with the GDPR[28]. Questionnaires may be used to collect this information.

These checks and the subcontractor's services must be governed by contractual clauses, which may include a prohibition on further subcontracting[29].

1.3.2 Sector-specific obligations to assess third parties

1.3.2.1 Assessment of money laundering and terrorist financing risks (AML-CFT)

The AML-CFT legislation requires companies in the financial sector and certain service providers exposed to money laundering risks (Articles L561-1 to L561-50 of the Monetary and Financial Code) to identify their customers by collecting information such as full name, date of birth, address, and contact details. For companies, the taxpayer must also collect details on shareholders and

24. *Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).*

25. *Ibid.,* Article 24 et seq.
26. *Ibid.,* Article 5.
27. *Ibid.,* Article 30.
28. *Ibid.,* Article 28 et seq.
29. *Ibid.*

beneficial owners. This information must be verified by collecting and checking supporting documents.

The risk level of the third party is assessed based on its sector of activity, geographical location, and background.

Monitoring measures are then applied according to the level of risk identified. Enhanced *due diligence* is required for high-risk customers, involving additional checks on the origin of funds and business relationships. Transactions must be monitored continuously to identify any suspicious activity.

The information collected must be verified regular

1.3.2.2 Monitoring of cybersecurity and cyber resilience of digital subcontractors

Two texts provide for the monitoring of cybersecurity and cyber resilience measures of digital service providers:

- **The NIS 2 Directive:** monitoring subcontractors' compliance with cybersecurity standards in sectors of public interest [30].

The directive requires entities operating in sectors of public interest (health, transport, etc.) and meeting certain thresholds to monitor the cybersecurity measures implemented by their third-party partners and their ability to respond to any resulting IT incidents.

Among other things, companies must assess their subcontractors' cybersecurity and risk management policies and their compliance with cybersecurity standards (e.g., ISO 27001). Entities must also ensure that their partners have response plans and notification and cooperation procedures in the event of a security breach. Finally, they must ensure that their partners have implemented training and awareness programs for their operational staff on cybersecurity best practices.

30. *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS 2),* December 14, 2022.

These controls can be carried out by conducting security audits, collecting documents proving the contractor's compliance with these obligations, and submitting questionnaires to subcontractors.

- **The DORA Regulation:** monitoring compliance with cybersecurity standards and the operational resilience of subcontractors [31]

The DORA regulation requires financial entities to ensure that their third-party digital service providers comply with cybersecurity standards and operational resilience requirements.

In particular, they must ensure that their subcontractors comply with the provisions of the regulation. To this end, they may identify the data security and risk management measures in place, such as encryption and access controls, verify business continuity plans in the event of an incident, and verify the third party's compliance with IT security standards (e.g., ISO 27001). Subject entities must also identify and address risks of dependence on third-party digital service providers, as well as those arising from second-tier subcontractors.

The controls that regulated entities will have to put in place over their service providers will take the form of resilience tests during which crisis situations are simulated (intrusion into the IT system, virus infection, peaks in activity, etc.). Regular audits will also be carried out to ensure that procedures and policies are in place, particularly with regard to digital risk management, and that employees are trained in cybersecurity best practices.

31. *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector,* December 14, 2022.

DORA: Article 30 of the DORA Regulation sets out contractual provisions that must be included in all information and communication technology (ICT) service contracts entered into by financial entities, as well as clauses for contracts relating to important or critical functions within the meaning of the Regulation.

Mandatory clauses for all ICT service provider contracts	Clauses imposed on contracts relating to important or critical functions
Description of the services provided, the functions concerned, and the conditions for any subcontracting of a service affecting a critical function.	Detailed description of service levels.
Locations where services are provided, data is processed, and information requirements in the event of change.	Notice periods and obligation to notify the financial institution, in particular of any event affecting the service provider's ability to provide services supporting critical functions.
Obligations in terms of data availability, authenticity, integrity, and confidentiality	The obligation to implement and test contingency plans and put in place measures, tools, and policies to ensure an appropriate level of security.
Provision and access to data in the event of termination of the contract.	The service provider's obligation to participate in the financial institution's penetration tests.
Description of service levels.	Right to continuously monitor the service provider's performance (enhanced audit rights).
The service provider's obligation to provide assistance free of charge in the event of an incident.	The terms and conditions for terminating the relationship in order to reduce the risk of disruption to the financial institution.
The obligation to cooperate with the competent authorities and those of the financial authority.	The obligation to implement and test emergency plans and put in place measures, tools, and policies that guarantee an appropriate level of security.
Termination rights and notice periods.	
Conditions for ICT service providers to participate in digital security awareness programs and digital operational resilience training.	

Financial entities must also keep a register of ICT service contracts currently in force and provide the competent authorities with data on new ICT service contracts once a year (number, category of service providers, type of service, and functions concerned). The terms and conditions for the termination of contracts are also set out in Article 28(7°) of the Regulation.

NIS 2: The NIS 2 Directive encourages the entities concerned to include contractual provisions relating to cybersecurity in their ICT service contracts without specifying the content of these clauses: "*Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers**.*"

* Recital 85, NIS 2.

1.3.2.3 Control of exports of dual-use goods

Exporters of dual-use goods [32] must verify the location of the goods being shipped and the parties involved in the transaction.

Export licenses are granted according to the nature of the goods in accordance with a classification established by law.

Exporters must conduct thorough *due diligence* on their customers to identify the risks they pose, particularly with regard to international sanctions. They must also verify the end user and their use of the exported goods to prevent unauthorized use [33].

Measures are also applied after export, including keeping detailed records of transactions [34].

This information may be collected through questionnaires, database searches, and the collection of supporting documents [35].

1.3.2.4 Cyber Resilience Act

The Cyber Resilience Act (CRA) [36] requires manufacturers of digital products (software and hardware) such as smartphones sold on the European market to comply with strict cybersecurity requirements [37].

In particular, they must ensure that their products' vulnerabilities to cyberattacks are addressed and that measures are in place to protect their users' personal data and ensure secure access [38]. Incidents must be subject to regularly tested documentation and business

32. "*Dual-use goods*": products, including software and technologies, that can be used for both civilian and military purposes; they include goods that can be used for the design, development, manufacture, or use of nuclear, chemical, or biological weapons or their means of delivery, including any goods that can be used for non-explosive purposes and can also be used in any way in the manufacture of nuclear weapons or other nuclear explosive devices; *Regulation (EU) 2021/821 of the European Parliament and of the Council*, May 20, 2021.
33. *Ibid.* Article 8 and 9.
34. *Ibid.*
35. *Ibid.*
36. Regulation (EU) 2024/2847 of October 23, 2024 on cyber resilience *(Cyber Resilience Act)*.
37. *Ibid.* Article 13 et seq.
38. *Ibid.,* Annex I.

continuity procedures [39]. Regular updates to the security system must be carried out to remedy identified vulnerabilities.

They must also ensure that members upstream in their value chain comply with these security standards [40].

Other parties involved in the marketing of the product, namely importers and distributors, must ensure that the manufacturer complies with the provisions of the CRA. To this end, they may conduct audits, submit questionnaires to manufacturers, and include contractual clauses governing their production [41].

A summary of these legal obligations in table form is available in Appendix 2 on page 67.

1.4 Prioritize comprehensive risk mapping of the value chain

Some of the aforementioned texts also provide for the implementation of risk mapping to identify the categories of third parties to be assessed. It is therefore in the best interest of companies to carry out comprehensive risk mapping of the value chain, which will enable them to represent the exposure of third parties or categories of third parties to risks, operational and/or legal [42].

This pooling of resources is encouraged by regulators such as the *AFA*, which states in its Recommendations that "*For companies that have already carried out risk mapping work in a broader context or on types of risk other than corruption* [43], *these existing approaches can be capitalized upon* [44]."

39. *Ibid.*
40. *Ibid.*, Article 13 § 2.
41. *Ibid.*, Articles 23-25.
42. OECD, *Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions,* 2025.
43. United Nations Office on Drugs and Crime, *An Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide,* 2013, chapters II et III.
44. AFA, *Notice on the recommendations of the French Anti-Corruption Agency intended to assist legal entities in preventing and detecting acts of corruption, influence peddling, extortion, illegal taking of interest, embezzlement of public funds, and favoritism,* January 12, 2021.

Similarly, with regard to third-party assessments, the *AFA* specifies that "*Third-party assessments must be distinguished from the customer due diligence obligations to which persons defined in Article L. 561-2 of the Monetary and Financial Code are subject in the context of the fight against money laundering and terrorist financing (Article L.561-1 et seq. of the Monetary and Financial Code)*[45]. *They may nevertheless be implemented through a single mechanism, provided that the latter makes it possible to highlight the specific risk of corruption*[46]."

The advantage of the "*single mechanism*" promoted by the regulator is that it identifies third parties or categories of third parties within the value chain that are likely to present several categories of risk, thereby enabling an assessment to be carried out that addresses all risks and meets all obligations.

Thus, a third party presenting risks of economic dependence may also present vulnerabilities in terms of anti-corruption measures to maintain the contractual relationship. Similarly, a third party under sanction, which, in the context of operations covered by AML-CFT, implies an immediate cessation of business relations, constitutes a strong warning sign for the assessment of other types of risks, such as reputational risk.

This point is reiterated in the draft Practical Information Sheets in point 61:

"*Attention may be paid to the results of assessments carried out under other provisions, in coordination with dedicated compliance teams, particularly in the areas of financial security, international sanctions, anti-money laundering and counter-terrorist financing, duty of care, data protection, etc. In this regard, the role of the governing body, which is responsible for the proper coordination of procedures, is essential because it has an overall view*[47]."

Therefore, comprehensive mapping of risks in the value chain makes it possible to identify categories of third parties presenting risks according to pre-established criteria (nature of the activity, geographical area, volume of activity, etc.), enabling the definition of a third-party assessment policy.

45. AFA, *Recommendations 2020,* pt 205.
46. *Ibid.,* pt 206.
47. AFA, *Practical Information Sheets, op. cit.,* pt. 61.

II. Define a third-party assessment policy in line with your mapping

2.1 Define the categories of third parties to be assessed according to risk

Value chain mapping should enable the identification of the categories of third parties with which the company has relationships. A risk value can be determined for each of these categories according to risk criteria defined by the mapping. These values can then be used to automatically define the nature and level of detail of the assessment to be carried out.

The Practical Information Sheets therefore recommend establishing homogeneous groups of third parties with common risk criteria. For example, with regard to the risk of exposure to corruption, the Practical Information Sheets highlight [48]:

- the nature of the relationship with third parties (long-term relationship, economic dependency, etc.);
- the third party's sector of activity;
- the geographical location of the third party ("*country risk*");
- the third party's interaction with public actors [49].

> **Please note:**
> The diagram below can help identify risks that may impact the value chain and the due diligence to be performed. Appendix 2 Summary table of legal obligations for third-party assessment is intended to facilitate the identification of general and sector-specific third-party assessment obligations according to the company's profile and the activity carried out.

48. AFA, *Practical Information Sheets, op. cit.*, pt 51.
49. *Ibid.*

1 DENTIFYING AND ASSESSING THE RISKS IN MY VALUE CHAIN

What events caused by third parties (suppliers, customers, government agencies, etc.) could have a positive or negative impact on my value chain?

- Financial risk: customer or supplier default
- Economic dependence on suppliers: risk related to the termination of contractual relationships
- Strategic dependence on a third party: risk of disruption in the supply of a product or service essential to the fulfillment of our offer
- The third party does not provide sufficient guarantees to access our IT system
- Third-party integrity risk
- Image risk linked to the third party (the third party does not comply with its due diligence obligations in its own value chain)
- Business relations with third parties are restricted or prohibited by international sanctions, embargoes, restrictions related to the dual use of goods

How can I identify risks within my value chain? The nature of the due diligence to be performed according to my third-party assessment policy

- What is the minimum level of due diligence to be performed on third parties?
  - Financial risk
  - Duty of care
  - Verification of sanctions
- In-depth verification in the event of alerts

2 HOW IS THE TPRM PROCEDURE MANAGED WITHIN THE COMPANY?

- Who performs first-level due diligence?
- Who performs second-level due diligence?
- Who decides whether or not to continue the relationship with a third party identified as risky?

3 HOW IS THE TPRM PROCEDURE CONTROLLED?

- Definition of control and audit plans
- Who performs the controls? (prevention of conflicts of interest)
- What are the levels of control?
  Level 1: operational
  Level 2: compliance
  Level 3: Audit

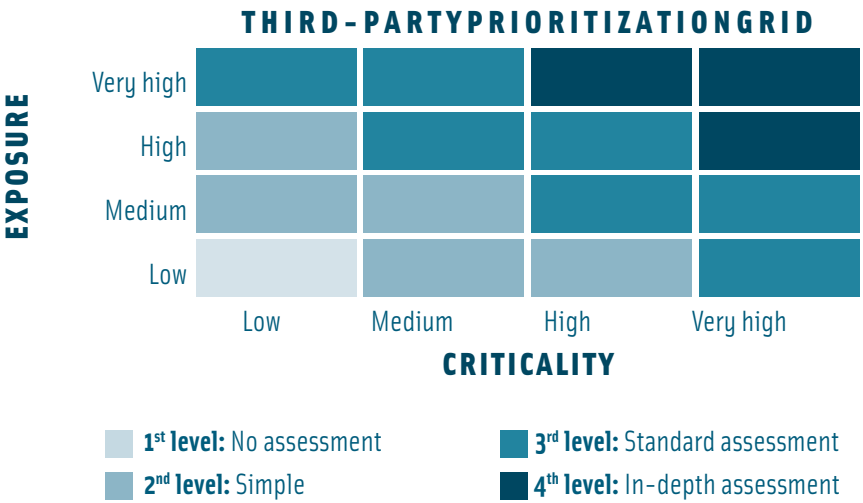
The AFA recommends digitizing third party assessments to facilitate control and auditing

The third party assessment policy should therefore inform the operational level whether the third party, given its category, should be assessed:

- If the third party, given its category, should be assessed.

Except for specific legal obligations requiring the assessment or systematic collection of information on certain types of third parties (e.g., AML-CFT or *due diligence* obligations), the company has the discretion to determine the categories of third parties to be assessed and the methods used to do so. These are defined with regard to the risks identified for the category of third parties concerned and may also take into account practical aspects of the assessment: the need to obtain information about the third party quickly, the third party's ability to cooperate in providing the expected information, etc. The choice of due diligence to be performed and the practical methods used are therefore important for achieving the objectives of the TPRM [50].

The table on the following page summarizes the levels of due diligence carried out with regard to the criticality and exposure of the third party to risks. The due diligence to be carried out is linked to the category of third party concerned and the risks associated with it. The table below summarizes the levels of assessment with regard to the criticality and exposure of the third party to risks.



50. AFA, *Recommendations 2020, passim.*

LEVEL OF DUE DILIGENCE PERFORMED

First level: no assessment

Lorsque les tiers ne présentent aucun risque, aucune vérification n'est nécessaire. Cette situation est quasiment inexistante dans la pratique, compte tenu de la complexité des réglementations applicables et enjeux business.

Second level: low risk

When the third party presents a very low level of risk, it is subject to simplified checks, which may include:

Searches on freely accessible sources (asset freeze register, INPI register, etc.) or automated searches on databases for which there is a charge

Consultation of company archives

Third level: medium or high risk

When the third party presents a medium or high level of risk, they may be subject to:

Questionnaires

Research on specialized databases

Self-assessment methods previously mentioned

Fourth level: very high risk

When the third party presents a very high level of risk, as indicated by warning signs from previous assessments or factors mentioned by operational staff, it is subject to in -depth assessments.

These include:

Interviews with audit

External reports produced by managers, specialized service providers (consulting firms, law firms, etc.)

2.2 Define the nature of the due diligence to be performed

Due diligence consists of obtaining data about the third party in order to assess them. There are several methods of due diligence that will enable you to obtain more or less detailed data about third parties.

A distinction can be made between assessments that provide continuous updates of information and thus enable ongoing monitoring (risk monitoring) and those that provide more in-depth information at a specific point in time (control evaluation).

2.2.1 Databases

Risk monitoring provides instant information on third parties by searching databases that are available online, either free of charge (open data) or for a fee.

- **Open Data**

A lot of information about companies is now available free of charge online. Open-Source Intelligence (OSINT) is the practice of searching for information about third parties online. The Osint framework website [51] helps identify information sites. Similarly, the *AFA* has identified open databases that facilitate the search for information for assessing the integrity of third parties [52]. It should be noted that France, through the Digital Republic Act, has promoted access to public data, including through APIs [53].

- **Paid databases**

Service providers offer access to databases where information is structured, making it easier to search for information. Some databases may specialize in certain types of information (politically exposed persons, sanctions), specific geographical areas, or offer several categories of information (financial information and integrity, for example).

51. https://osintframework.com/
52. AFA, *Collection of practical fact sheets: Public information databases useful for assessing the integrity of third parties*, March 9, 2023, [online], available at: https://www.agence-francaise-anticorruption.gouv.fr/fr/document/afarecueil-fiches-pratiques-bases-publiques (accessed on September 23, 2025).
53. Law No. 2016-1321 of October 7, 2016 for a Digital Republic, JORF No. 0235 of October 8, 2016 [online], available at: https://www.data.gouv.fr/dataservices

• **Benefits and limitations of risk monitoring**

L'intérêt du risk monitoring est de disposer d'une information immédiate sur le tiers qui peut être actualisée selon une fréquence que l'entreprise peut déterminer elle-même. Un changement de statut du tiers générant une alerte pourra être transmis à l'évaluateur pour permettre de réaliser des investigations complémentaires.

Often presented with the promise of automating third-party assessments and providing associated scores, risk monitoring does, however, have its limitations. **First,** users must deal with false positives, i.e., homonyms, in order to identify the right person to assess. They must also analyze the information collected in order to identify serious risks. The Practical Information Sheets highlight the risk associated with the rate of homonymy [54]. Risk monitoring therefore requires processing and analysis of the information obtained, which may exceed the skills of the operational level often responsible for risk monitoring. In addition, the *AFA*, in its Practical Information Sheets, warns about the automatic rating systems provided by digital solutions, specifying that users must be able to determine their own rating system with regard to risk mapping [55].

Secondly, the information obtained on the third party is inherently limited and most often results from legal information disseminated by the company, public authorities, or the media and social networks when the third party has been the subject of a press investigation. Access to certain information, such as the identity of beneficial owners, has also been restricted by court order (ECLI:EU:2022:912) in order to protect privacy. Consultation of the register of beneficial owners is therefore restricted to companies or individuals with a legitimate interest within the meaning of Article L. 561-46-2.-I of the Monetary and Financial Code (including persons subject to AML-CFT and Sapin 2 obligations).

The assessor will therefore not find useful information concerning their relationship with the third party, such as the identification of a possible

54. AFA, *Practical Information Sheets, op. cit.,* pt 83.
55. *Ibid.,* pt 97.

conflict of interest, exclusively through risk monitoring. These considerations lead the *AFA* to qualify the use of digital solutions if they only offer the possibility of searching databases. "*In any case, the use of a digital solution can be useful for conducting an initial assessment, but requires human analysis in order to adjust the assessment, particularly for the most high-risk third parties*[56]."

2.2.2 Self-assessment questionnaire and document management

- **Self-assessment questionnaire**

The self-assessment questionnaire allows the company to obtain direct information from the third party being assessed on the basis of a questionnaire. This questionnaire may cover several topics and be more or less detailed depending on the risks identified. The Practical information sheets (like the *AFA* recommendations) specifically target this method of gathering information by recommending that it be signed by the respondent and accompanied by supporting documents. The *AFA* also insists that, in the case of a questionnaire covering several topics (financial security, CSR, etc.), the section on corruption should be sufficient to allow for a genuine assessment[57]. In addition, the Practical Information Sheets detail relevant information that may be requested from the third party[58].

The questionnaire allows information to be obtained directly from the third party and therefore, provided that the third party is cooperative and provides accurate and recent data, it offers reliable answers. Responding to a questionnaire also constitutes a form of commitment on the part of the third party, which could expose them to legal liability in the event of deliberately inaccurate answers.

Consequently, on the one hand, the contract[59] concluded with the third party could be declared null and void on the grounds of fraudulent conceal-

56. AFA, *Practical Information Sheets, op. cit.,* pt 85.
57. *Ibid.,* pt 72.
58. *Ibid.,* pt 75.
59. Articles 1131 and 1178 of the *Civil Code*.

ment if the concealed information was decisive in forming consent [60]. On the other hand, the third party could be held civilly liable for fraudulent misconduct [61]. Without ruling on this point of law, the *AFA* states in its Practical Information Sheets that "*the third party's refusal to disclose the requested information constitutes a very high risk signal*[62]."

Managing the questionnaire can present difficulties in answering the questions and gathering the requested documents. The assessor must send the questionnaire to the right person, follow up on it, and analyze the responses. In addition, the questionnaire provides a snapshot of the third party at the time of their response, without monitoring over the duration of the contractual relationship, even if the questionnaire can be sent out again at regular intervals.

- **Document management**

The third party's assessment may also consist of providing documents proving its capabilities or skills. This may be the case, for example, for the duty of vigilance, which requires the service provider to be asked to provide documents proving their administrative compliance (*K-BIS*, *URSSAF* vigilance certificate, list of foreign workers) [63]. Other requests may be added to this: insurance certificates, professional accreditations, etc.

It should also be noted that AML-CFT obligations require the identification of the customer and verification of their identity [64], in particular by collecting and verifying identity documents [65].

60. Articles 1130 and 1137 of the *Civil Code*.
61. Articles 1240 and 1241 of the *Civil Code*.
62. AFA, *Practical Information Sheets, op. cit.,* pt 78.
63. Article L.8222-1 et seq. of the *Labor Code*.
64. Articles R561-5 and L561-5 of the *Monetary and Financial Code*.
65. See: https://acpr.banque-france.fr/fr/regulations/official-register/guidelines.

2.2.3 In-depth assessments and third-party audits

In-depth assessments may be necessary in certain situations presenting particularly high risks, particularly given the importance of the relationship in the value chain and the opacity of the actual owners of their capital (beneficial owners) or their production process (risk of human rights' violations). These assessments will be carried out by actors with local information or in the form of interviews, external surveys, audits, and *due diligence* for mergers and acquisitions (M&A) or joint ventures. It is recommended that these audit possibilities with third parties be provided for contractually.

2.3. TPRM policy and governance

The collection and processing of data from the TPRM process and the decision-making process regarding whether to enter into or maintain a relationship with a third party require the mobilization of several levels of resources within the company. Indeed, the volume of third parties in the value chain and the information requested normally requires the involvement of operational staff in this collection process. The resulting alerts can manage a validation workflow enabling decisions to be made regarding the third party by the expert level (legal/compliance/IT department, etc.) and, in the absence of consensus between the operational and expert levels, by arbitration by the governing body [66].

This three-tier organization is recommended by the *AFA* both in its recommendations and in its Practical Information Sheets [67].

2.3.1 Definition of the role of TPRM stakeholders

- **Operational level teams**

Data collection from third parties must be carried out at the operational level, given its direct relationship with the third party. In order to facilitate the task of operational staff, it is necessary to determine in advance the nature of the due diligence to be carried out (database queries, sending

66. AFA, *Practical Information Sheets, op. cit., passim.*
67. *Ibid.* pt 70 et seq.

questionnaires and collecting documents, etc.) according to the level of risk of the third party, with regard to the category to which it belongs [68].

It should be noted that the Practical Information Sheets also suggest the use of an internal questionnaire by the operational level "*completed by staff performing operational functions within the company based on the information gathered and/or knowledge of the relationship*" [69].

It is essential to collect and use the information available within the company on the history of the relationship with the third party, where it exists and if it is up to date. This may be the case if departments or services have carried out third-party assessments to meet the needs of certain departments (purchasing, CSR, etc.). It is also important to be able to access the company's IT tools (ERP, purchasing IS, CRM), which may contain information useful for evaluating the third party.

In this regard, the risk level of the third party category (and therefore the associated level of diligence) may be increased by the operational department in light of the information it has and has obtained as a result of its direct relationship with the third party concerned.

The objective of this phase is therefore to enable the collection of information tailored to the category of third parties concerned and to enable initial processing of the information to identify serious risks.

At this stage, it is advisable to prioritize the automation of information processing to relieve the operational level of this task. Alerts can thus be generated automatically if risk monitoring reveals the existence of international sanctions, convictions, or politically exposed persons (PEPs). Similarly, the absence of responses or incomplete responses to certain questions in a questionnaire on issues deemed sensitive may generate alerts.

In the absence of an alert, the operational level may validate the third party or, depending on the automation of the process, automatic validation will be performed by the assessment tool.

68. See Appendix 4, Third-party integrity risk signals.

69. AFA, *Practical Information Sheets, op. cit.*, pt 72.

- **The legal/compliance function**

The legal/compliance department may be involved in the event of alerts and if the operational department wishes to continue with the third-party onboarding process despite these alerts.

The objective here is to analyze the risks in order to verify, first and foremost, that the alerts generated reveal real risks and are not biased by the criteria used for automation.

At this stage, a more detailed questionnaire may be sent to the third party, or a risk analysis may be carried out by an external auditor.

Referral to the expert level should lead to a recommendation for validation (accompanied, where appropriate, by a treatment plan) or rejection. In the absence of consensus between the operational and expert levels on the validation of the third party, it is up to this level to refer the matter to the governing body for a final decision.

Ms. **Catherine Delhaye-Kulich**, Chief Ethics, Compliance, and Data Protection Officer at the Valeo Group, shares her insights on the importance of TPRM and compliance in business.

What message should be conveyed to raise awareness?

It is important to communicate clearly so that the departments and employees concerned understand the issues and consequences for the business of a flawed TPRM approach. Indeed, due to the numerous regulations that now require *due diligence* to be carried out, as well as customer requirements with regard to their supply chain in the broadest sense, TPRM is now an essential part of conducting business in a calm and sustainable manner.

For example, European economic sanctions, which have been very popular since the start of the war in Ukraine, prohibit the import of certain products manufactured wholly or partly in Russia, as well as transactions with a large number of entities and individuals of Russian origin.

Another example is China's decision to make the export of rare earths, which are essential for the manufacture of electric vehicles,

wind turbines, and microchips, subject to the granting of export licenses. One of the conditions for obtaining these licenses is that products manufactured from these materials must not be intended for the US military industry.

Finally, the United States prohibits the importation and sale on US territory of vehicles equipped with certain software and certain equipment of Chinese or Russian origin or from entities controlled by Chinese or Russian nationals.

It is therefore absolutely essential to know who you are working with and to verify that the relationship is not subject to restrictions. These checks apply to suppliers, customers, and the destination and use of certain technologies. Failure to exercise due diligence, or exercising due diligence in a superficial or incomplete manner, may lead a company to interact with partners under sanctions or to import or export products subject to restrictions.

This exposes the company to legal and reputational risks. It can also cause difficulties for its customers or suppliers. These are therefore risks that could seriously impact the business. There is no need to apologize for implementing an effective TPRM, but rather present it as a prerequisite for doing business.

Is it essential to involve operational staff in carrying out the first level of due diligence?

An Ethics and Compliance Department must work with various departments within the company to assess third parties (particularly purchasing, sales, logistics, and R&D).

It is generally the Ethics and Compliance Department that defines, depending on the situation, the methodology to be followed and the level of diligence to be exercised. It also defines action plans, or even the prerequisites to be implemented and complied with in the event of a relationship with a high-risk third party, and monitors their proper execution.

The Ethics and Compliance Department also monitors regulatory developments closely so that it can inform the Executive Committee

of the impact of new regulations on the business. For example, geopolitical tensions in recent years have made it necessary to monitor sanctions imposed by the EU and the US in particular, as well as counter-sanctions imposed by China.

Can we now claim that certain third parties are not at risk and therefore not assess them?

Some third parties may present a very low risk due to their activities and location. Assessments can therefore be adapted to the risks identified. Conversely, some third parties are by nature subject to specific *due diligence* obligations (PFAS, deforestation, etc.). Finally, compliance with international sanctions and the absence of corruption are essential.

In conclusion, third-party management is an essential part of any compliance program. It helps protect the company in many areas and contributes to its sustainability.

- **The role of the governing body**

The governing body intervenes in the process to make a decision to accept or reject the risk, particularly when there is no consensus on the decision to be made between the operational and compliance levels. This decision must be based on comprehensive information that has been collected and processed by the operational and compliance functions.

2.3.2 Formalizing a TPRM policy and governance

Implementing a TPRM procedure therefore involves defining roles and tasks to be performed in order to collect data and to process it, actions preceding the decision to enter into a relationship with the third party. Indeed, a TPRM policy must lead to decisions being made about the relationship with the third party, which are either to approve the relationship, terminate it, not enter into it, or carry out additional due diligence to document a decision. The Practical Information Sheets reiterate the purpose of the procedure[70],

70. *Ibid.,* pt 105.

specifying that "*decisions are formalized and recorded on a secure network*" [71]. Thus, the digital solution chosen by the company must be able to record decisions, as well as the parties involved in the assessment, and provide a history of the due diligence performed and its date in order to provide audit trails.

Similarly, the policy should define how often third-party assessments should be updated.

It is therefore recommended that a policy be formalized to this effect, which can be validated by the governing body. The purpose of this exercise is to identify in advance any sticking points that stakeholders may have regarding the roles and tasks assigned to them by the policy and to have them arbitrated, if necessary, by the governing body.

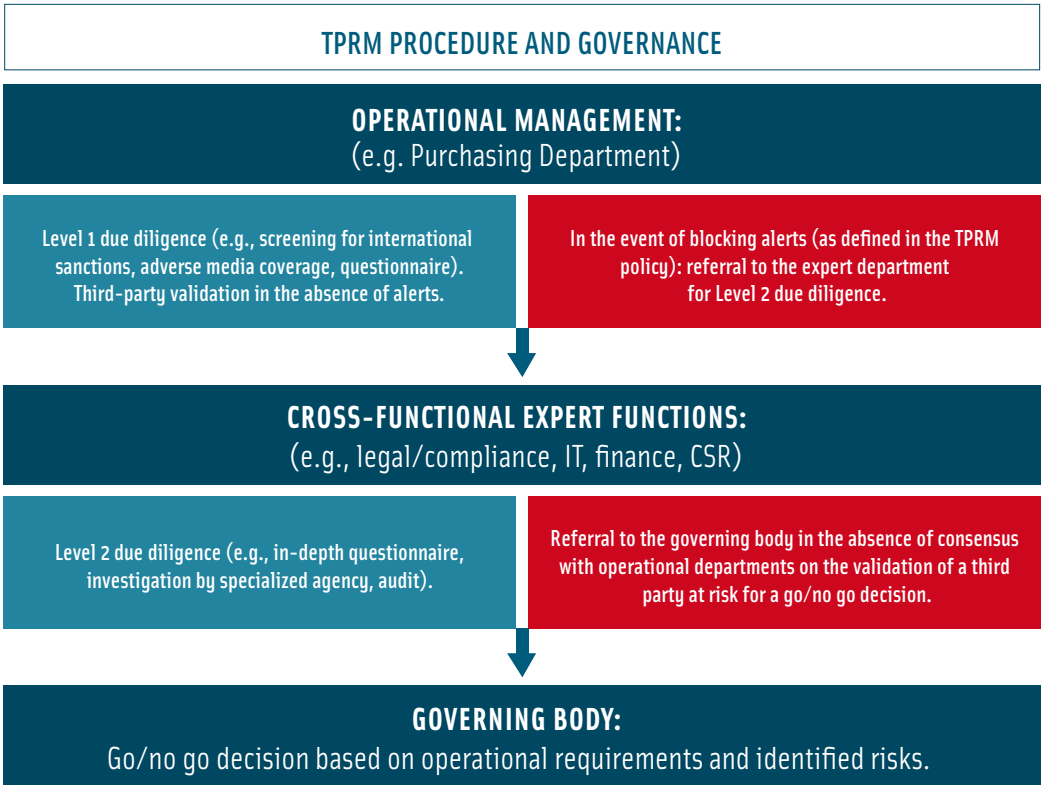
A formalized policy will also enable internal control to verify its application.

Finally, this exercise will enable the expression of needs in the research or development of a tool to digitize the TPRM procedure.

The importance of formalizing the assessment policy is emphasized by the *AFA* in its recommendations and in the Practical Information Sheets. In the latter document, the *AFA* specifies

"Regardless of the weighting method chosen, the approach must be formalized in a procedure in order to be correctly applied, controlled, and audited" [72].

71. *Ibid.,* pt 108.
72. *Ibid.,* pt 53.



Ms. **Makeda Cardenas**, Compliance Officer for La Poste Group, shares her insights on the importance of TPRM and compliance in business.

Can you tell us about your responsibilities and your role in third-party assessment?

We are part of the Group's purchasing department. We evaluate third-party suppliers for the Group and ensure deployment for subsidiaries. The supplier compliance project is jointly led by the Group's Compliance Department, which also ensures deployment for other categories of third parties (non-commercial partners, customers, etc.).

Our proximity to purchasing allows us to better integrate the integrity assessment process into the referencing of third-party suppliers,

which allows for a smoother onboarding cycle and easier access to information gathered by purchasing that may have an impact on integrity assessment, including risks of economic dependence on the third party.

How are third-party assessment procedures organized, and what are the specific characteristics of a public company in this regard?

The Group is subject to several legal obligations involving third-party assessments. The assessment we carry out when establishing a relationship must cover these obligations (GDPR, Sapin 2, duty of care), and our team performs its due diligence in accordance with these obligations. Any cyber risk posed by the third party is managed by our IT department.

The assessment is carried out after the contract has been signed, when the third party has responded to a call for tenders in accordance with public procurement rules. The result of the assessment cannot be used as grounds for a priori exclusion from public procurement. However, it does enable us to draw up a plan for dealing with third parties identified as posing a risk.

Assessments are carried out on two levels. First, a database search is conducted to identify international sanctions and/or embargoes, in addition to negative press coverage and financial information. Monitoring is carried out throughout the contractual relationship. If risks have been identified, we carry out due diligence using a questionnaire, which remains a relevant tool for gathering information to correctly identify risks, even if third parties may be heavily solicited in this regard.

What measures are implemented when a third party is identified as risky?

Risks may be identified when a company's regulatory compliance system or maturity in these areas is deemed insufficient. We can therefore work with the company to encourage it to improve the quality of its program. We thus establish a compliance partnership with the third party.

For third parties whose risk level is not considered low but with whom we must maintain a business relationship (the only one operating in a given territory, the only one able to provide the service, etc.), we can implement security measures, such as an enhanced training program for teams working with them. The risk-based approach takes precedence throughout the business relationship, as well as when defining remedial actions.

What are your expectations regarding the digital tools that support your TPRM approach?

Firstly, the ability of the tools to adapt to our third-party assessment policy, which is dictated by our risk identification. It must therefore have good configuration capabilities. Conversely, using a tool requires users to express their needs.

The use of a tool is essential given the volume of information to be processed. However, the risk with database screening in particular is that users can be overwhelmed by the volume of information and alerts, which are not always relevant due to false positives. It is therefore necessary to reprocess the information, which can be tedious. The use of artificial intelligence can be promising if the error rate is marginal.

2.4 Working with a third party identified as a risk

Due diligence on third parties carried out under the TPRM may reveal risks associated with initiating or maintaining relationships with the third party. This identification may lead to a decision to refuse a business relationship with the third party. However, arbitration is sometimes necessary when the relationship with the third party is essential to the organization (e.g., a strategic supplier). The decision to work with a risky third party therefore results from the refusal or acceptance of risk, which must be taken at the highest level of the company. This situation is addressed by the *AFA* in its Practical Information Sheets: "*The company may find itself in a situation where it has no choice but to establish or continue a rela tionship with a third party that presents a risk of corruption, From third-party assessment to Third Party Risk*

Management where verification is difficult to carry out. In this situation, it must implement appropriate remedial measures" [73].

Thus, the relationship with a high-risk third party can be maintained, but accompanied by a treatment plan. First, the company employees in charge of the relationship with the third party must be trained, and it may be decided that the third party will be managed collectively, offering a better assessment of the risks. The contractual policy towards the third party may also be adapted by requiring the third party to identify and address its risks with objectives that may be sanctioned by a termination clause in the event of non - achievement. Finally, continuous monitoring of the third party may be implemented, allowing for regular reassessment of the relationship with the third party. The Practical Information Sheets discuss remediation measures in relationships with third parties identified as risky [74]).

73. *Ibid.,* pt 59.
74. *Ibid.,* pt 109.

III. Deploying and controlling TPRM in business processes

3.1 Deployment

One of the difficulties in deploying a TPRM process within a company is mobilizing the operational level to collect and process first-level information. This is because the process is perceived as time-consuming and offering no added value in relation to the tasks assigned to operational staff. This perception is often reinforced by the attitude of senior management, who do not always recognize the strategic nature of TPRM and fail to allocate the necessary resources to this task.

It is therefore necessary to change the discourse on third-party assessment in order to shift it from a simple regulatory obligation enforced by a regulator to a strategic approach linked to value chain risk management, i.e., to the very process of value creation within the company.

As we have seen, TPRM provides a comprehensive view of third-party risks, rather than a fragmented one based on assessments carried out according to the needs of the departments involved. Any authorized person can therefore check whether the third party with whom they are considering contracting has already been assessed and find the information they need. Pooling the information gathered on third parties saves time in the contracting process, thereby increasing the speed and efficiency of operational processes. The deployment of the process itself requires change management: training that is not only focused on the tasks to be performed, but also gives meaning to the approach.

- Gradual ramp-up of actions to be carried out with the setting of objectives,
- Regular meetings to check that these objectives have been achieved,
- Identifying and resolving difficulties.

It may be advisable to work with a test department that can then communicate internally about its experience as a "*pioneer*" in adopting TPRM.

Similarly, it is recommended that a sponsor be identified in each department who can provide local support to colleagues.

The Practical Information Sheets recommend that corporate groups implement an anti-corruption compliance network that will play a role in monitoring the third-party assessment system. The *AFA* specifies that the person responsible for deploying and monitoring the third-party assessment system may also disseminate any useful information or methodological elements to the network of referents [75].

Digitizing the process allows the person responsible for deployment to be informed of the due diligence carried out within the company or its subsidiaries. The tool can also be used to send alerts or methodological points, such as changes to questionnaires or requests for documents.

The Practical Information Sheets remind users that the third-party assessment process is constantly evolving and must be adapted to the risks that may arise from changes in the company's internal or external environment.

3.2 Process control

Like any process in place within a company, the TPRM may be subject to internal control to verify its functioning and effectiveness. Controlling the appropriation of a process by its stakeholders is indeed crucial, and it may be threatened by various circumstances such as the departure from the company of individuals who have been trained in its use or a lack of resources within management.

It should be noted that control of the third-party assessment process is required by compliance programs, in particular the Sapin 2 law, which provides in paragraph 8 of Article 17 for "*a system for internal control and assessment of the measures implemented*" [76]. This requirement is also reiterated in the AFA's Practical Information Sheets [77].

75. *Ibid.,* pt 137.
76. Law No. 2016-1691 of December 9, 2016 on transparency, the fight against corruption, and the modernization of economic life (Sapin 2).
77. AFA, *Practical Information Sheets, op. cit.,* pt. 139.

Among the advantages of digitizing the TPRM process, internal control of the system will be greatly simplified by the information provided by the tool: is the third-party assessment procedure being followed when onboarding a third party? How many assessments have been carried out by the departments concerned? etc. This point is also highlighted in the Practical Information Sheets: "*the use of a digital tool can be useful for effectively managing the monitoring of the third-party assessment system*" (Point of attention No. 8).

IV. The digitization of the TPRM process

The benefits of digitizing TPRM are apparent at every stage of the process: data collection and processing in a secure environment, third-party validation workflow, integration of the process into the company's IT systems to facilitate its smooth operation and enable a high level of automation, and internal control of the process.

4.1. Third-party data collection and processing

Digitization facilitates the collection of third-party data, whether obtained internally or externally.

- **Internally**

The use of APIs enables communication with the company's internal information systems that hold information on third parties. This is the case for ERP or source-to-pay solutions that have information, at a minimum identification, on third parties.

Conversely, the TPRM solution can also, again via API, intervene in the third-party onboarding process by suspending account creation if the third party is rejected following evaluation.

Company departments or subsidiaries may have a history of relationships with third parties that is not necessarily centralized. The TPRM tool, particularly the questionnaire module, can facilitate the collection of internal information on third parties.

- **Externally: centralization of multiple information channels via API and synthesis of information via AI**

Digitizing the TPRM process makes it possible to combine methods of collecting data on third parties[78] on a single interface, thereby providing a comprehensive view of the third party.

APIs make it possible to query multiple databases. AI has a role to play in processing the information obtained by facilitating the management of false positives, but also by synthesizing the information obtained on the third party and providing a risk score.

Provided that a satisfactory qualitative analysis rate is achieved, the use of AI in the TPRM process opens up interesting prospects for facilitating the automation of the process by promoting the allocation of human resources to third parties presenting the highest risks.

- **Securing data obtained through the TPRM process and managing it in accordance with the GDPR**

The TPRM process is still often implemented using office software (Word, Excel, Forms, Drive, etc.). The security they offer for the data collected is relative, in the sense that questionnaires are sent by email and the information is stored in the databases of the providers of these solutions. However, it is easier to require a TPRM solution publisher to locate its databases in Europe.

Having a digital tool also makes it easier to manage GDPR obligations (archiving or deleting data in accordance with the company's data retention policy or at the legitimate request of the data subject).

4.2. Digitizing the validation workflow to benefit stakeholders

Digitizing the TPRM process facilitates collaboration between stakeholders, but also their individual actions.

78. See 2.2 above, "Defining the nature of the due diligence to be performed".

- **Simplified collaboration**

When digitized, the validation workflow optimizes collaboration between stakeholders in the TPRM process. Assessments carried out by operational staff are accompanied by alerts that require the compliance officer to intervene in the absence of a response or in the event of an unsatisfactory response. Raw information is thus filtered as soon as it is assessed by the operational staff, allowing the compliance officer to focus solely on the third parties that pose the greatest risk.

Digitizing the validation workflow also streamlines communication between stakeholders. Using a shared interface, operational staff can contact the compliance officer and send them all the information relating to high-risk third parties in just a few clicks.

- **Digitization supporting the individual actions of those involved in the assessment**

For operational staff
Digitizing the TPRM process through the use of APIs and AI can offer a high level of automation, thereby preventing the well-known fatigue associated with a time-consuming and bureaucratic process that discourages operational staff.

For the TPRM solution administrator
The TPRM solution administrator, most often the legal/compliance manager, has a comprehensive overview of how TPRM works within the company. This makes it easier for them to intervene. As mentioned above, the compliance officer is not obliged to intervene in cases with the lowest risk levels. This allows them to focus their efforts and resources on the most risky third parties and conduct more in-depth assessments. They can also design appropriate treatment plans if the decision is made to continue the relationship.

The procedures carried out as part of a digitalized TPRM process are also recorded in third-party files. These spaces centralize the data collected by operational staff and the compliance officer, thereby facilitating access to information for the latter, particularly for analysis purposes.

- **Digitization at the service of third parties**

Third parties also benefit from the advantages of using specialized TPRM solutions. They are able to respond to all assessments submitted to them on a single interface. In addition to offering security guarantees, these platforms make the assessor's requests easier to understand and facilitate the third party's response.

As part of the due diligence carried out using a self-assessment questionnaire, features may enable the third party to distribute questions or blocks of questions internally to facilitate the collection of information from colleagues depending on the nature of the requests made (e.g., financial information to the finance department, etc.).

The third party is also automatically reminded by the interface, particularly in the event of a delayed response.

4.3 Digitization of the TPRM process and integration into the company's IT tools

The purpose of TPRM is to consolidate the information held by the company on third parties, which may be collected by various departments and for various purposes.

It is therefore common for companies to have a platform for managing their *due diligence* obligations (verification of the *Kbis*, *URSSAF* due diligence certificate, and list of foreign workers) and database *screening* tools for obtaining information on integrity assessments and financial scoring.

However, these tools often do not communicate with each other and are not integrated, whereas a third party that does not comply with the duty of care may pose integrity risks.

As mentioned above, APIs enable tools to communicate and thus create an integrated TPRM process. This approach facilitates the automation of due diligence and informed decision-making on collaboration with third parties.

4.4 Monitoring the application of procedures

Digitization facilitates the compliance officer's monitoring of the application of the TPRM policy by operational staff.

The actions carried out by stakeholders in a digitized TPRM process are recorded in a log that also includes the dates and identities of their authors.

The compliance officer, who has an overview of these actions, is thus able to assess the application of the third-party assessment policy by operational staff for internal control purposes, in accordance with Article 17, II, 8° of the Sapin 2 law. In this capacity, they have audit trails that they can provide to the authorities to demonstrate the company's compliance with legal requirements.

To conclude this discussion on TPRM, Ms. **Carmen Briceno**, Legal and Compliance Director at Raja Group and Head of the AFJE Compliance Commission, shares her expertise on third-party assessment, which she considers a strategic, operational, and collective imperative for companies.

> Like John Donne's poem "*No man is an island*," no company exists in isolation. Every organization is inevitably linked to a network of partners, suppliers, customers, and intermediaries within an economic, social, and legal fabric where interdependence is the norm.
>
> These relationships are not only inherent to commercial activity, but also essential to the competitiveness and growth of companies, regardless of their size or sector of activity. However, they are not without risk. A business partner involved in illegal or unethical practices can have major legal, financial, and reputational consequences for the contracting company.
>
> European and international legislation now establishes corporate liability for breaches by company's business partners, particularly when due diligence has not been exercised. Some sector-specific regulations even prohibit the marketing of products without prior assessment of suppliers. Others, such as the UK Bribery Act of 2010 and the Economic Crime and Corporate Transparency Act of 2023, go even further: with the offenses of failure to prevent bribery and

failure to prevent fraud, a company can be held criminally liable if an associated person commits an act of corruption or fraud for its benefit, unless it can demonstrate that it has put adequate procedures in place. These measures reflect a shift toward proactive corporate responsibility in preventing criminal behavior by third parties.

In this context, third-party assessment is no longer a mere administrative formality. It is an essential lever for risk management, regulatory compliance, and social responsibility.

Multiple obligations, concrete obstacles

In practice, as we have seen in the work of the *AFJE* compliance expert group, companies and their compliance teams are faced with a multitude of obligations: combating corruption, complying with international sanctions, combating money laundering and terrorist financing, duty of care, specific customer requirements, voluntary CSR commitments, etc. This complexity is compounded by operational obstacles: limited access to reliable databases, disparate and incomparable sources depending on jurisdiction, information gaps in certain areas, lack of internal resources, and lack of interdepartmental coordination

Structural principles for an effective approach

Faced with these challenges, authorities and international organizations agree on several fundamental principles. A risk-based approach, backed by regularly updated "*active*" mapping, is essential. The tone set by senior management (tone from the top) is a key principle: the credibility and effectiveness of the system depend on clear and transparent policies, a comprehensive and cross-functional approach, appropriate resource allocation, active regulatory monitoring, and regular reporting to governance bodies.

The role of digital tools

In this digital age, the use of technological tools that comply with regulations (GDPR, ethical principles of AI) is essential to support this complex process. Automated, configurable, and manually controlled *due diligence* technologies, artificial intelligence, and specialized databases increase efficiency, traceability, and geographic coverage.

Collective action: a lever that should not be overlooked

Beyond individual initiatives, collective action is a powerful lever for structuring and disseminating best practices. In certain sectors, standardized *due diligence* questionnaires have been developed to facilitate the assessment of third parties, particularly to help SMEs. A concrete example is the European Commission's *due diligence* ready! portal for conducting due diligence on the supply chain of extractive industries. These tools make it possible to pool efforts, reduce costs https://single-market-economy.ec.europa.eu/sectors/raw-materials/due-diligence-ready_en), and ensure sectoral consistency in compliance requirements.

Professional associations have a key role to play in disseminating these best practices. The *AFJE* actively contributes to this through the work of its Compliance Commission (news on the LinkedIn page @AFJE Compliance), the publication of the magazine *JEM* (*Juristes d'entreprise magazine*), whose November special issue is devoted to compliance, the organization of in-person and online conferences, and participation in consultations with the authorities. This White Paper is a concrete example of best practices to be promoted and interprofessional collaboration.

Conclusion

A risk-based, proportionate, documented third-party integrity assessment process that is supported by management and adequately equipped is now a strategic lever for reconciling legal certainty, operational efficiency, and sustainable value creation.

Assessing your third parties means prioritizing your risks, affirming your values, and building your credibility.

Bibliography

I. International organizations

United Nations (UN)

United Nations Office on Drugs and Crime (UNODC), *An Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide*, 2013, chapiters II and III.

Organization for Economic Cooperation and Development (OECD)

OECD, *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions,* 1997, available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0378.

OECD, *Corporate Anti-Corruption Compliance Drivers, Mechanisms, and Ideas for Change,* 2020, available at: https://www.oecd.org/ content/dam/oecd/en/publications/reports/2020/09/corporate-anti-corruption-compliance-drivers-mechanisms-and-ideas-for-change_1a9c17f8/4245d0fc-en.pdf.

OECD, *Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions,* 2025.

Financial Action Task Force (FATF)

FATF, *Guidance on politically exposed persons and heads of international organizations,* 2021, available at: https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/pep/pep-eng.

World Bank

World Bank, *Integrity Compliance Guidelines*, 2018, available at: https://thedocs.worldbank.org/en/doc/302151536766276403-0240022018/WBG-Integrity-Compliance-Guidelines-CH.

II. European Union law

Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (*General Data Protection Regulation*), OJEU, L 119, May 4, 2016, p. 88.

Directive (EU) 2024/1760 of the European Parliament and of the Council of June 13, 2024 on corporate sustainability due diligence, OJEU, L 1760, June 13, 2024.

European Commission, *Commission Delegated Regulation (EU) 2023/2772 of July 31, 2023 supplementing Directive (EU) 2022/2464 of the European Parliament and of the Council as regards sustainability reporting standards,* OJEU, L 277, Oct. 22, 2023, p. 465.

Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022 on measures for a high common level of cybersecurity across the Union (*NIS 2 Directive*).

Regulation (EU) 2022/2554 of the European Parliament and of the Council of December 14, 2022 on digital operational resilience for the financial sector (*DORA Regulation*).

Regulation (EU) 2024/2847 of the European Parliament and of the Council of October 23, 2024 on horizontal cybersecurity requirements for products with digital elements (*Cyber Resilience Act*).

Regulation (EU) 2021/821 of the European Parliament and of the Council of May 20, 2021, setting up a Union regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items.

III. Domestic law (France)

Law No. 2016-1691 of December 9, 2016 on transparency, the fight against corruption, and the modernization of economic life (*Sapin II Law*), JORF, Dec. 10, 2016, text No. 2, available at: https://www.legifrance.gouv.fr/jorf/id/JORFSCTA000033558530.

Law No. 2017-399 of March 27, 2017 on the duty of care of parent companies and contracting companies, JORF, No. 74, March 28, 2017.

Law No. 2016-1321 of October 7, 2016 on a digital republic, JORF No. 0235 of October 8, 2016. Labor Code, Art. L.8222-1 et seq.

Civil Code, Art. 1130, 1131, 1137, 1178, 1240, and 1241.

Monetary and Financial Code, Art. L.561-5 and R.561-5.

IV. Doctrine and institutional relations

French Anti-Corruption Agency (AFA)

AFA, *Recommendations to help legal entities prevent and detect corruption, influence peddling, extortion, illegal taking of interest, embezzlement of public funds, and favoritism*, Dec. 4, 2020, § 205-207, available at: https://www.agence-francaise-anticorruption.gouv.fr.

AFA, *Opinion on recommendations to help legal entities prevent and detect acts of corruption*, Jan. 12, 2021.

AFA, *Collection of practical fact sheets – Public information bases useful for assessing the integrity of third parties*, March 9, 2023, available at: https://www.agence-francaise-anticorruption.gouv.fr/fr/document/afarecueil-fiches-pratiques-bases-publiques.

AFA, *National assessment of anti-corruption measures in companies*, 2024, available at: https://www.agence-francaise-anticorruption.gouv.fr.

AFA, *Draft practical information sheets on implementing third-party assessment measures with regard to the risk of corruption within companies*, July 2025.

AFA, *Presentation of foreign standards promoting integrity in business*, 2023.

Other doctrinal sources

PORTER, Michael E., *Competitive Advantage: Creating and Sustaining Superior Performance*, Free Press, New York, 1985, 557 p

V. Comparative law

United Kingdom

UK Bribery Act 2010, law of April 8, 2010, available at: https://www.legislation.gov.uk/ukpga/2010/23/contents/enacted.

Economic Crime and Corporate Transparency Act 2023, October 26, 2023, c. 56, available at: https://www.legislation.gov.uk/ukpga/2023/56/enacted.

Ministry of Justice, *Guidance about procedures that relevant commercial organisations can put in place to prevent persons associated with them from bribing* (section 9, Bribery Act 2010), 2025, available at: https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

United States

Foreign Corrupt Practices Act (FCPA), 1977.

U.S. Department of Justice and Securities and Exchange Commission, *A Resource Guide to the U.S. Foreign Corrupt Practices Act,* 2nd ed., 2020, available at: https://www.justice.gov/criminal/criminal-fraud/file/1292051/dl .

U.S. Department of Justice, *Justice Manual. 9-47.120 – FCPA Corporate Enforcement Policy,* 2019, available at: https://www.justice.gov/criminal/criminal-fraud/file/838416/dl.

U.S. Department of Justice – Criminal Division, *Evaluation of Corporate Compliance Programs,* 2020, available at: https://www.justice.gov/criminal/criminal-fraud/ page/file/937501/dl?inline=.

Germany

Law on Corporate Due Diligence in Supply Chains (Lieferkettensorgfaltspflichtengesetz – LkSG), BGBl. I, No. 46, July 22, 2021, p. 2959.

Netherlands

Child Labor Duty of Care Act, Parliamentary Document 34506-A, May 14, 2019.
Human Rights and Environmental Due Diligence Act, 2024.

Brazil

Lei Anticorrupçao, August 1, 2013.

VI. Practical sources and institutional websites

CNIL, *Practical Guide to the GDPR – Personal Data Security*, 2024.

ENISA, *Technical Implementation Guidance on Cybersecurity Risk Management Measures,* June 2025, available at: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf.

OSINT Framework, available at: https://osintframework.com/. French government APIs: https://api.gouv.fr/les-api/api_data_gouv.

OFAC, *Sanctions List Search,* available at: https://sanctionssearch.ofac.treas.gov/. Asset Freeze Register, available at: https://gels-avoirs.dgtresor.gouv.fr/List. AML-CFT, available at: https://lcb-ft.fr.

ACPR, *Official Register Guidelines,* available at: https://acpr.banque-france.fr/fr/reglementation/registre-officiel/lignes-directrices.

AFJE, *Video on international sanctions,* available at: https://www.afje.org/ressources/compliance-video-sur-les-questions-relatives-aux-sanctions-internationales--494.

Appendices

Appendix 1: Checklist of points to verify in the context of third-party risk management

I. General checks

1. IDENTIFICATION OF THE PERSONBEINGASSESSED

A. Natural person

- Name
- First name
- Address
- Date and place of birth
- Contact

B. Legal entity

B-1 Identification
- K BIS or local equivalent
- SIRET number
- SIREN number
- VAT No.

DUNS No.
- Existence of sanctions/convictions

B-2 Legal form
- Legal form
- Listing on a regulated market

B-3 Governance: Corporate officers
- Name
- First name
- Date of birth and place of birth
- Existence of penalties/convictions
- Existence of conflicts of interest between the third party's corporate officers and the company

B-3 bis Governance: Other governance bodies

Identified element	Information gathered			
2. Identification of beneficial owners	Name	First name	Date and place of birth	Existence of sanctions/ convictions
3. Identification of public officials and politically exposed persons	Participation of public officials or PPE within the third party's organization	Presence of public officials or public officials' spouses among the third party's shareholders or beneficial owners	Identification of potential conflicts of interest due to the presence of a public official or PEP in the shareholding or governance of the third party	
4. Identification of current and past business relationships between the third party and the ordering entity	History of relations with the third party (contract references, dates)	Services currently provided by the third party (contract description)		
5. Combating undeclared work (duty of care)	Verification of compliance with reporting obligations (URSSAF compliance certificate, list of foreign workers, k bis)			

II. Identification of risks related to the service provided

Identified element	Information gathered			
1. Effective performance of the service/ Identification of subcontractors	Use of subcontractors by the service provider to perform the contracted service	Identity of subcontractors	Tasks performed by subcontractors	Links (family, interests, etc.) likely to give rise to conflicts of interest with the subcontractor
2. Identification of risks in relation to geographical areas and activities	Location where the service is provided (country)	Identification of the location/country of production sites and assessment of risks in countries with a high risk of corruption (according to Transparency International's ranking)	Identification of activities requiring administrative authorizations/ licenses	Use of intermediaries/ agents
3. dentification of risks of economic dependence of the third party	Percentage of the third party's turnover currently generated by the client company and relationship with the third party's overall turnover			
4. Financial information	Balance sheets for the last three financial year,	Financial solvency information (ratings) provided by a central bank	Identification of the bank receiving payments related to the contrac	BAN of the account receiving payments related to the contract and certification of the IBAN

III. Identification of information to be collected due to legal assessment obligations

A. Identification of the subcontractor's compliance with the DORA regulation				
Importance of the service provided to the financial institution (nature, role in its service provision, % of turnover concerned, etc.)	Plan de continuité d'activité	Plan de gestion des incidents	Existence de sous-traitants chez le prestataire	Moyens mis en œuvre par le tiers pour contrôler la sécurité des sous-traitants et leur conformité aux exigences de DORA
Certifications obtained in the field of personal data protection/IT security	Cybersecurity measures implemented	Information security policy	Digital operational resilience testing	

B. Identification of the subcontractor's compliance with the GDPR				
Purpose and duration of the service	Nature and purpose of processing	Type of personal data processed and categories of data subjects	Place where data is stored	Retention period for personal data
Keeping a processing record	Measures put in place to ensure data processing complies with GDPR requirements: • Guarantee of compliance with the principle of necessity • Guarantee of data retention period • Guarantee of the number of people with access to the data • Guarantee of the scope of data pocessing • Guarantees related to data deletion			Information systems security policy in place (need to obtain proof)
Presence of a DPO, DPO certification level	Use of subsequent data processors	Controls designed to ensure the subcontractor's compliance with GDPR data protection standards	Confidentiality obligation for employees in contact with the personal data collected	Certifications obtained in the field of personal data protection /IT security
Cybersecurity measures in place	Information security policy			

C. Identification of the subcontractor's compliance with the NIS 2 directive			
Information security policy implemented	Cyber risk analysis policy in place	Incident management plan	Business continuity plan (backup, disaster recovery, and crisis management procedures)
Existence of subcontractors working for the service provider	System for monitoring subcontractors' cybersecurity measures	Security measures applied to networks and information systems (particularly during their acquisition, development, and maintenance)	Policy for monitoring the effectiveness of existing cyber risk management measures
Basic cyber hygiene practices (backups, software updates, etc.) and staff training in cybersecurity	Data encryption and encoding system	Policy for controlling access and managing assets	Measures to secure authentication
Human resources security policy (management of data collected during recruitment, employees' personal data, etc.)	Secure emergency communication systems set up within the entity	Certifications obtained in the field of personal data protection/IT security	Procedure for reporting significant incidents in place

D. Identification elements relating to funds (AML-CFT)

Natural person	Legal entity
Financial and professional situation (annual income and occupation)	Financial situation (annual turnover)
Proof of residence	Proof of address
Source of funds	Source of funds
Destination of funds	Existence of third parties and nature of the relationship between the customer and third parties
Existence of third parties and nature of the links between the client and third parties	Articles of association
	Corporate purpose
	Business sector

E. Identification elements relating to export controls (related to the nature of the goods AND/OR SERVICES)

Identity of the end user: **- Natural person (see IB. Identification of the legal entity)** **- Legal entity (see IB. Identification of the legal entity)**	Identity of stakeholders involved in the transaction (intermediaries, subcontractors, etc.)	Beneficial owners of the end user	Identity of the beneficial owners of the parties involved in the transaction
Proof of identity of the parties involved (intermediary, end user, etc.)	International sanctions imposed on the third party or a stakeholder	Means of financing the acquisition	Measures implemented to control the risk of misappropriation

F. Identification elements relating to the monitoring of human rights' and environmental violations by actors in the value chain	
Environmental impact of the third party's activity: • Water pollution • Soil pollution • Greenhouse gas emissions • Waste and recycling	Measures to ensure the safety of workers involved in third-party activities • Measures taken to guarantee employees' fundamental rights (freedom of association, freedom of union membership, etc.) • Compliance with safety measures prescribed by law for employees • Other measures designed to ensure employee safety
- Actions implemented by the third party to monitor human rights and environmental violations in its supply chain	- Certifications received by the third party in the areas of human rights and environmental protection

G. Identification elements relating to the fight against corruption		
- Identification of anti-corruption standards applicable by the third party (Sapin 2, UK Bribery Act, FCPA)	- Code and procedures for combating corruption in force within the company	- Processes implemented under the Sapin 2 law (internal alert system, third-party assessment, risk mapping, etc.) FCPA, UK, Bribery Act

IV. Identification of information to be collected due to legal assessment obligations

CSR Information			
Third party CSR approach and supporting documents	Data collection within the value chain due to the CSRD	Annual CO_2 emissions volume	Annual CO_2 emissions of members of the value chain

Appendix 2: **Summary table of legal obligations for third-party assessment**

Text	General third-party assessment obligation	Threshold for obligation	Geographic location	Sector-specific obligation	Nature of due diligence to be performed
Combating undeclared work/ Duty of care. (France)		Companies using service providers for amounts exceeding €5,000 excluding tax	Companies established in France		Collection and verification of: -URSSAF certificate -List of foreign workers -K-BIS extract or equivalent -Tax compliance certificate
AML-CFT (France, Europe) Order No. 2020-115 of February 12 2020 strengthening the national system for combating money laundering and terrorist financing. Directive (EU) 2018/843		No threshold	Within the territory of the European Union Or Companies established outside the EU whose activities target European residents	Financial sector players (banks, electronic money institutions, etc.) and Professions likely to be involved in money laundering (lawyers, notaries, judicial officers, etc.)	Database screening (PEP, sanctions, etc.) Questionnaire relating to the client's identity and the nature of the funds (source, use, etc.) Collection of supporting documents Verification of the identity of the third party (using a method approved by the regulations, e.g., a service provider using biometrics)

Text	General third-party assessment obligation	Threshold for obligation	Geographical location	Sector-specific obligation	Nature of due diligence to be performed
Export control (Europe) Regulation (EU) 2021/821 of May 20, 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items		No threshold	Exports of goods outside European territory Transit of goods within European territory	Production/supply of dual-use goods	Questionnaire on the end use of the goods Database screening (international sanctions, adverse media, etc.) Collection and verification of stakeholder identities (end users, intermediaries, etc.) Document management (invoices, export accompanying documents, usage reports)
Digital Operational Resilience Act (DORA) (Europe) European Regulation 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector		No threshold	-Companies offering financial services within the European Union - Providers offering digital services to financial entities covered by this text	Companies in the financial sector (banking, insurance, electronic money institutions, etc.)	Third-party criticality assessment questionnaire (determining the financial entity's level of dependence on the service provider) Cybersecurity and resilience questionnaire (service provider's IT security measures, incident management procedures, tests performed, etc.) Contractual clauses governing the use of subcontracting by the service provider Audits of the subcontractor's cybersecurity and data protection measures. Maintenance of a register of ICT service providers listing all providers involved in the operation of the financial entity's information systems

Text	General obligation to assess third parties	Obligation threshold	Geographical location	Sectoral obligation	Nature of the diligence to be performed
GDPR (Europe) General Data Protection Regulation (EU Regulation 2016/679)		No threshold	Company established within the EU Or Company established outside the EU whose activity targets European residents	Any company involved in collecting/processing personal data	Audit to verify the subcontractor's compliance with GDPR rules (retention period, data processing register, etc.) Questionnaire on the procedures put in place to ensure data security (physical protection measures, software, backups, etc.) Collection of documents proving compliance with GDPR rules (certifications, etc.) Questionnaires to identify subsequent processors Contractual clauses limiting/regulating subsequent subcontracting and data transfers outside the EU
NIS 2 (Europe) Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union		Companies exceeding: +50 employees $1 million in revenue (with some exceptions) (measures applied to SMEs are less stringent)	Company with an establishment within the EU Or Company established outside the EU whose activity targets European residents	Public and private companies in sectors of general interest: health, finance, waste management, etc.	Regular audits of the compliance of the subcontractor's cybersecurity and data protection measures with the standards of the directive (business continuity plan, disaster recovery plan, staff training, etc.) Cybersecurity and resilience questionnaire (IT security measures in place, incident management procedure) Contractual clause incorporating the requirements of the Cybersecurity Directive
Cyber resilience act (Europe) European Regulation 2024/2847 of November 20 2024 on horizontal cybersecurity requirements for products with digital elements			Companies contributing to the marketing on the European market of products containing digital elements whose use includes a connection to a network (manufacturers, importers, distributors)	Companies that manufacture/import/distribut e digital products Digital product: software or hardware product and its remote data processing solutions, including software and hardware components sold separately Example: connected devices (smartphones, etc.), software associated with these devices, components of these devices	Questionnaires relating to product risks and vulnerabilities (measures to eliminate vulnerabilities, security updates, access protection, data protection and processing, resilience measures, etc.) Contractual clauses incorporating the requirements of the directive

Appendix 3: **Questionnaire and documents to be provided for the audit of entities subject to the SAPIN 2 law**

G. Assessment of the integrity of third parties: customers, primary suppliers, intermediaries[79]

G.1. Do you have one or more databases listing all your third parties? Have you identified homogeneous groups of third parties with comparable risk profiles? If so, how and what is their level? In particular, has the corruption risk mapping of the controlled entity been used? If so, how?
G.2. Does the audited entity have a specific third-party assessment system or one that incorporates corruption risks? Is this third-party assessment system broken down by homogeneous groups of third parties with comparable risk profiles? If so, what typologies has the audited entity adopted?
Provide any documents relating to the third-party assessment system with regard to the risks of corruption within the audited entity.

G.4. Indicate the functions or departments responsible for assessing the integrity of third parties according to the different types. Is an external service provider used to assess these third parties? Provide any documents defining the roles and responsibilities of employees in charge of or supporting the assessment of third parties.
G.5. Is the third-party integrity assessment system implemented within the controlled entity (particularly within groups, business lines, divisions, business units, or subsidiaries)? If so, how?
Are there different systems within certain groups, business lines, divisions, business units, or subsidiaries?
G.6. How were the due diligence procedures to be performed (method,

79. https://www.agence-francaise-anticorruption.gouv.fr/fr/document/questionnaire-et-pieces-fournir-au-controle-des-entites-assujetties-larticle-17-juillet-2021.

frequency, nature of procedures, etc.) by homogeneous groups of third parties defined? Provide any documents describing the due diligence procedures to be performed by homogeneous groups of third parties.

G.7. What due diligence is performed based on the risks identified (in particular through the use of open source data, documents requested from third parties, consultation of internal and external lists, interviews, audits, etc.)? Following the due diligence performed, is a specific risk rating or an overall risk rating assigned?

G.8. What is the validation process (opinion, consultation, decision) following the third-party assessment?

G.9. What are the procedures for updating and monitoring third-party assessment files (in particular their frequency, defined according to the nature and level of risk, and the department responsible for updating and monitoring them)?

G.10. How are non-compliant files handled (e.g., incomplete files or questionnaires, expired update deadlines)? Provide any documents relating to the handling of non-compliant files.

G.11. Are there any exemption procedures for the third-party assessment system (covering, where applicable, specific transactions or projects, a specific category of third parties, a defined threshold level, etc.)? If so, what are they and what are the criteria?

G.12. Specify the procedures and time limits for retaining and archiving third-party assessment files.

G.13. Who is responsible for first-level control? Describe the control method used to ensure compliance with the third-party assessment procedure and the completeness of the files (in particular, required documents, mandatory opinions, and approvals).

G.14. Who is responsible for second-level control? Present the control method used to ensure that first-level controls are properly executed and that the third-party assessment system is functioning correctly.

G.15. Is there a third-level control to ensure that the third-party assessment

system complies with regulatory and internal requirements and is effectively implemented and maintained? If so, who performs it?

G.16. Is the third-party assessment system supported by one or more information systems? If so, which ones? Provide any documents relating to this or these information systems.

G.17. What vigilance measures, specific to the risks identified, are taken, where applicable, following the assessment, to control risks during the relationship with the third party at risk (in particular, appropriate procedures and update frequencies, targeted controls, monitoring of financial flows)?

G.20. Are there any specific assessment procedures for other types of third parties (beneficiaries of sponsorship or partnership initiatives, acquisition targets, lobbyists, business partners, etc.), where applicable, through specific audits or accounting controls?

G.21. If the controlled entity has decided to communicate its anti-corruption commitment to third parties, how is this communication carried out (in particular, contractual clauses, external communication)? Provide any documents evidencing the communication of this commitment.

Appendix 4: **Examples of integrity risk signals**

EXAMPLES OF INTEGRITY RISK SIGNALS
A Partner is owned or controlled by public officials or civil servants, or employs them.
The third party is owned or controlled by a director, officer, or employee of our company or members of their immediate family.
The third party is recommended by a public official or expressly requested by a customer, unless technical requirements dictate otherwise.
The third party suggests that it could avoid or expedite certain formalities or a bidding process.
The third party has been subject to criminal proceedings related to corruption, either directly or through its legal representatives.
The third party clearly lacks the necessary skills or resources.
The third party refuses to provide relevant background information or to submit to an audit.
The third party refuses a contractual clause requiring the co-contractor, and in particular an intermediary, to justify services in support of its payment request.
The third party refuses to include anti-corruption provisions in a contract.
The third party requests terms and conditions that are unusual or contrary to market practices and/or when the specific nature of the services provided is unclear.
The third party proposes unusual payment methods or financial arrangements (payment in cash, to another account, in another country).
The third party offers or promises lavish benefits or gifts that exceed customary practice: prepaid tourist trips, invitations to high-profile sporting or cultural events.

Glossary

AFA: French Anti-Corruption Agency
AFJE: French Association of Corporate Lawyers
API: Application Programming Interface
CA: Turnover
COMEX: Executive Committee
CRA: Cyber Resilience Act
CRM: Customer Relationship Management
CSRD: Corporate Sustainability Reporting Directive
CSDDD: Corporate Sustainability Due Diligence Directive
DORA: Digital Operational Resilience Act
IT Department: Information Technology Department
DUNS: Data Universal Numbering System
ECCTA: Economic Crime and Corporate Transparency Act
ERP: Enterprise Resource Planning
FCPA: Foreign Corrupt Practices Act
AI: Artificial Intelligence
IBAN: International Bank Account Number
JEM: Corporate Lawyer Magazine (AFJE)
KBIS: Official document certifying the legal existence of a company in France
AML-CFT: Anti-Money Laundering and Counter-Terrorist Financing
MSA: Mutualité Sociale Agricole
NIS: Network and Information Systems Security
OFAC: Office of Foreign Assets Control
UN: United Nations
OSINT: Open Source Intelligence
PEP: Politically Exposed Person
SME: Small and Medium-sized Enterprise
R&D: Research and Development
GDPR: General Data Protection Regulation
CSR: Corporate Social Responsibility
IS: Information System
SIREN: Company identification number
SIRET: Establishment Identification Number
ISMS: Information Security Management System
ICT: Information and Communication Technologies
TPRM: Third Party Risk Management VAT: Value Added Tax
EU: European Union
UK: United Kingdom
URSSAF: Union for the Collection of Social Security Contributions and Family Allowances
US: United States