TPRM

De l'évaluation des tiers au Third Party Risk Management

Livre blanc du Strategic Compliance Studies Committee de French Compliance Society

FRENCH COMPLIANCE SOCIETY

TPRM

De l'évaluation des tiers au Third Party Risk Management

Livre blanc du Strategic Compliance Studies Committee de French Compliance Society

FRENCH COMPLIANCE SOCIETY

English version available at:
https://www.evaltiers.eu

EN PARTENARIAT AVEC

AFJE Les Juristes d'Entreprise

Forward

ÉVALTIERS www.evaltiers.eu

VERDUN VERNIOLE AVOCATS

AVERTISSEMENT

Le présent livre blanc a été réalisé par des professionnels de la compliance sur la base de leur expérience et de leurs réflexions sur la mise en œuvre des obligations légales d'évaluation des tiers et plus généralement sur une démarche de *Third Party Risk Management* pour y répondre. L'analyse proposée dans ce document ne préjuge pas de la position du législateur, du régulateur ou du juge, ni de celle d'Aramis Group et de Hertz Corporation sur ce sujet. Ce livre blanc ne saura être interprété comme du conseil juridique et n'engage pas ses auteurs ou leurs sociétés ou organisations respectives.

AUTEURS

Stéphanie Corbière

Head of Legal and compliance & Secretary of the board, Aramis Group, Coresponsable de la Commission Managers Juridiques et Copilote du Groupe scientifique IA de l'AFJE, membre du Strategic Compliance Studies Committee

Camélia Gardot

Directrice Compliance, Hertz Corporation, membre du Strategic Compliance Studies Committee

Franck Verdun

Avocat à la cour, fondateur de Verdun Verniole avocats et Eval'tiers, membre de la French Compliance Society

AVEC LA PARTICIPATION DE

Carmen Briceno, Directrice juridique & conformité Groupe chez Raja, Responsable de la Commission compliance de l'AFJE

Catherine Delhaye-Kulich, Chief Ethics, Compliance and Data Protection Officer, chez le Groupe Valeo

Isabelle Cadet, Maître de Conférences IAE Paris-Sorbonne, Université Paris 1 Panthéon-Sorbonne

Makeda Cardenas, Compliance Officer, pour le Groupe la Poste

Ling Ho, Partner Forward Global

Stéphanie Dominguez, Dirigeante Actuo

Sommaire

Introduction

L'évaluation du tiers est l'action qui consiste à recueillir des informations sur un partenaire afin de vérifier tant l'opportunité d'engager la relation que de la poursuivre.

Il n'est pas besoin de souligner l'importance de la relation entre l'entreprise et sa chaîne de valeur et les tiers qui la composent (fournisseurs, prestataires, clients). Celle-ci conditionne en effet sa capacité à produire et vendre ses offres. Elle participe donc à la finalité de l'entreprise qui est la création de valeur. Dès lors, procéder à une gestion des risques de la chaîne de valeur incluant l'évaluation des tiers avec qui l'entreprise envisage de nouer une relation contractuelle s'apparente à une bonne pratique de gestion.

Cependant, les caractéristiques même de la chaîne de valeur rendent la gestion de ses risques complexe :

- Nombre important de parties prenantes : du côté amont (fournisseurs, prestataires de services), ce volume peut rapidement devenir considérable. La démarche d'évaluation des tiers nécessite ainsi de mobiliser de nombreux interlocuteurs au sein de l'entreprise et de leur confier des tâches de recueil d'informations perçues comme chronophages et peu créatrices de valeur. C'est ainsi que les obligations d'évaluation des tiers dans les programmes de conformité sont souvent identifiées comme la mesure la plus délicate à mettre en œuvre. Dans le « Diagnostic national sur les dispositifs anti corruption dans les entreprises 2024 », l'Agence Française Anti-Corruption (AFA) relève que « *les entreprises rencontrent des difficultés sur la volumétrie et la diversité des tiers à évaluer, nécessitant des ressources importantes. Les entreprises ne trouvent pas toujours les outils adaptés à cette procédure, notamment pour recueillir des informations qui peuvent être purement déclaratives et manquer de fiabilité*[1] ».

1. Agence Française Anticorruption (AFA), *Diagnostic national sur les dispositifs anticorruption dans les entreprises,* 2024, disponible sur diagnostic national entreprises 2024_AFA.pdf.

La gestion des risques de la chaîne de valeur doit donc s'attacher à déterminer quels sont les tiers à évaluer et suivant quelles diligences afin d'éviter une consommation de ressources démesurées. Le régulateur et en particulier l'AFA précise ce point dans ses recommandations « *La nature et la profondeur des évaluations à réaliser et des informations à recueillir sont déterminées en fonction des différents groupes homogènes de tiers présentant des profils de risques comparables, tels que la cartographie des risques permettent de les dresser. Ainsi, les groupes de tiers jugés pas ou peu risqués pourront ne pas faire l'objet d'une évaluation ou faire l'objet d'une évaluation simplifiée, tandis que les groupes les plus risqués nécessiteront une évaluation approfondie*[2] ».

- Multiplicité des interactions internes avec les tiers sans gouvernance centralisée : au sein de l'entreprise même, des collaborateurs peuvent être en relation avec les mêmes tiers, dans le cadre de leurs fonctions respectives, sans disposer d'une vision globale du tiers et des risques qui y sont associés. La gestion des risques de la chaîne de valeur doit donc permettre d'offrir une information complète sur le tiers identifié à risque, quel que soit le motif de l'entrée en relation.

La gestion des risques de la chaîne de valeur doit donc s'attacher à identifier les risques qui naissent de la relation avec les tiers et qui peuvent avoir de graves conséquences sur l'entreprise.

Deux catégories principales de risques peuvent impacter la chaîne de valeur. En premier lieu les **risques opérationnels**, ainsi à titre d'exemples :

- défaut de compétences et de ressources suffisantes du tiers, notamment financières, pour répondre aux obligations contractuelles souscrites ;
- dépendance économique du tiers susceptible d'entraîner une requalification de la relation contractuelle, ou bien à l'inverse, dépendance stratégique vis-à-vis des services ou ressources livrées par le tiers ;

2. AFA, *Recommandations de l'Agence française anticorruption destinées à aider les personnes morales à prévenir et à détecter les faits de corruption, trafic d'influence, concussion, prise illégale d'intérêts, détournement de fonds publics et favoritisme* [en ligne], 4 déc. 2020, § 207.

- risque cyber lié à la non-conformité technique du tiers prestataire ;
- risque d'image liée à des carences éthiques, de violation des droits humains ou d'atteintes graves à l'environnement dont le tiers serait à l'origine et qui pourraient impacter le donneur d'ordre.

En second lieu, les risques juridiques qui résultent d'un défaut de conformité aux obligations légales d'évaluation des tiers résultants de diverses législations, notamment ceux liés l'intégrité, à la lutte contre le blanchiment, au financement du terrorisme, aux infractions relatives aux droits humains, et ceux résultants de la sous-traitance de données personnelles.

La multiplicité des risques liés à la relation avec les tiers dans la chaîne de valeur impose de mettre en œuvre une approche globale de gestion des risques connue sous le nom de *third party risk management* (TPRM). Basé sur une approche par les risques, le TPRM doit permettre d'identifier et d'évaluer dans la chaîne de valeur de l'entreprise tant ses risques opérationnels majeurs que de répondre aux obligations légales d'évaluation des tiers auxquelles l'entreprise est soumise. Ainsi l'objet du TPRM est de préserver et d'optimiser la création de valeur par l'entreprise au-delà de permettre une simple conformité légale à l'obligation d'évaluer ses tiers (I).

L'approche TPRM facilite la définition d'une politique d'évaluation des tiers à l'entreprise. Celle-ci, basée sur une cartographie globale des risques de la chaîne de valeur doit permettre d'identifier et d'évaluer les risques des catégories de tiers à évaluer, et de définir des diligences d'évaluation selon les risques identifiés. Cette approche holistique évite des process d'évaluations de tiers redondants et chronophages et prévient ainsi un défaut de mutualisation de l'information sur le tiers au sein même de l'entreprise.

La politique d'évaluation des tiers a pour finalité la prise de décision sur la relation avec le tiers : validation de la relation sans restriction, validation avec mise en œuvre d'un plan de traitement, rejet du tiers, celui-ci pouvant être définitif ou temporaire (II).

La politique d'évaluation des tiers doit être effectivement déployée dans l'entreprise, ce qui implique une prise en main et des actions réalisées par les collaborateurs de l'entreprise en relation avec les tiers. En outre, le processus doit pouvoir être contrôlé afin de vérifier que la politique d'évaluation des tiers est respectée (III).

Le processus plaide pour sa digitalisation compte tenu de la multiplicité des acteurs internes en charge de l'évaluation des tiers (opérationnels, conformité, instance dirigeante), des informations à recueillir du tiers ou de bases de données externes, puis à traiter afin de fonder une décision de rejet ou de validation (IV).

L'AFA a publié pour consultation au mois de juillet 2025 un projet de fiches pratiques (ci-après « Fiches Pratiques ») sur la mise en œuvre d'un dispositif d'évaluation des tiers au regard du risque de corruption au sein des entreprises. (https://www.agence-francaise-anticorruption.gouv.fr/fr/lafa-lance-consultation-publique-jusquau-30-septembre-2025-sur-projet-fiches-pratiques-relatives)[3].

Cette publication vise spécifiquement la procédure d'évaluation des tiers prévue par l'article 17 4° de la loi dite Sapin 2 et nous y ferons référence tout au long du présent Livre blanc. Les fiches pratiques abordent en effet des sujets communs avec une approche TPRM, tels que la gouvernance de la procédure, l'évaluation des risques du tiers et de la catégorie à laquelle il appartient, et la nature des diligences d'évaluation à réaliser.

3. *Projet de Fiche Pratique,* [en ligne], juillet 2025.

I. Le Third Party Risk Management, une démarche qui résulte du management des risques de la chaîne de valeur

Le *Third Party Risk Management* a pour objectif de proposer un processus d'évaluation des tiers en lien avec le management global des risques de la chaîne de valeur. C'est en effet en identifiant les vulnérabilités des parties prenantes de la chaîne de valeur que l'entreprise peut mettre en œuvre des mesures de traitements qui pérennisent et améliorent son processus de création de valeur (1). Ces risques peuvent être inhérents à l'entreprise et à ses acteurs (2). Ils peuvent également résulter d'obligations légales obligeant les entreprises à mettre en œuvre des diligences particulières (3).

1.1 La notion de chaîne de valeur et de tiers

La notion de chaîne de valeur est issue du management stratégique des entreprises et des travaux réalisés par M. Porter dans les années 1980 [4]. L'objet de la chaîne de valeur était alors d'identifier les différents « *maillons* » de l'activité de l'entreprise afin d'évaluer leur contribution à la création de valeur finale de l'offre de l'entreprise. Cet exercice permet d'identifier les activités cruciales à la création de valeur afin de les optimiser et permettre ainsi à l'entreprise de fournir une offre susceptible de créer l'avantage concurrentiel (soit l'offre créant le plus de valeur pour le client par rapport à la concurrence).

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

La notion de chaîne de valeur est désormais utilisée de façon plus large, notamment grâce à la RSE. Ainsi la Directive *Corporate Sustainability Reporting* (CSRD) définit la chaîne de valeur comme « *L'ensemble des activités, ressources et relations liées au modèle économique de l'entreprise ainsi qu'à l'environnement extérieur dans lequel elle exerce ses activités (...) La chaîne de valeur comprend les acteurs situés en amont et aval de l'entreprise (les fournisseurs, par exemple) fournissent des produits ou des services qui servent à l'élaboration des produits ou services de l'entreprise. Les entités situées en aval de l'entreprise (les distributeurs et les clients, par exemple) reçoivent des produits ou services de l'entreprise*[5] *(...)*».

Cette notion se rapproche également de la notion de chaine d'approvisionnement qui est définie comme « *L'ensemble des activités ou des opérations menées par les entités en amont de l'entreprise, qui fournissent des produits ou des services dont entreprise se sert pour élaborer et produire ses propres produits ou services. Cela concerne les entités situées en amont avec lesquelles l'entreprise entretient une relation directe (souvent appelées fournisseurs de premier rang) ou une relation d'affaires indirecte*[6]».

Ainsi, la définition de la chaîne de valeur formulée par la CSRD permet à l'entreprise de définir le périmètre, sur lequel pourra s'opérer son management des risques incluant le *third party risk management.*

- **La notion de tiers :**

L'AFA défini le tiers comme toute personne extérieure à l'entreprise avec qui elle est, ou souhaite être en relation[7]. La notion de tiers selon l'AFA concerne les personnes avec lesquelles l'entreprise entretient des relations contractuelles mais aussi toutes celles avec laquelle elle envisage de nouer une relation, quelle que soit sa nature juridique. Le tiers peut ainsi être une personne physique, une personne morale de droit privé ou de droit public.

5. Annexe 2, *Règlement délégué (UE) 2023/2772 de la Commission du 31 juillet 2023 complétant la directive (UE) 2022/2464 du Parlement européen et du Conseil en ce qui concerne les normes d'information en matière de durabilité,* Journal officiel de l'Union européenne, 22 octobre 2023, p. 1-465.

6. *Ibid.* et Règlement (UE) 2023/1115 relatif à la mise à disposition sur le marché de l'Union et à l'exportation à partir de l'Union de certains produits de base et produits associés à la déforestation et à la dégradation des forêts.

7. AFA, *Fiche Pratique*, juillet 2025.

L'AFA ne définit pas de critères juridiques ou économiques qui permettraient de définir ou d'identifier les tiers à l'entreprise.

Cette définition large du tiers invite les entreprises à identifier l'ensemble des personnes qui interagissent avec elles pour appliquer une approche par les risques, fondée sur la cartographie des risques du programme de conformité anti corruption afin de définir les tiers à évaluer.

Risque financier	Le tiers ne dispose pas (ou plus, en cours d'engagement) des ressources financières pour honorer ses obligations contractuelles. Cette dimension intègre également le *credit management* dans la relation client.
Risque de dépendance	Le donneur d'ordre peut être dépendant de son cocontractant parce qu'il est le seul à fournir des compétences ou ressources rares indispensables à la réalisation de son offre. Un cocontractant peut être dépendant au plan économique du donneur d'ordre, ce qui peut entraîner un risque de requalification juridique de la relation ou d'indemnisation au titre de l'abus de dépendance économique.
Risque lié aux facteurs géographique/ politique	La zone géographique où se trouve domicilié le cocontractant peut être à l'origine de risques spécifiques : absence, instabilité ou inconsistance de la réglementation applicable, événements sociaux ou politiques rendant l'exécution des obligations impossibles… A noter que la responsabilité des filiales opérant dans ces zones peut engager celle de leur société mère en application de textes spécifiques : devoir de vigilance, *UK Bribery Act** etc.
Risque de réputation lié à l a sous-traitance	Le cocontractant peut avoir recours à une chaîne de sous-traitants mal identifiés pouvant être à l'origine de risque de réputation. Il s'agit ici du risque du « quatrième partie » soit par exemple le fournisseur de celui de premier rang.
Risque lié à la faible maturité conformité/ juridique du tiers	Le cocontractant peut disposer d'une faible maturité juridique/compliance pouvant être à l'origine de risques réputationnel ou juridique pour le donneur d'ordre.

* *UK Bribery Act* 2010, Loi du 8 avril 2010, Royaume-Uni, Section 7 « Failure to Prevent Bribery », disponible sur Bribery Act 2010.

Risque lié à la sous-traitance d'opérations de traitement des données personnelles	L'entreprise doit s'assurer que le tiers disposant d'un accès aux données personnelles qu'elle traite est conforme à ses obligations de sous-traitant de données en matière de transparence, de limitation et de traçabilité des données, de protection des données, de conseil et d'assistance du client. Ces obligations sont mises en œuvre par un dispositif contractuel, mais le responsable de traitement peut également interroger par questionnaire le sous-traitant sur les modalités techniques et organisationnelles mises en œuvre pour y répondre.
Les risques IT ou cyber liées à la relation de l'entreprise avec les tiers	La notion de chaîne de valeur telle que définie par la CSRD restitue la notion « d'entreprise étendue » qui se traduit par une intégration des tiers par voie numérique. Si cette intégration est une source de création de valeur (rapidité de l'échange et du traitement de l'information) elle peut être source de risques opérationnels liés à un manque de maturité IT ou cyber des tiers. La norme ISO/IEC 27001 constitue un référentiel de système de management de la sécurité de l'information (SMSI) permettant de mesurer le niveau de maturité du système d'information du tiers qui entrera en relation avec celui de l'entreprise*. Une analyse d'écart (gap analysis) entre les préconisations d'ISO 27001 et l'existant du SI du tiers permettra d'identifier et de traiter les risques.

* CNIL, *Guide Pratique RGPD, Sécurité des données personnelles*, 2024 ; ENISA, *Technical Implementation Guidance on Cybersecurity Risk Management Measures* [en ligne], juin 2025, p.21-30.

1.2 Les risques inhérents à la chaîne de valeur

Le processus de management de risques appliqué à la chaîne de valeur permet donc d'identifier des catégories de tiers sensibles compte tenu de leur place et de leur apport à la chaîne de valeur (fournisseurs stratégiques, etc...) et, par un processus d'évaluation adapté au sein de ces catégories, d'identifier la vulnérabilité des tiers qui la composent.

1.3 Les obligations légales visant à procéder à l'évaluation des tiers

L'évaluation des tiers permet d'identifier des risques qui peuvent impacter la chaîne de valeur et l'entreprise et qui peuvent également avoir des conséquences négatives sur l'ordre public lui-même.

Ainsi les pouvoirs publics ont progressivement mis en œuvre des législations visant à contraindre les entreprises à évaluer leurs tiers afin d'identifier des risques d'infractions susceptibles de créer des troubles graves à l'ordre public, de respecter les politiques étatiques de sanctions internationales.

On peut distinguer des obligations de nature générale (s'appliquant à toutes les entreprises à partir d'un certain seuil d'effectif ou de chiffre d'affaires) et des obligations liées à la nature des opérations réalisées et qui seront donc sectorielles.

1.3.1 Obligations générales d'évaluation des tiers

1.3.1.1 Les obligations anticorruption

- L'article 17 4° de la loi française dite Sapin 2 oblige à la mise en place de procédures d'évaluation de tiers en lien avec une cartographie d'exposition aux risques de corruption afin d'apprécier l'intégrité et la réputation des tiers avant de s'engager dans une relation commerciale. Ces diligences peuvent inclure des vérifications sur leur historique, leur structure de propriété, leur conformité avec les lois anticorruption, et leur réputation dans le secteur. L'Autorité Française Anticorruption (AFA) a publié un projet de Fiches Pratiques visant à aider les entreprises à mettre en œuvre cette obligation[8].

- Le *UK Bribery Act* 2010[9] est une législation britannique qui vise à lutter contre la corruption au Royaume-Uni et à l'étranger. Le texte invite les entreprises à mettre en œuvre des mesures adéquates pour lutter contre la corruption, ce qui implique un processus d'évaluation des risques liés aux tiers. Cette loi est désormais renforcée par la création d'une infraction *failure to prevent fraud par l'Economic Crime and Corporate Transparency Act* (ECCTA). Les entreprises sont tenues d'évaluer leurs tiers et d'effectuer des diligences raisonnables afin de prévenir la fraude et les malversations commises par leurs tiers[10].

8. AFA, *op. cit.*
9. UK Bribery Act, *op. cit.*
10. L'infraction « *failure to prevent fraud* » instituée par l'*Economic Crime and Corporate Transparency* Act 2023 est entrée en vigueur le 1er septembre 2025 (Royaume-Uni, *Commencement Regulations* 2025, S.I. 2025/349).

- Le *Foreign Corrupt Practices Act*[11] (FCPA) est une loi américaine qui interdit aux entreprises et aux individus de procéder à des actes de corruption à destination de fonctionnaires étrangers dans le but d'obtenir ou conserver des affaires. Le Department of Justice (DOJ) des États-Unis et la *Securities and Exchange Commission (SEC)* ont fourni des orientations sur les bonnes pratiques pour se conformer au *FCPA*, y compris l'évaluation des risques liés aux tiers[12].

- La loi brésilienne anticorruption[13], (Loi nº 12.846/2013 ou *Lei Anti-corrupção*), impose aux entreprises des responsabilités en matière de prévention de la corruption, ce qui inclut implicitement l'évaluation des risques liés aux tiers. Les entreprises sont ainsi encouragées à effectuer une *due diligence* sur les tiers avec lesquels elles font affaire, en particulier ceux qui présentent un risque accru de corruption. Cela peut inclure des vérifications sur la réputation, les antécédents, et les pratiques commerciales des tiers.

Il est à noter que certains textes (ex. FCPA ou *UK Bribery act*) ont une portée extra territoriale. Ils peuvent s'appliquer à des entreprises de nationalité étrangère en raison de critères comme le lieu des faits, la nationalité des dirigeants, voire, dans le cas du FCPA, la cotation sur un marché boursier américain ou le paiement en dollars américains.

1.3.1.2 Les obligations en matière de vigilance sur la protection de l'environnement et des droits humains

La loi française sur le devoir de vigilance[14], promulguée en 2017, impose aux grandes entreprises de mettre en place un plan de vigilance pour identifier et prévenir les risques d'atteintes aux droits humains et aux libertés fondamentales, de dommages environnementaux graves et de corruption, résultant de leurs activités ainsi que de celles de leurs filiales, sous-traitants et fournisseurs.

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,* 2eeéd., 2020.
13. *Lei Anticorrupçao,* 1er aout 2013
14. Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre.

Dans ce cadre, Les entreprises doivent mettre en place des procédures pour évaluer la situation des fournisseurs et sous-traitants en ce qui concerne le respect des droits humains et de l'environnement. Cela peut inclure des audits, des questionnaires, et des vérifications sur site.

La loi allemande[15] sur les chaînes d'approvisionnement, connue sous le nom de *Lieferkettengesetz* impose aux entreprises des obligations spécifiques concernant l'évaluation des risques liés aux droits humains et à l'environnement dans leurs chaînes d'approvisionnement. Le texte inclut des dispositions qui obligent les entreprises à examiner et à gérer les risques associés à leurs partenaires commerciaux, y compris les fournisseurs et sous-traitants.

La loi norvégienne, *Norwegian Transparency Act* ou *Åpenhetsloven* prevoit une obligation de *due diligence*, afin d'identifier, prévenir et atténuer les atteintes réelles ou potentielles aux droits humains et aux conditions de travail dans la chaîne de valeur. Cette obligation concerne tous les partenaires de l'entreprise notamment les fournisseurs indirects. Les entreprises sont ainsi tenues de publier un rapport annuel pour justifier leur mise en conformité.

La loi néerlandaise[16], dite *Wet Zorgplicht Kinderarbeid* ou *Child Labour Due Diligence Act*, impose aux entreprises de prévenir le recours au travail des enfants dans leur chaine d'approvisionnement. Elles sont tenues de vérifier s'il existe un risque de travail des enfants. Lorsque le risque est identifié, elles doivent établir un plan d'action et publier une déclaration sur les mesures adoptées. Ces obligations s'imposent à toutes les entreprises immatriculées aux Pays-Bas mais également sur toutes celles intervenant dans le marché néerlandais au moins deux fois par an sauf lorsqu'elles sont expressément exclues par la loi. Toutefois, adoptée en 2019, la loi n'est pas encore applicable et sa date d'entrée en vigueur n'est pas connue. Un projet de loi s'inspirant de la *Corporate Sustainability Due Diligence Directive*, nommé Wet zorgplicht mensenrechten en milieu[17] prévoit d'élargir son champ

15. *Lieferkettensorgfaltspflichtengesetz,* 22 juillet 2021.
16. *Wet zorgplicht kinderarbeid,* Kamerstuk 34506-A, 14 mai 2019.
17. *Wet zorgplicht mensenrechten en milieu,* 2024

d'application en introduisant une obligation de *due diligence* en matière environnementale.

La *Corporate Sustainability Due Diligence Directive (CSDDD)*[18] est une directive européenne dont le périmètre et les obligations sont actuellement discutés dans le cadre du processus européen *Omnibus*. La CSDDD impose aux entreprises selon leurs seuils des obligations en matière de diligence raisonnable en ce qui concerne les impacts sur les droits humains et l'environnement des acteurs de leur chaîne d'activités. Ces diligences visent à identifier, prévenir, atténuer et rendre compte des impacts négatifs sur les droits humains et l'environnement dans leurs chaînes de valeur, y compris ceux liés aux activités de leurs tiers (fournisseurs, sous-traitants, etc.).

1.3.1.3 L'identification et la surveillance des sanctions internationales

Les sanctions internationales sont des mesures coercitives prises par un ou plusieurs pays, ou par des organisations internationales comme les Nations Unies ou l'Union européenne, pour contraindre un État, une entité ou des individus à changer de comportement ou de politique. A noter que la commission compliance de l'AFJE a publié une vidéo sur les sanctions internationales[19].

Concernant les entreprises, l'existence de sanctions doit être vérifiée pour la personne morale, ses actionnaires (hors sociétés cotées) et ses bénéficiaires effectifs. (voir la définition de la notion dans : *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). Une surveillance continue par *monitoring* doit être effectuée pour vérifier tout changement de statut au cours de la relation commerciale. L'existence de sanctions peut en général être vérifiée dans des registres tels

18. *Directive (UE) 2024/1760 du Parlement européen et du Conseil du 13 juin 2024 relative à la diligence raisonnable en matière de durabilité des entreprises.*

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

que le registre du gel des avoirs[20] pour les mesures de sanctions prises par la France, l'UE et l'ONU et sur le site de l'OFAC pour celles prises par les Etats Unis[21]. Le cabinet d'avocats NOVLAW met également à disposition un site permettant un accès gratuit aux sanctions internationales prises par la France, l'UE, la Grande Bretagne et les Etats Unis[22].

1.3.1.4 L'obligation de vigilance en matière de travail dissimulé

En France, l'obligation de vigilance du donneur d'ordre prévue aux articles L. 8222-1 et suivants du Code du travail[23] impose aux entreprises ayant recours à des sous-traitants pour des contrats d'un montant supérieur à 5 000 euros HT, de recueillir des pièces justifiant le respect de leurs sous-traitants de leurs obligations déclaratives, à savoir :

- un extrait Kbis ;
- une attestation de vigilance délivrée par l'Union de recouvrement des cotisations de sécurité sociale et d'allocations familiales (URSSAF) ou par la Mutualité sociale agricole (MSA) le cas échéant ;
- une attestation de régularité fiscale ;
- une liste de travailleurs étrangers.

Les vérifications doivent être effectuées tous les six mois jusqu'à la fin du contrat.

En cas de manquement à cette obligation, le donneur d'ordre peut être tenu solidairement responsable des faits de travail dissimulé reprochés à son sous-traitant et pourra alors être condamné au remboursement de ses dettes fiscales et sociales, au paiement d'amendes et se voir exclu de manière permanente de la participation à des marchés publics.

20. https://gels-avoirs.dgtresor.gouv.fr/List
21. https://sanctionssearch.ofac.treas.gov/
22. https://sanctions.fr/
23. Article L.8222-1 et suivants du code du travail.

1.3.1.5 L'évaluation des mesures destinées à assurer protection des données personnelles

Le règlement général sur la protection de données (« RGPD »)[24] impose aux responsables de traitement de données appartenant à des résidents de l'UE de s'assurer du respect des normes de protection des données personnelles par les sous-traitants intervenant dans leurs opérations de traitement[25].

Parmi les vérifications à réaliser on peut notamment citer, le contrôle des certifications du tiers, l'analyse de sa politique de sécurité de l'information et de sa procédure de gestion des incidents, l'audit de ses pratiques de gestion des données afin de contrôler sa conformité aux dispositions du RGPD (durée de conservation des données[26], registre de traitement[27]...). Le responsable de traitement devra également contrôler le recours par son sous-traitant à d'autres sous-traitants, et veiller à ce qu'il soit réalisé en conformité avec le RGPD[28]. Des questionnaires peuvent être utilisés, afin de recueillir ces informations.

Ces vérifications ainsi que les prestations du sous-traitant doivent être encadrées par des clauses contractuelles, pouvant notamment prévoir l'interdiction de sous-traitants ultérieurs[29].

1.3.2 Obligations sectorielles d'évaluation des tiers

1.3.2.1 L'évaluation des risques de blanchiment de fonds et de financement du terrorisme (LCB-FT)

La législation relative à la LCB-FT prévoit l'obligation pour les entreprises du secteur financier et certains prestataires exposés aux risques de blanchiment (L561-1 à L561-50 du code monétaire et financier) d'identifier leurs clients en collectant des informations

24. *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données).*

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

telles que le nom complet, la date de naissance, l'adresse et les coordonnées. Pour les entreprises, l'assujetti doit également recueillir des détails sur les actionnaires et les bénéficiaires effectifs. Ces informations doivent faire l'objet de vérifications par le recueil et le contrôle de pièces justificatives.

Le niveau de risque du tiers est évalué en fonction de son secteur d'activité, de sa localisation géographique et de ses antécédents.

Des mesures de surveillance sont ensuite appliquées selon le niveau de risque identifié. Une *due diligence* renforcée est requise pour les clients à haut risque, impliquant des vérifications supplémentaires sur l'origine des fonds et les relations d'affaires. Les transactions doivent être surveillées en continu pour identifier toute activité suspecte.

Les informations collectées doivent être vérifiées régulièrement.

1.3.2.2 Le contrôle des mesures de cybersécurité et de cyber résilience des sous-traitants numériques

Deux textes prévoient le contrôle des mesures de cybersécurité et de cyber résilience des prestataires de services numériques :

- **La Directive NIS 2 :** le contrôle de la conformité des sous-traitants aux normes de cybersécurité dans les secteurs d'intérêt général[30].

La directive prévoit l'obligation pour les entités évoluant dans des secteurs relevant de l'intérêt général (santé, transports...) et atteignant des seuils définis, de contrôler les mesures de cybersécurité mises en place par leurs tiers partenaires et de leur capacité à faire face aux incidents informatiques en résultant.

Les entreprises doivent, entre autres, évaluer les politiques de sécurité et de gestion des risques cyber de leurs sous-traitants et leur conformité aux normes de cybersécurité (ex. ISO 27001). Les entités doivent également s'assurer que leurs partenaires disposent de plans de réponse et de mécanismes de notification et de

30. *Directive (UE) 2022/2555 concernant la sécurité des réseaux et des systèmes d'information (NIS2),* 14 décembre 2022.

coopération en cas de défaillance de sécurité. Enfin elles doivent s'assurer que leurs partenaires ont mis en place une formation et une sensibilisation de ses opérationnels aux bonnes pratiques en matière de cybersécurité.

Ces contrôles peuvent s'effectuer en réalisant des audits de sécurité, en recueillant des documents justifiant du respect du cocontractant de ces obligations et en soumettant des questionnaires aux sous-traitants.

- **Le règlement DORA :** le contrôle du respect des normes de cybersécurité et de la résilience opérationnelle du sous-traitant[31]

La réglementation DORA impose aux entités financières de s'assurer du respect de normes de cybersécurité et de la résilience opérationnelle de leurs fournisseurs de services numériques tiers.

Elles doivent notamment s'assurer de la conformité de leurs sous-traitants aux dispositions du règlement. Elles peuvent pour cela, identifier les mesures de sécurité des données et de gestion des risques mises en place, comme le chiffrement et les contrôles d'accès, vérifier les plans de continuité des activités en cas d'incident et la conformité du tiers aux normes de sécurité informatique (ex. ISO 27001). Les entités assujetties doivent par ailleurs veiller à identifier et à traiter les risques de dépendance vis-à-vis d'un prestataire numérique tiers, ainsi que ceux issus des sous-traitants de rang 2.

Les contrôles des entités assujetties sur leurs prestataires prendront la forme de tests de résilience durant lesquelles des situations de crises sont simulées (intrusion dans le système informatique, infection virale, pics d'activité...). Des audits réguliers permettront également de s'assurer des procédures et politiques mises en place, en matière de gestion des risques numériques notamment, et de la formation des employés aux bonnes pratiques de cybersécurité.

31. *Règlement (UE) 2022/2554 relatif à la résilience opérationnelle numérique du secteur financier,* 14 décembre 2022.

NOTA BENE : Points de vigilance contractuelle – Les textes récents en matière de cybersécurité

DORA : L'article 30 du règlement DORA prévoit des dispositions contractuelles imposées à l'ensemble des contrats de prestations de services en technologie de l'information et de la communication (TIC) conclus par les entités financières, et des clauses destinées aux contrats portant sur des fonctions importantes ou critiques au sens du règlement.

Clauses obligatoires pour l'ensemble des contrats de prestataires TIC	Clauses imposées aux contrats portant sur des fonctions importantes ou critiques
Description des services fournis, des fonctions concernées et des conditions d'une éventuelle sous-traitance sur un service touchant une fonction critique.	Description détaillée des niveaux de service
Lieux de fourniture des services, de traitement des données et obligation d'information en cas de changement	Délais de préavis et obligation de notification de l'entité financière, notamment de tout évènement affectant la capacité du prestataire à fournir des services soutenant des fonctions critiques.
Obligation en termes de disponibilité, d'authenticité, d'intégrité et de confidentialité des données	L'obligation de mise en œuvre et de test des plans d'urgence et de mise en place des mesures, outils et politiques garantissant un niveau approprié de sécurité.
Mises à disposition et accès aux données en cas de fin du contrat	L'obligation pour le prestataire de participer aux tests de pénétration de l'entité financière
Description des niveaux de services	Droit de suivi permanent des performances du prestataire (droit d'audit renforcé)
L'obligation d'assistance sans frais du prestataire en cas d'incident	Les modalités de fin de la relation permettant de réduire les risques de perturbation pour l'entité financière.
L'obligation de coopération avec les autorités compétentes et celles de l'autorité financière	L'obligation de mise en œuvre et de test des plans d'urgence et de mise en place des mesures, outils et politiques garantissant un niveau approprié de sécurité.
Droits de résiliation et délais de préavis	
Conditions de participation du prestataire TIC aux programmes de sensibilisation à la sécurité numérique et aux formations à la résilience opérationnelle numérique.	

Les entités financières doivent également tenir un registre répertoriant les contrats de prestations TIC en cours d'exécution et fournir une fois par an aux autorités compétentes les données relatives aux nouveaux contrats de services TIC (nombre, catégorie de prestataires de services, type de service et fonctions concernées). Des modalités de résiliation de droit des contrats sont par ailleurs fixées par l'article 28 (7) du règlement.

NIS 2 : La directive NIS 2 incite les entités concernées à intégrer des dispositions contractuelles liées à la cybersécurité dans leurs contrats de services TIC sans préciser le contenu de ces clauses : « les entités essentielles et importantes devraient en particulier être encouragées à intégrer des mesures de gestion des risques en matière de cybersécurité dans les accords contractuels conclus avec leurs fournisseurs et prestataires de services directs* ».

* Considérant 85, *NIS 2*.

1.3.2.3 Le contrôle des exportations de biens à double usage

Les exportateurs de biens à double usage[32] doivent procéder à des vérifications concernant la localisation des biens envoyés et les parties prenantes de l'opération.

Des licences d'exportation sont accordées selon la nature des biens au regard d'une classification établie par la loi.

Les exportateurs doivent effectuer une *due diligence* approfondie sur leurs clients pour identifier les risques qu'ils présentent, notamment au regard de sanctions internationales reçues. Ils doivent également vérifier l'utilisateur final et son utilisation des biens exportés pour prévenir les usages non autorisés[33].

Des mesures sont également appliquées à la suite des exportations, notamment, la tenue de registres détaillés des transactions réalisées[34].

Ces différents renseignements pourront être collectés au moyen de questionnaires, de recherches sur bases de données et de recueil de pièces justificatives[35].

1.3.2.4 Cyber Resilience Act

Le *Cyber Resilience Act (CRA)*[36] impose aux fabricants de produits numériques (logiciels et matériels) tels que les smartphones commercialisés sur le marché européen de respecter des exigences strictes en matière de cybersécurité[37].

32. « biens à double usage » : les produits, y compris les logiciels et les technologies, susceptibles d'avoir une utilisation tant civile que militaire; ils incluent les biens susceptibles d'être utilisés aux fins de la conception, de la mise au point, de la fabrication ou de l'utilisation d'armes nucléaires, chimiques ou biologiques ou de leurs vecteurs, y compris tous les biens qui peuvent à la fois être utilisés à des fins non explosives et intervenir de quelque manière que ce soit dans la fabrication d'armes nucléaires ou d'autres dispositifs nucléaires explosifs ; *Règlement (UE) 2021/821 du Parlement et du Conseil* du 20 mai 2021
33. *Ibid.* article 8 et 9.
34. *Ibid.*
35. *Ibid.*
36. *Règlement (UE) 2024/2847 du 23 octobre 2024 relatif à la cyberrésilience (Cyber Resilience Act).*
37. *Ibid.* Article 13 et suivants.

Ils doivent notamment s'assurer du traitement des vulnérabilités de leurs produits aux attaques informatiques et de la mise en œuvre de mesures protégeant les données personnelles de leurs utilisateurs et assurant la sécurisation des accès[38]. Les incidents doivent faire l'objet de procédures de documentation et de continuation d'activité régulièrement testées[39]. Des mises à jour régulières du système de sécurité doivent être réalisées afin de remédier aux vulnérabilités identifiées.

Ils doivent également s'assurer du respect de ces normes de sécurité par les membres en amont de leur chaîne de valeur[40].

Les autres acteurs intervenant dans la commercialisation du produit à savoir les importateurs et distributeurs doivent quant à eux s'assurer du respect par le fabricant des dispositions du CRA. Ils pourront pour ce faire procéder à des audits, soumettre des questionnaires aux fabricants et prévoir des clauses contractuelles encadrant leur production[41].

Une synthèse sous forme de tableau de ces obligations légales est disponible en annexe II page 67.

1.4 Privilégier une cartographie globale des risques de la chaîne de valeur

Certains des textes précités prévoient également la mise en œuvre de cartographies des risques qui serviront à identifier les catégories de tiers à évaluer. Il y a donc tout intérêt à procéder à la réalisation d'une cartographie globale des risques de la chaîne de valeur qui permettra de représenter l'exposition des tiers ou des catégories de tiers aux risques, que ceux-ci soient d'origine opérationnelle et/ou juridique[42].

38. *Ibid.,* Annexe I.
39. *Ibid.*
40. *Ibid.,* Article 13 § 2.
41. *Ibid.,* Article 23-25.
42. OECD, *Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions,* 2025.

Ce travail de mutualisation est encouragé par le régulateur comme l'AFA, qui dans ses Recommandations précise que « Pour les entreprises ayant déjà conduit des travaux de cartographie des risques dans un cadre plus large ou sur d'autres types de risques que ceux de corruption[43], ces démarches préexistantes peuvent être capitalisées[44] ».

De même, concernant l'évaluation des tiers, l'AFA précise que « *Les évaluations des tiers doivent être distinguées des obligations de vigilance à l'égard de la clientèle auxquelles sont assujetties les personnes définies à l'article L. 561-2 du code monétaire et financier dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme (article L.561-1 et suivants du code monétaire et financier)*[45]*. Elles peuvent néanmoins être mises en œuvre à travers un dispositif unique, pour autant que ce dernier permette de faire ressortir le risque spécifique de corruption*[46] ».

L'intérêt du « *dispositif unique* » encouragé par le régulateur est d'identifier les tiers ou catégories de tiers au sein de la chaîne de valeur susceptibles de présenter plusieurs catégories de risques et donc de prévoir une évaluation susceptible de traiter tous les risques et de répondre à toutes les obligations.

Ainsi un tiers présentant des risques de dépendance économique pourra également présenter des fragilités sous l'angle de la lutte contre la corruption pour maintenir la relation contractuelle. De même, un tiers sous sanction, qui, dans le cadre des opérations visées par le LCB-FT, implique une cessation immédiate des relations commerciales, constitue un signal d'alerte fort pour l'évaluation d'autres types de risques comme celui de l'atteinte à la réputation.

43. United Nations Office on Drugs and Crime, *An Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide,* 2013, chapitres II et III.
44. AFA, *Avis relatif aux recommandations de l'Agence française anticorruption destinées à aider les personnes morales à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêts, de détournement de fonds publics et de favoritisme,* 12 janvier 2021.
45. AFA, *Recommandations 2020,* pt 205.
46. *Ibid.,* pt 206.

Ce point est rappelé dans le projet des Fiches Pratiques au point 61 :

« *Une vigilance pourra être portée sur les résultats d'évaluations réalisées en vertu d'autres dispositions, en coordination avec les équipes conformité dédiées, notamment en matière de sécurité financière, sanctions internationales, lutte contre le blanchiment d'argent et le financement du terrorisme, devoir de vigilance, protection des données etc. À cet égard, le rôle de l'instance dirigeante, chargée de la bonne coordination des procédures, est essentiel car elle dispose d'une vision globale*[47] ».

Dès lors, une cartographie globale des risques de la chaîne de valeur permet d'identifier des catégories de tiers présentant des risques selon des critères préétablis (nature de l'activité, zone géographique, volume de l'activité…) permettant de définir une politique d'évaluation des tiers.

47. AFA, *Fiches pratiques, op. cit.,* pt 61.

II. Définir une politique d'évaluation des tiers en lien avec sa cartographie

2.1 Définir les catégories de tiers à évaluer selon les risques

La cartographie de la chaîne de valeur doit permettre d'identifier les catégories de tiers avec lesquels l'entreprise est en relation. Une valeur de risque pourra être déterminée pour chacune de ces catégories selon des critères de risque définis par la cartographie. Ces valeurs permettront ensuite de définir de façon automatisée la nature et le niveau de détail de l'évaluation à réaliser.

Les Fiches Pratiques invitent ainsi à établir des groupes de tiers homogènes présentant des critères de risque communs. À titre d'exemple, concernant le risque d'exposition à la corruption, les Fiches Pratiques relèvent[48] :

- la nature de la relation avec les tiers (relation longue durée, situation de dépendances économiques, etc) ;
- le secteur d'activité du tiers
- l'implantation géographique du tiers (« risque pays »)
- l'interaction du tiers avec les acteurs publics[49]

> **Nota bene :**
>
> Le diagramme ci-après peut faciliter l'identification des risques pouvant impacter la chaîne de valeur et les diligences à effectuer. L'annexe 2 Tableau de synthèse des obligations légales d'évaluation des tiers a pour objet de faciliter l'identification des obligations générales et sectorielles d'évaluation des tiers selon le profil de l'entreprise et l'activité exercée.

48. AFA, *Fiches Pratiques, op. cit.*, pt 51.
49. *Ibid.*

1 IDENTIFIER ET ÉVALUER LES RISQUES DE MA CHAÎNE DE VALEURS

Quels sont les événements dont les tiers sont à l'origine (fournisseurs, clients, administrations...) qui peuvent impacter positivement ou négativement ma chaîne de valeur ?

- Risque financier : défaut de paiement du client ou du fournisseur
- Dépendance économique du fournisseurs : risque lié à la rupture des relations contractuelles
- Dépendance stratégique vis-à-vis d'un tiers : risque de rupture d'approvisionnement d'un produit ou d'un service indispensable àla réalisation de notre offre
- Le tiers ne présente pas les garanties suffisantes pour accéder à notre SI
- Risque intégrité du tiers
- Risque d'image lié au tiers (le tiers n'est pas conforme aux obligations de vigilance dans sa propre chaîne de valeur)
- Les relations commerciales avec le tiers sont restreintes ou interdites par des sanctions internationales, des embargos, des restrictions liées au double usage des biens

Comment puis-je identifier les risques au sein de ma chaîne de valeur ? La nature des diligences à accomplir selon ma politique d'évaluation des tiers

- Quel est le niveau minimal de diligence à effectuer sur les tiers ?
  - Risque financier
  - Obligation de vigilance
  - Vérification des sanctions
- Vérification approfondie en cas d'alertes

2 COMMENT EST GÉRÉE LA PROCÉDURE DE TPRM DANS L'ENTREPRISE ?

- Qui réalise les diligences de premier niveau ?
- Qui réalise les diligences de deuxième niveau ?
- Qui décide de poursuivre ou non la relation avec un tiers identifié à risque ?

3 COMMENT EST CONTRÔLÉE LA PROCÉDURE DE TPRM ?

- Définition des plans de contrôle et d'audit
- Par qui sont réalisés les contrôles ? (prévention des conflits d'intérêts)
- Quels sont les niveaux de contrôle ?
  niveau 1 : opérationnel
  niveau 2 : conformité
  niveau 3 : audit

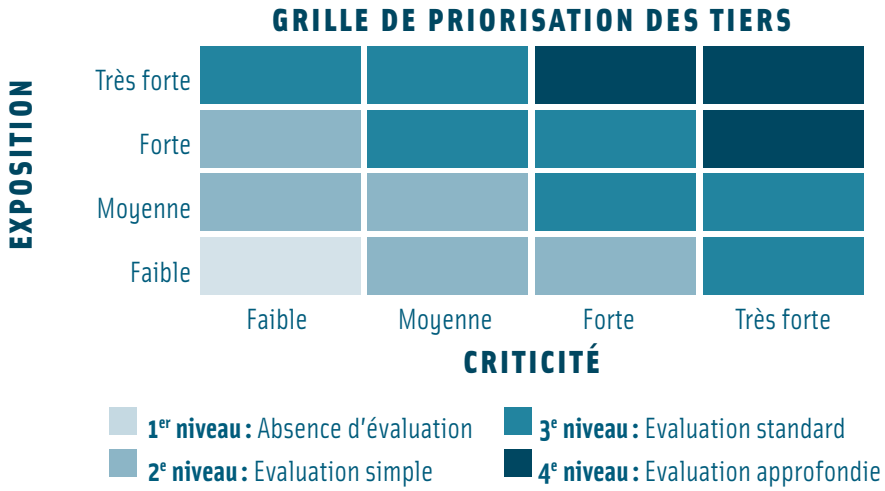
L'AFA recommande de digitaliser l'évaluation des tiers pour faciliter le contrôle et l'audit

Ainsi, la politique d'évaluation des tiers devra informer le niveau opérationnel si le tiers, compte tenu de sa catégorie, doit être évalué :

- Si le tiers, compte tenu de sa catégorie, doit être évalué.

Sauf obligations légales spécifiques qui obligent à l'évaluation ou au recueil d'information systématique sur certains types de tiers (ex. LCB-FT ou obligation de vigilance), l'entreprise a la faculté de déterminer les catégories de tiers à évaluer et selon quelles modalités. Celles-ci sont définies eu égard aux risques identifiés de la catégorie de tiers concernés et peuvent prendre également en compte des aspects pratiques de l'évaluation : nécessité d'obtenir rapidement l'information sur le tiers, capacité de celui-ci à coopérer pour fournir l'information attendue etc. Le choix de la diligence à effectuer et les modalités pratiques de celles-ci sont donc importants pour réaliser les objectifs du TPRM[50].

Le tableau de la page suivante synthétise les niveaux de diligences menées au regard de la criticité et de l'exposition du tiers aux risques. Les diligences à effectuer sont liées à la catégorie de tiers concernée et aux risques qui y sont attachés. La grille ci-dessous synthétise, quant à elle, les niveaux d'évaluations au regard de la criticité et de l'exposition du tiers aux risques.



50. AFA, *Recommandations 2020, passim.*

NIVEAU DE DILIGENCES MENÉES

Premier niveau : absence d'évaluation

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.

Deuxième niveau : risque faible

Lorsque le tiers présente un très faible niveau de risque, il est soumis à des vérifications allégées, il pourra s'agir de :

Recherches sur des sources libres d'accès (registre du gel des avoirs, registre de l'INPI…) ou de recherches automatisées sur des bases de données payantes

Consultation des archives de l'entreprise

Troisième niveau : risque moyen ou fort

Lorsque le tiers présente un niveau de risque moyen ou fort, il peut être soumis à :

Des questionnaires d'auto-évaluation

Des recherches sur bases de données spécialisées

Aux modes d'évaluations précédemment mentionnés

Quatrième niveau : risque très fort

Lorsque le tiers présente un niveau de risque très fort, attesté par des signaux d'alertes issus d'évaluations de niveaux précédents notamment ou de facteurs mentionnés par les opérationnels, il est soumis à des évaluations approfondies.

Il s'agit entre autres :

D'entretiens avec les dirigeants, d'audits

De rapports externes réalisés par des prestataires spécialisés (cabinets de conseils, cabinets d'avocats…)

2.2 Définir la nature des diligences à effectuer

Les diligences consistent à obtenir des données concernant le tiers afin de procéder à son évaluation. Il existe plusieurs modalités de diligence qui vont permettre d'obtenir des données sur les tiers plus ou moins approfondies.

Il est possible de distinguer les évaluations qui offrent une actualisation continue d'informations et permettent ainsi un contrôle permanent (*risk monitoring*) de celles qui permettent d'obtenir des informations plus approfondies à un instant déterminé (*control evaluation*).

2.2.1 Bases de données

Le *risk monitoring* permet d'obtenir des informations instantanées sur le tiers en interrogeant des bases de données disponibles en ligne, en accès libre (*open data*) ou payantes.

- **Open Data**

Beaucoup d'informations sur les entreprises sont aujourd'hui disponibles gratuitement en ligne. L'*Open-Source Intelligence (OSINT)* est la pratique qui consiste à rechercher de l'information sur les tiers en ligne. Le site *Osint framework*[51] permet d'identifier des sites d'informations. De même, l'AFA a identifié des bases de données ouvertes facilitant la recherche d'informations pour l'évaluation de l'intégrité des tiers[52]. Il est à noter que la France à travers la loi République numérique a favorisé l'accès aux données publiques y compris par le biais d'API[53].

- **Bases de données payantes**

Des prestataires proposent l'accès à des bases de données où l'information sera structurée ce qui facilite la recherche d'informations. Certaines bases peuvent se spécialiser sur certaines informations (personnes politiquement exposées, sanctions), sur des zones géographiques particulières, ou

51. https://osintframework.com/

52. AFA, *Recueil de fiches pratiques : Bases d'information publiques utiles à l'évaluation de l'intégrité des tiers*, 9 mars 2023, [en ligne], disponible sur : https://www.agence-francaise-anticorruption.gouv.fr/fr/document/afarecueil-fiches-pratiques-bases-publiques (consulté le 23 septembre 2025).

53. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016 https://api.gouv.fr/les-api/api_data_gouv.

proposer plusieurs catégories d'informations (informations financières et intégrité, par exemple).

- **Intérêt et limite du risque 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.

Souvent présenté avec la promesse d'automatiser les évaluations de tiers avec fourniture de *scoring* associé, le *risk monitoring* comporte cependant des limites. En premier lieu, l'utilisateur devra traiter les faux positifs, c'est-à-dire les homonymies, afin d'identifier la bonne personne à évaluer. Il devra également analyser l'information recueillie afin d'identifier un risque grave. Les Fiches Pratiques soulignent le risque lié au taux d'homonymie[54]. Le *risk monitoring* nécessite donc un traitement et une analyse de l'information obtenue qui peuvent excéder les compétences du niveau opérationnel souvent en charge du *risk monitoring*. De surcroît, l'AFA dans ses Fiches Pratiques alerte sur les systèmes de cotation automatique fournis par les solutions numériques, en précisant que l'utilisateur doit être en mesure de déterminer son propre dispositif de cotation au regard de la cartographie des risques[55].

En deuxième lieu, les informations obtenues sur le tiers sont par nature limitées et résultent le plus souvent d'informations légales qui sont diffusées par l'entreprise, les pouvoirs publics ou les médias et les réseaux sociaux lorsque le tiers a fait l'objet d'une investigation par la presse. L'accès à certaines informations, comme l'identité des bénéficiaires effectifs, a par ailleurs été restreint par décision de justice (ECLI:EU:2022:912) dans le but de protéger la vie privée. La consultation du registre des bénéficiaires effectifs est ainsi réservée aux entreprises ou personnes disposant d'un intérêt légitime au sens de l'article L. 561-46-2.-I du Code monétaire et financier (dont les personnes assujetties aux obligations LCB-FT et Sapin 2),

54. AFA, *Fiches Pratiques,* op. cit., pt 83.
55. *Ibid.,* pt 97.

L'évaluateur ne trouvera donc pas exclusivement dans le *risk monitoring* l'information utile concernant sa relation avec le tiers, comme l'identification d'un possible conflit d'intérêts, par exemple. Ces considérations conduisent l'AFA à relativiser l'usage de la solution numérique si elle n'offre que la possibilité d'interroger des bases de données « En tout état de cause, le recours à une solution numérique peut être utile pour réaliser une évaluation dans un premier temps, mais nécessite une analyse humaine afin d'ajuster l'évaluation, notamment pour les tiers les plus à risque[56].»

2.2.2 Questionnaire d'auto-évaluation et gestion documentaire :

- **Questionnaire d'auto-évaluation :**

Le questionnaire d'auto-évaluation permet à l'entreprise d'obtenir des informations directes du tiers évalué sur la base d'un questionnaire. Celui-ci pourra comporter plusieurs sujets et être plus ou moins approfondi selon les risques identifiés. Les Fiches Pratiques (comme les recommandations de l'AFA) visent expressément ce mode de recueil d'informations en recommandant qu'il soit signé par le répondant et accompagné de pièces justificatives. L'AFA insiste également pour que dans le cadre d'un questionnaire couvrant plusieurs sujets (sécurité financière, RSE...), la partie relative à la corruption soit suffisante pour permettre une véritable évaluation[57]. Par ailleurs les Fiches Pratiques détaillent des informations pertinentes pouvant être demandées au tiers[58].

Le questionnaire permet d'obtenir de l'information directement auprès du tiers et donc, à condition qu'il soit coopératif et qu'il fournisse des données exactes et récentes, offre ainsi de disposer de réponses fiables. La réponse à un questionnaire constitue également une forme d'engagement du tiers qui pourrait l'exposer juridiquement en cas de réponses délibérément inexactes.

56. AFA, *Fiches Pratiques*, op. cit., pt 85.
57. Ibid., pt 72.
58. Ibid., pt 75.

En conséquence, d'une part, la nullité du contrat[59] conclu avec le tiers pourrait être prononcée pour réticence dolosive dès lors que les informations dissimulées ont été déterminantes dans la formation du consentement[60]. D'autre part, sa responsabilité civile pourrait être engagée pour faute dolosive[61]. Sans se prononcer sur ce point de droit, l'AFA dans ses Fiches Pratiques précise que « le refus par le tiers de communiquer les éléments demandés constitue un signal de risque très élevé[62] ».

La gestion du questionnaire peut présenter des difficultés à répondre aux questions et rassembler les pièces demandées, l'évaluateur doit de son côté lancer le questionnaire à la bonne personne, le relancer et analyser les réponses. En outre, le questionnaire propose une photographie du tiers à l'instant de sa réponse, sans monitoring sur la durée de la relation contractuelle, même si une relance de questionnaire peut être effectuée à intervalle régulier.

- **Gestion documentaire :**

L'évaluation du tiers peut également consister en la fourniture de pièces justifiant de ses capacités ou de ses compétences. Ce peut être le cas notamment pour l'obligation de vigilance qui oblige à demander au prestataire des pièces démontrant sa conformité administrative (K-BIS, attestation de vigilance URSSAF, liste de travailleurs étrangers)[63]. Il est possible d'y ajouter d'autres demandes : attestations d'assurance, d'habilitations métiers...

A noter également que les obligations LCB-FT obligent à identifier le client et vérifier la véracité de l'identité[64] notamment par le recueil de documents d'identité et leur vérification[65].

59. Articles 1131 et 1178 du *code civil*.
60. Articles 1130 et 1137 *du code civil*.
61. Articles 1240 et 1241 du *code civil*.
62. AFA, *Fiches Pratiques,* op. cit., pt 78.
63. Article L.8222-1 et suivants du *code du travail*.
64. Articles R561-5 et L561-5 du *code monétaire et financier*.
65. V. https://acpr.banque-france.fr/fr/reglementation/registre-officiel/lignes-directrices.

2.2.3 Les évaluations approfondies et les audits de tiers

Des évaluations approfondies pourront s'avérer nécessaires dans certaines situations présentant des risques particulièrement élevés, notamment au vu de l'importance de la relation dans la chaîne de valeur et de l'opacité des détenteurs réels de leur capital (bénéficiaires effectifs) ou de leur process de production (risque de violation de droits humains). Ces évaluations seront réalisées par des acteurs disposant d'informations locales ou sous forme d'entretiens, d'enquêtes externes, d'audits et de *due diligence* pour des opérations de *Mergers and Acquisitions (M&A)* ou de *Joint venture*. Il est recommandé de prévoir contractuellement ces possibilités d'audits auprès du tiers.

2.3. Politique et gouvernance du TPRM

Le recueil et le traitement de la donnée issue du processus de TPRM et la prise de décision sur l'entrée ou le maintien de la relation avec un tiers nécessitent la mobilisation de plusieurs niveaux de ressources dans l'entreprise. En effet la volumétrie des tiers de la chaîne de valeur et des informations sollicitées implique normalement la participation des opérationnels dans cette collecte. Les alertes en résultant pourront gérer un *workflow* de validation permettant une prise de décision vis-à-vis du tiers par le niveau expert (juridique / conformité/ DSI...) et à défaut de consensus entre le niveau opérationnel et le niveau expert, par arbitrage de l'instance dirigeante[66].

Cette organisation en trois niveaux est préconisée par l'AFA tant dans les recommandations que dans les Fiches Pratiques[67].

2.3.1 Définition du rôle des parties prenantes du TPRM

- **Les équipes au niveau opérationnel**

Le recueil de la donnée auprès du tiers doit être réalisé par le niveau opérationnel compte tenu de son rapport direct avec le tiers. Afin de faciliter la tâche des opérationnels, il est nécessaire de déterminer en amont la nature

66. AFA, *Fiches Pratiques, op. cit., passim*.
67. *Ibid*. pt 70 et suivants.

de la diligence à effectuer (interrogations de bases de données, envoi de questionnaires et recueil de pièces...) selon le niveau de risque du tiers, au regard de la catégorie à laquelle il appartient[68].

Il est à noter que les Fiches Pratiques suggèrent également l'utilisation par le niveau opérationnel d'un questionnaire interne « *complété par le personnel exerçant les fonctions opérationnelles de l'entreprise sur la base des informations recueillies et/ou la connaissance de la relation*[69] ».

Il parait en effet essentiel de recueillir et d'utiliser l'information disponible dans l'entreprise sur l'historique de la relation avec le tiers quand elle existe et si elle est à jour. Ce peut être le cas si des directions ou services ont réalisé des évaluations de tiers pour répondre aux besoins de certaines directions (achats, RSE...) . Il convient également de pouvoir accéder aux outils informatiques de l'entreprise (ERP, SI achats, CRM) qui où peuvent se trouver des informations utiles à l'évaluation du tiers.

A cet égard, le niveau de risque de la catégorie du tiers (et donc le niveau de diligence associé) pourra être augmenté par l'opérationnel au vu des informations dont il dispose et qu'il a obtenues du fait de sa relation directe avec le tiers concerné.

L'objectif de cette phase est donc de permettre un recueil d'informations adapté à la catégorie de tiers concernée et de permettre un premier niveau de traitement de l'information pour identifier les risques graves.

Il y a lieu à ce stade de privilégier l'automatisation du traitement de l'information pour dispenser le niveau opérationnel de le faire. Ainsi des alertes pourront être créées automatiquement si le *risk monitoring* fait apparaître l'existence de sanctions internationales, de condamnations, ou de personnes politiquement exposées (PEP). De même l'absence de réponse ou des réponses incomplètes à certaines questions d'un questionnaire sur des questions jugées sensibles pourront générer des alertes.

En l'absence d'alerte, le niveau opérationnel pourra en revanche valider le tiers ou, en fonction de l'automatisation du process, une validation automatique sera faite par l'outil d'évaluation.

68. V. Annexe 4, Signaux de risque intégrité du tiers.

69. AFA, Fiches Pratiques, *op. cit.*,pt 72.

- **La fonction juridique/conformité**

Le niveau juridique/conformité pourra être saisi en cas d'alertes et dans l'hypothèse où le niveau opérationnel souhaite malgré celles-ci poursuivre la procédure d'intégration (*onboarding*) du tiers.

L'objectif est ici d'analyser les risques afin, en premier lieu, de vérifier que les alertes générées révèlent des risques réels et qu'elles ne sont pas biaisées par les critères retenus pour l'automatisation.

C'est à ce stade qu'un questionnaire plus approfondi pourra être adressé au tiers, ou le recours à une analyse de risque par le biais d'auditeur externe pourra être engagé.

La saisine du niveau expert doit conduire à une préconisation de validation (accompagnée le cas échéant d'un plan de traitement) ou de rejet. En l'absence de consensus entre le niveau opérationnel et expert sur la validation du tiers, il appartient à ce niveau de saisir l'instance dirigeante pour décision définitive.

Madame **Catherine Delhaye-Kulich**, Chief Ethics, Compliance and Data Protection Officer, chez le Groupe Valeo, partage son temoignage sur l'importance du TPRM et de la compliance dans le business.

Quel discours tenir pour sensibiliser ?

Il faut tenir un discours clair afin que les départements et collaborateurs concernés comprennent les enjeux et les conséquences sur le business, d'une démarche TPRM défaillante. En effet, du fait des nombreuses réglementations qui obligent aujourd'hui à conduire des *due diligence* ainsi que des exigences des clients à l'égard de leur supply chain au sens large, le TPRM est aujourd'hui un rouage essentiel d'une conduite des affaires sereine et durable.

À titre d'exemple, les sanctions économiques Européennes, très en vogue depuis le début de la guerre en Ukraine, prévoient l'interdiction d'importation de certains produits fabriqués en tout ou en partie en Russie ainsi que les transactions avec de très nombreuses entités et individus d'origine russe.

Autre exemple, la Chine a décidé de conditionner l'exportation de terres rares, essentielles à la fabrication de véhicules électriques, de turbines éoliennes et de puces électroniques, à l'octroi de licences d'exportation. L'une des conditions d'obtention de celles-ci est que les produits fabriqués à partir de ces matériaux ne soient pas destinés à l'industrie militaire américaine.

Enfin, les Etats-Unis interdisent l'importation et la vente sur le territoire américain, de véhicules équipés de certains software et de certains équipements d'origine chinoise ou russe ou issus d'entités dirigées par des Chinois ou des Russes.

Savoir avec qui l'on travaille et vérifier que la relation n'est pas soumise à restrictions est donc absolument fondamental. Ces vérifications concernent aussi bien les fournisseurs, que les clients ou la destination et l'utilisation des certaines technologies et l'absence de diligence ou des diligences lacunaires ou superficielles, peuvent conduire une entreprise à interagir avec des partenaires sous sanctions ou à importer ou exporter des produits soumis à restrictions.

Elle s'expose alors à des risques juridiques et réputationnels. Elle peut également mettre ses clients ou fournisseurs en difficultés. Il s'agit donc bien de risques susceptibles d'impacter sérieusement le business. Il ne faut donc pas s'excuser d'avoir à mettre en œuvre un TPRM efficace, mais le présenter comme une condition préalable du business.

Faut-il chercher impérativement à mobiliser les opérationnels pour qu'ils réalisent le premier niveau de diligence d'évaluation ?

Une Direction Ethique et Conformité doit collaborer avec différents départements de l'entreprise pour évaluer les tiers (achats, ventes, logistique et R&D en particulier).

C'est généralement la Direction Ethique et Conformité qui définit, selon les situations, la méthodologie à suivre et le niveau de diligences à réaliser. Elle définit également les plans d'actions, voire

les pré-requis à mettre en œuvre et respecter en cas de relation avec un tiers à risque et en contrôle la bonne exécution.

La Direction Ethique et Conformité assure également une veille réglementaire exigeante afin d'être capable d'informer le COMEX sur l'impact d'une nouvelle réglementation pour l'activité. Par exemple, les tensions géopolitiques de ces dernières années ont rendu obligatoires une veille accrue des sanctions édictées en particulier par l'UE et les US mais également des contre-sanctions édictées par la Chine.

Peut-on aujourd'hui prétendre que certains tiers ne sont pas à risque et donc ne pas les évaluer ?

Il peut arriver que certains tiers, eu égard à leur activité et à leur localisation présentent un risque très faible. On peut donc adapter les évaluations aux risques identifiés. Inversement, certains tiers sont par nature soumis à des obligations spécifiques de *due diligence* (PFAS, déforestation…). Enfin, le respect des sanctions internationales et l'absence de corruption sont des incontournables.

En conclusion, la gestion des tiers est un incontournable de tout programme de compliance. Elle aide l'entreprise à se protéger dans de très nombreux domaines et contribue à sa pérennité.

- **Le rôle de l'instance dirigeante**

L'instance dirigeante intervient dans le processus pour prendre une décision d'acceptation ou de refus du risque, notamment quand il n'y a pas de consensus sur la décision à prendre entre le niveau opérationnel et le niveau conformité. Cette décision doit être fondée sur une information complète qui aura été collectée et traitée par les fonctions opérationnelles et de conformité.

2.3.2 Formaliser une politique et une gouvernance de TPRM

La mise en œuvre d'une procédure de TPRM implique donc de définir des rôles et des tâches à réaliser tant pour procéder au recueil de la donnée que

pour procéder à son traitement, actions préludant à la prise de décision sur l'entrée en relation avec le tiers. En effet, une politique de TPRM doit conduire à prendre des décisions sur la relation avec le tiers qui est soit d'approuver la relation, soit d'y mettre un terme ou ne pas s'engager ou de réaliser des diligences complémentaires pour documenter une prise de décision. Les Fiches Pratiques rappellent la finalité de la procédure[70] en précisant par ailleurs que « les décisions sont formalisées et enregistrées sur un réseau sécurisé[71] ». Ainsi la solution digitale choisie par l'entreprise doit pouvoir enregistrer les décisions, mais également les parties prenantes de l'évaluation, restituer l'historique des diligences réalisées et leur date afin de constituer des pistes d'audits.

De même, la politique devra définir la fréquence de la mise à jour des évaluations de tiers.

Il est donc recommandé de formaliser une politique en ce sens qui pourra être validée par l'instance dirigeante. L'intérêt de cet exercice est d'identifier en amont des points de blocages qui pourraient être opposés par les parties prenantes sur les rôles et les tâches qui leur sont dévolues par la politique et de les faire arbitrer, le cas échéant, par l'instance dirigeante.

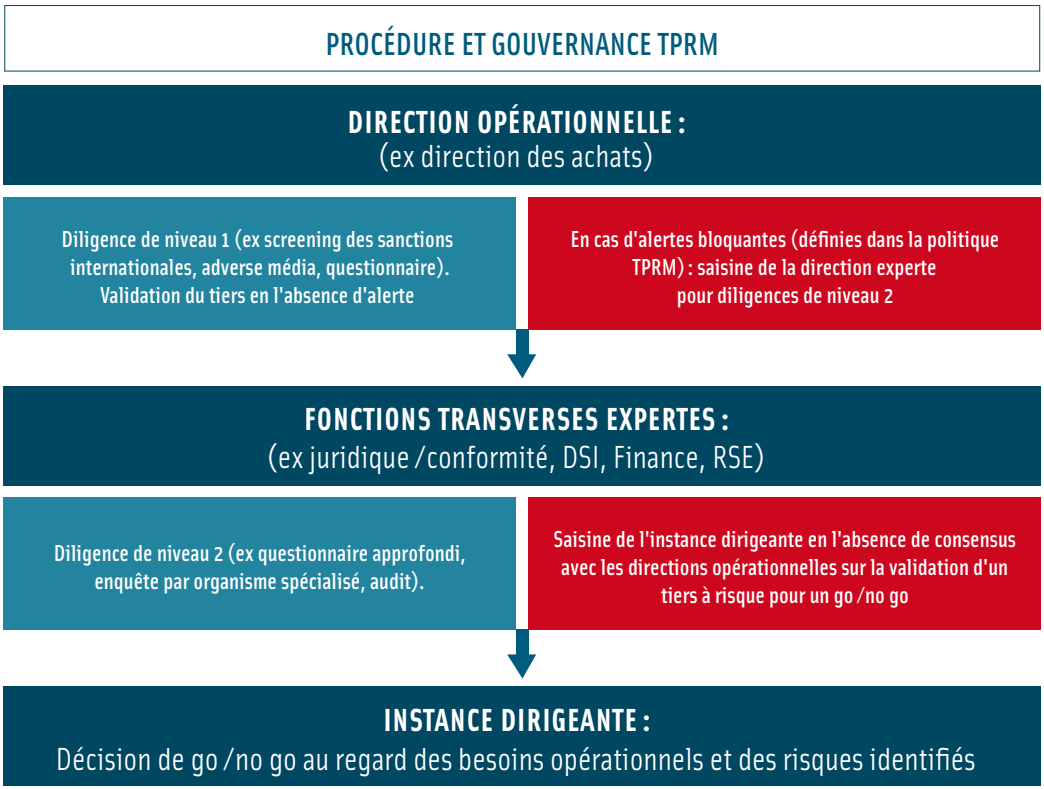
Une politique formalisée permettra également au contrôle interne de vérifier son application.

Enfin, cet exercice permettra l'expression des besoins dans la recherche ou la réalisation d'un outil permettant de digitaliser la procédure de TPRM.

L'importance de la formalisation de la politique d'évaluation est soulignée par l'AFA dans ses recommandations et dans les Fiches Pratiques. Dans ce dernier document, l'AFA précise

> « *Quelle que soit la méthode de pondération choisie, la démarche devra être formalisée dans une procédure pour être correctement appliquée, contrôlée et auditée*[72] ».

70. *Ibid.,* pt 105.
71. *Ibid.,* pt 108
72. *Ibid.,* pt 53.



Madame **Makeda Cardenas**, Compliance Officer, pour le Groupe la Poste, partage son témoignage sur l'importance du TPRM et de la compliance dans le business.

Pouvez-vous nous présenter vos fonctions et votre rôle dans l'évaluation des tiers ?

Nous faisons partie de la direction des achats du Groupe. Nous réalisons l'évaluation des tiers fournisseurs pour le Groupe, et assurons le déploiement pour les filiales. Le projet de la conformité des fournisseurs est co-porté par la Direction de la conformité du Groupe, qui assure par ailleurs le déploiement sur d'autre catégorie de tiers (partenaires non commerciaux, clients...)

La proximité avec les achats nous permet de mieux intégrer le processus de l'évaluation intégrité dans le référencement du

tiers fournisseur, ce qui permet d'intégrer le cycle d'*on boarding* avec plus de fluidité, ainsi que d'avoir plus facilement accès aux informations recueillies par les achats qui peuvent avoir une incidence sur l'évaluation intégrité, dont les risques de dépendance économique du tiers.

Comment sont organisées les diligences d'évaluation des tiers, quelles sont les spécificités d'une entreprise publique à cet égard ?

Le Groupe est soumis à plusieurs obligations légales impliquant une évaluation des tiers. Celle que nous réalisons à l'entrée en relation doit couvrir ces obligations (RGPD, Sapin 2, devoir de vigilance) et notre équipe réalise ses diligences au regard de ces obligations. Le risque cyber que peut porter le tiers est géré par notre DSI.

L'évaluation s'effectue postérieurement à la contractualisation, lorsque le tiers a répondu à un appel d'offres selon les règles de la commande publique. En effet, le résultat de l'évaluation ne peut constituer un motif d'exclusion a priori des marchés publics. En revanche, ils nous permettent de concevoir un plan de traitement du tiers identifié à risque.

Les évaluations s'opèrent à deux niveaux. En premier lieu, une recherche sur bases de données pour identifier les sanctions internationales et/ou embargo, outre la presse négative et l'information financière. Un monitoring est effectué tout au long de la relation contractuelle. Si des risques ont été identifiés, nous procédons à des diligences par questionnaire, celui-ci demeure un outil pertinent de recueil d'informations permettant d'identifier correctement les risques, même si les tiers peuvent être beaucoup sollicités à ce titre.

Quels sont les mesures de traitement mises en œuvre lorsque le tiers est identifié à risque ?

Des risques peuvent être identifiés quand son dispositif de conformité réglementaire ou quand sa maturité sur ces sujets est jugée insuffisante. Nous pouvons donc travailler avec lui pour l'inciter à rendre son programme plus qualitatif. Nous instaurons donc avec le tiers un partenariat de conformité.

Pour les tiers dont le niveau de risque n'est pas estimé faible mais avec lesquels nous devons maintenir la relation d'affaire (seul à opérer sur un territoire, seul pouvant effectuer la prestation…), nous pouvons mettre en œuvre de mesures de sécurité, par exemple un programme de formation renforcé pour les équipes en relation avec lui. L'approche par les risques prime durant toute la relation d'affaire, ainsi que lors de la définition des actions de remédiation.

Quelles sont vos attentes vis-à-vis des outils digitaux à l'appui de votre démarche de TPRM ?

En premier lieu, la capacité des outils à s'adapter à notre politique d'évaluation des tiers dictée par notre identification des risques. Il doit donc disposer d'une bonne capacité de paramétrage. A l'inverse, recourir à un outil nécessite un effort d'expression des besoins de la part des utilisateurs.

Le recours à un outil est indispensable compte tenu du volume d'informations à traiter. Néanmoins, le risque en particulier du *screening* de base de données est d'être submergé par le volume des informations, des alertes, pas toujours pertinentes, compte tenu des faux positifs. Il est donc nécessaire de retraiter l'information ce qui peut être fastidieux. L'utilisation de l'intelligence artificielle peut être prometteuse si le taux d'erreur est marginal.

2.4 Travailler avec un tiers identifié à risque

Les diligences sur le tiers effectuées au titre du TPRM peuvent faire apparaitre des risques à initier ou maintenir des relations avec le tiers. Cette identification peut conduire à une décision de refus de relation commerciale avec le tiers. Néanmoins un arbitrage est parfois nécessaire quand la relation avec le tiers est indispensable à l'organisation (ex-fournisseur stratégique). Le choix de travailler ou non avec un tiers à risque résulte donc du refus ou de l'acceptation du risque qui doit être pris au plus haut niveau de l'entreprise. Cette situation est abordée par l'AFA dans les fiches pratiques « *L'entreprise peut se retrouver dans une situation où elle n'a d'autres choix que d'établir ou de poursuivre une relation avec un tiers présentant un risque de corruption, pour*

lequel les vérifications sont difficiles à effectuer. Dans cette situation, elle devra mettre en place des mesures de remédiation adaptées[73]».

Ainsi, la relation avec un tiers à risque peut être maintenue, mais assorti d'un plan de traitement. En premier lieu, les collaborateurs de l'entreprise en charge de la relation avec le tiers devront être formés et il pourra être décidé que la gestion du tiers s'effectuera en collégialité offrant une meilleure appréciation des risques. La politique contractuelle vis-à-vis du tiers pourra également être adaptée en obligeant le tiers à identifier et traiter ses risques avec des objectifs pouvant être sanctionnés par une clause de résiliation en cas de non réalisation. Enfin, une mise sous surveillance continue du tiers sous forme de monitoring pourra être mise en œuvre permettant une réévaluation régulière de la relation avec le tiers. Les Fiches Pratiques évoquent les moyens de remédiation dans la relation avec un tiers identifié à risque[74].

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

III. Déployer et contrôler le TPRM dans les process de l'entreprise

3.1 Le déploiement

Une des difficultés du déploiement d'un process de TPRM dans l'entreprise est la mobilisation du niveau opérationnel dans la collecte et le traitement des informations de premier niveau. En effet, la démarche est perçue comme chronophage et sans valeur ajoutée par rapport aux missions confiées aux opérationnels. Cette perception est souvent renforcée par l'attitude de l'instance dirigeante qui ne perçoit pas toujours le caractère stratégique du TPRM et qui n'alloue pas les ressources nécessaires à cette tâche.

Il est donc nécessaire de modifier le discours sur l'évaluation des tiers afin de la faire migrer de la simple obligation réglementaire sanctionnée par un régulateur à son approche stratégique liée au management des risques de la chaîne de valeur, c'est-à-dire au processus de création de valeur même de l'entreprise.

Le TPRM, on l'a vu, permet d'offrir une vision complète des risques liés aux tiers et non plus segmentée selon les évaluations qui sont réalisées selon les besoins des directions en relation avec lui. Toute personne autorisée pourra donc vérifier si le tiers avec lequel elle envisage de contracter a déjà fait l'objet d'une évaluation et y trouver les informations qui lui sont utiles. La mutualisation des informations recueillies sur le tiers permet donc un gain de temps dans la contractualisation ajoutant ainsi en rapidité et en efficacité aux processus opérationnels.

Le déploiement du processus en tant que tel nécessite une conduite du changement : une formation qui ne soit pas uniquement centrée sur les tâches à réaliser, mais qui donne du sens à la démarche.

- Montée en charge progressive des actions à réaliser avec détermination d'objectifs,

- Rendez-vous réguliers pour vérifier l'acquisition desdits objectifs,

- Identification et résolution des difficultés

Il peut être opportun de travailler avec une direction test qui pourra ensuite communiquer en interne sur son expérience de « pionnier » sur l'adoption du TPRM.

De même, il est recommandé d'identifier un sponsor dans chaque direction qui pourra être un support de proximité pour ses collègues.

Les Fiches Pratiques recommandent aux groupes de société de mettre en œuvre un réseau de conformité anticorruption qui aura à jouer un rôle dans le contrôle du dispositif d'évaluation des tiers. L'AFA précise que le responsable chargé du déploiement et du suivi du dispositif d'évaluation des tiers peut également diffuser au réseau de référent toutes informations ou éléments méthodologiques utiles[75].

La digitalisation du processus permet au responsable du déploiement d'être informé des diligences réalisées au sein de l'entreprise ou de ses filiales. L'outil peut également lui servir à diffuser des alertes ou des points de méthodologies, comme des modifications de questionnaires ou de demandes de pièces.

Les Fiches Pratiques rappellent en effet que le processus d'évaluation des tiers est en dynamique constante et doit être adapté aux risques qui peuvent naître de l'évolution contexte interne ou externe de l'entreprise.

3.2 Le contrôle du processus

Comme tout processus en vigueur dans l'entreprise, le TPRM peut faire l'objet d'un contrôle interne pour vérifier son fonctionnement et son efficacité. Le contrôle de l'appropriation d'un processus par ses parties prenantes est en effet majeur, et il peut être menacé par des circonstances diverses comme le départ de l'entreprise des personnes ayant été formées à son usage ou par un manque de ressources au sein des directions.

75. *Ibid.,* pt 137.

Il est à noter que le contrôle du processus d'évaluation des tiers est demandé par les programmes de conformité, en particulier la loi Sapin 2 qui prévoit à l'alinéa 8° de l'article 17 « *Un dispositif de contrôle et d'évaluation interne des mesures mises en œuvre*[76] ». Cette exigence est également rappelée dans les Fiches Pratiques de l'AFA[77].

Parmi les avantages de la digitalisation du processus de TPRM, le contrôle interne du dispositif sera grandement simplifié par les informations délivrées par l'outil : la procédure d'évaluation des tiers est-elle respectée à l'occasion de l'*onboarding* d'un tiers ? Combien d'évaluations ont été réalisées par les directions concernées ? etc. Ce point est aussi souligné par les Fiches Pratiques « *l'utilisation d'un outil digital peut être utile pour piloter efficacement le suivi du dispositif d'évaluation des tiers* » (Point d'attention n°8).

76. Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (Sapin 2).
77. AFA, *Fiches Pratiques, op. cit.*,pt 139.

IV. La digitalisation du processus de TPRM

L'avantage de la digitalisation du TPRM apparaît à tous les niveaux du processus : recueil et traitement de la donnée dans un contexte qui la sécurise, *workflow* de validation du tiers, intégration du processus dans les SI de l'entreprise pour faciliter la fluidité de son usage et permettre un haut niveau d'automatisation, contrôle interne du processus.

4.1. Le recueil et le traitement de la donnée sur le tiers

La digitalisation facilite le recueil de la donnée sur le tiers que celle-ci soit obtenue en interne ou en externe.

- **En interne :**

L'utilisation des API permet de communiquer avec les systèmes d'information internes à l'entreprise qui détiennent des informations sur les tiers. C'est le cas des ERP, ou des solutions *source to pay* qui disposent d'informations, a minima d'identification, sur les tiers.

La solution TPRM peut également à l'inverse, et toujours par API, intervenir dans le processus d'onboarding du tiers en suspendant une création de compte en cas de rejet du tiers à la suite de son évaluation.

Les directions ou filiales de l'entreprise peuvent disposer d'un historique de relations avec un tiers dont l'accès ne sera pas nécessairement centralisé. L'outil TPRM, notamment par le module questionnaire, peut faciliter le recueil d'informations internes sur le tiers.

- **En externe : la centralisation de multiples canaux d'information par API et la synthèse d'informations par IA**

La digitalisation du processus de TPRM permet de combiner les modes de recueil de données sur le tiers[78] sur une même interface et offrir ainsi une vision complète du tiers.

Les API permettent d'interroger plusieurs bases de données. L'IA a un rôle à jouer dans le traitement de l'information obtenue en facilitant la gestion des faux positifs, mais aussi par la synthèse de l'information obtenue sur le tiers, et la fourniture d'un *scoring* de risque.

Sous réserve d'obtenir un taux d'analyse qualitative satisfaisant, l'utilisation de l'IA dans le processus TPRM ouvre des perspectives intéressantes pour faciliter l'automatisation du processus en favorisant l'allocation des ressources humaines aux tiers présentant les risques les plus élevés.

- **La sécurisation de la donnée obtenue par le processus de TPRM et leur gestion conforme au RGPD**

Le processus de TPRM est encore souvent mis en œuvre par des solutions bureautiques (Word, Excel, Forms, Drive...). La sécurité qu'elles offrent pour les données collectées est relative, dans le sens où les questionnaires sont adressés par mail et que les informations sont conservées sur des bases de données des fournisseurs de ces solutions. Il est en revanche plus facile d'exiger d'un éditeur de solution TPRM la présence de ses bases de données en Europe.

Disposer d'un outil digital permet également de mieux gérer les obligations liées au RGPD (archivage ou suppression des données selon la politique de conservation des données définie par l'entreprise ou sur demande légitime de l'intéressé).

4.2. La digitalisation du workflow de validation au service des parties prenantes

La digitalisation du processus de TPRM facilite la collaboration de ses parties prenantes, mais aussi leur action individuelle.

78. V. *supra* 2.2 « Définir la nature des diligences à effectuer ».

- **Une collaboration simplifiée**

Lorsqu'il est digitalisé, le *workflow* de validation optimise la collaboration des parties prenantes du processus de TPRM. Les évaluations réalisées par les opérationnels sont assorties d'alertes qui imposent l'intervention du responsable de conformité en l'absence de réponse ou en cas de réponse insatisfaisante. L'information brute est ainsi criblée dès l'évaluation de l'opérationnel et permet au responsable de conformité de porter son attention uniquement sur les tiers les plus à risques.

La digitalisation du *workflow* de validation fluidifie également la communication des parties prenantes. Sur une interface commune, l'opérationnel peut saisir le responsable de conformité et lui transmettre toutes les informations relatives aux tiers présentant des risques en quelques clics.

- **La digitalisation au service de l'action individuelle des parties prenantes de l'évaluation**

Pour les opérationnels :

La digitalisation du processus TPRM par l'utilisation des API et de l'IA peut offrir un haut niveau d'automatisation et prévenir ainsi la fameuse fatigue d'un processus chronophage et bureaucratique décourageant les opérationnels.

Pour l'administrateur de la solution TPRM :

L'administrateur de la solution TPRM, le plus souvent le responsable juridique/conformité, dispose d'une vision globale du fonctionnement du TPRM dans l'entreprise. Il peut donc plus facilement intervenir. Comme mentionné ci-avant, le responsable de conformité est dispensé d'intervenir dans les dossiers présentant les niveaux de risque les plus faibles. Il peut ainsi concentrer ses efforts et ressources sur les tiers les plus à risque et mener des évaluations plus approfondies. de même concevoir des plans de traitement appropriés si la décision est prise de poursuivre la relation.

Les procédures réalisées dans le cadre d'un processus digitalisé de TPRM sont par ailleurs consignées dans des dossiers de tiers. Ces espaces centralisent les données recueillies par les opérationnels et le responsable de conformité et facilitent ainsi l'accès aux informations de ce dernier notamment à des fins d'analyse.

- **La digitalisation au service des tiers**

Le tiers bénéficie également des avantages liés à l'utilisation de solutions spécialisés en matière de TPRM. Il est en effet en mesure de répondre à l'ensemble des évaluations qui lui sont soumises sur une interface unique. En plus d'offrir des garanties en matière de sécurité, ces plateformes rendent plus compréhensibles les demandes de l'évaluateur et facilitent la réponse du tiers.

Dans le cadre des diligences effectuées par questionnaire d'auto-évaluation, des fonctionnalités pourront permettre au tiers de diffuser des questions ou bloc de questions en interne pour faciliter le recueil d'informations auprès de collègues selon la nature des demandes formulées (ex-information financière à la direction financière, etc.).

Le tiers est par ailleurs automatiquement relancé par l'interface notamment en cas de retard de réponse.

4.3 Digitalisation du processus de TPRM et intégration dans les outils SI de l'entreprise

Le TPRM a pour objectif de globaliser l'information détenue par l'entreprise sur le tiers et qui peut être recueillie par diverses directions et pour divers usages.

Ainsi, il est courant de constater que les entreprises disposent d'une plateforme pour gérer l'obligation de vigilance (vérification du Kbis, de l'attestation de vigilance URSSAF et de la liste de travailleurs étrangers) et d'outils de *screening* de bases de données pour obtenir des informations sur l'évaluation de l'intégrité, et de scoring financier.

Or, très souvent ces outils ne communiquent pas et ne sont pas intégrés, alors qu'un tiers non conforme à l'obligation de vigilance peut présenter des risques en matière d'intégrité.

Les API, comme précédemment évoqué, permettent aux outils de communiquer et donc de créer un processus de TPRM intégré. Cette approche facilite l'automatisation des diligences et une prise de décision documentée sur la collaboration avec le tiers.

4.4 Le contrôle de l'application des procédures

La digitalisation favorise le contrôle du responsable de conformité de l'application de la politique de TPRM par les opérationnels.

Les actions réalisées par les parties prenantes d'un processus digitalisé de TPRM sont répertoriées dans un historique où figurent également les dates et identité de leurs auteurs.

Le responsable de conformité qui dispose d'une vision d'ensemble sur ces actions est ainsi mis en mesure d'évaluer l'application de la politique d'évaluation des tiers par les opérationnels à des fins de contrôle interne, conformément à l'article 17, II, 8° de la loi Sapin 2. Il dispose à ce titre de pistes d'audits qu'il pourra fournir aux autorités afin de démontrer la conformité de la société aux exigences légales.

Pour clore cette réflexion sur le TPRM, **Madame Carmen Briceno**, Directrice juridique et conformité Groupe Raja, Responsable de la commission Compliance de l'AFJE, partage son expertise sur l'évaluation des tiers, qu'elle considère comme un impératif stratégique, opérationnel et collectif pour les entreprises.

> À l'instar du poème de John Donne « aucun homme n'est une île », aucune entreprise ne vit en autarcie. Chaque organisation est inéluctablement liée à un réseau de partenaires, de fournisseurs, de clients et d'intermédiaires, au sein d'un tissu économique, social et juridique où l'interdépendance est la norme.
>
> Ces relations sont non seulement inhérentes à l'activité commerciale, mais également essentielles à la compétitivité et à la croissance des entreprises, quelle que soit leur taille ou leur secteur d'activité. Pourtant, elles ne sont pas sans risque. Un partenaire commercial impliqué dans des pratiques contraires à la loi ou à l'éthique peut entraîner des conséquences juridiques, financières et réputationnelles majeures pour l'entreprise donneuse d'ordre.
>
> Les législations au niveau européen et international consacrent désormais la responsabilité des entreprises pour les manquements de leurs partenaires commerciaux, en particulier lorsque aucune diligence raisonnable n'a été exercée. Certaines réglementations sectorielles vont jusqu'à interdire la mise sur le marché de produits

sans évaluation préalable des fournisseurs. D'autres, comme le *UK Bribery Act de 2010* et *l'Economic Crime and Corporate Transparency Act de 2023*, vont encore plus loin : avec les infractions de *failure to prevent bribery* et *failure to prevent fraud*, une entreprise peut être tenue pénalement responsable si une personne associée commet un acte de corruption ou de fraude pour son bénéfice, sauf si elle peut démontrer avoir mis en place des procédures adéquates. Ces dispositifs traduisent une évolution vers une responsabilité proactive des entreprises dans la prévention des comportements délictueux de leurs tiers.

Dans ce contexte, l'évaluation des tiers ne relève plus d'une simple formalité administrative. Elle constitue un levier essentiel de maîtrise des risques, de conformité réglementaire et de responsabilité sociétale.

Des obligations multiples, des obstacles concrets

En pratique, comme nous avons pu le constater dans le cadre des travaux du groupe d'experts compliance de l'AFJE, les entreprises et leurs équipes conformité sont confrontées à une pluralité d'obligations : lutte contre la corruption, respect des sanctions internationales, lutte contre le blanchiment des capitaux et le financement du terrorisme, devoir de vigilance, exigences particulières de clients, engagements RSE volontaires… Cette complexité est aggravée par des obstacles opérationnels : accès limité à des bases de données fiables, sources disparates et non comparables selon les juridictions, lacunes d'information dans certaines zones, manque de ressources internes ou de coordination interservices.

Des principes structurants pour une démarche efficace

Face à ces défis, les autorités et les organisations internationales s'accordent sur plusieurs principes fondamentaux. Une approche fondée sur les risques, adossée à une cartographie « vivante » régulièrement mise à jour, est indispensable. La tonalité donnée par l'instance dirigeante (*tone from the top*) constitue un principe cardinal : la crédibilité et l'efficacité du dispositif reposent sur des politiques claires et transparentes, une démarche globale et transverse, une allocation de ressources adaptée, une veille réglementaire active et un reporting régulier aux organes de gouvernance.

Le rôle des outils numériques

Dans cette ère numérique, le recours à des outils technologiques conformes à la réglementation (RGPD, principes éthiques de l'IA) s'impose comme une évidence pour accompagner cette démarche complexe. Les technologies de *due diligence* automatisée, paramétrables et contrôlées manuellement, l'intelligence artificielle et les bases de données spécialisées permettent de gagner en efficacité, en traçabilité et en couverture géographique.

L'action collective, un levier à ne pas négliger

Au-delà des démarches individuelles, l'action collective constitue un levier puissant pour structurer et diffuser les bonnes pratiques. Dans certains secteurs des questionnaires de *due diligence* standardisés ont été développés pour faciliter l'évaluation des tiers, en particulier pour aider les PME. Un exemple concret est le portail *due diligence ready*! de la Commission Européenne pour la conduite du devoir de diligence à l'égard de la chaîne d'approvisionnement des industries extractives. Ces outils permettent de mutualiser les efforts, de réduire les coûts (https://single-market-economy.ec.europa.eu/sectors/raw-materials/due-diligence-ready_fr) et d'assurer une cohérence sectorielle dans les exigences de conformité.

Les associations professionnelles ont un rôle clé à jouer dans la diffusion de ces bonnes pratiques. L'AFJE y contribue activement à travers les travaux de sa commission Compliance (ses actualités sur la page LinkedIn @AFJE Compliance), la publication de la revue JEM, (Juristes d'entreprise magazine) dont le hors-série de novembre est consacré à la compliance, l'organisation de conférences en présentiel et en ligne, et la participation aux consultations des autorités. Ce Livre Blanc constitue un exemple concret de bonnes pratiques à promouvoir et de collaboration interprofessionnelle.

Conclusion

Une démarche d'évaluation de l'intégrité des tiers, fondée sur les risques, proportionnée, documentée, soutenue par la direction et outillée de manière adéquate, constitue aujourd'hui un levier stratégique pour concilier sécurité juridique, efficacité opérationnelle et création de valeur durable.

Évaluer ses tiers, c'est prioriser ses risques, affirmer ses valeurs et construire sa crédibilité.

Bibliographie

I. Organisations internationales

Organisation des Nations Unies (ONU)

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

Organisation de coopération et de développement économiques (OCDE)

OCDE, Convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales, 1997, disponible sur : https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0378.

OCDE, *Conformité des entreprises à la lutte contre la corruption : moteurs, mécanismes et idées de changement*, 2020, disponible sur : 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.

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

Groupe d'action financière (GAFI)

GAFI, *Directive sur les personnes politiquement vulnérables et les dirigeants d'une organisation internationale*, 2021, disponible sur : https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/pep/pep-fra.

Banque mondiale

Banque mondiale, *Lignes directrices en matière d'intégrité*, 2018, disponible sur : https://thedocs.worldbank.org/en/doc/302151536766276403-0240022018/WBG-Integrity-Compliance-Guidelines-CH.

II. Droit de l'Union européenne

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (*Règlement général sur la protection des données*), JOUE, L 119, 4 mai 2016, p. 88.

Directive (UE) 2024/1760 du Parlement européen et du Conseil du 13 juin 2024 relative à la diligence raisonnable en matière de durabilité des entreprises, JOUE, L 1760, 13 juin 2024.

Commission européenne, *Règlement délégué (UE) 2023/2772 de la Commission du 31 juillet 2023 complétant la directive (UE) 2022/2464 du Parlement européen et du Conseil en ce qui concerne les normes d'information en matière de durabilité*, JOUE, L 277, 22 oct. 2023, p. 465.

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant la sécurité des réseaux et des systèmes d'information (*directive NIS 2*).

Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 relatif à la résilience opérationnelle numérique du secteur financier (*règlement DORA*).

Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 relatif à la cyberrésilience (*Cyber Resilience Act*).

Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 fixant un régime de contrôle des exportations, du courtage, de l'assistance technique, du transit et du transfert des biens à double usage.

III. Droit interne (France)

Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (*loi Sapin II*), JORF, 10 déc. 2016, texte n° 2, disponible sur : https://www.legifrance.gouv.fr/jorf/id/JORFSCTA000033558530.

Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre, JORF, n° 74, 28 mars 2017.

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF n° 0235 du 8 octobre 2016.

Code du travail, art. L.8222-1 et s.

Code civil, art. 1130, 1131, 1137, 1178, 1240 et 1241.

Code monétaire et financier, art. L.561-5 et R.561-5.

IV. Doctrine et rapports institutionnels

Agence française anticorruption (AFA)

AFA, *Recommandations destinées à aider les personnes morales à prévenir et à détecter les faits de corruption, trafic d'influence, concussion, prise illégale d'intérêts, détournement de fonds publics et favoritisme*, 4 déc. 2020, § 205-207, disponible sur : https://www.agence-francaise-anticorruption.gouv.fr.

AFA, *Avis relatif aux recommandations destinées à aider les personnes morales à prévenir et à détecter les faits de corruption*, 12 janv. 2021.

AFA, *Recueil de fiches pratiques – Bases d'information publiques utiles à l'évaluation de l'intégrité des tiers*, 9 mars 2023, disponible sur : https://www.agence-francaise-anticorruption.gouv.fr/fr/document/afarecueil-fiches-pratiques-bases-publiques.

AFA, *Diagnostic national sur les dispositifs anticorruption dans les entreprises*, 2024, disponible sur : https://www.agence-francaise-anticorruption.gouv.fr.

AFA, *Projet de fiches pratiques sur la mise en œuvre de la mesure d'évaluation des tiers au regard du risque de corruption au sein des entreprises*, juillet 2025.

AFA, *Présentation des référentiels étrangers promouvant l'intégrité dans la vie des affaires*, 2023.

Autres sources doctrinales

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

V. Droit comparé

Royaume-Uni

UK Bribery Act 2010, loi du 8 avril 2010, disponible sur : https://www.legislation.gov.uk/ukpga/2010/23/contents/enacted.

Economic Crime and Corporate Transparency Act 2023, 26 octobre 2023, c. 56, disponible sur : https://www.legislation.gov.uk/ukpga/2023/56/enacted.

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

États-Unis

Foreign Corrupt Practices Act (FCPA), 1977.

U.S. Department of Justice et Securities and Exchange Commission, A Resource Guide to the U.S. Foreign Corrupt Practices Act, 2e éd., 2020, disponible sur : 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, disponible sur : https://www.justice.gov/criminal/criminal-fraud/file/838416/dl.

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

Allemagne

Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten (*Lieferkettensorgfaltspflichtengesetz – LkSG*), BGBl. I, n° 46, 22 juillet 2021, p. 2959.

Pays-Bas

Wet zorgplicht kinderarbeid, Kamerstuk 34506-A, 14 mai 2019.

Wet zorgplicht mensenrechten en milieu, 2024.

Brésil

Lei Anticorrupçao, 1er août 2013.

VI. Sources pratiques et sites institutionnels

CNIL, *Guide pratique RGPD – Sécurité des données personnelles*, 2024.

ENISA, T*echnical Implementation Guidance on Cybersecurity Risk Management Measures*, juin 2025, disponible sur : 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, disponible sur : https://osintframework.com/.

API gouvernementales françaises : https://api.gouv.fr/les-api/api_data_gouv.

OFAC, *Sanctions List Search*, disponible sur : https://sanctionssearch.ofac.treas.gov/.

Registre du gel des avoirs, disponible sur : https://gels-avoirs.dgtresor.gouv.fr/List.

LCB-FT, disponible sur : https://lcb-ft.fr.

ACPR, *Lignes directrices du registre officiel*, disponible sur : https://acpr.banque-france.fr/fr/reglementation/registre-officiel/lignes-directrices.

AFJE, *Vidéo sur les sanctions internationales*, disponible sur : https://www.afje.org/ressources/compliance-video-sur-les-questions-relatives-aux-sanctions-internationales--494.

Annexes

Annexe 1: **Checklist des points à vérifier dans le cadre du Third party risk management**

I. Vérifications de nature générales

1. IDENTIFICATION DE LA PERSONNE ÉVALUÉE

A. Personne physique

- Nom
- Prénom
- Adresse
- Date et lieu de naissance
- Contact

B. Personne morale

B-1 Identification

- K BIS ou équivalent local
- N° SIRET
- N° SIREN
- N° de TVA
  N° DUNS
- Existence de sanctions/condamnations

B-2 Forme sociale

- Forme juridique
- Cotation sur un marché réglementé

B-3 Gouvernance : Mandataires sociaux

- Nom
- Prénom
- Date de naissance et lieu de naissance
- Existence de sanctions/condamnations
- Existence de conflits d'intérêts entre les mandataires sociaux du tiers et l'entreprise

B-3 bis Gouvernance : Autres organes de gouvernance

Élément identifié	Renseignements recueillis			
2. Identification des bénéficiaires effectifs	**Nom**	**Prénom**	**Date et lieu de naissance**	**Existence de sanctions / condamnations**
3. Identification des agents publics et PPE	Participation d'agents publics ou de PPE au sein de l'organisation du tiers	Présence d'agents publics ou de PPE dans l'actionnariat du tiers ou ses bénéficiaires effectifs	Identification des conflits d'intérêts potentiels du fait de la présence d'un agent public ou une PPE dans l'actionnariat ou la gouvernance du tiers	
4. Identification des relations commerciales présentes et passées entre le tiers et l'entité donneuse d'ordre	Historique des relations avec le tiers (référence contrats, date)	Prestation actuellement assurée par le tiers (description du contrat)		
5. Lutte contre le travail dissimulé (obligation de vigilance)	Vérification de la conformité aux obligations déclaratives (attestation de vigilance URSSAF, liste de travailleurs étrangers,k bis)			

II. Identification des risques liés à la prestation effectuée

Élément identifié	Renseignements recueillis			
1. Réalisation effective de la prestation/ Identification des sous-traitants	Recours du prestataire à des sous-traitants pour l'exécution de la prestation contractuelle	Identité des sous-traitants	Tâches assurées par les sous-traitants	Liens (famille, intérêt...) susceptibles d'engendrer des conflits d'intérêts avec le sous-traitant
2. Identification des risques au regard des zones géographiques et des activités	Lieu de réalisation de la prestation (pays),	Identification du lieu/pays des sites de production et évaluation des risques dans des pays à haut risque corruption (au regard du classement Transparency International),	Identification des activités nécessitant des autorisations administrative/ licence	Recours à des intermédiaires / agents
3. Identification des risques de dépendance économique du tiers	% du CA du tiers réalisé actuellement auprès de la société donneuse d'ordre et rapport avec le CA global du tiers.			
4. Informations financières	Bilans des 3 derniers exercices,	Informations de solvabilité financière (cotations) fournies par une banque centrale,	Identification de la banque recevant les paiements liés contrat	IBAN du compte recevant les paiements liés au contrat et certification de l'IBAN

III. Identification des informations à recueillir du fait d'obligations légales d'évaluation

A. Identification de la conformité du sous-traitant au règlement DORA				
Importance du service fourni pour l'organisme financier (nature, rôle dans sa prestation de service, % du CA concerné…)	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 obtenues en matière de protection des données personnelles/ sécurité informatique	Mesures de cybersécurité mise en place	Politique de sécurité de l'information	Test de résilience opérationnelle numérique	

B. Identification de la conformité du sous-traitant au RGPD				
Objet et durée de la prestation	Nature et finalité du traitement	Type de données personnelles traitées et catégories de personnes concernées	Lieu de conservation des données	Délai de conservation des données personnelles
Tenue d'un registre de traitement	Mesures mise en place pour assurer la conformité du traitement de données aux exigences du RGPD : • Garantie du respect du principe de nécessité • Garantie de la durée de conservation des données • Garantie du nombre de personnes ayant accès aux données • Garantie de l'étendue du traitement des données • Garanties liées à la suppression des données			Politique de sécurité des systèmes d'information mise en place (nécessité d'obtenir un justificatif)
Présence d'un DPO, niveau de certification du DPO	Recours à des sous-traitants de données ultérieurs	Contrôles destinés à assurer la conformité du sous-traitant aux normes de protection de données du RGPD	Obligation de confidentialité des employés travaillant au contact des données personnelles recueillies	Certifications obtenues en matière de protection des données personnelles/ sécurité informatique
Mesures de cybersécurité mise en place	Politique de sécurité de l'information			

C. Identification de la conformité du sous-traitant au règlement NIS 2			
Politique de sécurité de l'information mise en place	Politique d'analyse des risques cyber mise en place	Plan de gestion des incidents	Plan de continuité d'activité (procédures de sauvegarde, de reprise après sinistre et de gestion de crise)
Existence de sous-traitants travaillant pour le prestataire	Dispositif de contrôle des mesures de cybersécurité des sous-traitants	Mesures de sécurité appliquées aux réseaux et systèmes d'information (notamment lors de leur acquisition, développement et maintenance)	Politique de contrôle de l'efficacité des mesures de gestion des risques cyber en place
Pratiques de base en matière de cyber hygiène (sauvegardes, mises à jour des logiciels…) et formation du personnel à la cybersécurité mise en place	Dispositif de cryptage et de chiffrement des données	Politique de contrôle d'accès et de gestion des actifs mise en place	Mesures sécurisant l'authentification
Politique de sécurité des ressources humaines (gestion des données collectées à lors des recrutements, données personnelles des salariés…)	Systèmes sécurisés de communication d'urgence mis en place au sein de l'entité	Certifications obtenues en matière de protection des données personnelle/ sécurité informatique	Procédure de rapport des incidents importants mise en place

D. Éléments d'Identification relatifs aux fonds (LCB-FT)

Personne physique	Personne morale
Situation financière et professionnelle (Revenus annuels et emploi occupé)	Situation financière (CA annuel)
Justificatif de domicile	Justificatif de domicile
Provenance des fonds	Provenance des fonds
Destination des fonds	Existence de tiers et nature des liens entre le client et les tiers
Existence de tiers et nature des liens entre le client et les tiers	Statuts
	Objet social
	Secteur d'activité

E. Éléments d'identification relatifs du contrôle des exportations (liés à la nature du bien et/ou des services)

Identité de l'utilisateur final : - Personne physique (Cf IB. Identification de la personne morale) - Personne morale (Cf IB. Identification de la personne morale)	Identité des parties prenantes intervenant dans la transaction (intermédiaires, sous-traitants...)	Bénéficiaires effectifs de l'utilisateur final	Identité des bénéficiaires effectifs des intervenants à la transaction
Justificatifs de l'identité des parties prenantes (intermédiaire, utilisateur final...)	Sanctions internationales reçues par le tiers ou à une partie prenante	Moyens de financement de l'acquisition	Mesures de contrôle des risques de détournement mises en place

F. Éléments d'identification relatifs au contrôle des atteintes aux droits humains et à l'environnement par les acteurs de la chaine de valeur	
Impact environnemental de l'activité du tiers : **• Pollution des eaux** **• Pollution des sols** **• Émissions de gaz à effet de serre** **• Déchets et recyclage**	Mesures destinées à garantir la sécurité des travailleurs impliqués dans l'activité du tiers • Mesures prises pour garantir le bénéfice des salariés de leurs droits fondamentaux (liberté d'association, liberté syndicale…) • Respect des mesures de sécurité prescrites par la loi à destination des salariés • Autres mesures destinées à assurer la sécurité des salariés
- Actions mises en œuvre par le tiers pour contrôler les atteintes aux droits humains et à l'environnement dans sa chaine d'approvisionnement	- Certifications reçues par le tiers en matière de droits humains et de protection de l'environnement

G. Éléments d'identification relatifs à la lutte contre la corruption		
- Identification des référentiels anticorruption applicable par le tiers (Sapin 2, UK Bribery act, FCPA),	- Code et procédure destinés à lutter contre la corruption en vigueur dans l'entreprise,	- Processus issus de la loi Sapin 2 mis en place (alerte interne, évaluation des tiers, cartographie de risques…) FCPA, UK Bribery act

IV. Identification des informations à recueillir du fait d'obligations légales d'évaluation

Informations RSE			
Démarche RSE du tiers et justificatifs	Recueil de données au sein de la chaîne de valeur du fait de la CSRD	Volume d'émissions de CO_2 annuel	Volume annuel d'émissions de CO_2 des membres de la chaîne de valeur

Annexe 2 : Tableau de synthèse des obligations légales d'évaluation des tiers

Texte	Obligation générale d'évaluation des tiers	Seuil d'obligation	Situation géographique	Obligation sectorielle	Nature de la diligence à effectuer
Lutte contre le travail dissimulé/ Obligation de vigilance. (France)		Entreprises ayant recours à des prestataires de services pour des montants supérieurs à 5000 euros HT	Entreprises établies en France		Recueil et vérification de : -l'attestation URSSAF -La liste des travailleurs étrangers -L'extrait K-BIS ou équivalent -L'attestation de régularité fiscale
LCB-FT (France, Europe) Ordonnance n° 2020-115 du 12 février 2020 renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme. Directive (UE) 2018/843		Pas de seuil	Sur le territoire de l'union européenne Ou Entreprise établie hors de l'UE dont l'activité cible des résidents européens	Acteurs du secteur financier (banques, établissement de monnaie électronique...) et Professions susceptibles d'être impliquées dans des faits de blanchiment de fonds (avocats, notaire, commissaires de justice ...)	Screening de base de données (PEP, sanctions...) Questionnaire relatif à l'identité du client et à la nature des fonds (provenance, utilisation...) Recueil de pièces justificatives Vérification de l'identité du tiers (utilisation d'une méthode agrée par la règlementation, exemple : prestataire ayant recours à la biométrie)

Texte	Obligation générale d'évaluation des tiers	Seuil d'obligation	Situation géographique	Obligation sectorielle	Nature de la diligence à effectuer
Export control (Europe) Règlement (UE) 2021/821 du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage		Pas de seuil	Exportations de biens hors du territoire européen Transit de biens sur le territoire européen	Production/ fourniture de biens à double usages	Questionnaire relatif à l'utilisation finale du bien Screening de base de données (sanctions internationales, adverse média...) Recueil et vérification de l'identité des parties prenantes (utilisateur final, intermédiaires...) Gestion documentaire (factures, document d'accompagnement des exportations, compte-rendu d'utilisation)
Digital Operational Resilience Act (DORA) (Europe) Règlement européen 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier		Pas de seuil	- Entreprise proposant des services financiers sur le territoire de l'Union européenne - Prestataire offrant des services numériques à des entités financières couvertes par ce texte	Entreprises du secteur financier (banque, assurance, établissement de monnaie électronique...)	Questionnaire d'évaluation de la criticité du tiers (détermination du niveau de dépendance de l'entité financière au prestataire) Questionnaire cybersécurité et résilience (mesures de sécurité informatique du prestataire, procédure de gestion des incidents, tests réalisés...) Clauses contractuelles d'encadrement de l'usage de la sous-traitance par le prestataire Audits des mesures de cybersécurité et de protection des données du sous-traitant Tenue d'un registre des prestataires de TIC répertoriant l'ensemble des prestataires participant au fonctionnement des systèmes d'information de l'entité financière

Texte	Obligation générale d'évaluation des tiers	Seuil d'obligation	Situation géographique	Obligation sectorielle	Nature de la diligence à effectuer
RGPD (Europe) Règlement général sur la protection des données (règlement UE 2016/679)		Pas de seuil	Entreprise établie sur le territoire de l'UE Ou Entreprise établie hors UE dont l'activité cible des résidents européens	Toute entreprise réalisant de la collecte/ du traitement de données personnelles	Audit de contrôle du respect des règles du RGPD par le sous-traitant (durée de conservation, registre de traitement des données…) Questionnaire sur les procédures mises en place pour assurer la sécurité des données (mesures de protection physique, logiciels, sauvegardes…) Recueil de pièces justifiant du respect des règles du RGPD (certifications…) Questionnaires d'identification des sous-traitants ultérieurs Clauses contractuelles limitant/encadrant la sous-traitance ultérieure et le transfert de données hors UE
NIS 2 (Europe) Directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union		Entreprises dépassant : +50 salariés +1M CA (sauf exception) (les mesures appliquées aux PME sont allégées)	Entreprise disposant d'un établissement sur le territoire de l'UE Ou Entreprise établie hors de l'UE dont l'activité cible des résidents européens	Entreprises publiques et privées de secteurs d'intérêt général : santé, finance, gestion des déchets…	Audits réguliers de la conformité des mesures de cybersécurité et de protection des données du sous-traitant aux standards de la directive (plan de continuité d'activité, plan de reprise d'activité, formation des personnels…) Questionnaire cybersécurité et résilience (mesures de sécurité informatique en place, procédure de gestion des incidents) Clause contractuelle reprenant les exigences de la directive en matière de cybersécurité
Cyber resilience act (Europe) Règlement européen 2024/2847 du 20 novembre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques			Entreprises contribuant à la commercialisation sur le marché européen de produits comportant des éléments numériques dont l'usage inclut une connexion à un réseau (fabricants, importateurs, distributeurs)	Entreprises fabricant / important/distribuant des produits numériques Produit numérique : produit logiciel ou matériel et ses solutions de traitement des données à distance y compris les composants logiciels et matériels vendus séparément Exemple : objets connectés (smartphones…), logiciels associés à ces objets, composants de ces objets	Questionnaires relatifs aux risques et vulnérabilités du produit (mesures de suppression des vulnérabilités, mises à jour de sécurité, protection des accès, protection et traitement des données, mesures de résilience,…) Clauses contractuelles reprenant les exigences de la directive

Annexe 3 : **Questionnaire et pièces à fournir au contrôle des entités assujetties à la loi SAPIN 2**

G. Évaluation de l'intégrité des tiers : clients, fournisseurs de premier rang, intermédiaires[79]

G.1. Disposez-vous d'une ou plusieurs bases de données recensant l'ensemble de vos tiers ?
Avez-vous identifié des groupes homogènes de tiers présentant un profil de risque comparable ? Si oui, comment et quel est leur niveau ? En particulier, la cartographie des risques de corruption de l'entité contrôlée a-t-elle été utilisée ? Si oui, comment ?

G.2. Au sein de l'entité contrôlée, existe-t-il un dispositif d'évaluation des tiers spécifique ou intégrant les risques de corruption ? Ce dispositif d'évaluation des tiers est-il décliné par groupes homogènes de tiers présentant un profil de risque comparable ? Si oui, quelles sont les typologies retenues par l'entité contrôlée ?
Présenter tout document relatif au dispositif d'évaluation des tiers au regard des risques de corruption de l'entité contrôlée.

G.4. Indiquer les fonctions ou services en charge de l'évaluation de l'intégrité des tiers suivant les différentes typologies. Est-il fait appel à un prestataire externe pour évaluer ces tiers ? Présenter tout document définissant les rôles et responsabilités des collaborateurs en charge ou en appui de l'évaluation des tiers.

G.5. Le dispositif d'évaluation de l'intégrité des tiers est-il décliné au sein de l'entité contrôlée (notamment au sein des groupes, métiers, divisions, pôles d'activité ou filiales) ? Si oui, comment ?
Existe-t-il des dispositifs différents au sein de certains groupes, métiers, divisions, pôles d'activité ou filiales ?

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

G.6. Comment les diligences à accomplir (modalité, fréquence, nature des diligences, etc.) par groupe homogène de tiers ont-elles été définies? Présenter tout document décrivant les diligences à accomplir par groupe homogène de tiers.

G.7. Quelles sont les diligences effectuées en fonction des risques identifiés (notamment par recours à des données en sources ouvertes, des documents demandés aux tiers, par la consultation de listes internes et externes, par des entretiens, par des audits, etc.) ? Suite aux diligences réalisées, une notation du risque spécifique ou détourée du risque global est-elle réalisée ?

G.8. Quel est le processus de validation (avis, consultation, décision) à l'issue de l'évaluation des tiers ?

G.9. Quelles sont les modalités de mise à jour et de suivi des dossiers d'évaluation des tiers (notamment leurs fréquences définies en fonction de la nature et du niveau de risque, le service responsable de la mise à jour et de son suivi) ?

G.10. Comment sont traités les dossiers non conformes (par exemple : dossiers ou questionnaires incomplets, échéance de mise à jour dépassée) ? Présenter tout document relatif au traitement des dossiers non conformes.

G.11. Existe-t-il des processus de dérogation au dispositif d'évaluation des tiers (portant le cas échéant sur des opérations ou projets particuliers, une catégorie de tiers spécifiques, un niveau de seuil défini, etc.) ? Si oui, lesquels et selon quels critères ?

G.12. Préciser les modalités et les délais de conservation et d'archivage des dossiers d'évaluation des tiers.

G.13. Qui est en charge du contrôle de premier niveau ? Présenter la méthode du contrôle permettant de s'assurer du respect de la procédure d'évaluation des tiers et de l'exhaustivité des dossiers (notamment pièces demandées, avis et visas obligatoires).

G.14. Qui est en charge du contrôle de deuxième niveau ? Présenter la méthode du contrôle permettant de s'assurer de la bonne exécution des contrôles de premier niveau et du bon fonctionnement du dispositif d'évaluation des tiers.

G.15. Existe-t-il un contrôle de troisième niveau pour s'assurer que le dispositif d'évaluation des tiers est conforme aux exigences réglementaires et internes et qu'il est efficacement mis en œuvre et tenu à jour ? Si oui, par qui est-il réalisé ?

G.16. Le dispositif d'évaluation des tiers s'adosse-t-il à un ou plusieurs systèmes d'information ? Si oui, lesquels ? Présenter tout document relatif à ce ou ces systèmes d'information.

G.17. Quelles sont les mesures de vigilance, spécifiques aux risques identifiés, prises, le cas échéant, à l'issue de l'évaluation, destinées à maîtriser les risques pendant la relation avec le tiers à risque (notamment procédures et fréquences de mises à jour adaptées, contrôles ciblés, suivi des flux financiers) ?

G.20. Existe-t-il une ou des procédures(s) d'évaluation spécifiques à d'autres types de tiers (bénéficiaires d'actions de mécénat ou de partenariat, cibles d'acquisition, lobbyistes, partenaires commerciaux, etc.), le cas échéant à travers des audits ou des contrôles comptables particuliers ?

G.21. Dans l'hypothèse où l'entité contrôlée a décidé de communiquer sur son engagement anticorruption auprès de ses tiers, comment cette communication se matérialise-t-elle (notamment clauses contractuelles, communication externe) ? Présenter tout document témoignant de la communication de cet engagement.

Annexe 4 : Exemples de signaux de risque intégrité

EXEMPLES DE SIGNAUX DE RISQUE INTÉGRITÉ
Un Partenaire est détenu ou contrôlé par des agents publics ou fonctionnaires d'État ou en emploie.
Le tiers est détenu ou contrôlé par un administrateur, dirigeant ou salarié de notre entreprise ou des membres de leur famille proche.
Le tiers est recommandé par un agent public ou expressément demandé par un client, sauf si des exigences techniques l'exigent.
Le tiers suggère qu'il pourrait éviter ou accélérer certaines formalités ou un processus d'appel d'offres.
Le tiers a fait l'objet de poursuites pénales, liées à des faits de corruption, directement ou par le biais de ses représentants légaux.
Le tiers a manifestement un manque de compétences ou de ressources.
Le tiers refuse de communiquer des informations pertinentes sur les antécédents ou de se soumettre à un audit.
Le tiers refuse une clause contractuelle obligeant le cocontractant et en particulier un intermédiaire à justifier des prestations à l'appui de sa demande de paiement.
Le tiers refuse d'inclure des dispositions en matière de lutte contre la corruption dans un contrat.
Le tiers demande des modalités inhabituelles ou contraires aux pratiques du marché et/ou lorsque la nature spécifique des services fournis n'est pas claire.
Le tiers propose des modes de paiement ou arrangements financiers inhabituels (paiement en espèces, sur un autre compte, dans un autre pays).
Le tiers propose des offres ou des promesses d'avantages ou de cadeaux somptuaires ou qui excèdent les usages : proposition de séjours touristiques prépayés, invitation à des événements sportifs ou culturels de premier rang.

Glossaire

AFA : Agence Française Anticorruption
AFJE : Association Française des Juristes d'Entreprise
API : *Application Programming Interface*
CA : Chiffre d'affaires
COMEX : Comité Exécutif
CRA : *Cyber Resilience Act*
CRM : *Customer Relationship Management*
CSRD : *Corporate Sustainability Reporting Directive*
CSDDD : *Corporate Sustainability Due Diligence Directive*
DORA : *Digital Operational Resilience Act*
DSI : Direction des Systèmes d'Information
DUNS : *Data Universal Numbering System*
ECCTA : *Economic Crime and Corporate Transparency Act*
ERP : *Enterprise Resource Planning*
FCPA : *Foreign Corrupt Practices Act*
IA : Intelligence Artificielle
IBAN : *International Bank Account Number*
JEM : Juriste d'Entreprise Magazine (AFJE)
KBIS : Document officiel attestant l'existence juridique d'une entreprise en France
LCB-FT : Lutte contre le blanchiment de capitaux et le financement du terrorisme
MSA : Mutualité Sociale Agricole
NIS : *Network and Information Systems Security*
OFAC : *Office of Foreign Assets Control*
ONU : Organisation des Nations Unies
OSINT : *Open Source Intelligence*
PEP : Personne Politiquement Exposée
PME : Petite et Moyenne Entreprise
R&D : Recherche et Développement
RGPD : Règlement Général sur la Protection des Données
RSE : Responsabilité Sociétale des Entreprises
SI : Système d'Information
SIREN : Numéro d'identification des entreprises
SIRET : Numéro d'identification des établissements
SMSI : Système de Management de la Sécurité de l'Information
TIC : Technologies de l'Information et de la Communication
TPRM : *Third Party Risk Management*
TVA : Taxe sur la Valeur Ajoutée
UE : Union Européenne
UK : Royaume-Uni
URSSAF : Union de Recouvrement des cotisations de Sécurité Sociale et d'Allocations Familiales
US : États-Unis

Design graphique : www.lendroit.com
Impression : Pixartprinting
Novembre 2025

TPRM

De l'évaluation des tiers au Third Party Risk Management

Livre blanc du Strategic Compliance Studies Committee de French Compliance Society

Le *Third Party Risk Management* (TPRM) constitue un facteur clé de la performance de la chaîne de valeur de l'entreprise. Cette approche vise à identifier et traiter de manière globale les risques et opportunités liés aux relations avec les tiers (fournisseurs, prestataires, partenaires, clients...). Son caractère stratégique est évident, compte tenu du rôle essentiel des tiers dans la création de valeur.

Au-delà de la conformité aux obligations légales d'évaluation des tiers (anticorruption, vigilance, LCB-FT, sanctions internationales...) et de la prise en compte des risques opérationnels (financiers, cyber, réputation...), le TPRM doit permettre de déployer et piloter des plans de traitement adaptés aux tiers à risque, dont la contribution à la création de valeur reste significative.

Comment sensibiliser les parties prenantes internes (instances dirigeantes et fonctions opérationnelles) à cette politique ? Comment positionner la fonction conformité comme architecte et copilote du TPRM, garantissant la cohérence globale des procès ? Quelles ressources, notamment digitales, lui affecter et quel ROI en attendre ? Comment intégrer le TPRM dans la culture d'entreprise et en faire un levier stratégique et un facteur d'avantage compétitif durable ?

Autant de questions abordées dans ce livre blanc initié par le *Strategic Compliance Studies Committee* de la *French Compliance Society*, enrichi par l'expertise et l'expérience d'enseignants-chercheurs et de praticiens.