

Comprendre et appliquer la due diligence : guide essentiel pour des relations d'affaires fiables

Dans un environnement économique marqué par l'interconnexion des marchés et la montée en puissance des exigences réglementaires (devoir de vigilance, loi Sapin II, RGPD, CSRD), les entreprises font face à une intensification des risques liés à leurs partenaires et fournisseurs. La gestion proactive de ces risques n'est plus une option : elle devient un levier stratégique pour sécuriser les opérations, préserver la réputation et garantir la conformité.

 **Optisure**, cabinet spécialisé en Due Diligence, accompagne les grandes organisations dans l'évaluation approfondie de leurs tiers, qu'il s'agisse de fournisseurs, de clients, de partenaires commerciaux ou de cibles d'acquisition. Grâce à une approche intégrée mêlant expertise sectorielle, analyse multidimensionnelle et outils digitaux, nous aidons nos clients à structurer des dispositifs de vigilance adaptés à leurs enjeux.

Notre mission : sécuriser vos relations d'affaires et vos opérations stratégiques par une évaluation complète et contextualisée des risques.

Dans cet article, nous vous proposons d'explorer les fondamentaux de la Due Diligence :

- Sa définition et ses spécificités
- Son cadre légal et réglementaire
- Les différents types de Due Diligence (précontractuelle, continue, transactionnelle)
- Les acteurs impliqués dans sa mise en œuvre
- Les étapes clés du processus d'investigation
- Et enfin, des outils pratiques pour structurer vos démarches

 Que vous soyez en phase de sélection de fournisseurs, en cours de partenariat ou sur le point de réaliser une opération de fusion-acquisition, **Optisure** vous aide à prendre des décisions éclairées, à anticiper les risques et à renforcer votre conformité.

Qu'est-ce que la Due Diligence ?

La définition

La Due Diligence, parfois traduite en français par « diligence raisonnable », désigne l'ensemble des investigations menées par une entreprise afin d'identifier, d'analyser et de maîtriser les risques associés à ses relations d'affaires. Concrètement, il s'agit d'un processus structuré d'évaluation qui permet d'examiner en profondeur la situation d'un tiers — qu'il s'agisse d'un fournisseur, d'un client, d'un sous-traitant ou d'un partenaire stratégique — avant ou pendant une collaboration. Cette démarche vise à sécuriser les engagements contractuels, à garantir la conformité réglementaire et à prévenir tout risque opérationnel, financier, juridique ou réputationnel.

Les Due Diligences vs. les concepts proches

La compréhension de cette pratique passe par sa comparaison avec des concepts similaires :

- L'audit est ponctuel. La Due Diligence est continue et s'inscrit dans la durée.
- Le contrôle interne examine les processus internes. La Due Diligence analyse les tiers.
- Le compliance monitoring vérifie la conformité réglementaire. La Due Diligence évalue tous les risques : financiers, opérationnels, réputationnels.

La Due Diligence se distingue des autres pratiques de vigilance par son approche globale et transversale. Elle embrasse l'ensemble des fonctions et des enjeux de l'entreprise, en mobilisant des expertises variées pour évaluer les risques sous toutes leurs formes. Ce processus structuré s'appuie sur huit grands axes d'investigation, que nous allons explorer en détail dans les prochaines sections.

Les trois moments de la Due Diligence

La Due Diligence s'opère à trois « moments » de la vie de l'entreprise : avant la signature d'un contrat, pendant la collaboration avec les tiers, ou encore avant une opération stratégique d'envergure.

1. La Due Diligence précontractuelle

Elle intervient avant toute signature d'un contrat avec un tiers (fournisseur, sous-traitant, prestataire, client). Cette investigation détermine si l'entreprise peut s'engager ou non dans la relation d'affaires.

Le périmètre et l'objet de cette analyse dépendent de la culture et de la maturité de l'entreprise, ainsi que des enjeux du contrat en question. En règle générale, **elle s'intéressera aux éléments suivants :**

- Les états financiers du tiers pour évaluer sa solidité financière ;
- Sa conformité aux obligations réglementaires (fiscales, sociales, environnementales) ;
- Sa structure de gouvernance et ses bénéficiaires effectifs ;
- Ses contentieux passés et en cours ;
- La validité de ses certifications métiers et accréditations sectorielles.

2. La Due Diligence continue

Il s'agit ici de surveiller en permanence les tiers avec lesquels l'entreprise travaille déjà. Cette surveillance permet de **détecter toute dégradation de situation nécessitant une action corrective**. On s'intéressera par exemple aux éléments suivants :

- La variation des indicateurs financiers clés (chiffre d'affaires, résultats, ratio d'endettement) ;
- Les changements dans l'actionnariat ou la direction ;
- Le renouvellement des certifications ;
- Le respect continu de leurs obligations légales.

3. La Due Diligence transactionnelle

À l'instar de la Due Diligence précontractuelle, cette analyse approfondie vise à sécuriser les opérations à fort enjeu stratégique telles que les fusions, acquisitions ou prises de participation. Elle permet d'évaluer avec précision :

- **La valeur économique réelle de la cible**, au-delà des apparences comptables ou des projections internes ;
- **Les engagements hors bilan et les passifs latents**, susceptibles d'affecter la viabilité ou la rentabilité de l'opération ;
- **Les leviers de création de valeur post-transaction**, notamment les synergies opérationnelles, commerciales ou technologiques ;
- **Les contraintes réglementaires propres à l'opération**, telles que les règles de concurrence, les agréments sectoriels ou les obligations de notification auprès des autorités compétentes.

Les trois axes opérationnels de la démarche de Due Diligence

Les Due Diligences s'articulent autour de trois processus complémentaires : la collecte documentaire, l'analyse des données et l'évaluation des risques.

1. La collecte documentaire

La première étape d'une Due Diligence globale consiste à organiser de manière rigoureuse la collecte et la consolidation des informations clés relatives à l'entité analysée. Cela inclut non seulement les documents légaux (extraits d'immatriculation, attestations fiscales et sociales), financiers (états comptables, rapports d'audit), opérationnels (certifications qualité, agréments techniques), et contractuels (polices d'assurance, conventions commerciales), mais aussi les éléments ESG, les données de cybersécurité, les indicateurs de gouvernance et les engagements extra-bilan.

Cette phase implique également une vérification systématique de l'authenticité des pièces fournies, leur traçabilité, ainsi qu'un suivi régulier de leur validité dans le temps. Elle constitue le socle d'une analyse plus large, permettant de croiser les données internes avec des sources externes, d'identifier les signaux faibles et de préparer les investigations approfondies sur les risques stratégiques, réglementaires, réputationnels ou opérationnels.

2. L'analyse des données

Cette phase vise à confronter les données internes collectées avec un ensemble de sources externes : bases de données réglementaires et financières, études sectorielles, listes de sanctions, registres publics, ainsi que les signaux faibles issus du marché (presse spécialisée, réseaux professionnels, veille réputationnelle, etc.).

L'objectif est double :

- **Détecter les incohérences** entre les différentes sources (par exemple, divergences entre les états financiers publiés et les notations sectorielles, ou entre les certifications revendiquées et les agréments officiels).
- **Évaluer la robustesse et la fiabilité des données**, en identifiant les zones d'ombre ou les éléments non documentés qui pourraient masquer des risques latents (structures opaques, engagements hors bilan, dépendances critiques, etc.).

Cette étape permet de construire une première cartographie des risques multidimensionnels — financiers, juridiques, opérationnels, ESG, réputationnels — et de prioriser les investigations complémentaires à mener. Elle constitue un pivot stratégique entre la collecte documentaire et l'évaluation finale des risques, en posant les bases d'une vigilance proactive et contextualisée.

3. L'évaluation des risques

Sur la base des documents collectés et des données analysées, l'entreprise réalise une cartographie détaillée des risques identifiés.

Ils peuvent être d'ordre financier (solvabilité, endettement), opérationnel (dépendance clients/fournisseurs), réglementaire (non-conformité, sanctions), réputationnel (controverses ESG), etc.

L'entreprise engage par la suite **les décisions habituelles de la gestion des risques**, notamment la quantification de la probabilité et de l'impact potentiel, la définition des seuils d'acceptabilité et les mesures de mitigation appropriées.

Le cadre légal des Due Diligences

Au fil des dernières décennies, les législateurs à travers le monde ont progressivement renforcé les exigences de vigilance imposées aux entreprises dans leurs relations d'affaires. Cette évolution normative répond à des impératifs universels : prévenir la corruption, protéger les droits humains, préserver l'environnement, et lutter contre le blanchiment d'argent dans des chaînes de valeur de plus en plus mondialisées.

Initialement fondée sur des engagements volontaires et des standards sectoriels, la Due Diligence s'est transformée en une obligation juridique structurante dans de nombreuses juridictions. À partir de la seconde moitié des années 2010, plusieurs cadres législatifs ont vu le jour :

-  **Le devoir de vigilance** en France,

-  **La loi sur la chaîne d’approvisionnement** en Allemagne (Lieferkettengesetz),
-  **La loi norvégienne sur la transparence,**
-  **Le Modern Slavery Act** au Royaume-Uni,
-  **Le RGPD** en Europe pour la protection des données,
-  Et plus récemment, le projet de **Directive européenne sur la diligence raisonnable en matière de durabilité des entreprises (CSDDD).**

Ces textes traduisent une tendance mondiale vers une responsabilisation accrue des entreprises, les obligeant à identifier, prévenir et atténuer les risques liés à leurs opérations, leurs partenaires et leurs chaînes d’approvisionnement.

La loi sur le devoir de vigilance (2017)

Cette loi oblige les sociétés mères et entreprises donneuses d'ordre de plus de 5 000 salariés en France (ou 10 000 dans le monde) à exercer une Due Diligence sur toute leur chaîne de valeur. Concrètement, elles doivent :

- Cartographier les risques d'atteintes graves aux droits humains, à la santé-sécurité et à l'environnement ;
- Évaluer la situation de leurs filiales, sous-traitants, prestataires et fournisseurs ;
- Mettre en place des actions de prévention et d'atténuation des risques ;

- Créer un mécanisme d'alerte ;
- Suivre l'efficacité des mesures.

La loi Sapin II (2016)

Pour les entreprises de plus de 500 salariés et 100 millions d'euros de chiffre d'affaires, la loi impose une Due Diligence anti-corruption structurée autour des actions suivantes :

- L'évaluation systématique des clients, fournisseurs de premier rang et intermédiaires ;
- La mise en place de procédures de contrôles comptables ;
- Un dispositif de formation pour les cadres et personnels exposés ;
- Un code de conduite qui définit les comportements à proscrire ;
- Un régime disciplinaire permettant de sanctionner les violations du code de conduite.

L'Agence Française Anticorruption (AFA) contrôle le respect des obligations imposées par la loi Sapin II. En cas de manquement, elle peut émettre des recommandations ou saisir la commission des sanctions de la Haute Autorité pour la transparence de la vie publique (HATVP), seule habilitée à prononcer des sanctions administratives.

Le RGPD (2018)

Le Règlement Général sur la Protection des Données impose aux entreprises une Due Diligence sur leurs sous-traitants en matière de traitement des données personnelles.

Cette obligation se traduit notamment par l'évaluation préalable des garanties techniques et organisationnelles du sous-traitant, la vérification des certifications et

des codes de conduite, le contrôle des transferts de données hors UE et l'audit régulier des mesures de sécurité mises en place.

La CNIL peut sanctionner le manquement à ces obligations de Due Diligence par des amendes allant jusqu'à 4 % du chiffre d'affaires mondial.

La directive CSRD (2024)

La directive européenne sur le reporting de durabilité des entreprises (Corporate Sustainability Reporting Directive ou CSRD) a significativement renforcé les obligations de Due Diligence en matière ESG (Environnement, Social, Gouvernance).

Dans le cadre du reporting extra-financier, elle impose aux entreprises concernées une Due Diligence approfondie sur leur chaîne de valeur pour :

- Évaluer les impacts sociaux et environnementaux de leurs activités ;
- Identifier les risques de durabilité qui affectent leur business model ;
- Collecter et vérifier les données extra-financières de leurs partenaires ;
- Documenter leur conformité aux standards européens de durabilité.

La vérification des informations publiées doit être certifiée par un organisme tiers indépendant.

Les parties prenantes clés dans la mise en œuvre des Due Diligences d'entreprise

De manière générale, la conduite d'une Due Diligence approfondie sur l'ensemble de l'écosystème opérationnel d'une entreprise de grande envergure mobilise des ressources internes spécialisées, appuyées ponctuellement par des consultants externes dans les situations complexes. Ces interventions ciblées peuvent concerner la valorisation d'actifs, l'étude de marchés internationaux, l'analyse de structures juridiques peu transparentes ou encore l'examen de transactions stratégiques à fort enjeu.

Les équipes internes de l'entreprise

C'est le **département Compliance** qui pilote le processus des Due Diligences. Il conçoit les grilles d'analyse des risques, déploie les procédures d'investigation et supervise leur application systématique.

Dans les grands groupes, des équipes spécialisées en Due Diligence se constituent progressivement, à mesure que la chaîne de valeur s'allonge et que les tiers se multiplient. Séparées des équipes conformité traditionnelles, elles viennent répondre à la complexité des exigences réglementaires (à la hauteur des risques encourus).

La Direction Juridique : Elle agit sur deux leviers essentiels : l'examen des dispositifs contractuels en place et l'identification des risques juridiques. Cette démarche inclut la vérification de la régularité des titres de propriété, la présence de sûretés consenties, l'analyse des clauses relatives au changement de contrôle, entre autres. Elle intègre également une cartographie des litiges antérieurs, en cours ou susceptibles d'émerger.

La Direction Financière : Elle mobilise ses équipes d'analyse pour apprécier la robustesse financière des partenaires et contreparties. Cette évaluation couvre les indicateurs de solvabilité, la configuration de l'endettement ainsi que la qualité des actifs détenus. Elle est également en mesure de produire des simulations financières prospectives. Son savoir-faire se distingue particulièrement dans le cadre des Due Diligences liées à des opérations de fusion, d'acquisition ou de restructuration..

La Direction des Achats : Elle incorpore les exigences de Due Diligence au cœur de ses mécanismes de sélection et d'évaluation des fournisseurs. Ce dispositif prévoit une collecte continue des pièces justificatives et la mise en place d'un système d'alerte en cas de détérioration des indicateurs de performance ou de non-conformité.

La Direction des Systèmes d'Information (DSI) : Elle procède à l'analyse des environnements technologiques des tiers, en évaluant leur niveau de sécurité informatique et leur conformité aux normes en matière de protection des données. Cette vérification est particulièrement renforcée en cas d'interconnexion des systèmes d'information avec ceux de l'entreprise.

Enfin, **les équipes RSE/ESG :** Elles mènent des analyses ciblées sur les dimensions environnementales et sociales, en vérifiant notamment les certifications écologiques, les politiques sociales en vigueur et le degré d'alignement avec les engagements RSE du groupe. Cette évaluation permet d'anticiper les risques réputationnels et de conformité liés aux partenaires ou aux opérations envisagées.

Les experts externes

Le recours à des compétences externes s'impose lorsque les investigations requièrent des moyens ou des garanties que les équipes internes ne peuvent assurer seules. Cela peut résulter d'une limitation des ressources disponibles, d'un impératif d'objectivité ou de l'absence d'expertises techniques spécifiques.

Les cabinets d'audit et de conseil en stratégie Elles interviennent prioritairement dans les Due Diligences transactionnelles à forte complexité, où leur expertise se manifeste par la modélisation de scénarios financiers avancés, l'analyse d'actifs spécifiques tels que la propriété intellectuelle ou le goodwill, ainsi que l'identification des synergies opérationnelles susceptibles d'être activées après la transaction.

Les cabinets d'avocats spécialisés Elles apportent une expertise ciblée sur des enjeux juridiques complexes, tels que la conformité aux cadres réglementaires sectoriels, la structuration de dispositifs contractuels sophistiqués et l'analyse des risques inhérents aux juridictions étrangères. Leur intervention s'impose généralement dans le cadre d'opérations transfrontalières ou au sein de secteurs soumis à une régulation renforcée.

Les sociétés d'intelligence économique Elles peuvent être mobilisées ponctuellement pour approfondir certaines investigations, grâce à leur capacité à recueillir et interpréter des données sensibles ou difficilement accessibles. Cela inclut l'analyse de structures actionnariales peu transparentes, la cartographie des réseaux d'influence, l'évaluation de la réputation sur les marchés émergents, ainsi que l'identification des risques liés aux régimes de sanctions internationales.

Enfin, **les bureaux de certification et les laboratoires accrédités** Elles assurent le contrôle de la conformité technique des procédés industriels ainsi que la vérification des certifications déclarées. Leur contribution est particulièrement stratégique dans les secteurs où les exigences en matière de qualité et de sécurité sont élevées, tels que l'aéronautique, la pharmacie ou l'agroalimentaire.

Les 6 étapes à suivre pour conduire les Due Diligences

Si la profondeur des investigations s'adapte généralement aux enjeux, les 6 étapes que nous allons proposer constituent le socle méthodologique commun aux grandes entreprises.

À noter : il s'agit ici des étapes à suivre pour les Due Diligences précontractuelles, avant la signature d'un contrat avec un fournisseur.

1. Définition du périmètre et cadrage de la mission

Le département Compliance, en collaboration avec les directions concernées, établit la liste des domaines à investiguer en fonction des risques liés au tiers et au secteur d'activité. Cette phase de cadrage détermine également le niveau de profondeur des vérifications nécessaires (via une approche par les risques).

Ce premier cadrage fixe les éléments structurants de la mission : le calendrier des investigations, les ressources à mobiliser (internes et externes), les livrables attendus et les critères d'acceptabilité des risques. Il définit également les rôles et responsabilités des différentes parties prenantes ainsi que les circuits de validation.

Un document de cadrage formalise ces éléments et sert de feuille de route pour le déroulement des investigations. Il précise notamment les points d'attention liés au contexte. Prenons l'exemple d'un fournisseur de composants électroniques pour l'industrie automobile, envisagé par l'entreprise.

2. Collecte préliminaire et analyse des données publiques

Les équipes internes rassemblent et analysent systématiquement toutes les informations publiques disponibles sur le tiers envisagé. **Objectif** : déceler d'éventuels signaux d'alerte avant d'engager des ressources plus conséquentes.

Les analystes explorent les bases de données financières et commerciales (rapports annuels, notations crédit), les registres publics (greffes des tribunaux, bulletins officiels), la presse spécialisée et généraliste ainsi que les réseaux sociaux

professionnels. Ils examinent également **les listes de sanctions internationales** et les bases de données sectorielles.

Cette phase établit une première cartographie de l'écosystème du tiers : la structure de son capital, ses dirigeants, ses implantations géographiques, ses principaux clients et fournisseurs déclarés.

⚠ Point de vigilance : 5 signaux d'alerte prioritaires

Ces signaux ne constituent pas nécessairement des motifs de rejet définitif, mais ils appellent des investigations approfondies lors des phases suivantes :

1. Changements fréquents de structure juridique ou d'actionnariat ;
2. Présence dans des juridictions à risque sans justification opérationnelle claire ;
3. Divergences importantes entre les données financières publiques et sectorielles ;
4. Historique de litiges ou de défaillances dans des relations commerciales similaires ;
5. Absence inhabituelle d'information sur certains aspects critiques de l'activité (sources de financement, engagements hors bilan...).

3. Établissement de la checklist documentaire et demande formelle

Cette étape marque le premier contact formel avec le tiers. L'équipe Compliance établit la liste exhaustive des documents à collecter, calibrée selon les conclusions de l'analyse préliminaire et le niveau de risque identifié.

La demande formulée au tiers est structurée par domaines d'investigation : documents juridiques (statuts, K-bis, procès-verbaux), financiers (états financiers

certifiés, rapports d'audit), opérationnels (certifications, agréments), et ESG (rapports RSE, certifications environnementales).

Pour reprendre l'exemple de notre fournisseur de composants électroniques, une attention particulière est portée aux certifications techniques et aux autorisations d'export.

La demande documentaire est transmise via un portail sécurisé qui assure la traçabilité des échanges. Un délai de réponse raisonnable est fixé, généralement entre deux et quatre semaines selon la complexité du dossier. Les équipes définissent également les formats acceptables pour chaque document (originaux certifiés, copies conformes, etc.). Cette phase prévoit également la signature d'un accord de confidentialité (NDA) bilatéral.

4. Analyse documentaire et vérification d'authenticité

Les équipes Compliance vérifient systématiquement l'authenticité des documents officiels auprès des sources primaires : registre du commerce pour le K-bis, autorités de certification pour les normes ISO.

L'analyse croise les informations entre les différents documents pour détecter d'éventuelles incohérences. Par exemple, entre la structure capitalistique déclarée et les signataires des comptes, ou entre le périmètre des certifications et l'activité réelle.

Pour les documents financiers, les analystes examinent notamment la concordance entre les différents états et la cohérence des données dans le temps. Les équipes documentent précisément leurs conclusions dans un rapport d'analyse standardisé en notant les points qui nécessitent des clarifications ou des compléments d'information.

5. Investigations complémentaires et entretiens

Sur la base des analyses documentaires, les équipes identifient les zones qui nécessitent des investigations plus approfondies. Idéalement, cette phase doit combiner des recherches ciblées et des entretiens avec les responsables clés du tiers.

Les investigations complémentaires consistent généralement en **des visites de sites industriels**, particulièrement pertinentes dans le cas de notre fournisseur de composants électroniques. Les équipes techniques vérifient sur place la réalité des capacités de production, les processus qualité et les conditions de stockage. Les équipes HSE examinent la conformité environnementale et les conditions de travail.

En parallèle, des entretiens structurés sont menés avec les dirigeants et responsables opérationnels du tiers. Ces échanges permettent de clarifier **les points en suspens** et d'évaluer la culture de conformité de l'organisation. Pour les aspects techniques critiques, des experts métiers participent aux entretiens.

Chaque investigation fait l'objet d'un rapport détaillé enrichi de preuves photographiques pour les visites sur site et de comptes-rendus signés pour les entretiens.

6. Évaluation finale des risques et recommandations

Cette dernière étape synthétise l'ensemble des investigations pour produire une évaluation globale des risques et formuler des recommandations claires pour la décision finale.

L'équipe Compliance **consolide les données collectées dans une matrice d'évaluation standardisée**. Chaque risque identifié est qualifié selon trois dimensions : sa probabilité d'occurrence, son impact potentiel et le niveau de maîtrise démontré par le tiers. Pour notre fournisseur de composants électroniques, une

attention particulière est portée aux risques de rupture d'approvisionnement et aux enjeux de propriété intellectuelle.

Les analystes évaluent également la capacité du tiers à améliorer ses dispositifs de contrôle. Cette "dynamique de progrès" influence significativement les recommandations, particulièrement dans les domaines où des écarts ont été constatés mais sont jugés remédiables.

Le rapport final présente une recommandation claire : favorable, favorable sous conditions, ou défavorable. Dans le cas d'un avis favorable sous conditions, les mesures de remédiation requises sont précisément détaillées et priorisées.