PME et donneurs d'ordre face aux nouveaux risques : comment sécuriser sa chaîne de valeur ?

Mouvement des Entreprises de France

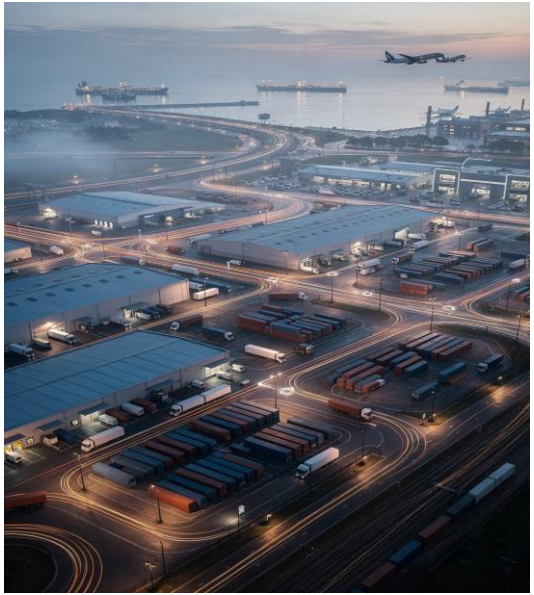
23 juin 2026

Introduction

« La chaîne de valeur est l'ensemble des activités créatrices de valeur qui permettent à une entreprise de concevoir, produire, commercialiser, livrer et soutenir ses produits ou services. »

Adapté de Michael E. Porter, Competitive Advantage, 1985

Introduction



Définition

L'ensemble des acteurs contribuant à la création de valeur : fournisseurs, sous-traitants, prestataires, partenaires technologiques, distributeurs, filiales. Une entreprise s'inscrit dans un **écosystème d'acteurs interdépendants**.

Pourquoi les PME sont concernées ?

Même sans être directement soumises aux réglementations (RGPD, NIS 2, vigilance, RSE), les PME en subissent les effets via les **exigences de leurs clients et donneurs d'ordre**.

Grandes entreprises

Risques réglementaires, financiers, administratifs et réputationnels

PME

Risque business : perte de contrat, exclusion d'appel d'offres, déréférencement

- Les grandes entreprises répercutent leurs obligations (cyber, données, durabilité, vigilance) sur leurs partenaires via des **exigences contractuelles**.

Déroulé du webinaire

1. Un environnement réglementaire en forte mutation
   Temps de questions/réponses
2. Les risques majeurs dans la chaîne des valeurs
   Temps de questions/réponses
3. La responsabilité dans la chaîne contractuelle
   Temps de questions/réponses
4. Cas pratiques de risques émergents
   Temps de questions/réponses
5. Comment se préparer concrètement
   Temps de questions/réponses

I. Un environnement réglementaire en forte mutation

1.1 Accumulation des règlementations européennes et françaises

*→ Le chef d'entreprise fait face aujourd'hui à un **empilement sans précédent de réglementations** qui interagissent entre elles*

RGPD
- RGPD (Règlement UE 2016/679) – Socle de protection pour la libre circulation de la donnée personnelle

NIS 2
- Directive NIS 2 (Directive UE 2022/2555) – Harmonisation du niveau de cybersécurité – oct. 2024 (en cours de transposition en France)

CRA
- Cyber Resilience Act (Règlement UE 2024/2847) – Sécurité des produits numériques - 2027

CSRD
- Directive UE 2022/2464 CSRD ("Corporate Sustainability Reporting Directive")

CS3D
- Directive UE 2024/1760 sur le devoir de vigilance des entreprises en matière de durabilité

Sapin II
- 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

Devoir de vigilance
- Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre

1.2 Évolution du rôle des autorités et de leur doctrine

- **Les autorités ne se contentent plus de sanctionner : elles orientent, publient des lignes directrices et attendent des entreprises une démarche proactive;**

- Passage d'une logique de sanction à une logique de supervision et d'orientation des acteurs économiques. Conséquences : développement croissant d'une doctrine de conformité (lignes directrices, recommandations, référentiels, FAQ, guides pratiques) → émergence d'un véritable « droit souple » (soft law) qui influence fortement les contrôle des autorités/agences et les pratiques des entreprises;

- Les autorités ne se contentent plus d'appliquer le droit : elles contribuent à en préciser l'interprétation opérationnelle. La conformité s'apprécie désormais à la lumière :

  - des textes législatifs et réglementaires ;
  - de la doctrine des autorités compétentes ;
  - des décisions de contrôle et de sanction
  - Conséquence : nécessité d'une veille réglementaire et doctrinale permanente
  - Enjeu pour les entreprises : anticiper les attentes du régulateur et non plus seulement respecter la lettre de la loi

- **Aujourd'hui on est obligé d'aller au delà de la loi, de s'abreuver de la doctrine des AAI;**

1.2 Évolution du rôle des autorités et de leur doctrine (Numérique)

→ CNIL & ANSSI : de l'accompagnement à la supervision

CNIL.

CNIL — Tournant répressif documenté

83 sanctions en 2025, dont 78 amendes pour **486 839 500 €** — montant inédit. 67 sanctions via procédure simplifiée ciblant TPE, PME et professions libérales. Priorités 2026 : **50 % des contrôles dédiés à la sécurité des données**.

ANSSI — Future autorité de supervision NIS 2

Audits de conformité NIS 2 prévus **3 ans après la promulgation** de la loi Résilience. Outils gratuits : **MonEspaceNIS2**, guides TPE/PME en 13 questions sur cyber.gouv.fr, alertes CERT-FR en temps réel sur cert.ssi.gouv.fr.

Point de vigilance : ne raisonnez pas avec les réflexes d'il y a 5 ans. L'argument « je suis trop petit pour être contrôlé » ne tient plus. La procédure simplifiée est précisément conçue pour traiter vite les dossiers impliquant des acteurs de taille modeste. Les PME sont dans le viseur.

1.2 Évolution du rôle des autorités et de leur doctrine (RSE)

→ *Trois autorités au cœur de la protection des marchés et de la probité des entreprises*

AMF — Autorité des Marchés Financiers

Garante de l'intégrité des marchés et de la protection de l'épargne publique.

AFA — Agence Française Anticorruption

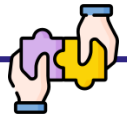
Prévention et détection des atteintes à la probité dans les organisations publiques et privées.

CNCC — Compagnie Nationale des Commissaires aux Comptes

Garante de la fiabilité et de la sincérité de l'information financière publiée

1.2 Évolution du rôle des autorités et de leur doctrine (RSE)

L'Action Conjointe contre la Corruption Privé
En 2025, l'AMF et l'AFA s'unissent face aux réseaux criminels exploitant des informations privilégiées, marquant une coopération sans précédent entre régulateurs

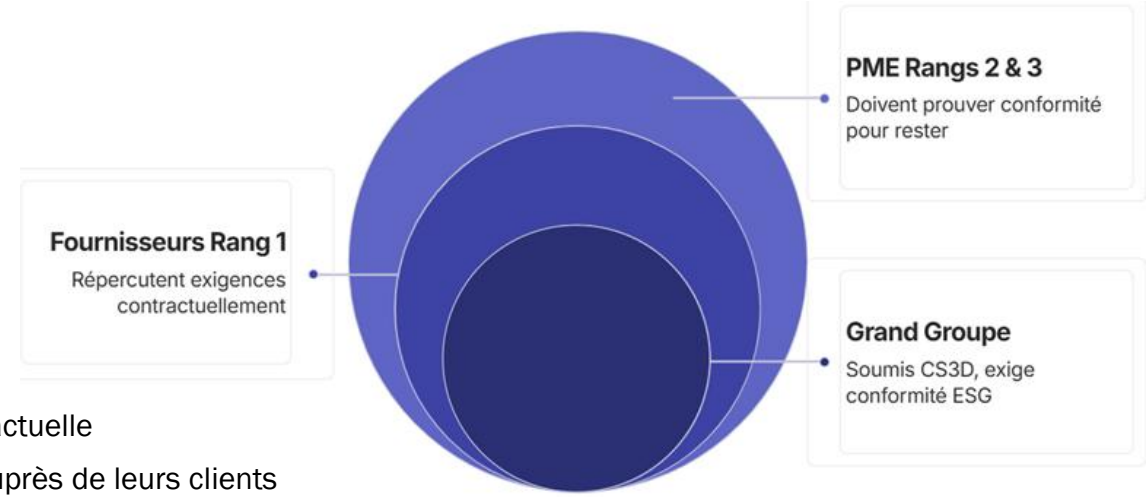


Ce que cela implique pour les entreprises

- Intégrer la **corruption privée** dans les cartographies de risques
- Renforcer les procédures de contrôle des accès aux informations sensibles
- Anticiper les zones de vulnérabilité liées aux réseaux d'initiés

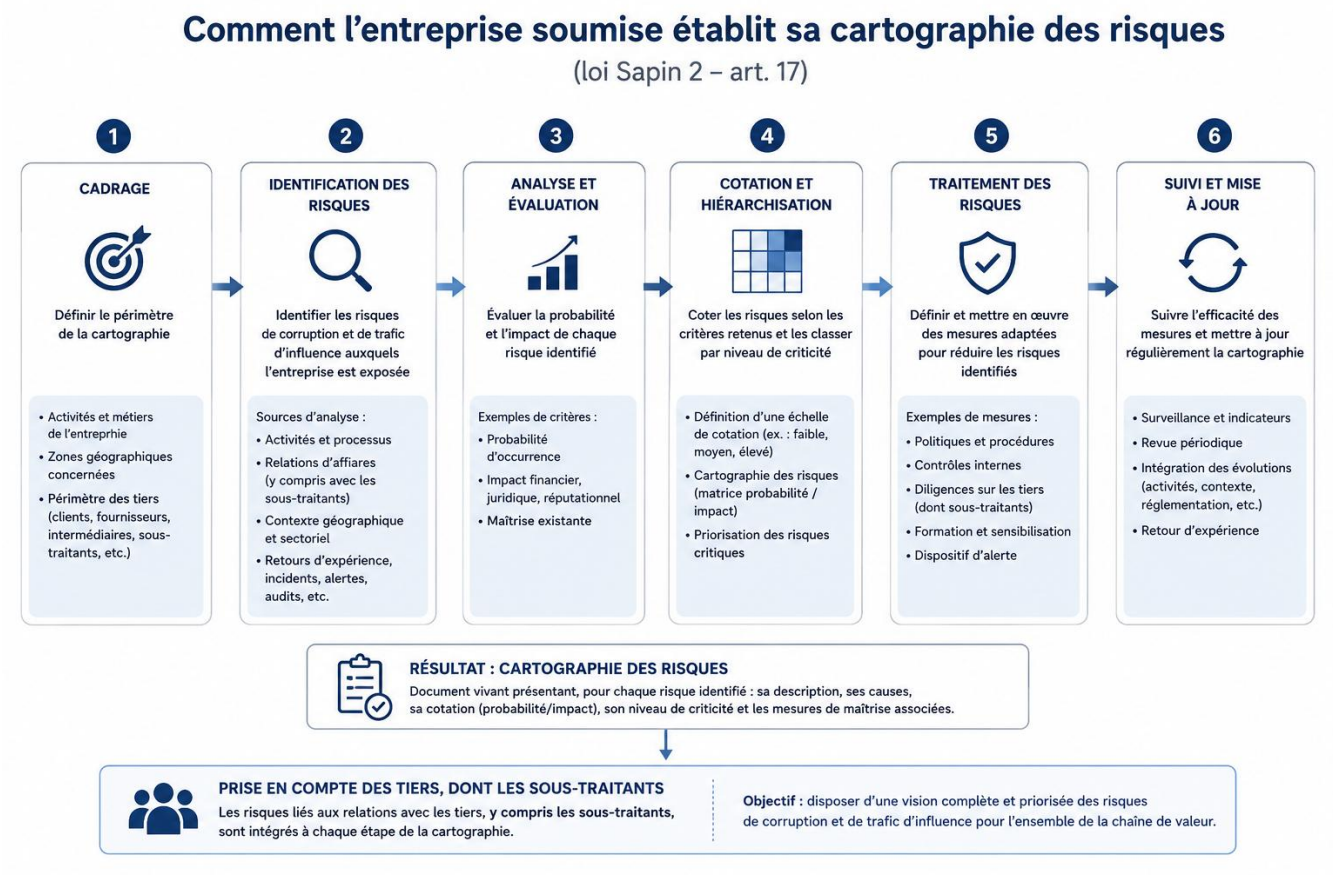
1.3 Pourquoi les PME sont désormais directement concernées (RSE)

Bien que la plupart de ces règlementations ne s'appliquent pas directement aux PME/TPE, elles ont tout intérêt à les prendre en compte car cela leur permet :



- De prendre en compte l'effet cascade contractuelle
- De se positionner de façon plus favorable auprès de leurs clients
- D'augmenter ses chances de financement
- De préserver sa réputation
- D'augmenter sa compétitivité et optimiser sa gouvernance

1.3 Pourquoi les PME sont désormais directement concernées (RSE)



1.3 Pourquoi les PME sont désormais directement concernées (Numérique)

- **Une menace cyber en constante intensification** : face à des attaquants toujours plus sophistiqués, industrialisés et capables de cibler un nombre croissant d'organisations, les systèmes d'information demeurent vulnérables, faisant de la cybersécurité un enjeu majeur de résilience économique et opérationnelle.

- **NIS 2 - un changement d'échelle de la régulation cyber européenne** : adoptée en 2022, la directive NIS 2 marque un tournant en élargissant considérablement le nombre d'entités concernées et en renforçant les exigences de cybersécurité, avec l'ambition d'élever le niveau de protection des acteurs essentiels et importants tout en consolidant la coopération européenne en matière de gestion des crises cyber.

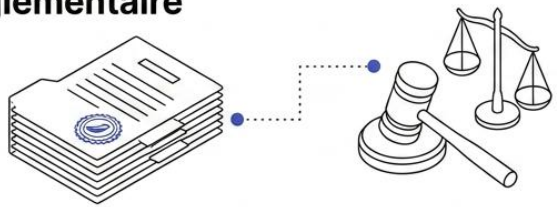
300	18K	1 366
Entités sous NIS 1	**Entités sous NIS 2**	**Incidents en 2025**
Seules 300 entités françaises étaient concernées sous l'ancienne directive.	15 000 à 18 000 entités françaises, dont une majorité de PME et ETI.	Incidents portés à la connaissance de l'ANSSI — niveau de menace qualifié d'« élevé et qui n'épargne personne ».

Même sans être directement assujetties à NIS 2, les PME sous-traitantes seront **soumises aux exigences de leurs clients régulés par voie contractuelle**. Les PME sont le maillon le moins protégé de la chaîne de valeur, et donc la cible prioritaire des attaquants souhaitant rebondir vers de plus grandes entreprises.

II. Les risques majeurs dans la chaîne des valeurs

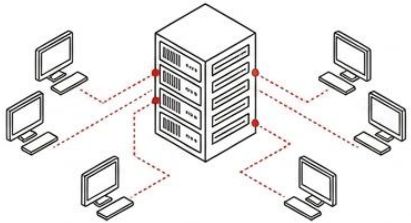
2.1 Cartographie des risques dans la chaîne de valeur

Risque de non-conformité réglementaire



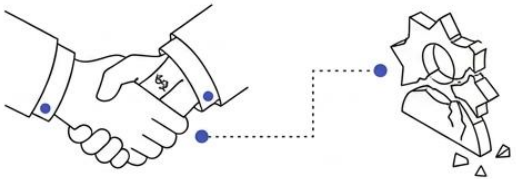
Sanctions CNIL, amendes, exclusion marchés publics.

Risque cyber



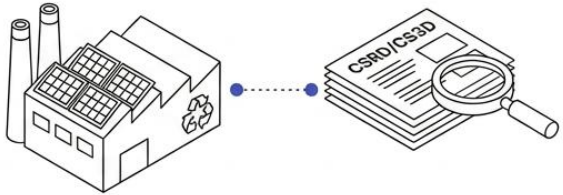
Attaques via fournisseurs, compromission des systèmes.

Risque réputationnel et commercial



Sapin II, corruption, atteinte image de marque.

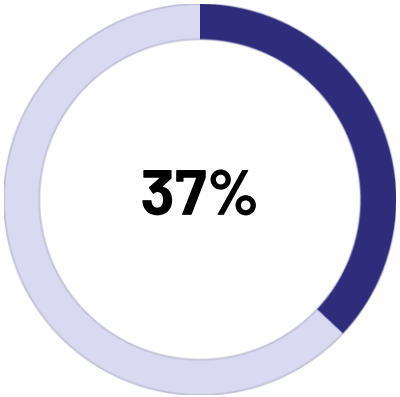
Risque ESG



Non-respect CSRD/CS3D, pression investisseurs.

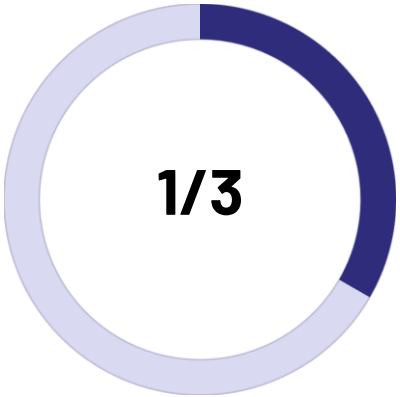
2.2 Risques cyber liés aux partenaires et fournisseurs (Numérique)

La menace cyber la plus immédiate pour une PME n'est pas toujours l'attaque frontale de ses propres systèmes. C'est la **compromission de l'un de ses partenaires ou prestataires** qui, en cascade, frappe ses propres données, ses clients, et ses engagements contractuels.



PME victimes de ransomware

Part des PME, TPE et ETI parmi les victimes de rançongiciels identifiées par l'ANSSI en 2024.



Progression structurelle

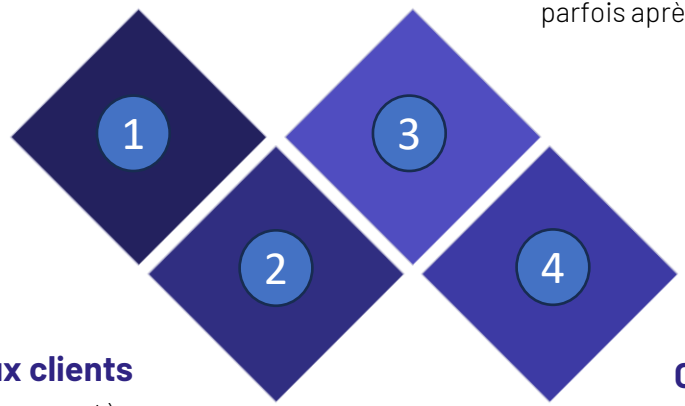
831 intrusions en 2022 → 1 112 en 2023 → 1 361 en 2024 → 1 366 en 2025. La progression est continue.

Le Panorama 2025 de l'ANSSI (CERTFR-2026-CTI-002) identifie que les **exfiltrations de données consécutives à la compromission d'un prestataire sont en augmentation significative**. Le ciblage des sous-traitants comme vecteur de compromission fait l'objet d'une section dédiée (section 3.C).

2.2 Risques cyber liés aux partenaires et fournisseurs (Numérique)

Prestataire vulnérable
L'attaquant cible un fournisseur peu protégé.

Exfiltration ou chiffrement
Données volées ou chiffrées parfois après des mois.



Accès aux clients
Accès obtenu aux systèmes des clients finaux.

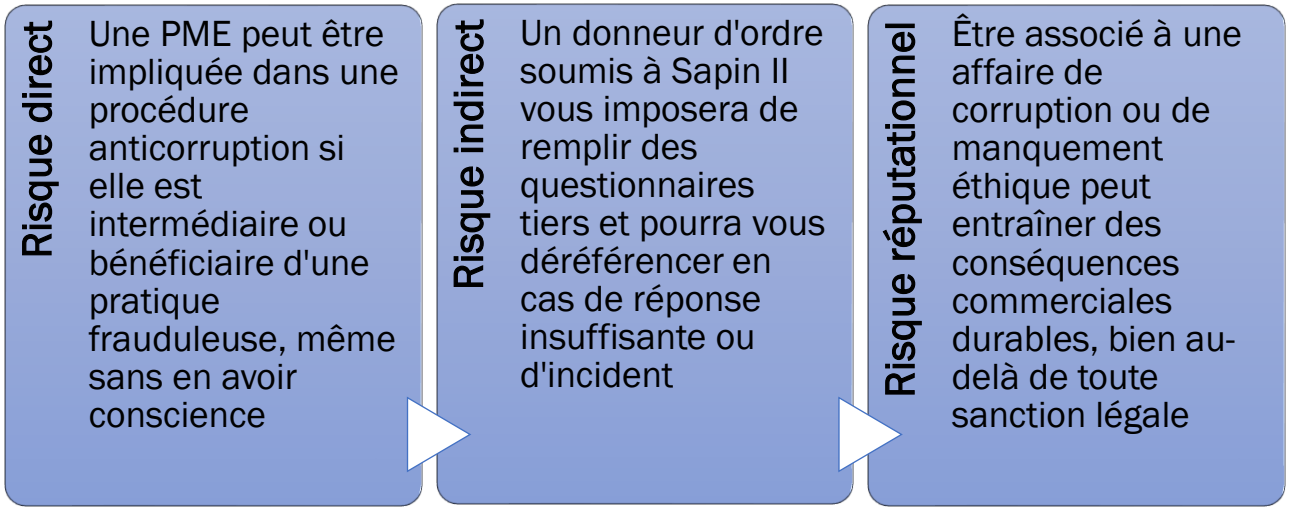
Coût pour la PME
Impact moyen 130 000–250 000 €.

Le considérant 56 de la Directive NIS 2 l'exprime sans détour : « *les petites et moyennes entreprises sont de plus en plus la cible d'attaques de la chaîne d'approvisionnement en raison de leurs mesures moins rigoureuses de gestion des risques* ». La relance complète des services peut prendre **plus de 6 semaines**.

2.3 Risques réputationnels et commerciaux (RSE)

- Différentes législations européennes et françaises représentent un risque réputationnel et donc commercial pour les entreprises :
- Prévention de la corruption (loi Sapin 2), le règlement contre le travail forcé, le règlement contre la déforestation ou encore la directive de lutte contre le greenwashing …

Un exemple avec le risque de corruption



2.3 Risques réputationnels et commerciaux (RSE)

- Les **appels d'offre publics ou privés** contiennent toujours plus de critères ESG. Ne pas anticiper ces demandes peut faire perdre des opportunités de business.

- La multiplicité des **contrôles d'audit** et donc du temps passé à préparer et répondre à ces contrôles

- La problématique de la **multiplication des labels** en matière environnementale et sociale peut être difficile à gérer et générer des coûts importants

2.3 Risques réputationnels et commerciaux (Numérique/Cyber)

La non-conformité cyber n'est pas seulement un risque réglementaire. C'est un **risque commercial direct et croissant**, qui se manifeste dans les relations avec les donneurs d'ordre, les assureurs, les banques et les partenaires.

Exclusion des chaînes d'approvisionnement

NIS 2 oblige les entités essentielles à **évaluer et documenter le niveau de sécurité de leurs prestataires**. Ne pas pouvoir répondre à un questionnaire de maturité cyber, c'est ne pas être sélectionné. Les acheteurs publics intègrent des clauses cyber dans leurs marchés.

Impact sur la cyber-assurance

Les assureurs exigent désormais : **MFA obligatoire**, politique de sauvegardes documentée et testée, plan de réponse à incident formalisé. **60 % des PME victimes** n'ayant pas anticipé ces exigences se retrouvent sans couverture après sinistre.

III. La responsabilité dans la chaîne contractuelle

3.1 La responsabilité dans la chaîne contractuelle

- Les réglementations fixent des obligations — mais c'est le contrat qui en détermine les modalités pratiques. La liberté contractuelle permet aux parties d'adapter les grandes règles sans y déroger :
  - Périmètre;
  - Fréquence;
  - Coût;
  - procédure contradictoire;
  - sanctions.
- Le contrat est à la fois un instrument de conformité et le terrain de la négociation où se joue la répartition des risques entre donneurs d'ordre et fournisseurs. C'est là que les PME doivent être mieux préparées.

3.2 Exemple : l'article 28 du RGPD – la colonne vertébrale de la sous-traitance data

L'article 28 impose une **formalisation obligatoire** de toute relation de sous-traitance impliquant des données personnelles via un accord sur les données à caractères personnelles également connu en anglais sous le nom de "*Data Processing Agreement* (DPA), signé avant tout traitement et qui se joint en annexe du contrat.

Contenu obligatoire du DPA

Objet, durée, nature et finalité du traitement, types de données, instructions documentées, confidentialité, sécurité, sous-traitance ultérieure, droits des personnes, restitution des données, coopération aux audits.

Responsabilité en cascade

Le sous-traitant initial doit obtenir l'autorisation écrite préalable avant tout recours à un sous-traitant ultérieur. En cas de défaillance de ce dernier, **le sous-traitant initial demeure pleinement responsable.**

En pratique

Chaque outil SaaS (CRM, RH, comptabilité cloud), chaque externalisation impliquant des données personnelles nécessite un DPA. Son absence expose les deux parties et est **sanctionnée directement par la CNIL** (bilan 2025).

3.2 Exemple : l’article 28 du RGPD – la colonne vertébrale de la sous-traitance data

- Le DPA doit être signé avant tout traitement de données personnelles. C'est une condition sine qua non de la conformité RGPD, pas une formalité administrative à régler a posteriori. En pratique :
  - Chaque outil SaaS que vous utilisez pour traiter des données de vos clients ou employés (CRM, RH, messagerie, comptabilité cloud) implique un DPA avec son éditeur.
  - Si vous externalisez des tâches impliquant des données personnelles (gestion des paies, maintenance informatique avec accès au réseau), vous devez signer un DPA avec ce prestataire.
  - Si vous êtes prestataire, votre client doit vous imposer un DPA. Son absence expose les deux parties.
  - L'absence de DPA est sanctionnée directement par la CNIL, comme le confirme le bilan 2025.

Source : Article 28 RGPD ; CNIL, modèle de DPA disponible sur cnil.fr ; CNIL, bilan 2025

3.2 Exemple : l'article 21 de NIS 2 – la sécurité de la chaîne d'approvisionnement

Niveau de sécurité minimum
MFA, sauvegardes, chiffrement, gestion des accès — par référence à ISO 27001 ou au référentiel ANSSI.

Clause d'audit
Droit de réaliser un audit de sécurité. Le refus ou l'obstruction constitue une violation directe (art. 28§3h RGPD).

Notification d'incident
Délai contractuel de 24 à 48 heures, aligné sur NIS 2 et RGPD. Tout retard engage la responsabilité du prestataire.

Clause pénale
Pénalités financières si un incident cyber chez le prestataire cause un préjudice démontrable au client.

Mesure obligatoire (art. 21)	Description	Impact PME sous-traitante
Gestion des risques	Analyse et cartographie des risques cyber	Doit pouvoir produire sa propre analyse
Sécurité chaîne appro (21§2d)	Évaluation des fournisseurs et prestataires TIC	Sera évaluée par son client régulé NIS2
Notification d'incident (art. 23)	Alerte précoce sous 24h, rapport sous 72h	Doit prévoir une procédure de notification
Continuité d'activité	PCA/PRA documenté et testé	Exigence contractuelle fréquente
Formation et sensibilisation	Programme de formation des collaborateurs	Critère de questionnaire fournisseur
Authentification renforcée	MFA sur les accès critiques	Condition sine qua non des contrats clients

Source : Directive (UE) 2022/2555, article 21 et article 23 — eur-lex.europa.eu

3.3 La clause d’audit : l’instrument principal du contrôle

- Les clauses d'audit peuvent couvrir des **périmètres très différents selon le texte applicable et la relation commerciale**. Un même contrat peut faire l'objet de plusieurs types d'audit simultanés, créant un risque de "**fatigue d'audit**".
- Il est dans l'intérêt des deux parties de **regrouper** et **rationaliser** les vérifications.
- **L'erreur la plus fréquente est de traiter la clause d'audit comme une clause standard copiée-collée**. La portée et l'équilibre de la clause doivent être calibrés en fonction de la nature de la relation, du type de risque couvert et de la taille respective des parties.

Audit cybersécurité

Vérification des mesures techniques : MFA, chiffrement, gestion des accès, tests d'intrusion.

Audit RGPD / données

Conformité des traitements, existence du DPA, droits des personnes, registre des traitements.

Audit RSE / CS3D

Conformité sociale, environnementale et déontologique dans la chaîne de valeur.

3.3 La clause d'audit : en position défensive – points à négocier

- **Le donneur d'ordre vous impose une clause d'audit souvent rédigée de façon très large, reflétant ses propres obligations légales sans adaptations à votre réalité :**

Périmètre

Limiter l'audit aux données et systèmes traités dans le cadre du contrat. Toute clause prévoyant un accès illimité est excessive et doit être réduite.

Fréquence

Exiger un plafond : une fois par an hors incident, deux fois maximum en cas de crise justifiée. Le CIGREF préconise de "limiter le nombre d'audits".

Préavis

Minimum 10 à 15 jours ouvrés, sauf incident grave dûment établi. Principe reconnu par la pratique contractuelle (LawInsider).

Coût

En droit français, les audits sont à la charge du commanditaire, sauf si l'audit révèle une faute directe du prestataire.

Confidentialité

Les informations communiquées sont couvertes par le secret des affaires (Directive UE 2016/943, loi n° 2018-670). Obligation stricte pesant sur l'auditeur mandaté.

Procédure contradictoire

Aucune décision (pénalités, résiliation, plan correctif) ne peut être prise sans transmission du rapport provisoire, délai de réponse et réunion de clôture.

3.3 La clause d'audit : pour auditer vos fournisseurs – points à intégrer

- **Une clause d'audit absente ou mal rédigée peut vous empêcher de démontrer votre conformité en cas de contrôle RGPD, NIS 2 ou devoir de vigilance. Il faut donc :**

- **Définir précisément l'objet par type de risque :**
  - Données personnelles, cyber, RSE, conformité sociale : chaque périmètre doit être distinct et ne pas glisser vers un autre sans accord des parties;
- **Mandater un auditeur tiers indépendant :**
  - Prestataire PASSI labellisé ANSSI pour la cyber, OTI accrédité COFRAC pour les audits RSE/CSRD. Prévoir les conditions d'approbation par le fournisseur;
- **Articuler audit et questionnaire fournisseur :**
  - Un questionnaire documentaire peut suffire en première approche, l'audit sur site;
- **Prévoir des suites contractuelles appropriées :**
  - Plan de remédiation/ plan correctif, suspension de certaines prestations, résiliation pour faute grave. Eviter les clauses de résiliation automatique disproportionnées;
- **Etendre le droit d'audit à la sous-traitance en cascade :**
  - Si le fournisseur sous-traite lui-même, le droit d'audit doit s'étendre aux sous-traitants de second rang, au moins les prestations à risque élevé (données sensibles, accès critiques).

IV. Cas pratiques de risques émergents

4.1) Reporting ESG demandé aux sous-traitants

Deux exemples récents en matière de devoir de vigilance et de corruption

La maison mère d'Yves Rocher condamnée pour manquement à son devoir de vigilance au sein d'une filiale turque

L'affaire remonte à une vague de licenciements lancée en 2018 par Kosan Kozmetik, filiale turque du groupe Rocher jusqu'en 2024, après l'arrivée du syndicat Petrol-Is dans l'usine, auquel de nombreux salariés avaient adhéré, avant d'être remerciés.

SOCIÉTÉ • ENTREPRISES

Paprec paie 17,5 millions d'euros pour sortir d'une procédure mêlant soupçons de corruption, d'entente et de favoritisme

Le groupe de collecte et traitement de déchets a obtenu une convention judiciaire éteignant les poursuites contre lui dans un dossier de corruption et de favoritisme, dont l'enquête se poursuit.

4.2) Risques émergents : l'IA comme nouveau vecteur de risque cyber

Le **Panorama de la cybermenace 2025 de l'ANSSI** (CERTFR-2026-CTI-002) consacre une section entière (2.A et 2.B) à l'évolution de l'outillage des attaquants, incluant l'utilisation croissante des capacités issues de l'intelligence artificielle. Sans parler de révolution, l'ANSSI note un **intérêt marqué des attaquants pour les outils d'IA**, notamment pour diversifier les techniques d'ingénierie sociale.

Menaces IA identifiées par l'ANSSI

Phishing personnalisé

L'IA générative permet de créer des courriels de phishing **sans fautes d'orthographe**, ciblés, connaissant votre nom, secteur, dirigeant et partenaires — beaucoup plus convaincants que les attaques précédentes.

Ingénierie sociale avancée

Usurpation d'identité vocale (**deepfake audio**), faux appels de dirigeants, faux services d'assistance informatique. La frontière entre humain et machine devient de plus en plus floue.

Vulnérabilités dans le code

Les outils d'IA (copilotes de code, automatisation) peuvent **introduire des vulnérabilités** si les développeurs ne vérifient pas la qualité sécuritaire des suggestions générées.

Risque prioritaire pour les PME

⚠ Le risque immédiat pour les PME est principalement le **phishing amélioré par IA** : un email ciblé qui connaît votre nom, votre secteur, le nom de votre dirigeant, vos partenaires — et qui vous demande de cliquer ou de transférer de l'argent.

Cadre réglementaire : AI Act (UE 2024/1689)

Le règlement IA européen, progressivement applicable depuis 2024, impose plusieurs obligations :

- **Transparence** sur les systèmes d'IA utilisés dans des contextes à risque
- **Interdictions** de certains usages : manipulation comportementale, notation sociale
- **Évaluations de conformité** obligatoires pour les systèmes à haut risque
- Les entreprises déployant des solutions d'IA doivent **vérifier leur conformité** à ce règlement

V. Comment se préparer concrètement

5.1) Prioriser ses risques

- Toutes les PME ne sont pas exposées de la même façon. La première étape est de cartographier ses risques spécifiques en fonction de son secteur, de sa taille, de ses donneurs d'ordre et de ses propres sous-traitants.

Inutile de vouloir tout traiter à la fois : commencez par **les risques les plus probables et les plus impactants.**

5.1) Prioriser ses risques – conseils pratiques

Cartographier

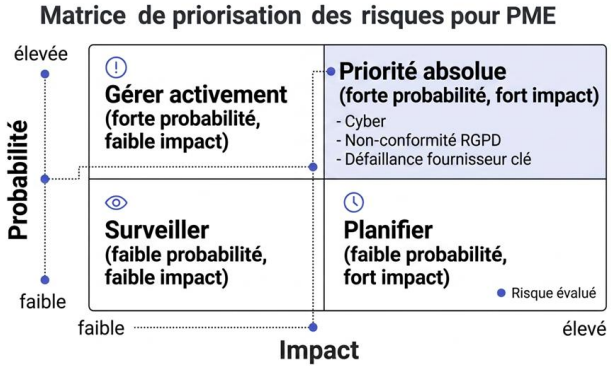
- Analyser votre activité;
- Analyser votre chaîne de valeur;
- Vérifier votre assujettissement aux textes règlementaires;

Evaluer

- Travailler par catégorie de risque (environnementaux, sociaux, gouvernance, flux de données, cyber);
- Estimer la probabilité et l'impact de chaque risque et **ne pas vouloir tout traiter à la fois;**
- Poser un diagnostic de conformité;

Impliquer les équipes

- Les équipes achats, RH, finances doivent être consultés
- Documenter chaque action : la traçabilité est indispensable



Les risques ESG et Cyber ne sont pas l'affaire d'un seul département

5.2) Mettre en place des processus simples de conformité à travers la comitologie

L'article 20 de NIS 2 est explicite : les organes de direction doivent **approuver les mesures de gestion des risques et superviser leur mise en œuvre**. Ils peuvent être tenus personnellement responsables des manquements.

Désigner un référent cyber

Pas nécessairement un expert interne — ce rôle peut être externalisé (prestataire MSSP). Il fait le lien entre la direction, les prestataires et les alertes ANSSI/CERT-FR.

Inscrire la cyber à l'agenda

Présentation semestrielle du niveau de risque, des incidents survenus et des investissements. Cette documentation est un élément de preuve en cas de contrôle.

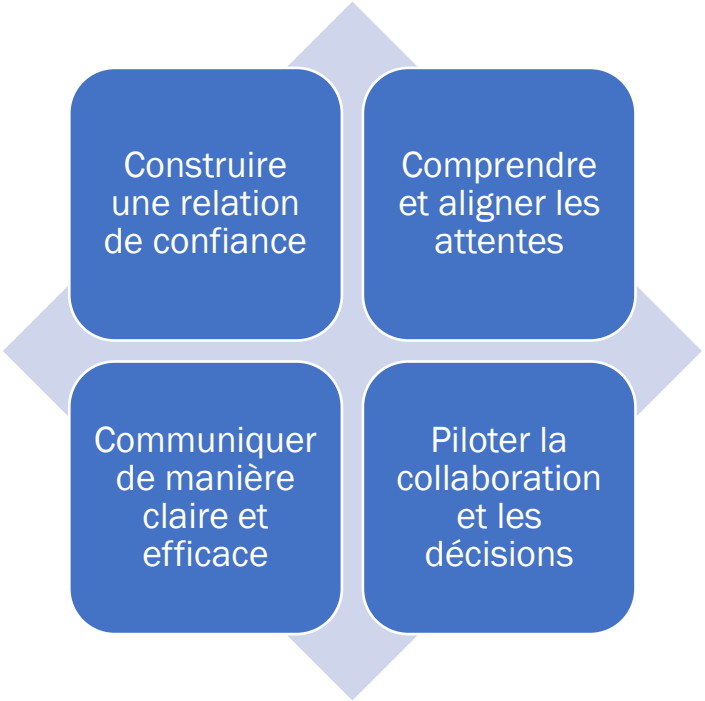
Processus de gestion des incidents

Qui notifie la CNIL (72h) ? Qui notifie l'ANSSI (24h) ? Qui prévient les clients ? Ces chaînes de décision doivent être écrites, affichées et testées **avant l'incident**.

Former les collaborateurs

Le vecteur numéro un reste le phishing. Une simulation annuelle et une formation aux réflexes de base sont des investissements à très fort rendement.

5.3) Dialoguer efficacement avec ses donneurs d'ordre et ses parties prenantes



Deux principes clés :

- Écouter pour comprendre avant d'agir
- Communiquer avec clarté et transparence

5.3) Dialoguer efficacement avec ses donneurs d'ordre et ses parties prenantes

ANTICIPER PLUTÔT QUE SUBIR

- **Préparer une fiche de synthèse de votre posture numérique et RSE** : mesures de cybersécurité en place, certifications éventuelles (ISO 27001, SecNumCloud pour les hébergeurs), dernière date de sensibilisation des équipes, mais également engagements RSE, politique éthique ou environnementale et éventuels labels obtenus.
- **Formaliser ce que vous faites déjà mais n'avez pas documenté** : politique de sauvegarde, procédure de gestion des accès, charte informatique, mais aussi charte éthique, politique achats responsables ou engagements sociaux. Si vous le faites mais ne le documentez pas, vous ne pouvez pas le prouver.
- **Vérifier que vous avez signé un DPA avec tous vos prestataires traitant des données personnelles pour votre compte** — et que vous avez votre propre DPA prêt pour vos clients — tout en vous assurant d'être en mesure de répondre aux demandes de vos donneurs d'ordre en matière de reporting ou d'engagements RSE.

NEGOCIER LES CLAUSES CONTRACTUELLES

- **Obligation de résultat vs. obligation de moyens :** qu'il s'agisse de cybersécurité ou d'engagements RSE, une obligation de résultat est rarement tenable. Privilégiez une obligation de moyens renforcée fondée sur des mesures documentées et une démarche d'amélioration continue.
- **Délai de notification d'incident :** un délai de 4 heures est difficilement tenable le week-end ou la nuit. Négociez un délai réaliste, y compris lorsque l'obligation concerne un incident susceptible d'affecter vos engagements de conformité ou de durabilité.
- **Droit d'audit illimité :** limitez la fréquence (une fois par an sauf incident), le périmètre (activités couvertes par le contrat uniquement) et les conditions de prévenance. Cette vigilance vaut aussi bien pour les audits cyber que pour les audits RSE.
- **Clause de responsabilité illimitée :** exigez un plafond de responsabilité contractuelle adapté à la taille de votre entreprise et aux risques réellement assumés, qu'ils concernent la sécurité numérique, les données personnelles ou les engagements RSE.

5.4) Partage de bonnes pratiques : un levier collectif de maîtrise des risques

- La maîtrise des risques ne repose pas uniquement sur des procédures : elle se construit aussi grâce au partage des expériences, à l'apprentissage collectif et à l'amélioration continue.
- Ressources pour structurer votre démarche
  - Groupements professionnels sectoriels : mutualisation des outils et retours d'expérience entre PME de même secteur
  - Guides thématiques :

Guide pratique anticorruption à destination des PME et des petites ETI

Les guides de la BPI en matière de RSE pour les PME et ETI : https://www.bpifrance.fr/nos-solutions-rse

5.5) Identification des bons prestataires pour accompagner les entreprises

L'importance de se faire accompagner :

De nombreux prestataires peuvent vous accompagner :

- Agences RSE et consultants ESG;
- Accompagnement CSRD, bilan carbone, réponse aux questionnaires EcoVadis et autres labellisations;
- Cabinets juridiques spécialisés : faites relire toute clause par un avocat spécialisé dans les récentes règlementations avant signature. Une clause mal négociée peut engager votre responsabilité pour un montant sans commune mesure avec la valeur du contrat;

ANNEXE

Tableau de synthèse réglementaire &
Ressources clés

Tableau de synthèse réglementaire

Ce tableau récapitule les textes applicables, leurs obligations clés pour les PME, les autorités compétentes, les sanctions encourues et les références officielles.

Texte	Obligations clés PME	Autorité	Sanctions max.	Référence
RGPD (UE 2016/679)	DPA (art. 28), sécurité (art. 32), notification violation 72h (art. 33)	CNIL	20 M€ ou 4 % CA mondial	eur-lex.europa.eu
NIS 2 (UE 2022/2555)	Gestion risques (art. 21), sécurité chaîne appro, notif. incident 24h/72h (art. 23)	ANSSI	10 M€ ou 2 % CA (EE)	eur-lex.europa.eu / monespacenis2
DORA (UE 2022/2554)	Résilience TIC, gestion risques tiers, tests TLPT (impact indirect)	ACPR/AMF	Selon entité	eur-lex.europa.eu
CRA (UE 2024/2847)	Sécurité produits numériques par conception, notif. vulnérabilités 24h	ANSSI/ENISA	À définir en droit FR	eur-lex.europa.eu
Loi Sapin II (art. 17)	Cartographie risques tiers, programme anti-corruption	AFA	200 K€ pers. / 1 M€ org.	légifrance.gouv.fr
CSRD (UE 2022/2464)	Reporting ESG incluant gouvernance cyber (ESRS G, S4)	AMF/OTI	À définir	eur-lex.europa.eu
LFI — Art. 311-1 CP	Sanctions pénales vol/fraude informatique (STAD — art. 323-1 CP)	Parquet	3 à 7 ans / 300K€	légifrance.gouv.fr

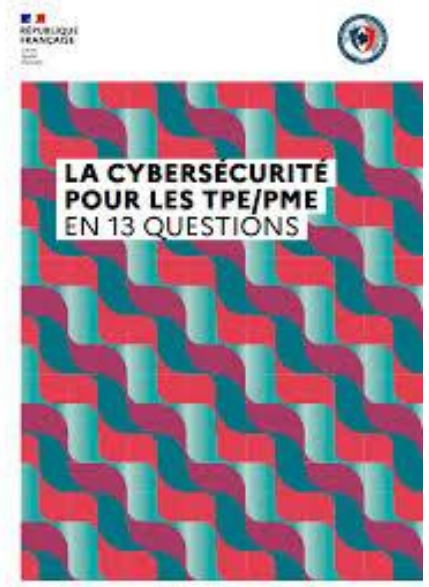
Ressources clés

Organisme / Ressource	Lien / Contact
ANSSI — Agence Nationale de la Sécurité des SI	ssi.gouv.fr / cyber.gouv.fr
CERT-FR — Alertes et bulletins	cert.ssi.gouv.fr
MonEspaceNIS2 — Vérifier son assujettissement	monespacenis2.cyber.gouv.fr
Cybermalveillance.gouv.fr — Aide aux victimes	cybermalveillance.gouv.fr
CNIL — Autorité de protection des données	cnil.fr
Notification violation CNIL	notifications.cnil.fr
Portail RSE — Obligations extra-financières	portail-rse.fr
EUR-Lex — Textes européens officiels	eur-lex.europa.eu
Légifrance — Textes français officiels	legifrance.gouv.fr

Ressources clés

ANSSI - La cybersécurité pour les TPE/PME en treize questions

18 février 2021



AFA - Guide pratique anticorruption à destination des PME et des petites ETI

Accompagnement

16 décembre 2021