TPSA

THIRD-PARTY SUPPLIER ACCOUNTABILITY

DOCUMENT DE POSITION

TPSA

Responsabilité des fournisseurs tiers

Un cadre pour une responsabilité normalisée en matière de sécurité
Entre les fournisseurs et leurs clients

Version 1.0, avril 2026

Auteur : Sébastien Poitrasson, Arthur Koenig Conseil

AK ARTHURKOENIG

Résumé exécutif

La dépendance croissante à l'égard des fournisseurs tiers pour les services informatiques critiques a créé une vulnérabilité systémique que les cadres de sécurité actuels ne parviennent pas à traiter adéquatement. Si des normes telles que CIS Controls v8, ISO/IEC 27001:2022 et des cadres réglementaires comme DORA et NIS2 reconnaissent l'importance de la sécurité de la chaîne d'approvisionnement, ils l'abordent exclusivement du point de vue du client : évaluer ses fournisseurs, gérer les risques liés aux tiers, vérifier leur niveau de sécurité.

Cette approche unilatérale présente une lacune fondamentale. Les fournisseurs sont évalués, interrogés et audités, mais aucun mécanisme standardisé ne permet de les **responsabiliser** de manière structurée, transparente et vérifiable. Les clients envoient des questionnaires de sécurité personnalisés ; les fournisseurs répondent par des assurances génériques. L'asymétrie d'information persiste et le niveau de sécurité réel de la chaîne d'approvisionnement demeure opaque.

Le cadre **de responsabilité des fournisseurs tiers (TPSA)** vise à combler cette lacune en créant un protocole bidirectionnel standardisé pour la transparence en matière de sécurité entre les fournisseurs et leurs clients. Plutôt que d'imposer des contraintes supplémentaires aux fournisseurs, le TPSA leur confère un **avantage concurrentiel** : un label qui atteste de leur responsabilité, simplifie les vérifications préalables à la clientèle et facilite la conformité réglementaire aux normes DORA, NIS2 et ISO 27001.

TPSA ne remplace pas les cadres existants. Il s'agit d'une **spécification complémentaire** conçue pour opérationnaliser les exigences de sécurité des tiers déjà imposées par ces normes, en établissant le lien manquant entre les obligations de gestion des risques du client et la transparence de la sécurité du fournisseur.

1. Le problème : un déficit de responsabilité en matière de sécurité des tiers

1.1 L’ampleur de la menace

Les attaques ciblant la chaîne d'approvisionnement sont devenues le vecteur privilégié des acteurs malveillants les plus sophistiqués. Plutôt que d'attaquer directement des organisations bien protégées, les adversaires ciblent leurs fournisseurs, exploitant les relations de confiance, les infrastructures partagées et les privilèges d'accès qui caractérisent les chaînes d'approvisionnement numériques modernes.

Le rapport Axa XL/Thales « Résilience à grande échelle », publié le 2 avril 2026, confirme que le risque cybernétique n’est plus une menace isolée, mais un phénomène systémique qui s’étend bien au-delà du périmètre de l’entreprise. En 2025, plus de 12 000 violations de données ont été recensées dans le monde, pour un coût moyen de 4,44 millions de dollars par incident. L’ENISA et la CISA signalent une augmentation de 47 % des incidents liés à la chaîne d’approvisionnement en 2025, une tendance qui devrait se poursuivre en 2026.

Les incidents retentissants continuent de démontrer l'effet domino : un seul fournisseur compromis peut paralyser des milliers d'organisations. Le problème fondamental n'est pas le manque de contrôles de sécurité, mais le manque **de visibilité et de responsabilisation** des tiers dont les organisations dépendent.

1.2 Le contexte actuel : une évaluation sans responsabilisation

Les cadres et outils existants abordent le risque lié aux tiers du point de vue du client :

- **CIS Controls v8, Safeguard 15** (Gestion des fournisseurs de services) : exige que les organisations évaluent et surveillent leurs fournisseurs de services, mais ne définit pas ce que le fournisseur doit divulguer ni comment.
- **ISO/IEC 27001:2022, Annexe A.5.19–5.23** : impose des politiques de sécurité des fournisseurs, une surveillance et une gestion des changements, mais ne définit pas le format, la profondeur et le mécanisme de la communication avec les fournisseurs.
- **DORA (Règlement 2022/2554), Articles 28-30** : impose des exigences détaillées en matière de gestion des risques liés aux TIC pour les entités financières, y compris des dispositions contractuelles, mais ne normalise pas le format de réponse du fournisseur.
- **Directive NIS2, article 21(2)(d)** : exige des mesures de sécurité de la chaîne d'approvisionnement, mais ne fournit aucun cadre opérationnel pour la responsabilité des fournisseurs.
- **SIG (Standardized Information Gathering), CAIQ (CSA)** : outils d'évaluation basés sur des questionnaires qui reposent sur l'autodéclaration du fournisseur sans vérification standardisée ni dialogue continu.
- **SOC 2** : basé sur un audit, périodique, confidentiel et axé sur les contrôles généraux du fournisseur, et non sur les actifs, les données ou les risques spécifiques pertinents pour un client donné.

Il en résulte un paysage fragmenté où les clients investissent des efforts considérables dans des évaluations sur mesure, les fournisseurs répondent à des dizaines de questionnaires différents aux formats variés, et la situation réelle en matière de sécurité de la chaîne d'approvisionnement reste mal comprise par les deux parties.

1.3 La pièce manquante : une responsabilité structurée et bidirectionnelle

Ce qui manque, ce n'est pas un nouvel outil d'évaluation, mais un **protocole de responsabilisation standardisé** qui :

1. Définit les informations que les fournisseurs doivent divulguer, sous quel format et avec quel niveau de détail.
2. Crée un canal bidirectionnel permettant aux clients de soumettre des scénarios de risque pertinents pour leur propre contexte, et auquel les fournisseurs doivent répondre formellement.
3. Elle correspond directement aux exigences réglementaires existantes, de sorte que son adoption génère une valeur de conformité immédiate pour les deux parties.
4. Fournit un label reconnaissable que les fournisseurs peuvent utiliser comme facteur de différenciation concurrentielle.

2. Le cadre TPSA : architecture et composants

Le cadre de responsabilisation des fournisseurs tiers se compose de quatre éléments interdépendants, chacun abordant une dimension spécifique du déficit de responsabilisation.

Composant	Nom	But
TPSA-01	Norme de divulgation des fournisseurs	Définit le format standardisé et le contenu obligatoire de la fiche de déclaration du fournisseur.
TPSA-02	Protocole de dialogue sur les risques	Formalise l'échange bidirectionnel de scénarios de risques entre clients et fournisseurs, en tirant parti d'EBIOS RM et de MITRE ATT&CK.
TPSA-03	Matrice de cartographie réglementaire	Associe chaque exigence TPSA aux contrôles CIS v8, ISO 27001:2022, DORA et NIS2.
TPSA-04	Étiquetage et certification	Définit les niveaux de maturité, les critères de certification et le processus d'audit pour l'étiquetage TPSA.

2.1 TPSA-01 : Norme de divulgation des fournisseurs

La fiche de divulgation du fournisseur est le document fondamental du cadre TPSA. Il s'agit d'une déclaration structurée et lisible par machine, publiée par le fournisseur, contenant les informations dont les clients ont besoin pour évaluer et contrôler la sécurité des services qui leur sont fournis.

Domaines de divulgation obligatoire

La fiche de déclaration couvre les domaines suivants, chacun contenant un ensemble défini de champs obligatoires et facultatifs :

- **Inventaire des actifs** : identification précise de tous les actifs (infrastructures, plateformes, applications, bases de données) qui traitent, stockent ou transmettent des données client. Cela inclut la classification des actifs, leur emplacement (géographique et logique) et leur statut (partagé/dédié).
- **Mesures de protection des données** : chiffrement au repos et en transit, pratiques de gestion des clés, mécanismes de ségrégation des données pour les environnements multilocataires et politiques de conservation/suppression des données.
- **Sauvegarde et restauration** : fréquence des sauvegardes, étendue, périodes de conservation, objectifs de temps de récupération (RTO) et objectifs de point de récupération (RPO) testés, et, surtout, la date et le résultat du dernier test de restauration de sauvegarde.
- **Contrôle d'accès** : mécanismes d'authentification, gestion des accès privilégiés, fréquence de révision des accès et contrôles d'accès orientés client (API, portails, consoles d'administration).

- **Gestion des vulnérabilités** : politique de gestion des correctifs et SLA, fréquence des analyses de vulnérabilité, calendrier des tests d'intrusion avec dates et portée du test le plus récent, et délais de correction.
- **Gestion des incidents** : capacités de détection des incidents, procédures et délais de notification (alignés sur les exigences de l'article 19 de la DORA le cas échéant), voies d'escalade et processus d'examen post-incident.
- **État de la certification et de la conformité** : certifications actuelles (ISO 27001, SOC 2, etc.), étendue de la certification, dates de validité et lacunes ou exclusions connues.

Informations partagées vs. informations spécifiques au client

Pour les fournisseurs exploitant des environnements multi-locataires, la fiche de divulgation est structurée en deux niveaux : une **divulgation commune** couvrant l'infrastructure partagée et les contrôles applicables à tous les clients, et une **annexe spécifique au client** détaillant les actifs particuliers, la classification des données et les mesures adaptées à chaque relation client individuelle.

Cette approche à deux niveaux minimise les obligations de divulgation pour le fournisseur tout en offrant à chaque client la transparence spécifique dont il a besoin.

2.2 TPSA-02 : Protocole de dialogue sur les risques

Le protocole de dialogue sur les risques est l'élément le plus novateur du cadre TPSA. Il établit un **canal formalisé et bidirectionnel** permettant aux clients et aux fournisseurs d'échanger des informations relatives aux risques dans un format structuré.

Le problème qu'il résout

Aujourd'hui, un client qui identifie une menace spécifique pesant sur son organisation ne dispose d'aucun moyen standardisé d'interroger son fournisseur : « Comment vos mesures de contrôle permettent-elles de contrer cette menace ? » L'analyse des risques du client et la politique de sécurité du fournisseur sont cloisonnées. Une banque qui identifie un groupe APT ciblant le secteur financier ne peut pas demander formellement à son fournisseur de services cloud d'évaluer la pertinence de cette menace pour les actifs spécifiques hébergeant ses données.

Le protocole de dialogue sur les risques résout ce problème en définissant un mécanisme d'échange structuré, fondé sur deux méthodologies établies :

Intégration EBIOS RM

Le protocole s'appuie sur la méthodologie EBIOS Risk Manager (publiée par l'ANSSI) comme cadre structurel du dialogue sur les risques :

- **Atelier 1 (Portée et contexte)** : largement prérempli par la fiche de divulgation du fournisseur (TPSA-01). Les actifs, les valeurs commerciales et le référentiel de sécurité sont déjà documentés.
- **Atelier 2 (Sources de risques)** : le client identifie ses sources de risques et ses objectifs de menace spécifiques (paires SR/OV) et les soumet au fournisseur via le protocole de dialogue sur les risques. Il se peut que le fournisseur n’ait pas envisagé que son infrastructure soit une cible pour des menaces spécifiques au secteur d’activité du client.
- **Ateliers 3 et 4 (Scénarios stratégiques et opérationnels)** : le client élabore des scénarios d’attaque à l’aide des techniques **MITRE ATT&CK** et les met en correspondance avec les actifs divulgués par le fournisseur. Ce dernier doit répondre formellement : quels contrôles couvrent chaque technique, quelles failles ont été identifiées et quelles mesures correctives sont prévues.
- **Atelier 5 (Traitement des risques)** : l’analyse partagée produit un plan de traitement des risques commun, avec une responsabilité claire des actions de chaque côté.

MITRE ATT&CK pour les scénarios opérationnels

Les scénarios opérationnels échangés via le protocole de dialogue sur les risques sont exprimés selon les techniques MITRE ATT&CK, offrant un langage commun, précis et univoque pour décrire les vecteurs d'attaque. Un client peut soumettre un scénario tel que : « SR-07 cible l'application publique du fournisseur (T1190), se propage latéralement via des services distants (T1021) vers le serveur hébergeant nos données, puis les exfiltre via un service web (T1567). » Le fournisseur répond par une évaluation structurée de ses contrôles face à chaque technique.

Intégration de TIBER-EU et de DORA (article 26)

L’article 26(4) de la DORA exige que les fournisseurs de services tiers critiques en matière de TIC participent à des exercices de tests d’intrusion axés sur les menaces (TLPT), conformément au cadre TIBER-EU. Le protocole de dialogue sur les risques TPSA soutient directement cette exigence.

- La fiche de divulgation du fournisseur fournit le **périmètre des actifs prédéfini** pour la définition du périmètre des tests TIBER-EU, éliminant ainsi des semaines de travail de cartographie de la part du fournisseur de renseignements sur les menaces.
- Les fiches de scénarios de risques utilisent le même format basé sur ATT&CK que les scénarios de menaces TIBER-EU, créant ainsi un **lien transparent** entre le dialogue continu sur les risques et les tests d'intrusion périodiques.
- Les résultats du TLPT sont réinjectés dans les fiches de divulgation mises à jour et les réponses au dialogue sur les risques, créant ainsi une **boucle d'amélioration continue** .

Amélioration de la classification par le dialogue bidirectionnel

Une propriété émergente essentielle du cadre TPSA est le **mécanisme de rehaussement de classification** . Lorsqu'un client informe un fournisseur, via le processus de retour d'information de la fiche de divulgation, que certains actifs contiennent des données classifiées à un niveau supérieur à celui évalué par le fournisseur (par exemple : « cet actif de stockage contient des données classifiées comme confidentielles pour notre organisation »), le fournisseur met à jour sa classification. Dans les environnements mutualisés, ce rehaussement profite à tous les clients hébergés sur la même infrastructure : la classification la plus élevée détermine le niveau de sécurité des actifs partagés.

Cet effet de « marée montante » inverse la dynamique actuelle où les environnements mutualisés convergent vers le plus petit dénominateur commun. Dans le cadre du TPSA, ils convergent vers la norme la plus élevée, ce qui profite à toutes les parties, y compris celles qui n'ont pas initié la requalification.

2.3 TPSA-03 : Matrice de cartographie réglementaire

Chaque exigence TPSA est associée aux contrôles ou articles correspondants dans :

- **CIS Controls v8** , en particulier Safeguard 15 (Gestion des fournisseurs de services) et les contrôles associés en matière de gestion des actifs, de protection des données, de contrôle d'accès et de réponse aux incidents.
- **La norme ISO/IEC 27001:2022** , Annexe A, contrôle les points A.5.19 à A.5.23 (Relations avec les fournisseurs), A.5.29 à A.5.30 (Continuité des TIC) et les contrôles de soutien dans tous les domaines.
- **DORA (Règlement 2022/2554)** , Articles 28 à 30 (Gestion des risques liés aux tiers dans le domaine des TIC), Article 26 (TLPT/TIBER-EU), Article 19 (Signalement des incidents).
- **Directive NIS2** , article 21(2)(d) (Sécurité de la chaîne d'approvisionnement) et dispositions connexes relatives à la gestion des risques et au traitement des incidents.

Cette cartographie remplit un double objectif. Pour **les clients** , elle fournit une preuve vérifiable que leur gestion des risques liés aux tiers est conforme aux exigences réglementaires : un auditeur qui demande « Comment gérez-vous la sécurité de vos fournisseurs conformément à l'article 21 de la norme NIS2 ? » obtient une réponse documentée et traçable. Pour **les fournisseurs** , elle démontre que la certification TPSA couvre simultanément les exigences de transparence en matière de sécurité de plusieurs cadres réglementaires, réduisant ainsi la charge de conformité liée aux questionnaires spécifiques à chaque cadre.

2.4 TPSA-04 : Système de labellisation et de certification

Le label TPSA est conçu pour fonctionner comme un signal de marché, analogue à la certification ISO 27001 ou à l'attestation SOC 2, mais spécifiquement axé sur la responsabilité des tiers.

Niveaux de maturité

Le système d'étiquetage définit trois niveaux de maturité :

Niveau	Exigences	Public cible
TPSA de base	Fiche de divulgation complète (TPSA-01) avec tous les champs obligatoires renseignés. Examen annuel.	Fournisseurs PME, prestataires de services non critiques. Responsabilité de premier niveau pour les organisations qui débutent leur démarche TPSA.
TPSA amélioré	Carte de divulgation complète et protocole de dialogue sur les risques (TPSA-02) actif. Capacité démontrée à recevoir et à traiter les scénarios de risque des clients. Examen semestriel.	Fournisseurs de niveau intermédiaire, fournisseurs SaaS, fournisseurs de services gérés au service de clients réglementés.
TPSA complet	Mise en œuvre complète des normes TPSA-01 et TPSA-02, incluant l'intégration avec TIBER-EU. Mise à jour continue des informations divulguées. Processus de reclassement éprouvé.	Fournisseurs tiers de services TIC critiques pour les entités réglementées par la DORA, principaux fournisseurs de cloud et d'infrastructure.

Processus de certification

La certification TPSA est réalisée par des organismes d'audit tiers accrédités (par exemple, AFNOR, Bureau Veritas, LSTI, BSI). Le cadre TPSA définit les critères d'audit ; les organismes accrédités effectuent l'évaluation et délivrent le label. Cette séparation garantit l'indépendance et s'appuie sur une infrastructure de certification établie.

L’auteur du cadre et les cabinets de conseil associés peuvent fournir des services de conseil, d’analyse des écarts et d’assistance à la mise en œuvre, mais ne réalisent pas d’audits de certification, conformément à la séparation établie entre le conseil et la certification dans l’écosystème ISO.

3. Positionnement stratégique

3.1 Un outil pour les fournisseurs, pas une contrainte

Le cadre TPSA est délibérément conçu comme un **outil facilitant les démarches des fournisseurs** , et non comme une contrainte imposée par les clients. Un fournisseur qui adopte le TPSA bénéficie des avantages suivants :

- **Différenciation concurrentielle** : la capacité d'affirmer aux prospects « nous sommes certifiés TPSA » remplace des dizaines de questionnaires de sécurité personnalisés par une seule certification reconnue.
- **Réduction des frais généraux liés aux vérifications préalables** : au lieu de répondre à des questionnaires uniques pour chaque client, le fournisseur utilise une fiche de divulgation standardisée qui satisfait aux exigences communes.
- **Alignement réglementaire** : la certification TPSA démontre la couverture des exigences tierces DORA, NIS2 et ISO 27001, ouvrant les portes aux marchés réglementés (banque, assurance, énergie, santé).
- **Confiance du client** : le protocole de dialogue bidirectionnel sur les risques démontre que le fournisseur prend au sérieux les risques spécifiques au client, ce qui permet de bâtir une confiance plus profonde et des relations commerciales plus durables.

3.2 Priorité à l'Europe, pertinence mondiale

Le positionnement initial de TPSA est européen, porté par la dynamique réglementaire de DORA (entrée en vigueur en janvier 2025) et de NIS2 (date limite de transposition : octobre 2024, application en cours). Ces réglementations créent une demande immédiate et concrète de responsabilisation standardisée des tiers. Cependant, le cadre est conçu pour être indépendant de toute réglementation dans son architecture de base : le format de la fiche de divulgation, le protocole de dialogue sur les risques et le système d'étiquetage sont universellement applicables. Des correspondances avec des cadres non européens (NIST CSF, NIST C-SCRM, SOX, APRA CPS 234) pourront être ajoutées à mesure que le cadre évoluera et que son adoption s'étendra au-delà du marché européen.

3.3 Complémentaires, non concurrentiels

TPSA ne concurrence pas les normes ou outils existants. Il occupe un créneau spécifique qu'aucun d'entre eux ne couvre actuellement :

Outil existant	Ce que ça fait	Qu'apporte le TPSA
Contrôles CIS v8	Indique au client ce qu'il doit faire concernant le risque fournisseur (Garantie 15).	Indique au fournisseur comment démontrer sa responsabilité dans un format standardisé.
ISO 27001	Nécessite des politiques et une surveillance de la sécurité des fournisseurs.	Définit le protocole opérationnel et le format de cette surveillance.
SOC 2	Audit périodique et confidentiel des contrôles des fournisseurs.	Divulgation continue, transparente et axée sur le client, avec un dialogue bidirectionnel sur les risques.
SIG / CAIQ	Questionnaires standardisés pour l'évaluation des fournisseurs.	Des informations standardisées à l'initiative du fournisseur, ainsi qu'un mécanisme de dialogue continu sur les risques.
DORA /NIS2	Obligations réglementaires en matière de gestion des risques liés aux tiers.	Un cadre opérationnel permettant de satisfaire à ces obligations grâce à des preuves documentées et vérifiables.

4. Conclusion et appel à contributions

Le cadre TPSA comble une lacune structurelle du paysage de la cybersécurité : l'absence d'un mécanisme de responsabilité bidirectionnel et standardisé entre les fournisseurs et leurs clients. En faisant évoluer le paradigme d'une évaluation pilotée par le client vers une divulgation initiée par le fournisseur et un dialogue mutuel sur les risques, le TPSA crée de la valeur pour toutes les parties prenantes.

- **Les fournisseurs** bénéficient d'un label concurrentiel, d'une réduction de la lassitude liée aux questionnaires et d'une conformité avec de multiples cadres réglementaires.
- **Les clients** bénéficient de preuves standardisées et vérifiables de la gestion de la sécurité par des tiers, de capacités de dialogue bidirectionnel sur les risques et d'un mécanisme de rehaussement de la classification pour les environnements partagés.
- **Les organismes de réglementation et les auditeurs** bénéficient d'un cadre traçable et vérifiable pour évaluer la conformité aux exigences tierces des normes DORA, NIS2 et ISO 27001.
- **L'écosystème** bénéficie d'un effet d'entraînement positif, les normes de classification les plus élevées dans les environnements multi-locataires profitant à tous les participants.

Ce document de position invite la communauté de la cybersécurité, les praticiens, les organismes de réglementation, les organismes de normalisation, les fournisseurs et les clients à contribuer à l'élaboration du cadre TPSA. La norme sera façonnée par les contributions de ses utilisateurs.

Contact et contributions

Sébastien Poitrasson , CISSP, Lead Implementer ISO 27001, CIS Supporter
Arthur Koenig Consulting

Annexe A : Glossaire

Terme	Définition
TPSA	Responsabilité des fournisseurs tiers. Le cadre défini dans ce document.
Fiche de divulgation	Un document structuré et normalisé publié par un fournisseur en vertu de la norme TPSA-01, décrivant sa posture de sécurité en ce qui concerne les données et les services destinés aux clients.
Fiche de scénario de risque	Un scénario de menace formalisé soumis par un client à un fournisseur dans le cadre de la norme TPSA-02, utilisant la structure EBIOS RM et les techniques MITRE ATT&CK.
Protocole de dialogue sur les risques	Le mécanisme d'échange bidirectionnel défini dans la norme TPSA-02 pour la communication structurée des risques entre clients et fournisseurs.
Rehaussement de la classification	Le mécanisme par lequel la classification plus élevée des données d'un client sur des actifs partagés incite le fournisseur à renforcer les contrôles de sécurité, au bénéfice de tous les locataires.
EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité, Risk Manager. La méthodologie d'analyse des risques publiée par l'ANSSI (France).
TIBER-UE	Équipe rouge éthique basée sur le renseignement sur les menaces. Le cadre européen pour les tests d'intrusion axés sur les menaces, mentionné à l'article 26 de la DORA.
TLPT	Tests d'intrusion axés sur les menaces, tels que définis dans les articles 26 et 27 de la DORA.