TPSA

THIRD-PARTY SUPPLIER ACCOUNTABILITY

T P S A - 0 2

Protocole de dialogue sur les risques

Cadre de responsabilité des fournisseurs tiers

Document de spécifications

Communication bidirectionnelle des risques entre fournisseurs et clients

Version 1.0 Avril 2026

Auteur : Sébastien Poitrasson, Arthur Koenig Conseil

AK ARTHURKOENIG

Le KRI Exchange ajoute une couche de surveillance quantitative et continue au protocole de dialogue sur les risques. Alors que les fiches de scénarios de risques (RSC) sont des exercices ponctuels qui évaluent la capacité du fournisseur à faire face à des scénarios de menaces spécifiques, les KRI fournissent des signaux continus et mesurables de l'état de

1. Introduction

1.1 Objectif

Ce document définit le **TPSA-02 : Protocole de dialogue sur les risques** , deuxième composante du cadre de responsabilité des fournisseurs tiers. Il précise les mécanismes, les formats, les processus et les échéanciers de **la communication bidirectionnelle sur les risques** entre un fournisseur et ses clients.

Le protocole de dialogue sur les risques comble une lacune fondamentale dans la gestion actuelle des risques liés aux tiers : l'absence d'un canal standardisé permettant aux clients de communiquer leur environnement de menaces spécifique à leurs fournisseurs, et aux fournisseurs de répondre par des évaluations structurées et vérifiables de leur posture défensive face à ces menaces.

Alors que la norme TPSA-01 (Supplier Disclosure Standard) établit la transparence de sécurité de base du fournisseur, la norme TPSA-02 crée un **dialogue vivant** qui s'adapte à l'évolution des menaces, aux contextes de risque spécifiques au client et aux exigences réglementaires, y compris les dispositions de DORA sur les tests d'intrusion axés sur les menaces (TLPT/TIBER-EU).

1.2 Portée

La norme TPSA-02 s'applique à tous les fournisseurs titulaires ou en cours de certification TPSA de niveau **ENHANCED** ou **FULL** . Les fournisseurs de niveau BASIC ne sont pas tenus de mettre en œuvre le Protocole de dialogue sur les risques, mais peuvent choisir de le faire volontairement.

Le protocole couvre trois types d'échanges : **les fiches de scénarios de risques** (scénarios de menaces initiés par le client), **les évaluations des risques fournisseurs** (réponses des fournisseurs) et **les messages de coordination TIBER-EU** (spécifiques aux contextes réglementés par la DORA). Chaque type d'échange possède un format, un cycle de vie et un calendrier définis.

1.3 Relation avec les autres composantes du TPSA

- **TPSA-01** : Le protocole de dialogue sur les risques s'appuie sur la fiche de divulgation du fournisseur comme source de données de base. Les scénarios de risque font référence aux actifs, aux contrôles et aux classifications documentés dans la fiche de divulgation.
- **TPSA-03** : les correspondances réglementaires identifient les éléments du protocole de dialogue sur les risques qui satisfont aux exigences spécifiques de DORA, NIS2 et ISO 27001.
- **TPSA-04** : le système d'étiquetage et de certification définit le niveau de maturité auquel le protocole de dialogue sur les risques devient obligatoire, ainsi que les critères d'audit pour évaluer la mise en œuvre du protocole.

1.4 Références normatives

Outre les références normatives énumérées dans le TPSA-01, les éléments suivants sont spécifiques au TPSA-02 :

- **EBIOS Risk Manager** (ANSSI, 2018), Ateliers 1 à 5 : structure et terminologie.
- **MITRE ATT&CK® Enterprise** (version actuelle), Tactiques, techniques et sous-techniques pour la description de scénarios opérationnels.
- **MITRE ATT&CK® pour ICS** (version actuelle), Pour les fournisseurs de services de systèmes de contrôle industriel (ICS/OT).
- **Cadre TIBER-EU** (BCE, 2018 ; mis à jour en 2024), Méthodologie d’équipe rouge éthique basée sur le renseignement sur les menaces.
- **Règlement DORA 2022/2554,** Articles 26–27 (Tests d’intrusion axés sur les menaces), Articles 28–30 (Gestion des risques liés aux TIC pour les tiers).
- **STIX 2.1** (OASIS), Format d'expression structurée des informations sur les menaces, pour l'échange de renseignements sur les menaces.

2. Architecture du protocole

2.1 Aperçu

Le protocole de dialogue sur les risques fonctionne comme un canal d'échange structuré, asynchrone et bidirectionnel entre un client et un fournisseur. Il ne s'agit pas d'un système de communication en temps réel, mais d'un **protocole formel d'échange de documents relatifs aux risques,** avec des formats, des exigences d'accusé de réception et des délais de réponse définis.

Type d'échange	Initiateur	Répondant	But
Fiche de scénario de risque (FSR)	Client	Fournisseur	Le client soumet un scénario de menace spécifique à son contexte et demande au fournisseur d'évaluer sa posture défensive face à cette menace.
Évaluation des risques fournisseurs (SRA)	Fournisseur	Client	Le fournisseur répond formellement à une fiche de scénario de risque par une évaluation structurée des contrôles, des lacunes et des plans de remédiation.
Coordination TIBER-UE (TEC)	L'une ou l'autre des parties	L'une ou l'autre des parties	Messages de coordination pour les exercices TLPT/TIBER-EU impliquant le fournisseur : définition du périmètre, planification, partage des résultats, suivi des mesures correctives.
Demande de reclassement (CUR)	Client	Fournisseur	Le client notifie au fournisseur une classification de données plus élevée sur des actifs spécifiques (tels que définis dans la section 4 de la TPSA-01).
Échange d'indicateurs clés de risque (KRI)	Fournisseur (publication) / Client (demande)	L'une ou l'autre des parties	Surveillance quantitative continue du profil de risque du fournisseur au moyen d'indicateurs standardisés. Permet une alerte précoce et le déclenchement ciblé du RSC en cas de dépassement des seuils.

2.2 Exigences relatives aux canaux

Tous les échanges effectués dans le cadre du protocole de dialogue sur les risques doivent transiter par un **canal sécurisé et authentifié** qui garantit la confidentialité, l'intégrité et la non-répudiation.

Authentification

Les deux parties s'authentifient à l'aide **de paires de certificats ED25519** , conformément au mécanisme de signature de la carte de divulgation défini dans la norme TPSA-01 (champ H-13). Chaque partie détient une clé privée et a enregistré la clé publique correspondante auprès de l'autre partie. Chaque message est signé par l'expéditeur et vérifié par le destinataire.

Confidentialité

Les messages sont chiffrés lors de leur transmission à l'aide du protocole TLS 1.3 (minimum) pour une protection au niveau du réseau. Leur contenu est également chiffré à l'aide de la clé publique du destinataire (NaCl/libsodium crypto_box ou équivalent), garantissant ainsi une confidentialité de bout en bout même en cas de compromission de la couche transport ou lors du passage des messages par des systèmes intermédiaires.

Agnosticisme des transports

Le protocole est **indépendant du transport** . Les messages peuvent être échangés via :

- L’ API **de la plateforme de référence TPSA** (points de terminaison REST définis dans la section 7, en projet).
- Portail propriétaire d'un fournisseur mettant en œuvre le format de message TPSA.
- **Courriel chiffré** (PGP/S/MIME) avec charges utiles JSON jointes, pour les environnements où l'intégration API n'est pas possible.
- **Échange hors ligne** (fichiers JSON signés sur support chiffré), pour les environnements isolés ou hautement restreints.

Quel que soit le mode de transport, le **format et le cycle de vie du message** restent identiques. La conformité est évaluée sur la base du format et du processus, et non du mode de transport.

2.3 Cycle de vie des messages

Chaque échange suit un cycle de vie en cinq étapes :

État	Transition	Description
BROUILLON	L'auteur crée	Message en cours de rédaction. Pas encore transmis. Peut faire l'objet d'une vérification interne avant envoi.
SOUMIS	L'auteur envoie	Le message est transmis au destinataire. Le délai d'accusé de réception commence.
RECONNU	Le destinataire confirme la réception	Le destinataire a confirmé la réception et accepté le message pour traitement. Le compte à rebours de la réponse a commencé.
A RÉPONDU	L'expéditeur envoie une réponse	Une réponse officielle (SRA, réponse CUR, mise à jour TEC) a été envoyée. L'initiateur l'examine.
FERMÉ	L'initiateur accepte ou escalade	La transaction est close. Les deux parties conservent l'intégralité du registre des transactions à des fins d'audit et de conformité.

2.4 Échéanciers

Action	BASIQUE	AMÉLIORÉ	COMPLET
Reconnaissance	N/A (protocole non requis)	10 jours ouvrables	5 jours ouvrables
Réponse à la RSC	N / A	30 jours ouvrables	15 jours ouvrables
Réponse à CUR	N / A	30 jours ouvrables	15 jours ouvrables
Réponse à la planification de l'étude de faisabilité de TEC	N / A	20 jours ouvrables	10 jours ouvrables
Escalade (pas de réponse)	N / A	Après le délai de réponse + 10 jours	Après le délai de réponse + 5 jours

Les délais sont exprimés en jours ouvrables à compter de la date de soumission (pour accusé de réception) ou de l'accusé de réception (pour réponse). Les procédures d'escalade sont définies à la section 6.

3. Fiche de scénario de risque (FSR)

3.1 Objectif et justification

La fiche de scénario de risque est le principal instrument par lequel un client communique une **menace spécifique et contextualisée** à un fournisseur et demande une évaluation formelle de la posture défensive de ce dernier face à cette menace.

Le RSC diffère fondamentalement d'un questionnaire de sécurité. Un questionnaire pose des questions génériques (« Chiffrez-vous les données au repos ? »). Le RSC présente un **scénario d'attaque concret,** pertinent au contexte des menaces du client, et demande au fournisseur de décrire ses défenses pour chaque étape du processus. Ceci impose un niveau de spécificité et de transparence que les questionnaires génériques ne peuvent garantir.

3.2 Alignement EBIOS RM

Le RSC est structuré autour de la méthodologie EBIOS Risk Manager (ANSSI), adaptée au contexte client-fournisseur. Chaque RSC correspond à des ateliers EBIOS RM spécifiques :

Atelier EBIOS	Fonction EBIOS RM	Cartographie TPSA	Source
WS1 Scope	Définir le périmètre, les valeurs commerciales, les actifs et le référentiel de sécurité existant.	Prérempli à partir de la fiche de déclaration du fournisseur (TPSA-01). Aucune saisie supplémentaire n'est requise pour le RSC.	Fournisseur (via TPSA-01)
WS2 Sources de risques	Identifier les sources de risque (SR) et leurs objectifs/motivations (OV).	Section A du RSC : Identification des sources de risque. Le client identifie les paires SR/OV pertinentes à son contexte.	Client
WS3 Scénarios stratégiques	Élaborer des scénarios d'attaque de haut niveau : SR → cible → événement redouté.	Section B du RSC : Scénario stratégique. Le client décrit le chemin d'attaque global à travers l'environnement du fournisseur.	Client
WS4 Scénarios opérationnels	Détaillez les modes d'attaque techniques en utilisant des techniques spécifiques.	Section C du RSC : Scénario opérationnel (MITRE ATT&CK). Le client associe l'attaque à des techniques ATT&CK spécifiques sur les actifs du fournisseur.	Client
WS5 Traitement des risques	Définir les mesures de traitement des risques et le risque résiduel.	Réponse à l'évaluation des risques fournisseurs (SRA). Plan conjoint de traitement des risques.	Fournisseur (SRA) + Joint

3.3 Structure RSC

Une fiche de scénario de risque est un document JSON composé d'un en-tête et de trois sections (A, B, C), chacune correspondant aux ateliers EBIOS RM 2, 3 et 4.

En-tête RSC

IDENTIFIANT	Champ	Type	Req.	Description
RSC-H01	**Identifiant RSC**	UUID	M	Identifiant unique de cette fiche de scénario de risque.
RSC-H02	**Nom du client**	String	M	Nom du client soumettant le scénario.
RSC-H03	**Contact client**	Object	M	Contact de sécurité pour ce RSC : nom, rôle, courriel, clé PGP.
RSC-H04	**Fournisseur cible**	String	M	Nom du fournisseur (doit correspondre à TPSA-01 H-01).
RSC-H05	**Référence de la carte de divulgation**	String	M	Référence à la version de la carte de divulgation par rapport à laquelle ce scénario est construit (TPSA-01 H-03).
RSC-H06	**Date de soumission**	ISO 8601	M	Date de soumission.
RSC-H07	**Priorité**	Enum	M	CRITIQUE, ÉLEVÉ, MOYEN, FAIBLE. Détermine la pondération du délai de réponse.
RSC-H08	**Contexte réglementaire**	Array	C	Réglementation applicable régissant ce RSC (par exemple, DORA art. 28, NIS2 art. 21). Obligatoire lorsque le RSC est régi par une réglementation.
RSC-H09	**Drapeau TIBER-UE**	Boolean	C	Indique si ce RSC fait partie d'un exercice TIBER-EU/TLPT ou s'y prépare. Déclenche un traitement spécifique à TIBER-EU (section 5).
RSC-H10	**Signature numérique**	ED25519	M	Signature du client sur le contenu RSC.

Section A : Identification des sources de risque (EBIOS WS2)

Cette section recense les acteurs malveillants et leurs objectifs pertinents pour le contexte du client. Le client ne demande pas au fournisseur d'identifier les menaces ; il l' **informe** des menaces qui le préoccupent et qui pourraient transiter par l'environnement du fournisseur.

IDENTIFIANT	Champ	Type	Req.	Description
RSC-A01	**Sources de risque**	Array	M	Liste des sources de risques (SR). Chaque entrée comprend : l'identifiant de la SR (par exemple, SR-01), le type de SR (parrainée par l'État, crime organisé, hacktiviste, initiée, concurrente, opportuniste), le nom ou la description de la SR, les TTP ou affiliations connues

				(par exemple, désignation du groupe APT) et un résumé de la motivation/de l'objectif.
RSC-A02	**Objectifs cibles**	Tableau	M	Pour chaque SR, les objectifs redoutés (OV) : exfiltration de données, interruption de service, espionnage, déploiement de ransomware, compromission de la chaîne d'approvisionnement, atteinte à la réputation, etc.
RSC-A03	**Contexte sectoriel**	Texte	M	Brève description du secteur du client, de l'environnement réglementaire et de la raison pour laquelle ces sources de risques spécifiques sont pertinentes (par exemple, « Établissement financier soumis à la DORA, ciblé par APT38 pour fraude liée à SWIFT »).
RSC-A04	**Références en matière de renseignement sur les menaces**	Tableau	O	Références aux sources de renseignements sur les menaces appuyant l'identification de la source du risque : avis du CERT, ensembles STIX, rapports de menaces des fournisseurs, CTI internes.

Section B : Scénario stratégique (EBIOS WS3)

Cette section décrit le schéma d'attaque principal : comment la source du risque atteint son objectif en transitant par l'environnement du fournisseur. Elle relie l'acteur malveillant à l'événement redouté par le client via les ressources du fournisseur.

IDENTIFIANT	Champ	Type	Req.	Description
RSC-B01	**Titre du scénario**	String	M	Titre court et descriptif (par exemple : « Exfiltration APT via API de plateforme SaaS »).
RSC-B02	**Point d'entrée**	Référence	M	Les actifs du fournisseur visés pour l'accès initial doivent faire référence aux identifiants des actifs figurant sur la fiche de divulgation (TPSA-01, D1-01).
RSC-B03	**Chemin d'attaque**	Text	M	Description narrative du parcours d'attaque stratégique : accès initial → déplacement latéral → objectif. Décrit comment l'attaquant se déplace du point d'entrée jusqu'aux données ou au service du client.
RSC-B04	**Actifs cibles**	Array	M	Le ou les actifs du fournisseur où l'événement redouté se produit (entrepôt de données, application, segment de réseau). Références : TPSA-01 D1-01.
RSC-B05	**Événement redouté**	Text	M	L'impact sur le client en cas de succès du scénario : violation de données, interruption de service, atteinte à l'intégrité du système, sanction réglementaire, etc.
RSC-B06	**Estimation de vraisemblance**	Enum	O	Évaluation par le client de la probabilité du scénario : TRÈS ÉLEVÉE, ÉLEVÉE, MOYENNE, FAIBLE, TRÈS FAIBLE. Fondée sur les renseignements relatifs aux menaces et l’exposition sectorielle.
RSC-B07	**Estimation de l'impact**	Enum	M	Évaluation par le client de l'impact potentiel : CRITIQUE, ÉLEVÉ, MOYEN, FAIBLE.

Section C : Scénario opérationnel, Cartographie MITRE ATT&CK (EBIOS WS4)

Cette section traduit le scénario stratégique en un **plan d'attaque technique** à l'aide des techniques MITRE ATT&CK®. Chaque étape de l'attaque est associée à une technique (ou sous-technique) ATT&CK spécifique, à un actif cible identifié dans la fiche de divulgation et au contrôle défensif attendu. Cette section permet d'obtenir la réponse la plus précise et la plus efficace possible du fournisseur.

IDENTIFIANT	Champ	Type	Req.	Description
RSC-C01	**Étapes d'attaque**	Array	M	Liste ordonnée des étapes d'attaque. Chaque étape comprend : le numéro de l'étape, l'identifiant de la technique ATT&CK (par exemple, T1190), le nom de la technique ATT&CK, la tactique ATT&CK (par exemple, Accès initial), l'identifiant de la ressource cible (à partir de TPSA-01 D1-01) et une description de la manière dont la technique est appliquée dans ce contexte de scénario.
RSC-C02	**Matrice ATT&CK**	Enum	M	Quelle matrice ATT&CK est utilisée : ENTREPRISE ou ICS ? Elle doit correspondre à la nature de l'environnement du fournisseur.
RSC-C03	**Cartographie de la chaîne de mise à mort**	Object	O	Cartographie optionnelle des étapes d'attaque selon les phases de la chaîne de destruction cybernétique de Lockheed Martin pour un contexte stratégique supplémentaire.
RSC-C04	**Attentes en matière de détection**	Array	O	Pour chaque étape de l'attaque, l'attente du client quant à la capacité de détection du fournisseur : DÉTECTER, PARTIELLE, AVEUGLE, INCONNUE.
RSC-C05	**Questions spécifiques**	Array	O	Questions libres auxquelles le client souhaite que le fournisseur réponde pour des étapes d'attaque spécifiques (par exemple, « Pour l'étape 3 (T1021.002) : surveillez-vous les sessions RDP vers le segment de base de données ? »).

4. Évaluation des risques fournisseurs (SRA)

4.1 Objectif

L'évaluation des risques fournisseurs SRA est la **réponse formelle** à une fiche de scénario de risque. Il ne s'agit pas d'une simple déclaration de conformité, mais d'une **analyse détaillée** des contrôles mis en place par le fournisseur pour chaque étape du scénario opérationnel du client. Le SRA transforme le TPSA d'un simple échange d'informations en un véritable **mécanisme de responsabilisation** .

4.2 Structure SRA

En-tête SRA

IDENTIFIANT	Champ	Type	Req.	Description
SRA-H01	**Identifiant SRA**	UUID	M	Identifiant unique de cette évaluation des risques fournisseurs.
SRA-H02	**Référence RSC**	UUID	M	Référence à la fiche de scénario de risque à laquelle il est répondu (RSC-H01).
SRA-H03	**Date de réponse**	ISO 8601	M	Date de cette réponse.
SRA-H04	**Assesseur**	Object	M	Nom, rôle et qualifications de la ou des pSRAonnes ayant effectué l'évaluation.
SRA-H05	**Étendue de l'évaluation**	Text	M	Confirmation que l'évaluation couvre toutes les étapes d'attaque du RSC, ou déclaration explicite des étapes qui n'ont pas pu être évaluées et pourquoi.
SRA-H06	**Signature numérique**	ED25519	M	Signature du fournisseur sur le contenu du SRA.

Organisme SRA : Évaluation par étape

L'élément central de l'analyse de réponse au sinistre (SRA) est une **réponse étape par étape** à chaque phase d'attaque définie dans la section C du RSC. Pour chaque phase d'attaque, le fournisseur fournit :

IDENTIFIANT	Champ	Type	Req.	Description
SRA-S01	**Référence des étapes**	Entier	M	Le numéro de l'étape d'attaque du RSC concerné.
SRA-S02	**Technique ATT&CK**	String	M	Confirmation de l'identifiant de la technique ATT&CK évaluée (doit correspondre à RSC-C01).
SRA-S03	**État de contrôle**	Enum	M	COUVERT : les contrôles existants couvrent cette technique. PARTIELLEMENT COUVERT : des contrôles existent, mais avec des limitations connues. LACUNE : aucun

				contrôle efficace n'est en place. NON APPLICABLE : la technique ne peut être appliquée dans cet environnement (justification requise).
SRA-S04	**Description des commandes**	Text	M	Description détaillée des contrôles spécifiques relatifs à cette technique : technologie, configuration, règles de surveillance, logique de détection, procédures de réponse.
SRA-S05	**Capacité de détection**	Enum	M	DÉTECTION : le système de surveillance du fournisseur permettrait d'identifier l'utilisation de cette technique. DÉTECTATION PARTIELLE : la détection est possible mais non certaine (par exemple, elle dépend du volume et du moment). NON DÉTECTÉE : cette technique spécifique ne peut être détectée.
SRA-S06	**Référence de preuve**	Array	C	Références aux éléments de preuve justifiant l'état du contrôle : captures d'écran de la configuration, identifiants des règles de surveillance, exemples de journaux d'audit, résultats de tests. Obligatoire lorsque l'état du contrôle est « COUVRÉ ».
SRA-S07	**Analyse des écarts**	Text	C	Pour un statut PARTIEL ou LACUNE : description de la lacune, de sa cause première et de l'exposition au risque. Obligatoire lorsque le statut de contrôle est ≠ COUVERT.
SRA-S08	**Plan de remédiation**	Object	C	Pour les contrôles PARTIELS ou CASSANTS : mesures correctives prévues, responsable, date d'achèvement prévue et contrôles intérimaires/compensatoires. Obligatoire lorsque le statut du contrôle est ≠ COUVERT.

Résumé SRA

IDENTIFIANT	Champ	Type	Req.	Description
SRA-R01	**Évaluation globale**	Enum	M	Évaluation globale : ADÉQUATE (toutes les étapes COUVERTES ou NON_APPLICABLES), PARTIELLEMENT ADÉQUATE (mélange de COUVERTES et PARTIELLES), INSUFFISANTE (une ou plusieurs LACUNES sur les étapes critiques).
SRA-R02	**Statistiques de couverture**	Object	M	Nombre d'étapes par statut : COUVERT, PARTIEL, LARGEUR, NON APPLICABLE.

SRA-R03	**Déclaration relative aux risques résiduels**	Text	M	Évaluation par le fournisseur du risque résiduel après prise en compte des contrôles existants et des mesures correctives prévues.
SRA-R04	**Feuille de route pour la remédiation**	Array	C	Liste consolidée de toutes les actions correctives pour chaque étape, avec priorités et échéancier. Obligatoire lorsqu'une étape a le statut PARTIEL ou LAISSÉE.
SRA-R05	**Recommandations**	Text	O	Recommandations du fournisseur au client pour la réduction des risques du côté client (par exemple, contrôles d'accès supplémentaires, surveillance, dispositions contractuelles).
SRA-R06	**Mise à jour de la carte de divulgation**	Boolean	M	Indiquez si les conclusions de l'analyse de la fiabilité des fournisseurs (SRA) entraîneront une mise à jour de la fiche de renseignements du fournisseur (TPSA-01). Si oui, indiquez la version et la date de mise à jour prévues.

5. Intégration TIBER-UE / TLPT

5.1 Contexte réglementaire

L'article 26(4) de la loi DORA exige que les fournisseurs de services tiers critiques en matière de TIC **participent aux exercices de tests d'intrusion axés sur les menaces (TLPT)** menés par leurs clients, conformément au cadre TIBER-EU. Ceci crée une obligation légale de coopération pour les fournisseurs lors d'exercices de simulation d'attaques.

Le protocole de dialogue sur les risques de l'Accord de partenariat transpacifique (TPSA) fournit l' **infrastructure opérationnelle nécessaire** à cette coopération, réduisant ainsi les coûts de coordination qui nécessitaient des semaines de négociations ad hoc à un processus structuré et prédéfini.

5.2 Messages de coordination TIBER-UE (TEC)

Le message de coordination TIBER-EU est un type d'échange spécifique au sein du protocole de dialogue sur les risques, conçu pour soutenir les trois phases d'un exercice TIBER-EU :

Phase 1 : Définition du périmètre (TEC-SCOPE)

Le client (ou son fournisseur de renseignements sur les menaces) envoie un message TEC-SCOPE au fournisseur. Ce message utilise la fiche de divulgation pour définir le périmètre de test :

- **Actifs cibles** : sélectionnés à partir du registre des actifs de la fiche de divulgation D1-01, déjà identifiés avec leur emplacement, leur modèle d'hébergement et leur classification.
- **Services concernés** : les services du fournisseur à inclure dans l'exercice TLPT.
- **Actifs/services exclus** : tous les actifs des fournisseurs explicitement exclus des tests, avec justification.
- **Période de test** : dates et heures proposées pour l'exercice.
- **Règles d'engagement** : limites convenues, procédures d'escalade et protocoles de communication pendant le test.

Comme la fiche de divulgation fournit déjà un inventaire structuré et à jour des actifs, la phase de cadrage est **considérablement accélérée** . Le fournisseur de renseignements sur les menaces n'a pas besoin d'effectuer de reconnaissance pour identifier les actifs du fournisseur : ceux-ci sont déjà documentés.

Phase 2 : Exécution (TEC-EXEC)

Lors de l'exercice TLPT, des messages TEC-EXEC peuvent être échangés pour :

- **Coordination des incidents** : si le SOC du fournisseur détecte l'activité de l'équipe rouge et déclenche une escalade, les coordinateurs de l'exercice peuvent avoir besoin de communiquer pour éviter toute perturbation.

- **Ajustements de périmètre** : si l'équipe rouge identifie des actifs non inclus dans le périmètre initial mais pertinents, ce dernier peut être élargi via un amendement TEC-EXEC.
- **Signaux de sécurité** : si l'équipe rouge rencontre des risques de production, un signal de sécurité peut interrompre l'exercice.

Phase 3 : Résultats et remédiation (TEC-RESULTS)

À l’issue de l’exercice, le message TEC-RESULTS formalise les résultats :

- **Résultats mis en correspondance avec les techniques ATT&CK** : en utilisant le même format que l'échange RSC/SRA, garantissant la cohérence et la traçabilité.
- **Performances de détection** : quelles techniques ont été détectées par le SOC du fournisseur, lesquelles ont été manquées et à quelle étape.
- **Plan de remédiation** : utilisant le format de remédiation SRA (SRA-S08), avec des dates cibles et des parties responsables.
- **Déclencheur de mise à jour de la carte de divulgation** : les constatations qui modifient la posture de sécurité ou la classification des actifs du fournisseur déclenchent une mise à jour TPSA-01.

Le message TEC-RESULTS crée une **boucle de rétroaction** entre les exercices TIBER-EU et le processus continu de fiche de divulgation/dialogue sur les risques. Les tests d'intrusion ne sont plus un exercice ponctuel, mais font partie d'un cycle de responsabilisation continu.

5.3 RSC préexistants en tant qu'entrées TIBER-EU

L'un des principaux atouts du cadre TPSA réside dans le fait que **les fiches de scénarios de risques (RSC) déjà soumises et évaluées peuvent servir de base à la conception des tests TIBER-EU** . Si un client a préalablement soumis une RSC décrivant un scénario d'APT et reçu une analyse de scénarios (SRA) indiquant une couverture partielle, le fournisseur de renseignements sur les menaces TIBER-EU peut utiliser ce scénario comme point de départ pour l'exercice TLPT, en ciblant précisément les failles identifiées. Ceci assure la continuité entre le dialogue continu sur les risques et les tests d'intrusion périodiques, garantissant ainsi que les exercices TLPT ne sont pas conçus de manière isolée, mais s'appuient sur le contexte de risque réel documenté par le processus TPSA.

6. Indicateur clé de risque (ICR) Échange

6.1 Objectif

Le KRI Exchange ajoute une couche de surveillance quantitative et continue au protocole de dialogue sur les risques. Alors que les fiches de scénarios de risques (RSC) sont des exercices ponctuels qui évaluent la capacité du fournisseur à faire face à des scénarios de menaces spécifiques, les KRI fournissent des signaux continus et mesurables de l'état de la sécurité opérationnelle du fournisseur en ce qui concerne les données et les services des clients.

Dans le cadre de l'analyse comparative de risques (ACR), les indicateurs clés de risque (ICR) remplissent trois fonctions. Premièrement, ils assurent **une visibilité continue** : les clients reçoivent des indicateurs réguliers et standardisés sans nécessiter un cycle complet d'analyse de risques de sécurité (ARS). Deuxièmement, ils servent de **système d'alerte précoce** : un ICR dépassant un seuil défini peut inciter le client à soumettre une ARS ciblée afin d'enquêter sur le problème sous-jacent. Troisièmement, ils définissent un **langage commun en matière d'appétit pour le risque** : en convenant des définitions et des seuils des ICR, le client et le fournisseur établissent une base de référence quantitative pour ce qui constitue un risque acceptable.

6.2 Structure KRI

Chaque KRI est défini à l'aide d'un format standardisé :

IDENTIFIANT	Champ	Type	Req.	Description
KRI-01	Identifiant KRI	String	M	Identifiant unique pour cet indicateur (par exemple, KRI-VULN-001).
KRI-02	Catégorie	Enum	M	Alignement des domaines : GESTION DES ACTIFS, PROTECTION DES DONNÉES, SAUVEGARDE, CONTRÔLE D'ACCÈS, VULNÉRABILITÉ, INCIDENT, CONFORMITÉ. Correspond aux domaines D1 à D7 de la norme TPSA-01.
KRI-03	Nom de la métrique	String	M	Nom lisible par l'humain (par exemple, « Taux de correction des vulnérabilités critiques dans les délais du SLA »).
KRI-04	Définition de la métrique	Text	M	Définition précise de la métrique : ce qui est mesuré, comment c'est calculé, source des données et périmètre de mesure.
KRI-05	Unité	String	M	Unité de mesure (pourcentage, nombre, heures, jours, ratio).
KRI-06	Fréquence	Enum	M	Fréquence de rapport : TEMPS_RÉEL, QUOTIDIEN, HEBDOMADAIRE, MENSUEL, TRIMESTRIEL.
KRI-07	Valeur actuelle	Number	M	Valeur mesurée la plus récente.
KRI-08	Date de mesure	ISO 8601	M	Date et heure de la dernière mesure.
KRI-09	Seuil acceptable	Number	M	La valeur à laquelle ou en dessous/au-dessus de laquelle l'indicateur est considéré comme relevant d'une tolérance au risque acceptable.
KRI-10	Seuil - Avertissement	Number	C	Valeur à partir de laquelle l'indicateur signale un risque élevé. Attire l'attention sans provoquer d'escalade. Obligatoire au niveau MAXIMUM.
KRI-11	Seuil - Critique	Number	C	Valeur à partir de laquelle l'indicateur signale un risque inacceptable et doit déclencher une alerte ou un dialogue immédiat. Obligatoire au niveau MAXIMUM.
KRI-12	S'orienter	Enum	O	Évolution au cours des 3 dernières périodes de mesure : AMÉLIORATION, STABILITÉ, DÉGRADATION.
KRI-13	Commentaire	Text	O	Commentaire contextuel du fournisseur sur la valeur actuelle (par exemple, explication d'une dégradation temporaire due à une migration planifiée).

6.3 Indicateurs clés de risque de référence

Les indicateurs clés de performance (KRI) suivants sont **recommandés comme ensemble de base** . Les fournisseurs de niveau AMÉLIORÉ doivent en publier au moins 5 ; ceux de niveau COMPLET doivent tous les publier. D'autres KRI peuvent être définis d'un commun accord entre le client et le fournisseur.

KRI ID	Catégorie	Métrique	Seuil recommandé (acceptable)
KRI-VULN-001	VULNÉRABILITÉ	Pourcentage de vulnérabilités critiques corrigées dans les délais du SLA (24 h)	≥ 95%
KRI-VULN-002	VULNÉRABILITÉ	Pourcentage de vulnérabilités élevées corrigées dans les délais du SLA (72 h)	≥ 90%
KRI-VULN-003	VULNÉRABILITÉ	Nombre de vulnérabilités critiques/élevées non corrigées antérieures à la date du SLA	0
KRI-BACKUP-001	SAUVEGARDE	Dernier test de restauration de sauvegarde réussi (il y a quelques jours)	≤ 90 jours
KRI-BACKUP-002	SAUVEGARDE	Taux de réussite des sauvegardes (30 derniers jours)	≥ 99,5 %
KRI-ACCESS-001	CONTRÔLE_D'ACCÈS	Pourcentage de comptes privilégiés avec l'authentification multifacteur activée	100%
KRI-ACCESS-002	CONTRÔLE_D'ACCÈS	Nombre de jours écoulés depuis la dernière révision des droits d'accès	≤ 90 jours
KRI-INCIDENT-001	INCIDENT	Délai moyen de détection (MTTD) pour les alertes critiques/élevées (heures)	≤ 1 heure
KRI-INCIDENT-002	INCIDENT	Nombre d'incidents de sécurité affectant les données clients (90 derniers jours)	Dépendant du contexte
KRI-AVAIL-001	GESTION DES ACTIFS	Disponibilité du service (30 derniers jours)	≥ 99,9 %
KRI-CONFORMITÉ-001	CONFORMITÉ	Jours avant la prochaine expiration de la certification	≥ 90 jours

6.4 Publication des KRI et KRI demandés par le client

KRI) publiés par le fournisseur sont inclus dans la fiche de divulgation (TPSA-01) en annexe ou dans l'annexe spécifique au client. Ils sont mis à jour à la fréquence définie dans le KRI-06. Pour les fournisseurs utilisant la plateforme de référence TPSA, les KRI sont accessibles via un point de terminaison API dédié.
KRI) demandés par le client : un client peut demander des KRI supplémentaires, spécifiques à son contexte de risque, via le protocole de dialogue sur les risques. La demande suit le cycle de vie standard des messages (SOUMIS → ACCUSÉ DE RÉCEPTION → RÉPONSE → CLÔTURÉ). Le fournisseur répond en acceptant le KRI (avec définition et seuil proposés), en proposant un indicateur alternatif ou en le refusant avec justification. Les KRI validés sont ajoutés à l'annexe spécifique au client.

6.5 Violation et escalade des KRI

Lorsqu'un KRI dépasse le **seuil d'alerte** , le fournisseur doit informer de manière proactive les clients concernés et fournir un commentaire (KRI-13) expliquant la situation et le calendrier de correction prévu.
Lorsqu'un indicateur clé de risque (KRI) atteint le **seuil critique** , le fournisseur doit en informer les clients concernés dans les délais définis à la section 2.4 (délais d'accusé de réception). Le client peut considérer une violation d'un KRI critique comme un motif pour soumettre une demande de service de sécurité (RSC) ciblée sur le domaine concerné.
Une dégradation persistante des KRI (3 périodes de mesure consécutives ou plus en état d'avertissement ou critique) doit être signalée lors du prochain audit de surveillance TPSA et peut être prise en compte dans l'évaluation de conformité de l'organisme de certification.

7. Escalade et résolution des conflits

7.1 Escalade en cas de non-réponse

Si un fournisseur ne répond pas ou n'accuse pas réception dans les délais définis à la section 2.4, la procédure d'escalade suivante s'applique :

1. **Rappel** : le client envoie un rappel officiel faisant référence à la soumission initiale et au temps écoulé. Ce rappel réinitialise le délai de réponse pour un cycle supplémentaire.
2. **Avis d'escalade** : si aucune réponse n'est reçue après le cycle de relance, le client adresse un avis d'escalade au responsable de la conformité désigné du fournisseur (TPSA-01, H-12). Cet avis est consigné comme une violation de protocole.
3. **Impact sur la conformité TPSA** : les avis d'escalade répétés ou non résolus doivent être signalés à l'auditeur de certification TPSA et peuvent affecter le statut d'étiquetage TPSA du fournisseur lors du prochain examen de certification.

La procédure d'escalade est conçue pour être proportionnée. Un seul retard est traité comme un problème opérationnel. Un manquement répété aux exigences constitue un problème de conformité qui affecte l'étiquette du fournisseur.

7.2 Litiges relatifs au contenu

Si le client conteste le contenu d'une évaluation des risques fournisseurs (par exemple, si le client estime que le statut de contrôle « COUVERT » est surestimé), la procédure suivante s'applique :

4. **Demande de clarification** : le client envoie un message de suivi demandant des preuves supplémentaires ou une justification de l’évaluation contestée.
5. **Examen conjoint** : si les éclaircissements sont insuffisants, chaque partie peut demander une séance d'examen conjoint (documentée au format de message TEC) pour discuter de l'évaluation contestée.
6. **Évaluation indépendante** : en cas de litiges non résolus, chaque partie peut faire appel à un évaluateur indépendant (choisi d'un commun accord ou désigné par l'organisme de certification TPSA) pour fournir un avis contraignant sur le statut de contrôle contesté.

Le processus de règlement des différends est volontairement simplifié dans ses premières étapes. La plupart des désaccords devraient être résolus par la clarification et le partage de preuves, sans nécessiter d'évaluation indépendante.

8. Exigences de conformité

8.1 Conformité du fournisseur (niveau AMÉLIORÉ)

Un fournisseur de niveau TPSA ENHANCED doit :

- Accepter les soumissions RSC de tout client muni d'une annexe spécifique au client valide.
- Accuser réception des RSC dans un délai de 10 jours ouvrables.
- Répondre par un SRA complet dans les 30 jours ouvrables suivant l'accusé de réception.
- Tenir un registre de tous les échanges, accessible à l'auditeur de certification TPSA.
- Désignez un contact nommé responsable des opérations du protocole de dialogue sur les risques.
- Prendre en charge au moins un des mécanismes de transport définis (API, courrier électronique chiffré ou échange hors ligne).

8.2 Conformité du fournisseur (niveau complet)

En plus des exigences renforcées, un fournisseur de niveau TPSA complet doit :

- Accuser réception des RSC dans un délai de 5 jours ouvrables.
- Veuillez répondre par un SRA complet dans un délai de 15 jours ouvrables.
- Soutenir les messages de coordination TIBER-EU (TEC) et démontrer la volonté de participer aux exercices TLPT.
- Implémentez l'API de la plateforme de référence TPSA ou un équivalent conforme.
- Mise à jour de la carte de divulgation de déclenchement (TPSA-01) dans les 15 jours lorsque les conclusions de l'analyse des risques de sécurité révèlent des changements importants dans la posture de sécurité.

8.3 Obligations du client

Le protocole de dialogue sur les risques impose également des obligations aux clients :

- Les RSC doivent être **correctement formées** : complètes, référencées aux actifs spécifiques de la fiche de divulgation et utilisant des techniques ATT&CK valides. Les fournisseurs peuvent refuser les RSC non conformes et demander leur correction.
- (RCF) doivent être **proportionnels** : leur nombre doit être proportionnel à l'importance de la relation fournisseur. Le système de certification TPSA peut définir des limites annuelles recommandées pour les RCF, selon le niveau de criticité du fournisseur.
- Les clients doivent fermer les échanges (passer à l'état FERMÉ) dans les 30 jours suivant la réception d'un SRA, ou soumettre une demande de clarification.
- Les renseignements sur les menaces partagés dans les RSC doivent être traités avec la confidentialité appropriée par les deux parties.

Annexe A : Exemple de fiche de scénario de risque

Exemple fictif : un client bancaire soumet un RSC au fournisseur SaaS CloudWorks SAS (de l'exemple TPSA-01) concernant un scénario d'exfiltration de données piloté par APT.

En-tête RSC

Champ	Valeur
Identifiant RSC	f47ac10b-58cc-4372-a567-0e02b2c3d479
Nom du client	Banque Européenne d'Investissement et de Commerce (BEIC)
Fournisseur cible	CloudWorks SAS
Référence de la carte de divulgation	Déclaration commune de CloudWorks v1.2.0 (01/04/2026)
Priorité	HAUT
Contexte réglementaire	Art. 28 de la DORA (risque lié aux TIC pour les tiers), Art. 26 de la DORA (préparation aux tests de transfert de technologie)
Drapeau TIBER-UE	faux (RSC autonome, ne faisant pas partie d'un exercice TLPT à ce stade)

Section A : Identification des sources de risque

ID SR	Type	Description	Objectif (OV)
SR-01	parrainé par l'État	APT38 (sous-groupe Lazarus)	Vols financiers et exfiltration de données ciblant les clients des banques. Compromission avérée de prestataires de services tiers pour accéder aux données financières des clients et aux documents internes.
SR-02	crime organisé	FIN7	Déploiement de rançongiciels et extorsion de données via la compromission de la chaîne d'approvisionnement. Cible fréquemment les plateformes SaaS destinées aux institutions financières.

Contexte sectoriel : BEIC est un établissement de crédit réglementé par la DORA. La plateforme CloudWorks DMP stocke des documents de conformité internes, des rapports d'audit et la correspondance avec les clients. La compromission de ces données pourrait entraîner des sanctions réglementaires, des fuites d'informations concurrentielles et une atteinte à la réputation de l'établissement.

Section B : Scénario stratégique

Champ	Valeur
Titre du scénario	Exfiltration de documents de conformité bancaire par un APT via l'API CloudWorks
Point d'entrée	CW-SRV-01 (DMP App Cluster), passerelle API publique
Chemin d'attaque	SR-01 exploite une vulnérabilité de la passerelle API CloudWorks (CW-SRV-01) pour obtenir un accès initial. L'attaquant se déplace ensuite du cluster d'applications vers la base de données principale (CW-DB-01) afin d'identifier les données des clients de BEIC, puis accède au stockage de documents (CW-STO-01) pour exfiltrer les documents clients chiffrés. L'attaquant déchiffre ensuite les documents à l'aide d'une clé compromise ou exfiltre des objets binaires chiffrés pour un déchiffrement hors ligne.
Actifs cibles	CW-DB-01 (métadonnées, mappage des locataires), CW-STO-01 (documents clients)
Événement redouté	Exfiltration de documents internes de conformité et de correspondance client de BEIC. Notification réglementaire requise en vertu de l'article 19 de la DORA. Risque de sanctions de la CSSF. Atteinte à la réputation auprès des clients institutionnels.
Estimation de l'impact	CRITIQUE

Section C : Scénario opérationnel (MITRE ATT&CK)

Matrice ATT&CK : ENTREPRISE

Étape	Technique	Nom	Tactique	Actif cible	Description
1	T1190	Exploiter une application publique	Accès initial	CW-SRV-01	Exploiter une vulnérabilité zero-day ou une vulnérabilité non corrigée connue dans la passerelle API CloudWorks.
2	T1059.004	Shell Unix	Exécution	CW-SRV-01	Exécutez des commandes sur le conteneur/pod compromis pour énumérer l'environnement Kubernetes.
3	T1078.004	Comptes cloud	Élévation des privilèges	CW-SRV-01	Exploiter des identifiants de compte de service compromis ou des secrets Kubernetes pour élever ses privilèges.
4	T1021.002	Services à distance : partages d’administration SMB/Windows	Mouvement latéral	CW-DB-01	Basculez du cluster d'applications vers le segment de base de données en utilisant des identifiants volés ou la confiance du maillage de services.
5	T1530	Données provenant du stockage cloud	Collection	CW-DB-01	Interrogez la base de données pour identifier l'identifiant du locataire de BEIC et les références documentaires dans l'index.
6	T1560.001	Archive via Utilitaire	Collection	CW-STO-01	Préparer et compresser les documents BEIC à partir du stockage d'objets en vue de leur exfiltration.
7	T1567.002	Exfiltration vers le stockage cloud	Exfiltration	CW-STO-01	Exfiltrer une archive de documents compressés vers un point de terminaison de stockage cloud contrôlé par l'attaquant.

Questions spécifiques du client au fournisseur :

- Étape 1 : Quel est l'état actuel des correctifs de la passerelle API ? Quand a eu lieu la dernière analyse de vulnérabilité des points de terminaison exposés au public ?
- Étape 3 : Les secrets Kubernetes sont-ils chiffrés au repos ? Existe-t-il une détection des secrets en cours d'exécution (par exemple, Falco, KubeArmor) ?
- Étape 4 : La segmentation du réseau est-elle appliquée entre le cluster d'applications et le segment de base de données ? À quel niveau (stratégie réseau, pare-feu, VLAN) ?
- Étape 5 : Les requêtes de base de données au niveau du locataire sont-elles enregistrées et surveillées pour détecter les schémas d'accès anormaux (par exemple, exportation en masse, portée de requête inhabituelle) ?
- Étape 7 : Le trafic sortant du segment de stockage est-il filtré ? Existe-t-il des règles d'alerte pour les transferts de données sortants importants ?

Annexe B : Exemple d’évaluation des risques fournisseurs (extrait)

Réponse de CloudWorks SAS à la fiche de scénarios de risques BEIC (Annexe A). Extrait présentant les étapes 1, 4 et 7.

Étape 1 : T1190, Exploiter une application accessible au public

Champ	Évaluation
État de contrôle	COUVERT
Description des commandes	La passerelle API est protégée par un pare-feu applicatif Cloudflare (règles OWASP Core + règles personnalisées). Le code applicatif fait l'objet d'une analyse SAST (SonarQube) à chaque commit et d'une analyse DAST (OWASP ZAP) hebdomadaire. Une analyse de vulnérabilité externe (Qualys) est effectuée chaque semaine. Les correctifs critiques sont appliqués sous 24 h (SLA). Dernier test d'intrusion externe (Synacktiv, 20/01/2026) : aucune vulnérabilité critique n'a été détectée sur l'API.
Capacité de détection	DÉTECTION, Corrélation entre la journalisation WAF et Wazuh SIEM. Les anomalies dans les schémas d'API déclenchent une alerte en moins de 5 minutes. CrowdStrike Falcon est déployé sur les nœuds de passerelle API.

Étape 4 : T1021.002, Transfert latéral vers la base de données

Champ	Évaluation
État de contrôle	PARTIEL
Description des commandes	La segmentation du réseau entre le cluster d'applications et la base de données utilise les NetworkPolicies Kubernetes (Calico). L'accès à la base de données requiert un certificat mTLS et un mot de passe. Aucun accès SSH direct aux nœuds de la base de données n'est autorisé.
Capacité de détection	PARTIEL — Calico enregistre les connexions refusées. Les connexions acceptées au segment de base de données sont enregistrées, mais ne sont actuellement pas corrélées au comportement de l’application. Un compte de service compromis avec un certificat mTLS valide ne déclencherait pas d’alerte.
Analyse des écarts	Lacune : aucune analyse comportementale des schémas de connexion à la base de données depuis le cluster d’applications. Un pod compromis disposant d’identifiants de service valides pourrait interroger la base de données sans être détecté si le schéma de requête ressemble au comportement normal de l’application.
Plan de remédiation	Action : déployer une solution de surveillance de l’activité des bases de données (DAM) avec profilage de base par compte de service. Outil : Imperva Data Security ou pgAudit + règles Wazuh personnalisées. Objectif : 3e trimestre 2026. Contrôle intermédiaire : examen hebdomadaire des journaux de connexion aux bases de données pour les connexions provenant de zones situées en dehors des plages d’adresses IP habituelles des pods.

Étape 7 : T1567.002, Exfiltration vers le stockage cloud

Champ	Évaluation
État de contrôle	ÉCART
Description des commandes	Le trafic sortant du segment de stockage n'est actuellement ni filtré ni surveillé pour détecter les anomalies de volume. Le service de stockage d'objets nécessite une sortie Internet pour la réplication vers le site de sauvegarde de Francfort (CW-STO-02).
Capacité de détection	BLIND, Aucune alerte concernant le volume de données sortantes du segment de stockage. Les journaux de flux réseau sont collectés mais non analysés pour détecter d'éventuels indicateurs d'exfiltration.
Analyse des écarts	Lacune critique : un attaquant ayant atteint le segment de stockage peut exfiltrer des données sans être détecté. Le trafic de réplication légitime vers FR5 rend difficile la détection des sorties malveillantes sans inspection du contenu.
Plan de remédiation	Action 1 : Mise en place d'une liste blanche de sortie – restriction du trafic sortant du segment de stockage vers le seul point de terminaison de sauvegarde FR5. Échéance : 30 jours (2e trimestre 2026). Action 2 : Déploiement de l'analyse NetFlow avec détection des anomalies de volume sur le segment de stockage. Outil : Suricata + règles Wazuh personnalisées. Échéance : 3e trimestre 2026. Contrôle intermédiaire : examen manuel quotidien des métriques de volume de sortie de CW-STO-01.

Résumé SRA (Extrait)

Champ	Valeur
Évaluation globale	PARTIELLEMENT_ADÉQUANT
Statistiques de couverture	COUVRÉ : 3/7 étapes. PARTIELLEMENT : 2/7 étapes. LARGEUR : 2/7 étapes. NON APPLICABLE : 0.
Risque résiduel	Le chemin d'exfiltration (étapes 6 et 7) représente un risque résiduel important. Un attaquant qui atteint le segment de stockage peut actuellement extraire des données sans être détecté. Le plan de correction vise à combler cette faille d'ici le troisième trimestre 2026. D'ici là, des mesures compensatoires (liste blanche de sortie, vérification manuelle des volumes) réduisent le risque, sans toutefois l'éliminer.
Mise à jour de la carte de divulgation	Oui. La déclaration commune TPSA-01 sera mise à jour vers la version 1.3.0 pour refléter le déploiement du DAM (mise à jour D4-07) et les contrôles de sortie (nouveau contrôle supplémentaire D2) une fois mis en œuvre.