Manuel du participant TISAX

Réalisez le processus d'évaluation TISAX et partagez le résultat d'évaluation avec votre partenaire

Publié par

ENX Association
une association conforme à la loi française de 1901,
enregistrée sous le numéro w923004198 auprès de la sous-préfecture de Boulogne-Billancourt, France

Adresses
20 rue Barthélémy Danjou, 92100 Boulogne-Billancourt, France
Bockenheimer Landstraße 97-99, 60325 Francfort-sur-le-Main, Allemagne

Auteur

Florian Gleich

Contact

tisax@enx.com
+49 69 9866927-77

Version

Date :	2023-12-07
Version :	2.7
Classification :	Public
ENX doc ID:	602-FR

Avis de droit d’auteur

Tous droits réservés par ENX Association.
ENX, TISAX et leurs logos respectifs sont des marques déposées d’ENX Association.
Les marques de tiers mentionnées sont la propriété de leurs détenteurs respectifs.

Table des matières

1. Aperçu . . . 8
1.1. Objectif . . . 8
1.2. Périmètre . . . 8
1.3. Public . . . 9
1.4. Structure . . . 9
1.5. Comment utiliser le présent document . . . 9
1.6. Nous contacter . . . 10
1.7. Le manuel du participant TISAX dans d'autres langues et formats . . . 10
1.7.1. À propos de la traduction en Français . . . 13
1.7.2. À propos du format en ligne . . . 13
1.7.3. À propos du format hors ligne . . . 13
1.7.4. À propos du format PDF . . . 14
2. Introduction . . . 15
2.1. Pourquoi TISAX ? . . . 15
2.2. Qui définit la notion de « sécurisé » ? . . . 15
2.3. Dans le secteur automobile . . . 16
2.4. Comment prouver efficacement la sécurité ? . . . 16
3. Le processus TISAX . . . 18
3.1. Aperçu . . . 18
3.2. Inscription . . . 19
3.3. Évaluation . . . 19
3.4. Échange . . . 20
4. Inscription (étape 1) . . . 21
4.1. Aperçu . . . 21
4.2. Vous êtes un participant TISAX . . . 21
4.3. Préparation de l'inscription . . . 24
4.3.1. Le fondement juridique . . . 24
4.3.2. Le périmètre d'évaluation TISAX . . . 25
4.3.2.1. Description du périmètre . . . 26
4.3.2.2. Périmètre d'évaluation standard . . . 26
4.3.2.3. Détermination du périmètre . . . 27
4.3.2.4. Adaptation du périmètre . . . 28
4.3.2.5. Sites du périmètre . . . 30
4.3.2.6. Nom du périmètre . . . 33
4.3.2.7. Contacts . . . 34

4.3.2.8. Publication et partage . . . 35
4.3.3. Objectifs d'évaluation . . . 37
4.3.3.1. Liste des objectifs de l'évaluation . . . 38
4.3.3.2. Objectifs d'évaluation et ISA . . . 40
4.3.3.3. Objectifs d'évaluation et labels TISAX . . . 40
4.3.3.4. Sélection de l'objectif d'évaluation . . . 41
4.3.3.5. Besoins de protection et niveaux d'évaluation . . . 45
4.3.3.6. Les objectifs d'évaluation et vos propres fournisseurs . . . 50
4.3.4. Frais . . . 51
4.4. Portail ENX . . . 53
4.5. Processus d'inscription en ligne . . . 53
4.5.1. Temps nécessaire . . . 53
4.5.2. Démarrez ici . . . 54
4.5.3. Compte sur le portail . . . 54
4.5.4. Inscription du participant . . . 55
4.5.5. Contact de participant . . . 55
4.5.6. Conditions générales . . . 56
4.5.7. Inscription du périmètre d'évaluation . . . 56
4.5.8. E-mail de confirmation . . . 59
4.5.8.1. Participant ID Participant ID (ID de participant) . . . 60
4.5.8.2. Scope ID (ID de périmètre) . . . 61
4.5.9. Informations de statut . . . 62
4.5.10. Modifications de vos informations d'inscription . . . 65
5. Évaluation (étape 2) . . . 66
5.1. Aperçu . . . 66
5.2. Auto-évaluation basée sur l'ISA . . . 66
5.2.1. Téléchargement du document ISA . . . 67
5.2.2. Compréhension du document ISA . . . 67
5.2.2.1. Catalogues de critères . . . 67
5.2.2.2. Chapitres . . . 75
5.2.2.3. Questions de contrôle . . . 76
5.2.2.4. Champs du formulaire d'auto-évaluation . . . 76
5.2.2.5. Objectif . . . 77
5.2.2.6. Exigences . . . 78
5.2.2.7. Niveaux de maturité . . . 78
5.2.3. Réalisation de l'auto-évaluation . . . 80
5.2.4. Interprétation du résultat d'auto-évaluation . . . 81

5.2.4.1. Analyse . . . 81
5.2.4.2. Le niveau de maturité cible (au niveau questions) . . . 85
5.2.4.3. Votre résultat (au niveau questions) . . . 85
5.2.4.4. La cible (au niveau note) . . . 88
5.2.4.5. Votre résultat (au niveau note) . . . 90
5.2.4.6. Êtes-vous prêt ? . . . 91
5.2.5. Traitement du résultat d'auto-évaluation . . . 93
5.3. Sélection de l'auditeur . . . 94
5.3.1. Informations de contact . . . 95
5.3.2. Couverture . . . 95
5.3.3. Demande d'offres . . . 95
5.3.4. Évaluation des offres . . . 96
5.4. Processus d'évaluation TISAX . . . 98
5.4.1. Aperçu . . . 98
5.4.2. Réunion de lancement . . . 98
5.4.3. Types d'évaluation TISAX . . . 99
5.4.4. Éléments de l'évaluation TISAX . . . 100
5.4.5. À propos de la conformité . . . 100
5.4.6. Votre préparation pour le processus d'évaluation TISAX . . . 103
5.4.7. Évaluation initiale . . . 103
5.4.7.1. La première réunion d'ouverture officielle . . . 104
5.4.7.2. Procédure d'évaluation . . . 104
5.4.7.3. Réunion de clôture . . . 104
5.4.7.4. Rapport d'évaluation TISAX . . . 104
5.4.8. Préparation du plan d'action corrective . . . 105
5.4.9. Évaluation du plan d'action corrective . . . 106
5.4.9.1. Raisons d'une évaluation du plan d'action corrective . . . 107
5.4.9.2. Combinaison avec l'évaluation initiale . . . 107
5.4.9.3. Exigences concernant le plan d'action corrective . . . 107
5.4.9.4. Labels TISAX provisoires . . . 108
5.4.10. Évaluation de suivi . . . 109
5.4.10.1. Calendrier . . . 109
5.4.10.2. Conditions préalables . . . 109
5.4.10.3. Expiration des labels TISAX provisoires . . . 109
5.4.11. Diagramme du processus d'évaluation TISAX . . . 109
5.4.12. Assessment ID (ID d'évaluation) . . . 113
5.4.13. Rapport d'évaluation TISAX . . . 114

5.4.14. Labels TISAX . . . 115
5.4.14.1. Hiérarchie des labels TISAX . . . 116
5.4.14.2. Période de validité des labels TISAX . . . 117
5.4.14.3. Renouvellement des labels TISAX . . . 117
6. Échange (étape 3) . . . 119
6.1. Principe . . . 119
6.2. La plateforme d'échange . . . 119
6.3. Conditions générales . . . 119
6.4. Permanence des résultats échangés . . . 120
6.5. Niveaux de partage . . . 120
6.6. Publier le résultat de votre évaluation sur la plateforme d'échange . . . 121
6.7. Partager le résultat de votre évaluation avec un partenaire particulier . . . 122
6.7.1. Conditions préalables . . . 123
6.7.2. Comment créer une autorisation de partage . . . 124
6.8. Partager le résultat de votre évaluation en dehors de TISAX . . . 125
6.8.1. Les raisons d'une gestion stricte du mécanisme d'échange . . . 125
6.8.2. Un guide concernant les références écrites publiques à TISAX . . . 125
6.8.3. Partage avec un partenaire qui n'est pas encore participant TISAX . . . 126
6.8.4. Partage avec des salariés de votre partenaire qui n'ont pas d'accès direct au portail ENX . . . 126
7. Annexes . . . 128
7.1. Annexe : exemple de facture . . . 128
7.2. Annexe : exemple d'e-mail de confirmation . . . 129
7.3. Annexe : exemple d'extrait de périmètre TISAX . . . 130
7.4. Annexe : Participant status (Statut du participant) . . . 131
7.4.1. Aperçu : Participant status (Statut du participant) . . . 131
7.4.2. Participant status "Incomplete" (Statut du participant « Incomplet ») . . . 133
7.4.3. Participant status "Awaiting approval" (Statut du participant « En attente d'approbation ») . . . 134
7.4.4. Participant status "Preliminary" (Statut du participant « Préliminaire ») . . . 134
7.4.5. Participant status "Registered" (Statut du participant « Inscrit ») . . . 136
7.4.6. Participant status "Expired" (Statut du participant « Expiré ») . . . 137
7.5. Annexe : Assessment scope status (Statut du périmètre d'évaluation) . . . 137
7.5.1. Aperçu : Assessment scope status (Statut du périmètre d'évaluation) . . . 137
7.5.2. Assessment scope status "Incomplete" (Statut du périmètre d'évaluation « Incomplet ») . . . 139
7.5.3. Assessment scope status "Awaiting your order" (Statut du périmètre

d’évaluation « En attente de votre commande ») . . . 140
7.5.4. Assessment scope status “Awaiting ENX approval” (Statut du périmètre d’évaluation « En attente d’approbation ENX ») . . . 140
7.5.5. Assessment scope status “Awaiting your payment” (Statut du périmètre d’évaluation « En attente de votre paiement ») . . . 142
7.5.6. Assessment scope status “Registered” (Statut du périmètre d’évaluation « Inscrit ») . . . 143
7.5.7. Assessment scope status “Active” (Statut du périmètre d’évaluation « Actif ») . . . 143
7.5.8. Assessment scope status “Expired” (Statut du périmètre d’évaluation « Expiré ») . . . 143
7.6. Annexe : Assessment status (Statut de l’évaluation) . . . 145
7.6.1. Aperçu : Assessment status (Statut de l’évaluation) . . . 145
7.6.2. Assessment status “Initial assessment ordered” (Statut de l’évaluation « Évaluation initiale commandée ») . . . 147
7.6.3. Assessment status “Initial assessment ongoing” (Statut de l’évaluation « Évaluation initiale en cours ») . . . 147
7.6.4. Assessment status “Waiting for corrective action plan assessment” (Statut de l’évaluation « En attente de l’évaluation du plan d’action corrective ») . . . 148
7.6.5. Assessment status “Waiting for follow-up” (Statut de l’évaluation « En attente de suivi ») . . . 149
7.6.6. Assessment status “Finished” (Statut de l’évaluation « Terminé ») . . . 149
7.7. Annexe : pourquoi nous déconseillons les « pré-évaluations » et les « analyses de l’écart » . . . 149
7.8. Annexe : périmètres d’évaluation sur mesure . . . 151
7.8.1. Périmètre d’évaluation étendu sur mesure . . . 151
7.8.2. Périmètre d’évaluation entièrement sur mesure . . . 152
7.9. Annexe : gestion du cycle de vie des données du participant . . . 153
7.9.1. Perte d’accès aux données du participant (portail ENX) . . . 153
7.9.2. Administration des contacts . . . 153
7.9.2.1. Comment ajouter un nouveau contact . . . 153
7.9.2.2. Comment supprimer un contact existant . . . 154
7.9.2.3. Comment modifier les détails d’un contact existant . . . 154
7.9.3. Administration des sites . . . 154
7.9.3.1. Comment demander la modification du nom de votre entreprise . . . 155
7.9.3.2. Comment demander la modification d’un site . . . 156
7.9.3.3. Comment demander la modification d’un nom de rue . . . 157
7.9.3.4. Comment ajouter un site supplémentaire . . . 158

7.10. Annexe : évaluation d'extension du périmètre . . . 158
7.11. Annexe : gestion du cycle de vie de l'ISA . . . 159
7.12. Annexe : documents utiles . . . 159
7.13. Annexe : gestion des réclamations . . . 160
7.13.1. Causes de réclamation . . . 160
7.13.1.1. Réclamations concernant ENX Association . . . 160
7.13.1.2. Réclamations concernant les auditeurs . . . 160
7.13.1.3. Conditions pour formuler une réclamation . . . 161
7.13.2. Contact pour les réclamations . . . 162
8. Historique du document . . . 163

1. Aperçu

1.1. Objectif

Bienvenue sur TISAX (Trusted Information Security Assessment Exchange).

L'un de vos partenaires vous a demandé d'attester que votre gestion de la sécurité de l'information respecte un niveau particulier d'exigence, comme prévu par « l'évaluation de sécurité de l'information » (ISA). Et à présent, vous souhaitez savoir comment répondre à cette demande.

L'objectif du présent manuel est de vous permettre de satisfaire la demande de votre partenaire — ou d'avoir une longueur d'avance en anticipant la démarche avant qu'un partenaire ne vous invite à l'effectuer.

Le présent manuel décrit les étapes que vous devez mettre en œuvre pour passer l'évaluation TISAX et pour en partager le résultat avec votre partenaire.

L'établissement et le maintien d'un système de gestion de la sécurité de l'information (ISMS) constituent déjà des missions complexes. Prouver à votre partenaire que votre gestion de la sécurité de l'information est à la hauteur ajoute encore plus de complexité. Le présent manuel ne vous aidera pas à gérer la sécurité de vos informations. Toutefois, il vous permet de démontrer le plus simplement possible à votre partenaire les efforts mis en œuvre dans ce contexte.

1.2. Périmètre

Le présent manuel s'applique à tous les processus TISAX auxquels vous pouvez participer.

Il contient tout ce que vous avez besoin de savoir pour mener à bien le processus TISAX.

Le manuel prodigue des conseils sur la manière de traiter les exigences en matière de sécurité de l'information qui représentent le fondement de l'évaluation. Mais il n'a pas pour objectif de vous offrir une formation générale sur ce que vous devez faire pour passer l'évaluation de sécurité de l'information.

1.3. Public

Les entreprises qui ont besoin ou souhaitent prouver un certain niveau de gestion de sécurité de l'information, conformément aux exigences de « l'évaluation de sécurité de l'information » (ISA), constituent le principal public auquel s'adresse le présent manuel.

Dès que vous serez activement impliqué dans les processus TISAX, vous pourrez profiter des informations fournies dans le présent manuel.

Les entreprises qui demandent à leurs fournisseurs de prouver certains niveaux de gestion de la sécurité de l'information en tireront profit également. Le présent manuel leur permet de comprendre ce que leurs fournisseurs sont tenus de faire pour répondre à leur demande.

1.4. Structure

Nous commencerons par une brève introduction à TISAX, puis nous passerons immédiatement aux instructions décrivant COMMENT entreprendre les diverses démarches. Vous trouverez tout ce dont vous avez besoin pour mener à bien le processus — dans l'ordre correspondant aux diverses étapes à suivre.

Le temps de lecture estimé du document est de 75 à 90 minutes.

1.5. Comment utiliser le présent document

Tôt ou tard, vous vous intéresserez probablement à la plupart des informations décrites dans le présent document. Pour que vous soyez correctement préparé, nous vous recommandons de lire l'intégralité du manuel.

Nous avons organisé le manuel sur la base de trois étapes principales du processus TISAX, de sorte que vous puissiez aller à la section dont vous avez besoin et lire le reste plus tard.

Le manuel utilise des illustrations pour faciliter la compréhension. Les couleurs des illustrations ont souvent une signification supplémentaire. Par conséquent, nous vous recommandons de lire le document sur un écran d'ordinateur ou sur une version papier en couleur.

Nous serions heureux de recevoir vos commentaires. Si vous pensez qu'il manque certaines informations dans le présent manuel ou qu'il n'est pas facile à comprendre, n'hésitez pas à nous en informer. Tous les futurs lecteurs du manuel et nous-mêmes vous serons reconnaissants du retour que vous nous donnerez.

Si vous avez déjà utilisé une version antérieure du manuel du participant TISAX, vous pourrez trouver quelques précieuses remarques à la fin du document à la Section 8, “Historique du document”.

1.6. Nous contacter

Nous sommes là pour vous guider tout au long du processus TISAX et pour répondre à toute question que vous pourriez avoir.

Envoyez-nous un e-mail à :	tisax@enx.com
Ou appelez-nous au numéro :	+49 69 9866927-77

Vous pouvez nous joindre durant les heures ouvrables normales en Allemagne (UTC+01:00).

Nous parlons tous l’anglais et l’allemand. L’un de nos collègues est de langue maternelle italienne.

Veuillez consulter la Section 7.13, “Annexe : gestion des réclamations”.

1.7. Le manuel du participant TISAX dans d’autres langues et formats

Le manuel du participant TISAX est disponible dans les autres langues et formats suivants :

Langue	Version	Format	Lien
Anglais	2.7	En ligne	https://www.enx.com/handbook/tisax-participant-handbook.html
		Hors ligne	https://www.enx.com/handbook/tisax-participant-handbook-offline.html
		PDF	https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf

Langue	Version	Format	Lien
Allemand	2.7	En ligne	https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html
		Hors ligne	https://www.enx.com/handbook/tisax-teilnehmerhandbuch-offline.html
		PDF	https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf
Français	2.7	En ligne	https://www.enx.com/handbook/tph-fr.html
		Hors ligne	https://www.enx.com/handbook/tph-fr-offline.html
		PDF	https://www.enx.com/handbook/tph-fr.pdf
Chinois	2.7	En ligne	https://www.enx.com/handbook/tph-cn.html
		Hors ligne	https://www.enx.com/handbook/tph-cn-offline.html
		PDF	https://www.enx.com/handbook/tph-cn.pdf
Espagnol	2.7	En ligne	https://www.enx.com/handbook/tph-es.html
		Hors ligne	https://www.enx.com/handbook/tph-es-offline.html
		PDF	https://www.enx.com/handbook/tph-es.pdf
Japonais	2.7	En ligne	https://www.enx.com/handbook/tph-jp.html
		Hors ligne	https://www.enx.com/handbook/tph-jp-offline.html
		PDF	https://www.enx.com/handbook/tph-jp.pdf
Portugais brésilien	2.7	En ligne	https://www.enx.com/handbook/tph-pt.html
		Hors ligne	https://www.enx.com/handbook/tph-pt-offline.html
		PDF	https://www.enx.com/handbook/tph-pt.pdf
Italien	2.7	En ligne	https://www.enx.com/handbook/tph-it.html
		Hors ligne	https://www.enx.com/handbook/tph-it-offline.html
		PDF	https://www.enx.com/handbook/tph-it.pdf

Langue	Version	Format	Lien
Coréen	2.7	En ligne	https://www.enx.com/handbook/tph-kr.html
		Hors ligne	https://www.enx.com/handbook/tph-kr-offline.html
		PDF	https://www.enx.com/handbook/tph-kr.pdf

Remarque importante :

La version anglaise est la version principale.
Les versions disponibles dans toutes les autres langues sont des traductions de la version anglaise.
En cas de doute, la version anglaise fait autorité.

1.7.1. À propos de la traduction en Français

Le présent manuel du participant TISAX est une traduction de la version anglaise.

Tous les documents de base de TISAX ont été rédigés en anglais (p. ex. : tous les contrats et exigences pour les auditeurs TISAX). Par conséquent, votre partenaire ou votre auditeur peut utiliser certains termes spécifiques à TISAX en anglais.

Pour vous permettre d'établir une correspondance entre les termes d'une langue à l'autre, nous avons conservé le terme TISAX original en anglais dans la traduction du manuel du participant TISAX ou l'avons mentionné entre parenthèses directement après la traduction.

1.7.2. À propos du format en ligne

Chaque section a un identifiant unique (format : ID1234).
Un ID fait référence à une section spécifique, indépendamment de la langue.

Si vous souhaitez accéder à une section spécifique, vous pouvez :

- faire un clic droit sur le titre de la section et copier le lien, ou
- cliquer sur le titre de la section et copier le lien à partir de la barre d'adresse de votre navigateur.

La plupart des illustrations sont disponibles dans une taille supérieure à celle affichée ici par défaut. Cliquez sur l'illustration pour accéder à sa version de taille supérieure.

1.7.3. À propos du format hors ligne

Le format hors ligne contient la plupart des éléments du format en ligne. Notez en particulier que les illustrations sont intégrées dans le fichier HTML. Vous n'avez besoin que d'un fichier pour utiliser le format hors ligne.

Par rapport au format en ligne, le format hors ligne ne contient pas :

- les images de taille supérieure
- les polices originales du format en ligne
  Les polices sont définies selon les réglages par défaut de votre navigateur.

1.7.4. À propos du format PDF

Si vous utilisez le format PDF sur votre ordinateur, vous pouvez toujours cliquer sur l'ensemble des références. Mais si vous imprimez la version PDF, vous ne retrouverez pas certains éléments tels que la numérotation des pages, et vous devrez rechercher les références vous-même.

2. Introduction

Les sections suivantes présentent le concept TISAX.

Si vous êtes pressé, vous pouvez les passer et commencer directement à la Section 4.3, “Préparation de l’inscription”.

2.1. Pourquoi TISAX ?

Ou en d’autres termes, que faites-vous ici ?

Pour répondre à cette question, nous commencerons par quelques réflexions sur la pratique commerciale en général et sur la protection des informations en particulier.

Vous avez un partenaire. Il détient des informations confidentielles et souhaite les partager avec son fournisseur — vous. La coopération entre votre partenaire et vous-même crée de la valeur. Les informations que votre partenaire partage avec vous constituent une part importante de cette création de valeur. Par conséquent, il souhaite les protéger de manière appropriée. Et il veut être certain que vous traitez ses informations avec le même soin.

Mais comment peut-il être sûr que ses informations sont entre de bonnes mains ? Il ne peut pas se contenter de vous « croire ». Votre partenaire a besoin de voir certaines preuves.

Deux questions se posent dans ce contexte. Qui définit la notion de traitement « sécurisé » de l’information ? Et deuxièmement, comment en apportez-vous la preuve ?

2.2. Qui définit la notion de « sécurisé » ?

Votre partenaire et vous-même n’êtes pas les seuls à être confrontés à ces questions pour la première fois. Chacun ou presque doit y répondre et la plupart des réponses présenteront des points communs.

Ainsi, standardiser la démarche permet d’éviter de devoir créer une solution au cas par cas pour un problème récurrent et de démarrer systématiquement d’une feuille blanche. Créer une norme représente un travail considérable, mais une fois cette norme définie, tous ceux qui la suivent pourront en profiter à chaque fois.

Il existe certainement différents points de vue concernant la démarche adéquate à adopter pour protéger les informations. Mais en raison des avantages susmentionnés, la plupart des entreprises misent sur l’approche normative. Une norme est la forme condensée de toutes les bonnes pratiques prouvées et éprouvées pour une problématique particulière.

Dans votre cas, des normes telles que la norme ISO/IEC 27001 (concernant les systèmes de gestion de la sécurité de l’information, ou ISMS) et leur mise en œuvre déterminent comment traiter les informations confidentielles de manière sécurisée et dans les règles de l’art. Une

norme telle que celle-là vous évite de devoir réinventer la roue à chaque fois. Mais plus important encore, les normes fournissent une base commune à deux entreprises qui doivent échanger des données confidentielles.

2.3. Dans le secteur automobile

Par nature, les normes indépendantes d'un secteur particulier sont conçues comme des solutions universelles et ne sont pas adaptées aux besoins spécifiques des sociétés automobiles.

Il y a longtemps, des associations ont vu le jour dans l'industrie automobile pour — entre autres — affiner et définir des normes adaptées aux besoins plus spécifiques du secteur. La « Verband der Automobilindustrie » (VDA) est l'une de ces associations. Dans le groupe de travail qui traite de la sécurité de l'information, plusieurs membres de l'industrie automobile sont arrivés à la conclusion qu'ils avaient des besoins similaires auxquels il conviendrait d'adapter les normes existantes en matière de gestion de la sécurité de l'information.

Leurs efforts conjoints ont donné lieu à la création d'un questionnaire qui couvre les exigences relatives à la sécurité de l'information largement reconnues dans l'industrie automobile. Il s'intitule « Information Security Assessment » (« Évaluation de la sécurité de l'information ») ou « ISA ».

Grâce à l'ISA, nous disposons désormais d'une réponse à la question « Qui définit la notion de "sécurisé" ? ». Par l'intermédiaire de la VDA, l'industrie automobile elle-même offre cette réponse à ses membres.

2.4. Comment prouver efficacement la sécurité ?

Si certaines entreprises recourent à l'ISA en interne uniquement, d'autres l'emploient pour évaluer la maturité de la gestion de la sécurité de l'information chez leurs fournisseurs. Dans certains cas, une auto-évaluation suffit dans le cadre de la relation commerciale. Toutefois, dans d'autres cas, les entreprises évaluent dans son intégralité la gestion de la sécurité de l'information de leur fournisseur (y compris par des audits sur site).

À l'heure où nous sommes tous de plus en plus sensibles à la nécessité de gérer la sécurité de l'information et où l'ISA est adoptée par un nombre croissant d'entreprises pour effectuer des évaluations dans ce cadre, les fournisseurs sont plus nombreux à faire face à des demandes similaires de la part de différents partenaires.

Ces partenaires continuaient d'appliquer des normes variées et avaient des opinions divergentes sur leur interprétation. Et si les fournisseurs devaient pour l'essentiel attester des mêmes choses, les démarches adoptées étaient différentes.

Plus les fournisseurs étaient invités par leurs partenaires à prouver leur niveau de gestion de la sécurité de l'information, plus ils se plaignaient des efforts répétés à fournir. Il est tout simplement contre-productif de devoir démontrer, audit après audit, les mêmes mesures de

gestion de la sécurité de l'information.

Que faire pour rendre la démarche plus efficace ? Pourrait-on imaginer de réutiliser le rapport d'un auditeur pour plusieurs partenaires ?

Les OEM et les fournisseurs dans le groupe de travail ENX responsable du maintien de l'ISA ont été attentifs aux plaintes de leurs fournisseurs. À présent, ils offrent à ces derniers ainsi qu'à l'ensemble des autres entreprises actives dans l'industrie automobile une réponse à la question « Comment prouver la sécurité? ».

La réponse est TISAX, l'acronyme de "Trusted Information Security Assessment Exchange" (« Échange fiable concernant l'évaluation de la sécurité de l'information »).

3. Le processus TISAX

3.1. Aperçu

Généralement[1], le processus TISAX débute après que l'un de vos partenaires vous a demandé de démontrer un certain niveau de gestion de la sécurité de l'information, conformément aux exigences de l'« Évaluation de la sécurité de l'information » (ISA). Pour répondre à cette demande, vous devez compléter les trois étapes du processus TISAX. La présente section vous donne un aperçu des étapes à suivre.

Le processus TISAX comprend les trois étapes suivantes :

Illustration 1. Aperçu du processus TISAX

1. Étape 1
   Inscription
2. Étape 2
   Évaluation
3. Étape 3
   Échange

1. Inscription
   Nous collectons des informations sur votre entreprise et sur les besoins à intégrer à l'évaluation.
2. Évaluation
   Vous vous soumettez à une ou plusieurs évaluations menées par l'un de nos auditeurs TISAX.
3. Échange
   Vous partagez le résultat de votre évaluation avec votre partenaire.

Chaque étape est subdivisée en sous-étapes. Celles-ci sont exposées dans les trois sections ci-dessous et décrites en détail plus loin, dans les sections correspondantes.

Remarque :

Nous voudrions pouvoir vous préciser le temps nécessaire à l'obtention du résultat de votre évaluation TISAX, mais ne sommes pas en mesure de vous donner un chiffre précis et fiable. La durée totale du processus TISAX dépend de trop nombreux facteurs. La grande diversité des tailles d'entreprise et des

> objectifs d'évaluation, sans compter la maturité d'un système de gestion de la sécurité de l'information, rendent impossible la fourniture d'une indication précise sur le temps nécessaire à l'évaluation.

3.2. Inscription

Votre première étape est l'inscription TISAX.

L'objectif principal de l'inscription TISAX est de collecter des informations sur votre entreprise. Nous utilisons un processus d'inscription en ligne pour vous aider à nous fournir ces informations.

Elle est la condition préalable à toutes les étapes ultérieures. Des frais d'inscription vous sont demandés.

Au cours du processus d'inscription en ligne :

- Nous vous demandons vos coordonnées et des informations de facturation.
- Vous devez accepter nos conditions générales.
- Vous pouvez définir le périmètre de votre évaluation de sécurité de l'information.

Pour entamer directement cette étape, veuillez vous référer à la Section 4, "Inscription (étape 1)".

Le processus d'inscription en ligne est décrit en détail à la Section 4.5, "Processus d'inscription en ligne". Mais si vous souhaitez commencer immédiatement, veuillez vous rendre sur le enx.com/en-US/TISAX/.

3.3. Évaluation

L'évaluation de sécurité de l'information constitue votre deuxième étape.

Elle se subdivise en quatre sous-étapes :

a. Préparation de l'évaluation
   Vous devez préparer l'évaluation. L'ampleur de la préparation dépend du niveau de maturité actuel de votre système de gestion de la sécurité de l'information. Votre préparation doit se fonder sur le catalogue ISA.
b. Sélection de l'auditeur
   Vous devez choisir l'un de nos auditeurs TISAX.
c. Évaluation(s) de la sécurité de l'information
   Votre auditeur mènera l'évaluation sur la base d'un périmètre d'évaluation correspondant aux exigences de votre partenaire. Le processus d'évaluation comprendra au moins l'audit

initial.
Si votre entreprise ne réussit pas immédiatement l'évaluation, le processus d'évaluation peut nécessiter des étapes supplémentaires.

d. Résultat de l'évaluation
Une fois que votre entreprise aura passé l'évaluation, votre auditeur vous fournira le rapport d'évaluation officiel TISAX. Le résultat de votre évaluation vous permettra également d'obtenir des labels TISAX[2].

Pour de plus amples informations sur cette étape, veuillez consulter la Section 5, "Évaluation (étape 2)".

3.4. Échange

Votre troisième et dernière étape consiste à partager le résultat de votre évaluation avec votre partenaire. Le contenu du rapport d'évaluation TISAX est organisé en niveaux. Vous pouvez déterminer le niveau maximum auquel votre partenaire aura accès.

Le résultat de votre évaluation est valable trois ans. En admettant que vous soyez toujours un fournisseur de votre partenaire à ce moment-là, vous devrez à nouveau suivre le processus en trois étapes[3].

Pour de plus amples informations sur cette étape, veuillez consulter la Section 6, "Échange (étape 3)".

Maintenant que vous avez une idée générale du processus TISAX, vous trouverez dans les prochaines sections des instructions sur la manière de mener à bien chaque étape.

4. Inscription (étape 1)

Le temps de lecture estimé de la section consacrée à l'inscription est de 30 à 40 minutes.

4.1. Aperçu

L'inscription TISAX est votre première étape. Elle est la condition préalable à toutes les étapes ultérieures.

Les sections suivantes vous guideront tout au long du processus d'inscription.

1. Nous commencerons par expliquer un nouveau terme essentiel.
2. Ensuite, nous vous donnerons des conseils pour vous aider à vous préparer pour le processus d'inscription en ligne.
3. Nous vous guiderons alors tout au long du processus d'inscription en ligne.

4.2. Vous êtes un participant TISAX

Permettez-nous d'abord de présenter un nouveau terme indispensable à comprendre. Jusqu'à présent, vous étiez un « fournisseur ». Vous êtes ici pour répondre à une exigence de votre « client ». Toutefois, TISAX elle-même ne fait pas vraiment de distinction entre ces deux rôles. Pour TISAX, chaque partie inscrite est un « participant ». Vous — tout comme votre partenaire — « participez » à l'échange des résultats d'évaluation de la sécurité de l'information.

Illustration 2. Inscription pour devenir un participant TISAX

1. Votre entreprise
2. Inscription TISAX
3. Participant TISAX

Pour distinguer d'emblée les deux rôles, nous vous désignons, en tant que fournisseur, « participant actif ». Nous désignons votre partenaire « participant passif ». En tant que « participant actif », vous passez l'évaluation TISAX et partagez le résultat de votre évaluation avec d'autres participants. Le « participant passif » est celui qui a demandé que vous passiez l'évaluation TISAX. Le « participant passif » reçoit le résultat de votre évaluation.

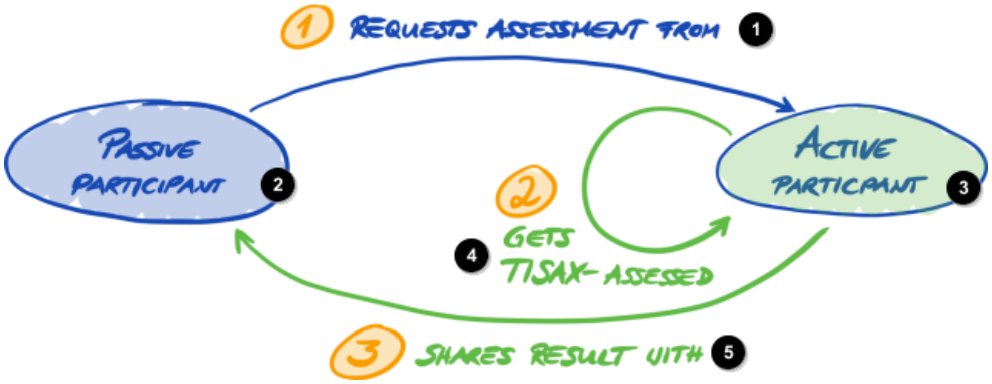


Illustration 3. Participant passif et participant actif

1. 1 Demande l'évaluation du
2. Participant passif
3. Participant actif
4. 2 Passe l'évaluation TISAX
5. 3 Partage le résultat avec

Toute entreprise peut revêtir les deux rôles. Vous pouvez partager un résultat d'évaluation avec votre partenaire, et demander simultanément à vos propres fournisseurs de passer l'évaluation TISAX.

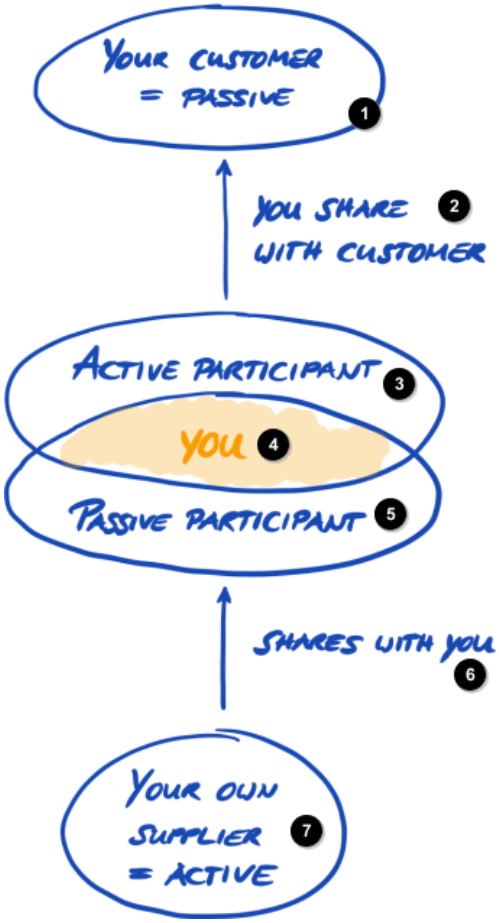


Illustration 4. Les participants TISAX peuvent être simultanément participants actifs et passifs

1. Votre client
   = passif
2. Vous partagez avec le client
3. Participant actif
4. Vous
5. Participant passif
6. Partage avec vous
7. Votre propre fournisseur
   = actif

Le fait de demander à vos propres fournisseurs de passer l'évaluation TISAX peut même être particulièrement conseillé s'ils traitent eux aussi des informations présentant des besoins de protection de votre partenaire.

4.3. Préparation de l’inscription

Dans la présente section, nous vous donnons des recommandations sur la manière de vous *préparer* à l’inscription. Nous décrivons le processus d’inscription en tant que tel en détail à la Section 4.5, “Processus d’inscription en ligne”.

Avant d’entamer le processus d’inscription en ligne, nous vous recommandons vivement :

- de collecter des informations à l’avance
- et de prendre certaines décisions.

4.3.1. Le fondement juridique

Généralement, vous devez signer deux contrats. Le premier contrat est conclu entre vous et ENX Association : les « Conditions générales de participation TISAX » (TISAX Participation General Terms and Conditions) ou « CG du participant TISAX » (TISAX Participant GTCs). Le second contrat est conclu entre l’un de nos auditeurs TISAX et vous. Pour l’inscription, nous ne vérifierons que le premier contrat.

Les CG du participant TISAX régissent nos relations mutuelles et vos relations avec d’autres participants TISAX. Elles déterminent nos droits et obligations à tous. Outre les clauses habituelles que vous trouvez dans la plupart des contrats, elles définissent le traitement des informations échangées et obtenues durant le processus TISAX. Un objectif majeur de ces règles est de respecter la confidentialité des résultats de l’évaluation TISAX. Comme tous les participants TISAX sont soumis aux mêmes règles, vous pouvez attendre de votre partenaire (en sa qualité de participant passif) qu’il protège adéquatement le résultat de votre évaluation TISAX.

Assez rapidement dans le processus d’inscription en ligne, nous vous demanderons d’accepter les CG du participant TISAX. Comme il s’agit d’un vrai contrat, nous vous recommandons de lire les CG du participant TISAX avant d’entamer le processus d’inscription en ligne. L’une des raisons en est que, selon votre rôle dans l’entreprise, il se peut que vous deviez obtenir une autorisation d’un juriste interne ou externe.

Vous pouvez télécharger les « Conditions générales de participation TISAX »[4] sur notre site Web à l’adresse :
enx.com/en-US/TISAX/downloads/

Téléchargement direct du PDF :
enx.com/tisaxgtcen.pdf

Au cours du processus d’inscription en ligne, nous vous demanderons de cocher deux cases obligatoires :

 We accept the TISAX Participation General Terms and Conditions (Nous acceptons les

Conditions générales de participation TISAX)

- ☐ We confirm knowledge of Applicant's release of Audit Providers' professional duties of secrecy acc. to Sec. IX.5. and X.3 of the TISAX Participation General Terms and Conditions; (🇫🇷 Nous confirmons avoir connaissance du fait que le demandeur est libéré du secret professionnel imposé aux auditeurs conformément aux sections IX.5 et X.3 des Conditions générales de participation TISAX)

Nous avons ajouté la seconde case à cocher, car certains de nos auditeurs TISAX sont des experts-comptables agréés. Ils sont tenus à des exigences particulières en matière de secret professionnel. Généralement, en vertu des exigences particulières en matière de secret professionnel, les experts-comptables agréés figurant parmi nos auditeurs ne sont pas autorisés à partager les informations avec nous. Dans ce cas précis, cela annulerait les options de contrôle dont nous avons besoin pour notre rôle de gouvernance. Nous avons donc besoin qu'ils soient libérés de cette contrainte. Peut-être souhaiterez-vous consulter ces clauses avant de cocher la case en question.

Si vous exigez habituellement un accord de confidentialité entre vous et toute partie qui traite des informations confidentielles, veuillez examiner les sections correspondantes de nos CG. Elles devraient répondre à toutes vos interrogations. De plus, vous n'avez généralement pas à nous fournir d'informations confidentielles quelles qu'elles soient.

Pour conclure la section juridique, notez que le système implique l'acceptation des mêmes règles par l'ensemble des participants. Par conséquent, nous ne pouvons accepter de conditions générales supplémentaires[5].

4.3.2. Le périmètre d'évaluation TISAX

Durant la deuxième étape du processus TISAX, l'un de nos auditeurs TISAX procédera à l'évaluation de la sécurité de l'information. Il doit savoir par où commencer et où s'arrêter. C'est pourquoi vous devez définir un « périmètre d'évaluation ».

Le « périmètre d'évaluation » décrit l'étendue de l'évaluation de sécurité de l'information. En termes simples, chaque partie de votre entreprise qui traite des informations confidentielles de votre partenaire est intégrée dans le périmètre d'évaluation. Vous pouvez considérer qu'il s'agit d'un élément majeur de la description de la tâche de l'auditeur. Il dicte ce que l'auditeur doit évaluer.

Le périmètre d'évaluation est important pour deux raisons :

a. Un résultat d'évaluation ne répondra à l'exigence de votre partenaire que si le périmètre d'évaluation correspondant couvre toutes les parties de votre entreprise qui traitent les informations de ce partenaire.
b. Un périmètre d'évaluation défini avec précision est une condition préalable essentielle à des calculs de coûts pertinents de la part de nos auditeurs TISAX.

Remarque importante :

ISO/IEC 27001 et TISAX

Tout d'abord, il convient de distinguer deux types de périmètre :
1) le périmètre de votre système de gestion de la sécurité de l'information (ISMS) et
2) le périmètre d'évaluation.
Ces deux champs ne sont pas nécessairement identiques.

Pour la certification ISO/IEC 27001, vous définissez le périmètre de votre ISMS (dans le « domaine de périmètre »). Vous êtes totalement libre de définir le périmètre de votre ISMS. Cependant, le périmètre d'évaluation (également appelé « périmètre de l'audit ») doit être identique au périmètre de votre ISMS.

TISAX vous demande également de définir votre ISMS. Mais le périmètre d'évaluation peut être différent.

Pour la certification ISO/IEC 27001, vous pouvez délimiter librement le périmètre d'évaluation en fonction de votre définition du périmètre de votre ISMS.

À la différence, pour TISAX, le périmètre d'évaluation est prédéfini. Le périmètre d'évaluation peut être plus réduit que celui de votre ISMS. Mais il doit être contenu dans le périmètre de votre ISMS.

4.3.2.1. Description du périmètre

La description du périmètre d'évaluation définit l'étendue de l'évaluation. Concernant la description du périmètre, vous devez choisir l'un des deux types de périmètres suivants :

1. Standard scope (Périmètre d'évaluation standard)
2. Custom scope (Périmètre d'évaluation sur mesure)
   a. Custom extended scope (Périmètre d'évaluation étendu sur mesure)
   b. Full custom scope (Périmètre d'évaluation entièrement sur mesure)

La section suivante traite du périmètre d'évaluation standard. Le périmètre d'évaluation standard est le bon choix pour plus de 99 % des participants. Par conséquent, nous aborderons les périmètres d'évaluation sur mesure uniquement dans la Section 7.8, "Annexe : périmètres d'évaluation sur mesure".

4.3.2.2. Périmètre d'évaluation standard

La description du périmètre d'évaluation standard est la base de l'évaluation TISAX. D'autres participants TISAX n'acceptent les résultats d'évaluation que s'ils sont basés sur la description

du périmètre d'évaluation standard.

La description du périmètre d'évaluation standard est prédéfinie et vous ne pouvez pas la modifier.

L'un des principaux avantages d'un périmètre d'évaluation standard est qu'il permet d'éviter de devoir fournir votre propre définition.

Voici la description du périmètre d'évaluation standard (version 2.0) :

```
The TISAX assessment scope defines the
scope of the assessment. The
assessment includes all processes,
procedures and resources under
responsibility of the assessed
organization that are relevant to the
security of the protection objects and
their protection goals as defined in
the listed assessment objectives at
the listed locations.
The assessment is conducted at least
in the highest assessment level listed
in any of the listed assessment
objectives. All assessment criteria
listed in the listed assessment
objectives are subject to the
assessment.
```

```
Le périmètre d'évaluation TISAX
définit le périmètre de l'évaluation.
Cette évaluation porte sur l'ensemble
des processus, procédures et
ressources placés sous la
responsabilité de l'organisation
évaluée qui sont pertinents pour la
sécurité des objets de protection et
leurs objectifs de protection tels
qu'ils sont définis dans les objectifs
d'évaluation listés dans les sites
listés.
L'évaluation est réalisée en
appliquant a minima le niveau
d'évaluation le plus élevé listé dans
l'un des objectifs d'évaluation listés.
L'évaluation porte sur l'ensemble des
critères d'évaluation listés dans les
objectifs d'évaluation listés.
```

Nous recommandons vivement de choisir le périmètre d'évaluation standard. Tous les participants TISAX acceptent les résultats d'évaluation de la sécurité de l'information qui se fondent sur un périmètre d'évaluation standard.

4.3.2.3. Détermination du périmètre

Votre prochaine étape, après la définition du type de périmètre, consiste à décider quels sites appartiennent au périmètre d'évaluation.

Si votre entreprise est petite (un seul site), la tâche est simple. Il vous suffit d'ajouter votre site au périmètre d'évaluation.

Si votre entreprise est grande, vous pouvez enregistrer plus d'un périmètre d'évaluation.

Le fait d'avoir un seul périmètre englobant tous les sites présente certains avantages :

- Vous disposez d'un seul rapport d'évaluation, d'un seul résultat d'évaluation et d'une seule date d'expiration.
- Vous pouvez bénéficier d'une réduction des coûts pour l'évaluation, dans la mesure où un auditeur TISAX unique doit évaluer une seule fois vos ressources, procédures et processus centraux.

Mais un périmètre unique a aussi ses inconvénients, notamment :

- Tous les sites doivent avoir les mêmes objectifs d'évaluation.
- Le résultat de l'évaluation n'est disponible qu'une fois que l'auditeur TISAX a évalué l'ensemble des sites. Cela peut avoir de l'importance si vous avez besoin rapidement d'un résultat d'évaluation.
- Le résultat de l'évaluation dépend de tous les sites qui passent l'évaluation. Si un seul site échoue, vous n'obtiendrez pas de résultat positif pour votre évaluation. Une manière de contourner cette situation serait de : a) retirer le site du périmètre, b) résoudre les problèmes, c) ajouter le site ultérieurement moyennant une évaluation d'extension du périmètre.

4.3.2.4. Adaptation du périmètre

Vous seul pouvez répondre à la question de savoir si vous devez avoir un ou plusieurs périmètres d'évaluation. Pour vous aider à prendre votre décision, vous pouvez répondre aux questions dans le diagramme suivant.

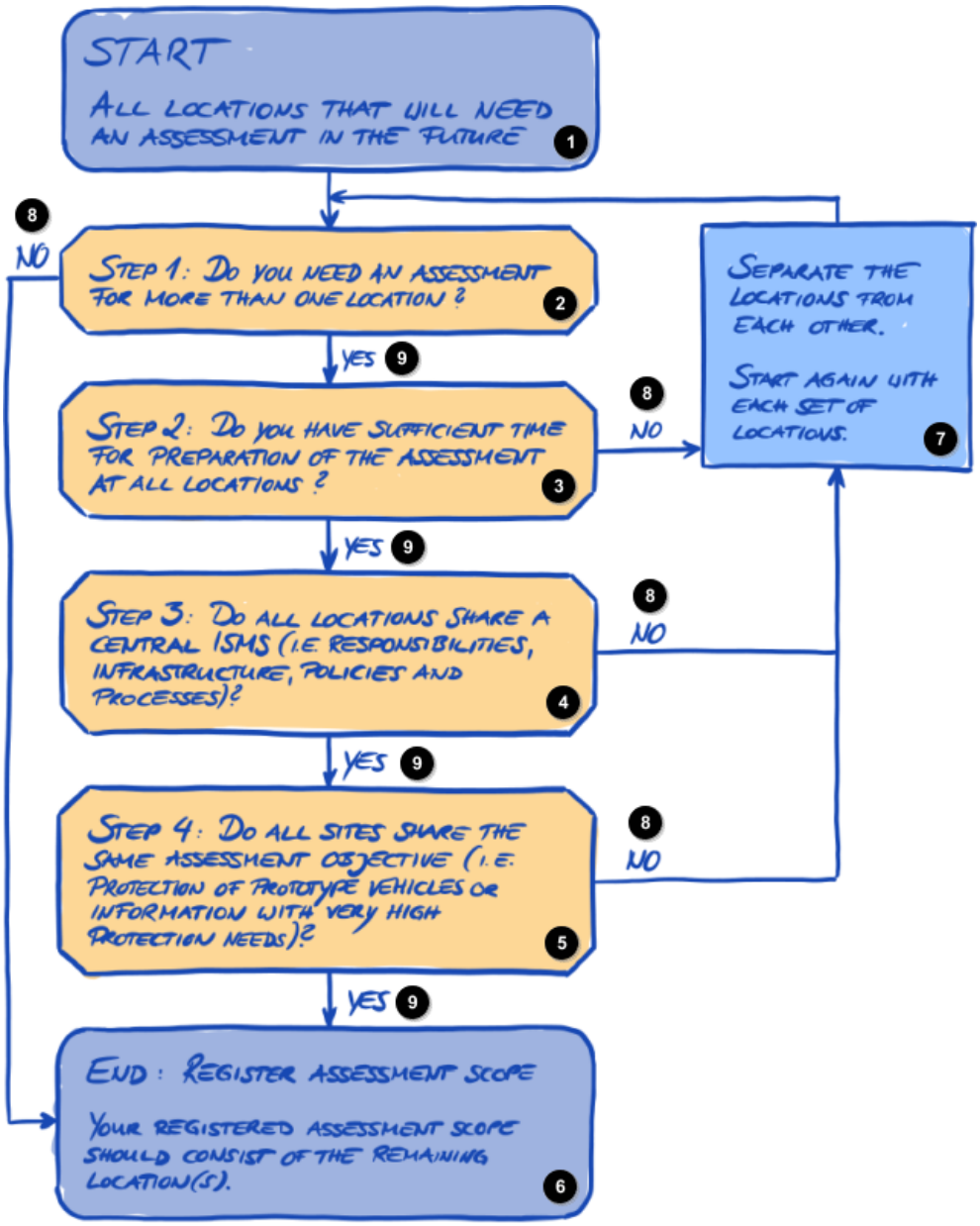


Illustration 5. Arbre décisionnel d'adaptation du périmètre

1. DÉPART
   Tous les sites qui auront besoin d'une évaluation à l'avenir
2. Étape 1 : avez-vous besoin d'une évaluation pour plus d'un site ?
3. Étape 2 : avez-vous assez de temps pour vous préparer à l'évaluation sur tous les sites ?
4. Étape 3 : tous les sites partagent-ils un ISMS central (en matière de responsabilités, d'infrastructures, de politiques et de processus) ?
5. Étape 4 : tous les sites partagent-ils le même objectif d'évaluation (à savoir la protection des véhicules prototypes ou des informations présentant des besoins de protection très importants) ?

6. Fin : enregistrez le périmètre d'évaluation
   Le périmètre d'évaluation que vous avez enregistré doit comporter le(s) site(s) restant(s).
7. Distinguez les sites les uns des autres.
   Recommencez avec chaque groupe de sites.
8. Non
9. Oui

Remarque :

Cette décision ne doit pas vous déconcerter. Vous pouvez modifier n'importe quel périmètre tant que l'auditeur n'a pas terminé l'évaluation.

Par exemple au cours de la préparation à votre évaluation, vous pouvez estimer que votre périmètre n'est pas adapté — et le modifier en conséquence. Ou votre auditeur peut recommander de modifier le périmètre au cours des premières étapes de l'évaluation.

Remarques supplémentaires :

- Techniquement, vous ne pouvez pas modifier le périmètre d'évaluation que vous avez défini au cours du processus d'inscription en ligne sur le portail ENX. Mais l'auditeur peut mettre à jour votre périmètre d'évaluation lorsqu'il télécharge le résultat de votre évaluation sur le portail ENX.
- Tout ajout au périmètre augmente les frais, et vous ne serez pas remboursé si vous retirez des sites du périmètre. Les auditeurs se basent sur le périmètre d'évaluation initial pour calculer leurs honoraires. Par conséquent, vous devrez également vous attendre à des changements.

4.3.2.5. Sites du périmètre

Maintenant que vous avez décidé des sites à intégrer dans votre périmètre d'évaluation, vous pouvez poursuivre en collectant certaines informations spécifiques aux sites.

Pour chaque site, nous sollicitons des informations telles que le nom et l'adresse de l'entreprise. Nous demandons aussi d'autres informations permettant à nos auditeurs TISAX de se faire une meilleure idée de la structure de votre entreprise. Vos réponses serviront de base à l'estimation du travail qu'ils auront à fournir.

Veuillez vous préparer à communiquer les renseignements suivants pour chacun de vos sites (l'astérisque rouge * indique les informations obligatoires dans le processus en ligne) :

Domaine	Options
Nom du site *	n/a
NUMÉRO D-U-N-S de D&B	n/a
Type de site *	Immeuble(s) détenu(s) et utilisé(s) exclusivement par l'entreprise Immeuble(s) loué(s) par l'entreprise Étage/bureaux loués par l'entreprise dans un immeuble partagé Bureaux partagés avec d'autres entreprises Propre centre de données Centre de données partagé
Protection passive du site *	Oui Non
Secteur *(Plusieurs sélections possibles)*	Technologie de l'information ☐ Services informatiques ☐ Services de télécommunication ☐ Développement logiciel
	Direction ☐ Conseil
	Médias ☐ Marketing ☐ Agence ☐ Services d'impression ☐ Photographie ☐ Services de traduction
	Recherche et développement ☐ Tests de véhicules ☐ Simulations de véhicules ☐ Construction de prototypes ☐ Modèles de voitures miniatures ☐ Services de développement ☐ Services de développement CAx

Domaine	Options
	Production Services de production Fabrication contractuelle Atelier Logistique
	Vente et service après-vente Importations, NSC Distribution Services financiers Assurance Règlement des réclamations
	Autres secteurs *(veuillez spécifier)*
Nombre de salariés sur le site : total *	0 1-10 11-100 101-1 000 1 001-5 000 Plus de 5 000
Nombre de salariés sur le site : IT *	0 1-10 11-25 26-50 Plus de 50
Nombre de salariés sur le site : sécurité informatique *	0 Temps partiel 1-5 6-25 Plus de 25
Nombre de salariés sur le site : sécurité du site *	0 Temps partiel 1-3 4-10 Plus de 10

Domaine	Options
Certifications pour ce site	ISO 27001 Autre *(veuillez spécifier)* ISAE 3402 SOC2

Tableau 1. Renseignements propres au site

Remarque :

Concernant le « secteur » : sélectionnez au mieux de vos connaissances. Il n'existe pas de bonne ou de mauvaise réponse parmi les options figurant ci-dessus. Si vous ne trouvez pas d'option qui correspond à votre type d'activité, veuillez simplement spécifier l'option appropriée sous « Autre ».

Pour chaque site, vous devez spécifier un "location name" (« nom du site »). Le nom du site a pour objectif de faire référence plus aisément au site lorsque vous intégrez celui-ci à un périmètre d'évaluation.

Nous recommandons de nommer les sites sur la base du modèle suivant :

Modèle : [Référence géographique]

Exemple : pour l'entreprise fictive « ACME »

- Francfort
  (pour un site établi dans la **ville** allemande de Francfort)

4.3.2.6. Nom du périmètre

Pour chaque périmètre, vous devez spécifier un "scope name" (« nom du périmètre »). Le nom du périmètre a pour objectif principal de vous permettre d'identifier facilement un périmètre dans la liste des périmètres sur le portail ENX. Nous vous conseillons de choisir un nom qui soit utile au lecteur et à vos collègues. Pour la communication externe, vous devrez utiliser l'ID de périmètre.

Vous pouvez spécifier le nom que vous souhaitez. Mais vous ne pouvez pas attribuer le même nom à plusieurs périmètres.

Si plus tard, vous souhaitez renouveler votre évaluation TISAX, vous devrez créer un nouveau périmètre (éventuellement identique au périmètre actuel). Par conséquent, nous recommandons d'ajouter l'année de l'évaluation au nom du périmètre.

Nous recommandons de nommer les périmètres sur la base du modèle suivant :

Modèle : [Référence géographique ou *fonctionnelle*] [Année de l'évaluation]

Exemples : pour l'entreprise fictive « ACME »

- 2024
  (sans référence géographique si votre entreprise n'a qu'un site)
- Francfort 2024
  (pour un périmètre comportant plusieurs sites dans la **ville** allemande de Francfort)
- Basse-Saxe 2024
  (pour un périmètre dont tous les sites se trouvent dans le **land** allemand de Basse-Saxe)
- Allemagne 2024
  (pour un périmètre dont tous les sites se trouvent dans la **République** d'Allemagne)
- EMEA 2024
  (pour un périmètre dont tous les sites se trouvent dans la **région** EMEA (« Europe, Moyen-Orient, Afrique »))
- Développement de prototypes 2024
  (référence *fonctionnelle* pour un périmètre dont tous les sites sont impliqués dans le développement de prototypes)

4.3.2.7. Contacts

Pour communiquer avec vous, nous collectons des informations sur les contacts au sein de votre entreprise.

Nous vous demandons de désigner pour votre entreprise au moins un contact en tant que participant TISAX en général et un autre pour chaque périmètre d'évaluation. Vous pouvez désigner des contacts supplémentaires.

Durant les préparations à votre inscription, vous devez décider qui sera un contact dans votre entreprise.

Nous vous demandons de fournir les données de contact suivantes :

	Données de contact	**Obligatoire ?**	**Exemple**
1.	Titres	Oui	Mme, M.
2.	Grade universitaire		Dr, Ph.D., autre
3.	Prénom	Oui	Jean
4.	Nom	Oui	Dupont

	Données de contact	Obligatoire ?	Exemple
5.	Intitulé de la fonction	Oui	Directeur de l’informatique
6.	Département	Oui	Technologie de l’information
7.	Numéro de téléphone principal	Oui	+49 69 986692777
8.	Numéro de téléphone secondaire		
9.	Adresse e-mail	Oui	jean.dupont@acme.com
10.	Langue de préférence	Oui	Anglais (défaut)
11.	Autres langues		Allemand, français
12.	Identifiant d’adresse personnelle		HPC 1234
13.	Adresse postale	Oui	Bockenheimer Landstraße 97-99
14.	Code postal	Oui	60325
15.	Ville	Oui	Francfort
16.	Land/province		
17.	Pays	Oui	Allemagne

Tableau 2. Données de contact

Remarque importante :

Nous recommandons de désigner au moins un suppléant pour chaque contact. Si un contact est provisoirement indisponible ou quitte l’entreprise, quelqu’un d’autre peut gérer les données de participant de votre entreprise.
Si vous devez désigner un nouveau contact (alors qu’il ne reste plus d’autres contacts valides), vous devez suivre un processus complexe. Notre processus garantit que seules les personnes qui sont capables de prouver qu’elles sont autorisées à représenter légalement l’entreprise peuvent approuver la désignation d’un nouveau contact principal.

4.3.2.8. Publication et partage

L’objectif principal de TISAX est de publier le résultat de votre évaluation pour d’autres participants TISAX et de le partager avec votre/vos partenaire(s).

Vous pouvez décider de la publication et du partage du résultat de votre évaluation durant le processus d’inscription ou plus tard, à n’importe quel moment.

Si vous vous soumettez au processus TISAX de manière préventive, vous pouvez déjà décider de publier le résultat de votre évaluation pour la communauté des participants TISAX. Autrement, il n’y a rien d’autre à préparer à ce stade.

Si votre partenaire vous a demandé de vous soumettre au processus TISAX, vous devrez tôt ou tard partager le résultat de votre évaluation. Vous pouvez déjà partager des informations de statut avec votre partenaire au cours de l'inscription. Une fois que le résultat de votre évaluation sera disponible, votre partenaire sera automatiquement autorisé à y accéder[6].

Vous avez besoin de deux éléments pour partager des informations de statut :

1. L'ID de participant TISAX de votre partenaire

   L'ID de participant TISAX identifie votre partenaire en tant que participant TISAX.

   Normalement, votre partenaire doit vous fournir son ID de participant TISAX.

   Pour vous simplifier la tâche, notre formulaire d'inscription comprend une liste déroulante des ID de participant de certaines entreprises qui reçoivent fréquemment des résultats partagés d'évaluation.[7]

2. Le niveau de partage requis

   Le niveau de partage définit le niveau d'accès au résultat de votre évaluation octroyé à votre partenaire.

   Soit votre partenaire demande un niveau de partage particulier, soit vous décidez jusqu'à quel niveau vous souhaitez donner accès à votre partenaire au résultat de votre évaluation.

   Pour de plus amples informations sur les niveaux de partage, veuillez consulter la Section 6.5, "Niveaux de partage".

Assurez-vous donc de disposer de ces informations.

Remarque :

- Vous pouvez toujours décider de publier ultérieurement le résultat de votre évaluation.
- Vous pouvez toujours créer ultérieurement une autorisation de partage pour votre partenaire.

Remarque importante :

Si vous ne publiez pas le résultat de votre évaluation ou ne le partagez pas, personne ne pourra le voir.

Remarque importante :

Vous ne pouvez pas annuler la publication ou le partage.

Pour plus de détails, veuillez consulter la Section 6.4, “Permanence des résultats échangés”.

Remarque :

Cela peut paraître étrange, mais vous pouvez partager le « résultat de l’évaluation » même si le processus d’évaluation n’a pas encore commencé. À ce stade précoce, vous partagez uniquement le « statut de l’évaluation ». Le participant avec lequel vous partagez le « résultat de l’évaluation » verra où vous en êtes dans le processus d’évaluation.

Certains participants TISAX doivent publier une version spéciale si vous devez montrer des labels TISAX alors que le processus d’évaluation n’est pas encore terminé. Dans ce cas, votre partenaire aura peut-être besoin de voir le « statut de votre évaluation » sur son compte sur le portail ENX.

Pour de plus amples informations sur le statut de l’évaluation, veuillez consulter la Section 7.6, “Annexe : Assessment status (Statut de l’évaluation)”.

Pour de plus amples informations sur la publication et le partage du résultat de votre évaluation, veuillez consulter la Section 6, “Échange (étape 3)”.

4.3.3. Objectifs d’évaluation

Vous devez définir votre/vos objectif(s) d’évaluation durant le processus d’inscription. L’objectif d’évaluation (assessment objective) détermine les exigences que votre système de gestion de la sécurité de l’information (ISMS) doit respecter. L’objectif d’évaluation est intégralement basé sur le type de données que vous traitez pour le compte de votre partenaire.

Dans les sections suivantes, nous décrivons les objectifs d’évaluation et fournissons des conseils concernant la sélection du/des objectif(s) d’évaluation adéquat(s).

L’utilisation des objectifs d’évaluation facilite la communication relative à TISAX avec votre partenaire et nos auditeurs TISAX, car ils font référence à un input prédéfini du processus d’évaluation TISAX.

Remarque :

Il se peut que certains partenaires vous demandent de passer l’évaluation TISAX avec un certain « niveau d’évaluation » (assessment level ou « AL ») plutôt que de spécifier un objectif d’évaluation.

Pour de plus amples informations sur les niveaux d’évaluation, veuillez consulter la Section 4.3.3.5, “Besoins de protection et niveaux d’évaluation”

(sous-section « Informations supplémentaires »).

4.3.3.1. Liste des objectifs de l'évaluation

L'évaluation TISAX comporte actuellement douze objectifs. Vous devez sélectionner au moins un objectif d'évaluation. Vous pouvez en sélectionner davantage.

Considérez votre objectif d'évaluation comme la référence pour votre système de gestion de la sécurité de l'information. L'objectif d'évaluation représente un input clé du processus TISAX. Tous les auditeurs TISAX fondent principalement leur stratégie d'évaluation sur l'objectif d'évaluation.

Les objectifs d'évaluation TISAX actuels sont les suivants :

Nº	Nom	Description
1.	Info high	Handling of information with high protection needs Traitement des informations présentant des besoins de protection importants
2.	Info very high	Handling of information with very high protection needs Traitement des informations présentant des besoins de protection très importants
3.	Confidential	Handling of information with high protection needs in the context of confidentiality (access to confidential information) Traitement des informations présentant des besoins de protection importants en matière de confidentialité (accès aux informations confidentielles)
4.	Strictly confidential	Handling of information with very high protection needs in the context of confidentiality (access to strictly confidential information) Traitement des informations présentant des besoins de protection très importants en matière de confidentialité (accès aux informations strictement confidentielles)
5.	High availability	Handling of information with high protection needs in the context of *availability* (high availability of information) Traitement des informations présentant des besoins de protection importants en matière de *disponibilité* (haute disponibilité des informations)

Nº	Nom	Description
6.	Very high availability	Handling of information with very high protection needs in the context of *availability* (very high availability of information) Traitement des informations présentant des besoins de protection très importants en matière de *disponibilité* (très haute disponibilité des informations)
7.	Proto parts	Protection of Prototype Parts and Components Protection des pièces et composants de prototypes
8.	Proto vehicles	Protection of Prototype Vehicles Protection des véhicules prototypes
9.	Test vehicles	Handling of Test Vehicles Traitement des véhicules de test
10.	Proto events	Protection of Prototypes during Events and Film or Photo Shoots Protection des prototypes durant les événements et les films ou les shootings photo
11.	Data	Data protection according to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR) Protection des données conformément à l’article 28 (« Sous-traitant ») du Règlement général européen sur la protection des données (RGPD)
12.	Special data	Data protection according to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR) with special categories of personal data as specified in Article 9 of the GDPR Protection des données conformément à l’article 28 (« Sous-traitant ») du Règlement général européen sur la protection des données (RGPD) concernant des catégories particulières de données à caractère personnel, comme spécifié à l’article 9 du RGPD

Tableau 3. Les objectifs d’évaluation TISAX actuels

Exemple : si vous effectuez des tests de conduite sur la voie publique, alors l’objectif d’évaluation « Test vehicles » constitue l’un de vos objectifs d’évaluation.

Remarque :

Vous ne pouvez sélectionner les objectifs d’évaluation « Info high » et « Info

very high » que jusqu'au 31 mars 2024.

Vous pourrez sélectionner les objectifs d'évaluation « Confidential » et « Strictly confidential » à partir du 1er avril 2024.

Pour de plus amples informations sur cette transition, veuillez consulter l'article suivant sur notre site Web :
CHANGES TO TISAX LABELS ACCOMPANYING ISA 6 RELEASE
enx.com/en-US/news/Changes-to-TISAX-Labels-ISA-six-Release/

Remarque importante :

Dans TISAX, « l'objectif d'évaluation » est généralement l'input du processus. Toutefois, certains partenaires sont susceptibles de vous demander de passer l'évaluation TISAX avec un certain « niveau d'évaluation » (AL).

Pour de plus amples informations sur la relation entre les besoins de protection et les niveaux d'évaluation, veuillez consulter la Section 4.3.3.5, "Besoins de protection et niveaux d'évaluation".

4.3.3.2. Objectifs d'évaluation et ISA

L'ISA comprend trois catalogues de critères (sécurité de l'information, protection des prototypes, protection des données). Chaque catalogue de critères se compose de plusieurs « questions de contrôle » et d'exigences qui leur sont associées.

Chaque objectif d'évaluation définit :

- le(s) catalogue(s) de critères ISA applicable(s)
- les questions de contrôle auxquelles vous devez répondre
- les exigences que vous devez remplir

Pour certains objectifs d'évaluation, seul un sous-ensemble de questions de contrôle et d'exigences s'applique.

Pour de plus amples informations générales sur les objectifs d'évaluation TISAX, les questions de contrôle et les exigences applicables, veuillez consulter la Section 5.2.2, "Compréhension du document ISA".

4.3.3.3. Objectifs d'évaluation et labels TISAX

Votre partenaire peut parler de « labels TISAX ». « Objectifs d'évaluation » et « labels TISAX » font à peu près référence à la même chose. La différence réside dans le fait que vous entamez le processus d'évaluation avec des « objectifs d'évaluation » et si vous réussissez l'évaluation, vous recevez les « labels TISAX » correspondants.

Exemple : votre partenaire vous demande d'obtenir le label TISAX « Info high ». Vous devez donc sélectionner l'objectif d'évaluation « Info high ».

L'illustration ci-dessous représente l'input et l'output du processus TISAX :

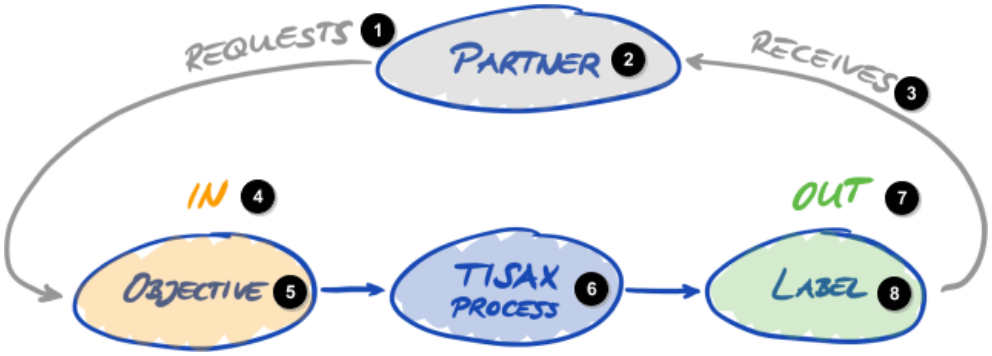


Illustration 6. Objectifs d'évaluation et labels TISAX

1. Demande
2. Partenaire
3. Reçoit
4. IN
5. Objectif
6. Processus TISAX
7. OUT
8. Label

Pour de plus amples informations sur les labels TISAX, veuillez consulter la Section 5.4.14, "Labels TISAX".

4.3.3.4. Sélection de l'objectif d'évaluation

Idéalement, votre partenaire vous indique précisément quels objectifs d'évaluation vous devez atteindre.

Vous devez sélectionner l'objectif d'évaluation sur la base de votre propre jugement si :

a. vous voulez passer l'évaluation TISAX avant qu'un partenaire vous le demande, ou
b. votre partenaire ne vous indique pas l'objectif d'évaluation à atteindre.

Remarque importante :

À ce stade, nous vous recommandons vivement de vous intéresser à vos autres

> partenaires. Avez-vous actuellement d'autres partenaires qui ont des exigences identiques ou plus élevées ? Attendez-vous des futurs partenaires qu'ils aient des exigences plus élevées ?
>
> Peut-être devriez-vous sélectionner des objectifs d'évaluation associés à des besoins de protection plus importants. Ainsi, vous éviterez les problèmes dans le cas où d'autres partenaires ont des exigences plus élevées.

Si vous devez sélectionner un objectif d'évaluation sur la base de votre propre jugement, vous trouverez peut-être utile d'analyser les aspects suivants :

Nº	Objectif d'évaluation	Information
1.	Info high	Vous pouvez trouver les besoins de protection (importants, très importants) dans la classification des documents établie par votre partenaire.
2.	Info very high	
3.	Confidential	Pour toutes les entreprises qui reçoivent et traitent des informations présentant des besoins de protection importants en matière de confidentialité ou étant généralement classées comme confidentielles selon le propre système de classification de l'entreprise (p. ex. : livre blanc de la VDA « Harmonization of classification levels » (« Harmonisation des niveaux de classification »)). Vous devez sélectionner ce label TISAX en particulier si la divulgation non autorisée des informations pourrait causer des dommages considérables (p. ex. : des atteintes à la réputation, des conséquences pénales ou des dommages pécuniaires).
4.	Strictly confidential	Pour toutes les entreprises qui réceptionnent et traitent des informations présentant des besoins de protection très importants en matière de confidentialité ou étant généralement classées comme strictement confidentielles ou secrètes selon le propre système de classification de l'entreprise (p. ex. : livre blanc de la VDA « Harmonization of classification levels » (« Harmonisation des niveaux de classification »)). Vous devez sélectionner ce label TISAX en particulier si la divulgation non autorisée des informations pourrait causer des dommages menaçant l'existence ou catastrophiques (p. ex. : des atteintes graves à la réputation, des conséquences pénales graves ou des dommages pécuniaires très importants).

Nº	Objectif d'évaluation	Information
5.	High availability	Pour toutes les entreprises dont la capacité de production ou de livraison des clients dépend de la disponibilité des produits ou services de ces entreprises, et pour lesquelles une panne causerait des dégâts considérables aux clients sur une courte durée. Exemple : fournisseurs juste-à-temps de matériaux de fabrication
6.	Very high availability	Pour toutes les entreprises dont la capacité de livraison et de production des clients dépend de la disponibilité à court terme des produits et services de l'entreprise, et pour lesquelles une panne causerait des dégâts considérables aux clients sur une très courte durée. Exemple : fournisseurs juste-à-temps pour lesquels une panne peut entraîner un arrêt total de la production avec un délai de redémarrage très long sur une courte durée.
7.	Proto parts	Pour toutes les entreprises qui, sur leurs propres sites, fabriquent, stockent ou utilisent des composants ou des pièces fournis par les clients, classés comme devant être protégés. Les exigences relatives à la sécurité physique et à la sécurité dans la zone environnante, les exigences organisationnelles et les exigences spécifiques pour le traitement des prototypes font partie de l'évaluation.
8.	Proto vehicles	Pour toutes les entreprises qui, sur leurs propres sites, fabriquent, stockent ou utilisent des véhicules fournis par les clients, classés comme devant être protégés. Les exigences relatives à la sécurité physique et à la sécurité dans la zone environnante (y compris l'existence d'ateliers et de garages protégés), les exigences organisationnelles et les exigences spécifiques pour le traitement des prototypes font partie de l'évaluation. Après une évaluation réussie, vous recevez automatiquement le label TISAX « Protection des pièces et composants de prototypes ».

Nº	Objectif d'évaluation	Information
9.	Test vehicles	Pour toutes les entreprises qui effectuent des tests et des essais routiers (p. ex. : essais routiers sur la voie publique ou sur des pistes de test) avec des véhicules fournis par les clients classés comme devant être protégés. Les exigences organisationnelles, les exigences spécifiques pour le traitement des prototypes, y compris le camouflage, et le traitement des véhicules durant les essais routiers sur la voie publique ou sur des pistes de test font partie de l'évaluation. Les exigences relatives à la sécurité physique et à la sécurité dans la zone environnante ne font pas nécessairement partie de l'évaluation. Si vos sites sont équipés en conséquence, nous vous recommandons aussi de sélectionner l'objectif d'évaluation « Protection des véhicules prototypes ».
10.	Proto events	Pour toutes les entreprises qui effectuent des présentations ou organisent des événements (p. ex. : études de marché, événements, événements marketing), réalisent des films et des shootings photo avec des véhicules, des composants ou des pièces fournis par les clients classés comme devant être protégés. Les exigences organisationnelles et les exigences spécifiques pour le traitement des prototypes, y compris les exigences relatives aux présentations, aux événements, aux films et aux shootings photo dans des pièces protégées et en public font partie de l'évaluation. Les exigences relatives à la sécurité physique et à la sécurité dans la zone environnante ne font pas nécessairement partie de l'évaluation. Si vos sites sont équipés en conséquence, nous vous recommandons aussi de sélectionner l'objectif d'évaluation « Protection des véhicules prototypes ».
11.	Data	Si vous traitez des données à caractère personnel en tant que sous-traitant conformément à l'article 28 du RGPD, vous devrez probablement sélectionner « Data ».

Nº	Objectif d'évaluation	Information
12.	Special data	Si vous traitez des catégories spéciales de données à caractère personnel (telles que des données de santé ou sur les croyances religieuses) en tant que sous-traitant conformément à l'article 28 du RGPD, vous devrez probablement sélectionner « Special data ».

Tableau 4. Conseil pour la sélection d'un objectif d'évaluation

Autres explications :

- Si votre partenaire vous a fait part d'exigences précises, vous n'avez généralement pas à discuter de vos objectifs d'évaluation avec lui. Toutefois, si vous n'avez pas obtenu d'exigences précises de la part de votre partenaire, nous vous recommandons vivement de consulter ce dernier avant d'entamer le processus d'évaluation.
- Pour chaque exigence, l'ISA décrit le cas échéant la différence de mise en œuvre entre les besoins de protection « importants » et « très importants ».
  Pour de plus amples informations à ce sujet, veuillez consulter l' Illustration 11, "Capture d'écran : principaux éléments des questions figurant dans le catalogue de critères ISA « Sécurité de l'information »".

4.3.3.5. Besoins de protection et niveaux d'évaluation

Votre partenaire détient divers types d'informations, dont certains méritent éventuellement un niveau de protection supérieur aux autres. L'ISA traite la problématique en différenciant trois « besoins de protection » (🇬🇧 "protection needs") : normal, important et très important. Votre partenaire classe ses informations et les lie généralement à des besoins de protection.

Plus le besoin de protection est important, plus votre partenaire souhaitera s'assurer qu'il peut en toute sécurité vous laisser traiter ses informations. Par conséquent, TISAX distingue trois « niveaux d'évaluation » (AL). Le niveau d'évaluation définit la méthode d'évaluation que l'auditeur doit appliquer. Plus le niveau d'évaluation est élevé, plus le travail est approfondi. Il en résulte une évaluation plus précise.

Le tableau ci-dessous indique les niveaux d'évaluation qui s'appliquent aux objectif d'évaluation TISAX :

Nº	Objectif d'évaluation TISAX	Niveau d'évaluation (AL)
1.	Info high	AL 2
2.	Info very high	AL 3
3.	Confidential	AL 2

Nº	Objectif d'évaluation TISAX	Niveau d'évaluation (AL)
4.	Strictly confidential	AL 3
5.	High availability	AL 2
6.	Very high availability	AL 3
7.	Proto parts	AL 3
8.	Proto vehicles	AL 3
9.	Test vehicles	AL 3
10.	Proto events	AL 3
11.	Data	AL 2
12.	Special data	AL 3

Tableau 5. Correspondance entre les objectifs d'évaluation TISAX et les niveaux d'évaluation

Niveau d'évaluation 1 (AL 1) :

Les évaluations correspondant au niveau d'évaluation 1 visent principalement des objectifs internes au sens premier d'une auto-évaluation (self-assessment).

Pour une évaluation correspondant au niveau d'évaluation 1, un auditeur vérifie l'existence d'une auto-évaluation déjà menée à bien. Il n'évalue pas le contenu de l'auto-évaluation. Il n'exige pas d'autres preuves.

Les résultats des évaluations correspondant au niveau d'évaluation 1 présentent un faible niveau de confiance, raison pour laquelle ils ne sont pas utilisés dans TISAX. Mais il est évidemment possible que votre partenaire demande ce genre d'auto-évaluation en dehors de TISAX.

Niveau d'évaluation 2 (AL 2) :

Pour une évaluation correspondant au niveau d'évaluation 2, l'auditeur effectue un test de plausibilité sur votre auto-évaluation (pour tous les sites appartenant au périmètre d'évaluation). Il confirme ce test en vérifiant les données probantes[8] et en menant un entretien avec la personne responsable de la sécurité de l'information.

L'auditeur effectue généralement l'entretien par conférence sur le Web. À votre demande, il peut mener l'entrevue en personne.

Si vous ne souhaitez pas envoyer à l'auditeur certaines de vos données probantes, vous pouvez

demander une inspection sur site. De cette manière, l'auditeur peut toujours vérifier vos données probantes « de manière ultra-confidentielle ».

Remarque :

Il existe une méthode alternative pour réaliser une évaluation de niveau 2. À la place du test de plausibilité, l'auditeur effectue une évaluation à distance complète. Cette méthode est parfois appelée « **niveau d'évaluation 2.5** ».

À la différence d'une évaluation de niveau 2, l'auditeur *vérifie* que votre ISMS remplit les exigences requises. Mais contrairement à une évaluation de niveau 3, l'auditeur ne réalise pas les activités sur site définies dans la section sur le niveau d'évaluation 3 ci-dessous.

Cette évaluation sera évaluée comme une évaluation de niveau 2.

L'approche AL 2.5 présente l'avantage d'être méthodiquement compatible avec AL 3. Il est donc possible de passer ultérieurement à une évaluation complète dans AL 3 avec un effort limité. Pour cela, il suffit à l'auditeur de réaliser les activités sur site indiquées dans la section sur le niveau d'évaluation 3 ci-dessous.

Nous recommandons des évaluations de niveau 2.5 dans les cas suivants :

1. À ce jour, vous avez besoin uniquement de labels TISAX impliquant une évaluation de niveau 2, mais vous ne pouvez pas exclure la possibilité que d'autres partenaires exigent des labels TISAX impliquant une évaluation de niveau 3. Une évaluation de niveau 2.5 permet de passer ultérieurement à une évaluation de niveau 3.
2. Vous avez des difficultés à réaliser une auto-évaluation suffisamment plausible. Pour le test de plausibilité, l'auto-évaluation doit être probante, compréhensible et étayée. La réalisation d'une auto-évaluation peut nécessiter un travail interne considérable, même pour les entreprises qui sont fondamentalement bien positionnées.

Pour de plus amples informations sur le changement de niveau d'évaluation, veuillez consulter la Section 7.10, “Annexe : évaluation d'extension du périmètre”.

Cette alternative est facultative et n'est pas requise pour remplir les exigences du niveau d'évaluation 2. La différence entre AL 2 et AL 2.5 ne sera pas visible pour les partenaires avec lesquels vous partagerez le résultat de votre évaluation.

Niveau d’évaluation 3 (AL 3) :

Pour une évaluation correspondant au niveau d’évaluation 3, l’auditeur procède à une vérification complète de la conformité de votre entreprise avec les exigences applicables. L’auditeur utilise votre auto-évaluation ainsi que les documents fournis pour préparer l’évaluation. Mais à la différence du niveau d’évaluation 2, l’auditeur vérifie tout. Il :

- examine les documents et les preuves
- effectue des entretiens programmés avec les propriétaires des processus
- observe les conditions locales
- observe l’exécution des processus
- effectue des entretiens *non* programmés avec les participants aux processus

Remarque :

Le texte suivant renvoie à plusieurs concepts qui seront expliqués ultérieurement dans ce document.

Avec AL 3, l’auditeur doit se rendre sur votre/vos site(s). Si, pour quelque raison que ce soit, ceci est momentanément impossible ou nécessiterait des efforts déraisonnables, votre auditeur pourra utiliser la **méthode d’évaluation à distance par vidéo** pour réaliser les activités sur site de l’évaluation.

Votre auditeur devra indiquer cela dans le rapport d’évaluation TISAX comme une non-conformité mineure. Dès que votre auditeur pourra se rendre sur votre/vos site(s), il devra procéder à une évaluation de suivi comprenant toutes les activités sur site précédemment irréalisables. Par ailleurs, vous devrez programmer l’évaluation de suivi même si vous n’avez pas encore procédé aux autres actions correctives.

En attendant que votre auditeur soit disponible pour les activités sur site, cette approche vous permet de partager des labels TISAX provisoires avec votre partenaire.

Niveaux d’évaluation et méthodes d’évaluation

Le tableau suivant fournit un aperçu simplifié des méthodes d’audit associées à chaque niveau d’évaluation :

Méthode d'évaluation	Niveau d'évaluation 1 (AL 1)	Niveau d'évaluation 2 (AL 2)	Niveau d'évaluation 3 (AL 3)
Auto-évaluation	Oui	Oui	Oui
Données probantes	Non	Test de plausibilité	Vérification approfondie
Entretiens	Non	Par conférence sur le Web[9]	En personne, sur site
Inspection sur site	Non	À votre demande	Oui

Tableau 6. Applicabilité des méthodes d'évaluation aux différents niveaux d'évaluation

Informations supplémentaires :

- Différence entre AL 2 et AL 3
  Méthodologiquement, les deux approches diffèrent grandement. Pour les évaluations effectuées avec le niveau d'évaluation 2, l'auditeur ne vérifie pas tout. Il contrôle uniquement la plausibilité. Par conséquent, l'auditeur ne peut pas utiliser les résultats d'une évaluation de niveau 2 comme base pour procéder à une évaluation de niveau 3. Les efforts nécessaires pour passer à une évaluation de niveau 3 sont essentiellement les mêmes que pour une nouvelle évaluation initiale.
- Test de plausibilité et vérification
  Pour simplifier à l'extrême, un test de plausibilité consiste à contrôler si une chose existe et *semble* exacte. À l'inverse, une vérification nécessite de vraiment contrôler qu'une chose est ce qu'elle prétend être.
- Classification des informations et besoins de protection
  La correspondance entre classification des informations (par exemple « confidentielles » ou « secrètes ») et besoins de protection peut différer d'un partenaire à l'autre. Par conséquent, nous ne sommes pas en mesure de vous fournir un tableau simple illustrant la correspondance exacte entre la classification des informations de votre partenaire et un besoin de protection.
- Il ne suffit pas de connaître un niveau d'évaluation.
  Certains partenaires sont susceptibles de vous demander de passer l'évaluation TISAX avec un certain niveau d'évaluation. Notez qu'il ne suffit pas de connaître le niveau d'évaluation pour entamer le processus TISAX. Un niveau d'évaluation n'a de sens qu'en combinaison avec un catalogue de critères ISA et un besoin de protection correspondant. Habituellement, les partenaires vous demandent d'obtenir un label TISAX (catalogue de critères plus besoin de protection). Toutefois, comme les besoins de protection correspondent directement aux niveaux d'évaluation, il vous suffit de connaître le(s) catalogue(s) de critères et le niveau d'évaluation.

- Hiérarchie des niveaux d'évaluation
  Des niveaux d'évaluation plus élevés incluent toujours les niveaux d'évaluation inférieurs. Par exemple si votre évaluation est basée sur un niveau d'évaluation 3, elle satisfera automatiquement toutes les demandes de niveau d'évaluation 2.
- Notre recommandation concernant les niveaux d'évaluation
  Si vous devez sélectionner un objectif d'évaluation (et ainsi implicitement un niveau d'évaluation correspondant) sur la base de votre propre jugement, nous vous recommandons de sélectionner des objectifs d'évaluation qui impliquent un niveau d'évaluation 3. Le travail à fournir pour les évaluations TISAX de niveau d'évaluation 3 n'est généralement pas plus important que celui nécessaire à un niveau d'évaluation 2.
  Les fournisseurs qui ont plusieurs partenaires sélectionnent souvent des objectifs d'évaluation impliquant un niveau d'évaluation 3. De cette façon, ils sont prêts pour toutes les demandes futures et ne doivent pas se préoccuper des différents niveaux d'évaluation.
- Autres considérations d'ordre commercial
  Concernant les niveaux d'évaluation, le coût total d'une évaluation TISAX correspond à la somme de votre travail en interne et du coût de l'évaluation. Si le coût d'une évaluation de niveau 2 est inférieur, il se peut que le travail à fournir en interne soit plus important. Cela s'explique par le fait qu'une évaluation de niveau 2 nécessite habituellement une auto-évaluation plus complète et une meilleure documentation interne. Pour des évaluations correspondant au niveau d'évaluation 3, l'auditeur considérera souvent qu'il dispose de données probantes suffisantes si vous lui montrez la manière dont vous faites les choses et lui fournissez des documents de base. Mais sans inspection sur site, l'auditeur sollicitera des documents précis. Par conséquent, il n'est pas inhabituel de privilégier le niveau d'évaluation 3 par rapport au niveau 2. Toutefois, ce choix est plutôt celui des entreprises de plus petite taille.

4.3.3.6. Les objectifs d'évaluation et vos propres fournisseurs

TISAX ne demande pas nécessairement de soumettre l'ensemble de vos propres fournisseurs aux mêmes exigences. Si votre objectif d'évaluation est « Sécurité des informations présentant des besoins de protection *très* importants », cela NE signifie PAS automatiquement que vos propres fournisseurs doivent atteindre le même objectif d'évaluation. Cela ne signifie pas non plus qu'ils doivent obtenir des labels TISAX.

Mais vous êtes toujours tenu de vérifier pour l'ensemble de vos fournisseurs si l'utilisation de leurs services augmente les risques ou en crée de nouveaux.

Deux exemples extrêmement simplifiés :

1. L'un de vos règlements prévoit qu'un e-mail ordinaire ne peut être utilisé pour des données associées à des besoins de protection très importants. Par conséquent, votre fournisseur d'e-mails n'a pas besoin d'obtenir le label TISAX pour des besoins de protection très importants. Vous pourriez en venir à une conclusion comparable si vous n'envoyez que des e-mails cryptés et que le fournisseur d'e-mails ne peut voir aucune des données présentant des

besoins de protection très importants.

2. Vous éliminez à la déchiqueteuse les documents imprimés associés à des besoins de protection très importants. Dans ce cas, bien entendu, le service d'élimination des déchets ne doit pas répondre aux mêmes exigences que vous.

Toutefois, l'évaluation du risque peut montrer que votre fournisseur est tenu lui aussi de répondre aux exigences correspondant à des besoins de protection très importants. Dans ce cas, des labels TISAX constituent une manière de vous apporter la preuve requise.

4.3.4. Frais

Nous percevons des frais. Notre liste de prix vous informe des frais applicables, des réductions possibles et de nos modalités de paiement.

Vous pouvez télécharger la liste de prix sur notre site Web à l'adresse :
enx.com/en-US/TISAX/downloads/
Téléchargement direct du PDF :
enx.com/pricelist.pdf

Certains aspects liés à la facture doivent être pris en compte durant votre préparation à l'inscription :

- Sélection de l'adresse de facturation
  Par défaut, nous enverrons la facture à l'adresse de participant que vous avez fournie. Mais vous avez la possibilité de nous communiquer une adresse différente pour la facture.

Remarque importante :

Assurez-vous que l'adresse de facturation est exacte. Les lois comptables exigent que l'adresse sur la facture corresponde exactement à l'adresse (de facturation) de votre entreprise. Pour des raisons de conformité, nous ne pouvons pas modifier l'adresse de facturation une fois que nous avons émis la facture.

- Référence de la commande
  Si vous avez besoin de voir un numéro de commande spécifique ou une information similaire sur votre facture, vous pouvez nous fournir une référence de commande.
- Numéro de TVA
  Tous nos honoraires sont soumis à la taxe allemande sur la valeur ajoutée (TVA) si elle s'applique.
  Nous avons besoin de ce numéro pour procéder aux paiements en provenance de l'UE. Il est obligatoire de fournir un numéro de TVA si votre adresse de facturation figure dans l'un des pays suivants :
  Allemagne, Autriche, Belgique, Bulgarie, Chypre (partie grecque), Croatie, Danemark,

Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Royaume-Uni, Slovaquie, Slovénie, Suède

- Gestion des fournisseurs

Remarque importante :

Notez qu'en raison de la mutualité entre tous les participants TISAX, nous ne pouvons accepter de conditions supplémentaires (telles que des conditions générales d'achat ou des codes de conduite).

Informations supplémentaires concernant notre processus de facturation :

- Nous ne pouvons accepter de conditions d'achat individuelles.
- Nous acceptons :
  - les transferts d'argent sur le compte bancaire spécifié sur la facture
  - les paiements par carte de crédit (durant le processus d'inscription, via notre fournisseur de services de paiement "Stripe")
- Notre facture contiendra les références suivantes de votre inscription :
  - Le nom et l'adresse e-mail de votre principal contact de participant
  - Le nom du périmètre d'évaluation

  Vous trouverez un exemple de facture en annexe à la Section 7.1, "Annexe : exemple de facture".

- Nous indiquons directement sur la facture la plupart des données dont vous avez besoin pour son traitement. Ces données et d'autres encore sont disponibles dans notre document « Information for Members and Business Partners ». Envoyez-nous un e-mail et nous vous ferons parvenir une version actuelle.

Remarque :

Nous sommes conscients que, dans une entreprise, le processus d'approbation interne des paiements prend parfois du temps. Par conséquent, vous pouvez procéder à la prochaine étape du processus TISAX avant même que nous ayons reçu le paiement. Mais gardez à l'esprit qu'il vous sera impossible de partager le résultat de votre évaluation si nous n'avons pas reçu votre paiement.
C'est pourquoi nous vous recommandons de vous assurer que nous envoyons la facture au bon destinataire et qu'elle contient une référence de commande le cas échéant. Peut-être souhaiterez-vous aussi vérifier en interne que quelqu'un a payé la facture.

Remarque importante :

Nous — ENX Association — facturons les frais. Il ne s'agit que d'une partie du coût total d'une évaluation TISAX. Votre auditeur TISAX facture les coût de la/des évaluation(s).

Pour de plus amples informations sur les coûts liés à l'auditeur, vous pouvez consulter la Section 5.3.4, "Évaluation des offres".

Remarque importante :

Les frais sont dus, indépendamment du fait que vous :

- poursuiviez ou non le processus TISAX.
- réussissiez le processus d'évaluation TISAX.

Par conséquent, la facture peut arriver avant que vous ayez entamé l'évaluation initiale.

4.4. Portail ENX

La prochaine section décrira le processus d'inscription en ligne au cours duquel vous saisissez l'ensemble des données que vous avez collectées comme recommandé dans la section précédente. Avant d'entamer le processus d'inscription en ligne, permettez-nous d'expliquer brièvement l'objectif et les avantages du portail ENX.

Le portail ENX nous permet de maintenir une base de données de tous les participants TISAX, et il joue un rôle important tout au long du processus TISAX. Durant le processus d'inscription TISAX, vous saisissez des données que les auditeurs TISAX pourront ensuite utiliser (si vous y consentez) pour calculer leurs offres et pour planifier les procédures d'évaluation. Tout au long du processus d'évaluation TISAX, vous utiliserez la plateforme d'échange sur le portail ENX pour partager le résultat de votre évaluation avec votre partenaire.

Le portail porte le nom de « portail ENX » et non « portail TISAX », car nous l'utilisons aussi pour gérer d'autres activités commerciales (comme le réseau ENX).

4.5. Processus d'inscription en ligne

Si vous vous êtes préparé conformément à nos recommandations ci-dessus (Section 4.3, "Préparation de l'inscription"), vous êtes prêt à démarrer le processus d'inscription en ligne.

4.5.1. Temps nécessaire

Le temps dont vous aurez besoin dépend fortement du nombre de périmètres et de sites que

vous enregistrez. Pour votre première inscription en tant que participant avec un seul périmètre et un seul site, le temps nécessaire à l'inscription sera d'au moins 20 minutes.

Nous vous recommandons de compléter l'inscription lors d'une seule session, car actuellement, il reste difficile de rattraper certaines étapes ultérieurement. Si vous avez quand même besoin de vous interrompre, nous vous contacterons pour vous demander toute donnée manquante.

4.5.2. Démarrez ici

Veuillez entamer votre inscription sur notre site Web à l'adresse :
enx.com/en-us/Account/Login/Register?returnUrl=%2FTISAX%2Ftisax-initial-registration%2F

En fait, il vous suffit de suivre les instructions à l'écran. Néanmoins, nous décrivons brièvement le processus ci-dessous.

4.5.3. Compte sur le portail

Votre première étape consiste à créer un compte pour vous-même sur le portail TISAX. Vous avez besoin d'un compte sur le portail pour pouvoir gérer les « données de participant » de votre entreprise.

Remarque :

Si le portail ENX indique que votre adresse e-mail est déjà utilisée, veuillez nous contacter. Ce message peut indiquer que, pour une quelconque raison, vous figurez déjà dans notre système.

Remarque :

Comme nous l'avons décrit, les comptes sur le portail ne sont pas nécessairement des « contacts de participant » ou des « contacts de périmètre » (cf. ci-dessous) avec un rôle actif dans le processus d'évaluation.

À l'inverse, un « contact de participant » ou un « contact de périmètre » n'inclut pas automatiquement les mêmes droits concernant la gestion des données de participant qu'un compte sur le portail. Cela signifie que des collègues désignés « contact de participant » ou « contact de périmètre » ne peuvent pas automatiquement accéder aux données de participant sur le portail ENX.

Si vous souhaitez attribuer le droit de gérer les données de participant à un contact que vous avez déjà créé sur le portail ENX (indépendamment du fait que vous lui ayez attribué un rôle), vous devez inviter le contact. Pour de plus amples informations, veuillez consulter la dernière remarque de la Section 4.5.5, “Contact de participant”.

4.5.4. Inscription du participant

Votre deuxième étape consiste à inscrire votre entreprise en tant que participant TISAX. Le « participant TISAX » est l'entreprise qui échange des résultats d'évaluation avec d'autres participants.

4.5.5. Contact de participant

Il s'agit de la personne qui est généralement chargée de toutes les questions relatives à l'évaluation de sécurité de l'information dans votre entreprise. Il peut s'agir de vous ou de quelqu'un d'autre au sein de votre entreprise.

Le contact de participant principal est généralement tout ce dont nous avons besoin. Si vous préférez que toutes les communications envoyées par nos soins et par nos auditeurs TISAX dans le cadre de cette inscription le soient aussi à d'autres personnes, veuillez ajouter des contacts de participant supplémentaires.

Remarque importante :

Nous recommandons de désigner au moins un suppléant pour chaque contact. Si un contact est provisoirement indisponible ou quitte l'entreprise, quelqu'un d'autre peut gérer les données de participant de votre entreprise.
Si vous devez désigner un nouveau contact (alors qu'il ne reste plus d'autres contacts valides), vous devez suivre un processus complexe. Notre processus garantit que seules les personnes qui sont capables de prouver qu'elles sont autorisées à représenter légalement l'entreprise peuvent approuver la désignation d'un nouveau contact principal.

Remarque :

Vous pouvez toujours ajouter ou retirer des contacts ultérieurement (même après avoir complété le processus d'inscription en ligne et même une fois que vous avez terminé les évaluations).

Remarque :

Vous ne pouvez pas utiliser des adresses électroniques de groupe pour les contacts de participant (comme « info@acme.com » ou « IT@acme.com »).

Cette règle est conforme aux exigences de l'ISA concernant l'authentification des utilisateurs.

Remarque :

Vous pouvez décider pour chaque contact si celui-ci doit avoir accès aux données de participant de votre entreprise. Soit :

1. Vous ajoutez simplement le contact. Le contact est sauvegardé dans notre système, mais ne peut se connecter et gérer des données.
2. Ou vous invitez le contact. Le portail ENX envoie alors un e-mail d'invitation au contact. Le contact doit suivre le lien d'invitation dans l'e-mail. Une fois que le contact a créé son propre compte personnel pour le portail ENX, il peut gérer les données de participant de votre entreprise.

Pour créer un nouveau contact, rendez-vous dans MON TISAX > ADMINISTRATEURS > Créer un nouvel administrateur TISAX

Pour inviter un contact, rendez-vous dans > MON TISAX > ADMINISTRATEURS > Allez à la fin de la ligne du tableau du contact et cliquez sur la flèche vers le bas > Modifier l'administrateur TISAX > Allez dans la section « ACCÈS AU PORTAIL ENX » > Sélectionnez « Oui » pour « INVITER CE CONTACT » > Cliquez sur « Enregistrer le contact »

4.5.6. Conditions générales

Votre troisième étape consiste à accepter les « Conditions générales de participation TISAX ».

Vous devriez vous référer aux notes explicatives à la Section 4.3.1, “Le fondement juridique”.

4.5.7. Inscription du périmètre d'évaluation

Votre quatrième étape consiste à enregistrer le périmètre d'évaluation pour votre évaluation de sécurité de l'information.

Nous vous demandons de :

1. donner un nom au périmètre d'évaluation.
   Le nom du périmètre a pour objectif principal de vous permettre d'identifier facilement un périmètre dans la liste des périmètres sur le portail ENX.
   Vous devriez vous référer aux notes explicatives à la Section 4.3.2.6, “Nom du périmètre”
2. choisir un type de périmètre d'évaluation.
   (standard, adapté)
   Vous devriez vous référer aux notes explicatives à la Section 4.3.2, “Le périmètre d'évaluation TISAX”.
3. spécifier le principal contact de périmètre.
   Il s'agit de la personne qui est généralement chargée de l'évaluation d'un périmètre particulier. Il peut s'agir de vous ou de quelqu'un d'autre au sein de votre entreprise.
   Le principal contact de périmètre est généralement tout ce dont nous avons besoin. Si vous

préférez que toutes les communications envoyées par nos soins dans le contexte de ce périmètre particulier le soient aussi à d'autres personnes, vous pouvez ajouter des contacts de participant supplémentaires.

4. sélectionner votre/vos objectif(s) d'évaluation.
   Vous devriez vous référer aux notes explicatives à la Section 4.3.3, "Objectifs d'évaluation".
5. ajouter un/plusieurs site(s) de périmètre d'évaluation.
   Nous vous demandons de spécifier tous les sites qui font partie du périmètre d'évaluation.
   Vous devriez vous référer aux notes explicatives à la Section 4.3.2, "Le périmètre d'évaluation TISAX".

Remarque :

Une fois que vous avez créé un nouveau site, vous ne pouvez plus le modifier. Pour des changements mineurs (modification du nom de l'entreprise, coquilles dans le nom de la rue, le code postal, la ville, etc.), veuillez nous contacter. Nous effectuerons les changements pour vous.

Remarque importante :

Cette remarque ne s'applique que si vous renouvelez vos labels TISAX.

Veuillez réutiliser les enregistrements des sites existants que vous avez créés et utilisés lors de l'inscription de votre périmètre précédent. Ne créez pas de nouvel enregistrement de site avec la même adresse.

Voici la raison : certains participants TISAX traitent automatiquement les résultats d'évaluation de leurs partenaires. Ils synchronisent leur propre système avec le portail ENX. La moindre petite différence peut compromettre la synchronisation. De plus, ainsi, vous n'encombrez pas les données de vos participants avec des doublons inutiles.

6. sélectionner les niveaux de publication et de partage (facultatif).
   Vous pouvez déjà décider de publier le résultat de votre évaluation pour d'autres participants TISAX et de le partager avec votre/vos partenaire(s). En principe, vous devriez nous autoriser au moins à indiquer que votre entreprise est un participant et que vous avez réussi le processus TISAX.
   Vous pouvez sans problème ignorer cette étape durant votre inscription initiale. Il vous est toujours possible de définir ultérieurement l'accès au résultat de votre évaluation.
   Vous devriez vous référer aux notes explicatives à la Section 4.3.2.8, "Publication et partage".

Remarque importante :

Vous ne pouvez pas annuler les autorisations de publication ou de partage.

> Pour plus de détails, veuillez consulter la Section 6.4, “Permanence des résultats échangés”.

7. spécifier qui reçoit la facture.
   Nous vous demandons de spécifier qui recevra notre/nos facture(s).
   Vous devriez vous référer aux notes explicatives à la Section 4.3.4, “Frais”.

Remarque :

Vous ne pouvez pas vraiment vous tromper ici. Si vous vous rendez compte ultérieurement que vous auriez dû enregistrer un périmètre légèrement différent (vous avez oublié un site, vous avez un autre objectif d’évaluation, etc.), l’auditeur pourra néanmoins procéder à l’évaluation.

Exemple : l’auditeur détermine que le périmètre comprend un site supplémentaire que vous n’avez initialement pas intégré au périmètre. L’auditeur procédera à l’évaluation et modifiera ensuite votre périmètre d’évaluation sur le portail ENX au moment de télécharger le résultat de l’évaluation.

Remarque :

Chaque périmètre d’évaluation a un cycle de vie. À ce stade, votre périmètre d’évaluation a le statut « Incomplet », « En attente de votre commande » ou « En attente d’approbation ENX ».

Pour de plus amples informations sur le statut d’un périmètre d’évaluation, veuillez consulter la Section 7.5.1, “Aperçu : Assessment scope status (Statut du périmètre d’évaluation)”.

Remarque :

Pour les grandes entreprises multisites, TISAX offre une évaluation de groupe simplifiée. Vous pouvez envisager cette option si :

- vous avez au moins trois sites dans votre périmètre[10] et
- votre système de gestion de la sécurité de l’information est établi et organisé de façon centralisée[11].

Une évaluation de groupe simplifiée requiert un travail initial plus important. Toutefois, plus vous avez de sites, plus ces efforts seront payants.

Pour de plus amples informations sur « l’évaluation de groupe simplifiée »,

veuillez consulter le document « TISAX Simplified Group Assessment ».

Vous pouvez télécharger « TISAX Simplified Group Assessment » sur notre site Web à l'adresse :
enx.com/en-US/TISAX/downloads/

Téléchargement direct du PDF :
enx.com/sga.pdf

Remarque :

Une fois que vous avez enregistré le périmètre d'évaluation, vous ne pourrez pas le modifier vous-même.

Si vous êtes en mesure de nous garantir de manière crédible que vous n'avez PAS encore envoyé votre « extrait de périmètre TISAX » à nos auditeurs, veuillez nous contacter. Nous pouvons le modifier pour vous.

Si vous avez déjà envoyé votre « extrait de périmètre TISAX » à (l'un de) nos auditeurs, vous créez simplement le(s) nouveau(x) site(s) sur le portail ENX (le cas échéant) et discutez de tout changement avec votre auditeur. Votre auditeur réalisera l'évaluation en se basant sur les modifications et mettra à jour les informations relatives au périmètre sur le portail ENX.

Remarque :

Vous ne pouvez pas supprimer un périmètre d'évaluation sur le portail TISAX. Si vous avez créé un périmètre d'évaluation par erreur, veuillez nous contacter. Nous effectuerons la suppression pour vous.

4.5.8. E-mail de confirmation

Une fois que vous aurez accompli toutes les étapes obligatoires ci-dessus, nous examinerons votre demande. Nous vous enverrons alors un e-mail de confirmation.

Cet e-mail comporte deux éléments importants :

- Une liste de contacts de tous les auditeurs TISAX
  Vous devez choisir l'un de nos auditeurs TISAX pour mener une évaluation portant sur votre périmètre d'évaluation. Vous pouvez utiliser les contacts pour solliciter des offres.
  Pour de plus amples informations sur la sélection des auditeurs, veuillez consulter la Section 5.3, "Sélection de l'auditeur".
- L'« Extrait du périmètre TISAX » en tant que fichier PDF joint

  Il contient :

- Les informations que nous avons sauvegardées dans notre base de données
- Votre ID de participant
  Veuillez consulter la Section 4.5.8.1, “Participant ID Participant ID (ID de participant)” ci-dessous.
- Votre/vos ID de périmètre
  Veuillez consulter la Section 4.5.8.2, “Scope ID (ID de périmètre)” ci-dessous.

Pour un exemple d’e-mail de confirmation, veuillez consulter la Section 7.2, “Annexe : exemple d’e-mail de confirmation”.

Pour un exemple d’« extrait de périmètre TISAX », veuillez consulter la Section 7.3, “Annexe : exemple d’extrait de périmètre TISAX”.

En principe, vous recevrez notre e-mail de confirmation dans les trois jours ouvrables.

Si vous n’avez pas de nouvelles de notre part sous sept jours ouvrables, veuillez vérifier que a) vous avez fourni toutes les informations et b) le statut du périmètre d’évaluation est « En attente d’approbation ENX ». Nous ne commencerons à traiter votre inscription que lorsque tout sera complet. Si vous pensez que tout est complet, mais que nous ne vous avons pas contacté, veuillez nous contacter.

Nous envoyons notre e-mail de confirmation au contact de participant principal.

Remarque :

Chaque périmètre d’évaluation a un cycle de vie. À ce stade, le périmètre d’évaluation a le statut « En attente d’approbation ENX ».

Pour de plus amples informations sur le statut d’un périmètre d’évaluation, veuillez consulter la Section 7.5.5, “Assessment scope status “Awaiting your payment” (Statut du périmètre d’évaluation « En attente de votre paiement »)”.

Les deux prochaines sous-sections fournissent des informations détaillées sur l’objectif de votre ID de participant et de l’ID de périmètre.

4.5.8.1. Participant ID Participant ID (ID de participant)

L’ID de participant :

- identifie un participant TISAX.
- est unique pour chaque participant.
- est attribué par nos soins au moment de compléter l’inscription.
- est une condition préalable à la commande d’une évaluation de sécurité de l’information

menée par l'un de nos auditeurs TISAX.

- a le format suivant :

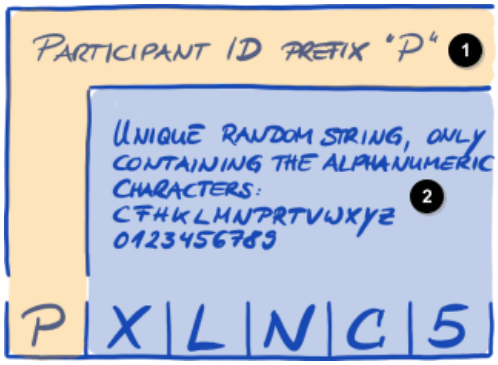


Illustration 7. Format de l'ID de participant[12]

1. Préfixe « P » (pour « Participant ») de l'ID de participant
2. Chaîne aléatoire unique contenant exclusivement des caractères alphanumériques :
   CFHKLMNPRTVWXYZ
   0123456789

Remarque :

Il existe deux façons de trouver votre ID de participant :

1. Vérifiez votre « extrait de périmètre TISAX ».
   Veuillez consulter la Section 4.5.8, "E-mail de confirmation" ci-dessus.
2. Connectez-vous sur le portail ENX, allez dans la barre de navigation principale et sélectionnez "DASHBOARD" (🇫🇷 « TABLEAU DE BORD »). Vous y trouverez votre ID de participant.

4.5.8.2. Scope ID (🇫🇷 ID de périmètre)

Votre ID de périmètre :

- identifie un périmètre d'évaluation.
- est unique pour chaque périmètre d'évaluation.
- est attribué par nos soins au moment de compléter l'inscription.
- constitue une condition préalable pour être autorisé à commander une évaluation de sécurité de l'information menée par l'un de nos auditeurs TISAX.
- a le format suivant :

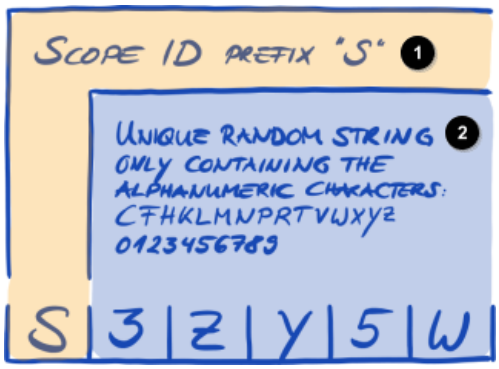


Illustration 8. Format de l'ID de périmètre

1. Préfixe « S » (pour « Scope ») de l'ID de périmètre
2. Chaîne aléatoire unique contenant exclusivement des caractères alphanumériques :
   CFHKLMNPRTVWXYZ
   0123456789

Remarque :

Il existe deux façons de trouver votre ID de périmètre :

1. Vérifiez votre « extrait de périmètre TISAX ».
   Veuillez consulter la Section 4.5.8, "E-mail de confirmation" ci-dessus.
2. Connectez-vous sur le portail ENX, allez dans la barre de navigation principale, sélectionnez « MON TISAX », puis « PÉRIMÈTRES ET ÉVALUATIONS ». Vous y trouverez votre/vos ID de périmètre.

Remarque :

Chaque périmètre d'évaluation (identifié par son ID) a un cycle de vie.

Pour de plus amples informations sur le statut d'un périmètre d'évaluation, veuillez consulter la Section 7.5, "Annexe : Assessment scope status (Statut du périmètre d'évaluation)".

4.5.9. Informations de statut

À ce stade, il existe deux statuts importants que nous utilisons pour décrire votre position dans le processus TISAX :

1. Statut du participant
2. Statut du périmètre d'évaluation

Le diagramme suivant illustre les conditions à remplir pour atteindre un certain statut :

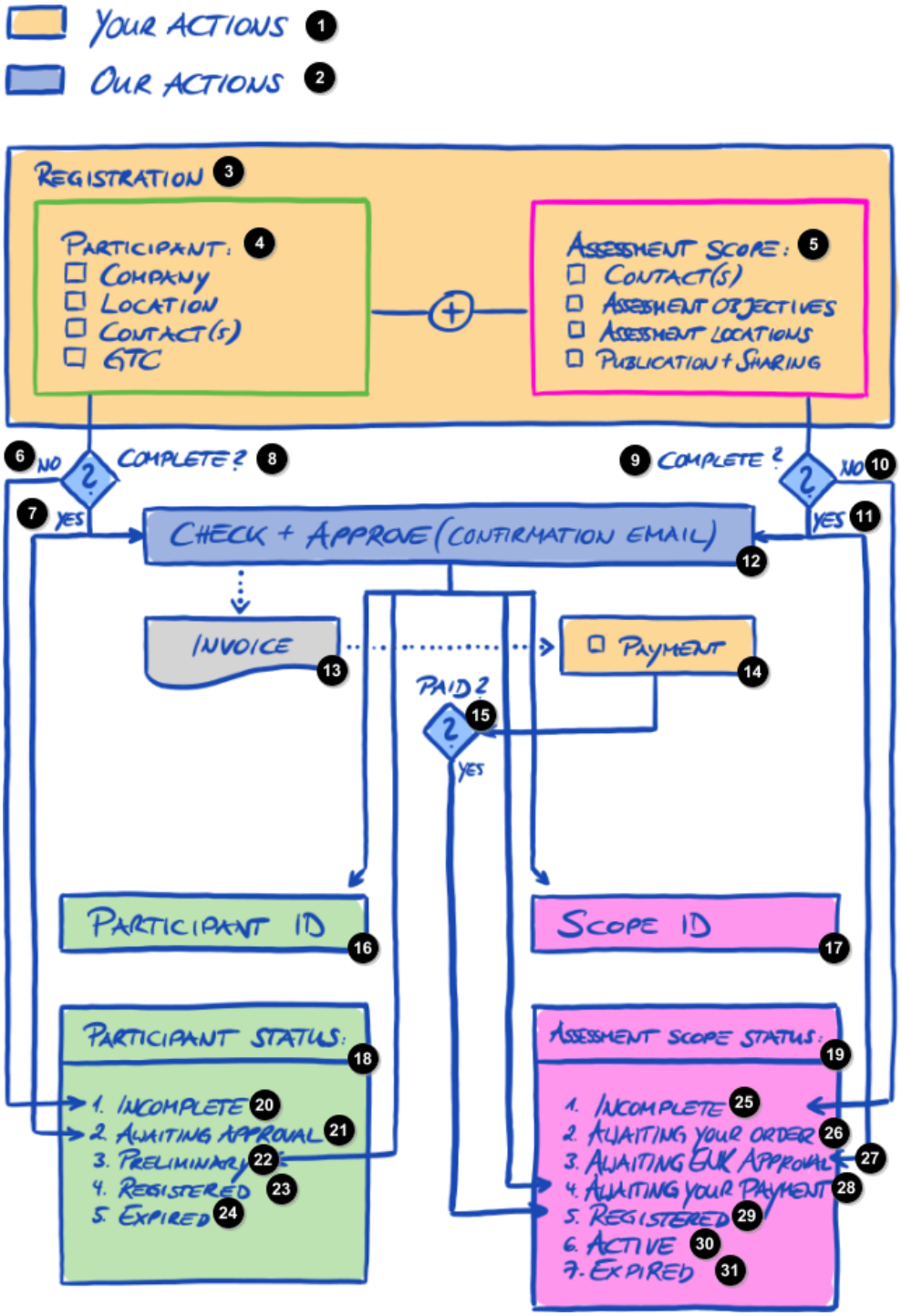


Illustration 9. Conditions relatives au statut du participant et au statut du périmètre d'évaluation

1. Vos actions
2. Nos actions
3. Inscription

4. Participant :
[ ] Entreprise
[ ] Site
[ ] Contact(s)
[ ] CG

5. Périmètre d’évaluation :
[ ] Contact(s)
[ ] Objectifs d’évaluation
[ ] Sites d’évaluation
[ ] Publication + partage

6. Non

7. Oui

8. Complet ?

9. Complet ?

10. Non

11. Oui

12. Vérifier + approuver (e-mail de confirmation)

13. Facture

14. [ ] Paiement

15. Payé ?

16. ID de participant

17. ID de périmètre

18. Statut du participant :

19. Statut du périmètre d’évaluation :

20. 1. Incomplet

21. 2. En attente d’approbation

22. 3. Préliminaire

23. Inscrit

24. Expiré

25. 1. Incomplet

26. 2. En attente de votre commande

27 3. En attente d’approbation ENX

28 4. En attente de votre paiement

29 5. Inscrit

30 6. Actif

31 7. Expiré

Vous trouverez en annexe les définitions des statuts et les étapes à réaliser pour accéder au prochain statut.

Pour de plus amples informations sur :

- le statut du participant, veuillez consulter la Section 7.4, “Annexe : Participant status (🇫🇷 Statut du participant)”.
- le statut du périmètre d’évaluation, veuillez consulter la Section 7.5, “Annexe : Assessment scope status (🇫🇷 Statut du périmètre d’évaluation)”.

4.5.10. Modifications de vos informations d’inscription

Remarque :

Pour toutes les réponses concernant le cycle de vie des données, veuillez consulter la Section 7.9, “Annexe : gestion du cycle de vie des données du participant”. Elle contient des instructions pour les cas où vous souhaitez modifier ou mettre à jour des données telles que le nom de l’entreprise ou vos coordonnées.

Félicitations, vous êtes désormais inscrit en tant que participant TISAX. Vous êtes prêt à passer à l’étape suivante du processus TISAX.

5. Évaluation (étape 2)

Le temps de lecture estimé de la section consacrée à l'évaluation est de 30 à 35 minutes.

5.1. Aperçu

L'évaluation TISAX est votre deuxième étape. C'est à ce stade que l'essentiel du travail doit être réalisé pour mener à bien l'évaluation TISAX.

Les sections suivantes vous guideront tout au long du processus d'évaluation :

1. Dans un premier temps, nous vous expliquerons comment vous pouvez utiliser l'auto-évaluation ISA pour déterminer si vous êtes prêt à passer une évaluation TISAX.
2. Ensuite, nous vous guiderons dans le choix de l'un de nos auditeurs TISAX.
3. Nous décrirons alors votre cheminement tout au long du processus d'évaluation.
4. Enfin, nous vous expliquerons la « conclusion du processus » : le résultat de votre évaluation et les labels TISAX qui y sont associés.

5.2. Auto-évaluation basée sur l'ISA

Pour être prêt à passer une évaluation TISAX, vous devez d'abord vous assurer que votre système de gestion de la sécurité de l'information (ISMS) fonctionne de façon irréprochable. Pour vérifier que votre ISMS correspond au niveau de maturité attendu, vous devez effectuer une auto-évaluation basée sur l'ISA.

L'« évaluation de sécurité de l'information » (ISA) est un catalogue de critères publié par l'« Association allemande de l'industrie automobile » (Verband der Automobilindustrie e.V. – VDA). Il s'agit de la norme utilisée dans l'industrie automobile pour procéder aux évaluations de sécurité de l'information.

Les sections suivantes fournissent des instructions pratiques pour effectuer une auto-évaluation basée sur l'ISA.

Les explications, exemples et captures d'écran dans le présent manuel se fondent sur la version 5 de l'ISA.

Remarque :

Vous trouverez des informations sur les modifications effectuées par rapport aux versions précédentes de l'ISA dans la feuille Excel « Historique des changements ».

Remarque :

> Pour de plus amples informations sur la version de l'ISA applicable à votre évaluation lorsque la VDA publie une nouvelle version, veuillez consulter la Section 7.11, "Annexe : gestion du cycle de vie de l'ISA".

5.2.1. Téléchargement du document ISA

Débutez votre auto-évaluation en téléchargeant le document ISA.

Vous pouvez le télécharger depuis notre site Web :
enx.com/en-US/TISAX/downloads/

Téléchargement direct du fichier Excel :
portal.enx.com/isa5-en.xlsx

Le document ISA est également disponible en allemand :
enx.com/de-de/TISAX/downloads/

5.2.2. Compréhension du document ISA

Avant de débuter votre auto-évaluation, voici quelques explications qui pourraient vous être utiles. Elles vous sont données en complément aux explications officielles et aux définitions exposées dans le document ISA, et se concentrent surtout sur une utilisation dans le cadre des évaluations TISAX.

5.2.2.1. Catalogues de critères

L'ISA a actuellement trois « catalogues de critères »[13] :

1.	Sécurité de l'information	Information Security
2.	Protection des prototypes	Prototype Protection
3.	Protection des données	Data Protection

Chaque catalogue de critères a sa propre feuille Excel :

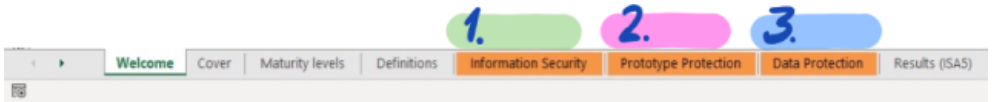


Illustration 10. Capture d'écran : catalogues de critères ISA en tant que feuilles Excel

Quel catalogue de critères est pertinent pour vous ? Cela dépend de votre/vos objectif(s) d'évaluation.

Chaque objectif d'évaluation définit quelles exigences de quel catalogue de critères s'appliquent. Pour certains objectifs d'évaluation, seules les exigences d'*un* catalogue de critères s'appliquent.

Pour d'autres, les exigences de *plusieurs* catalogues de critères s'appliquent.

Les objectifs d'évaluation susmentionnés correspondent à ces catalogues de critères :

Nº	Objectif d'évaluation (Assessment objective)	Catalogue(s) de critères ISA
1.	Info high	Information Security (Sécurité de l'information)
2.	Info very high	Information Security (Sécurité de l'information)
3.	Confidential	Information Security (Sécurité de l'information)
4.	Strictly confidential	Information Security (Sécurité de l'information)
5.	High availability	Information Security (Sécurité de l'information)
6.	Very high availability	Information Security (Sécurité de l'information)
7.	Proto parts	Prototype Protection (Protection des prototypes)
8.	Proto vehicles	Prototype Protection (Protection des prototypes)
9.	Test vehicles	Prototype Protection (Protection des prototypes)
10.	Proto events	Prototype Protection (Protection des prototypes)
11.	Data	Information Security (Sécurité de l'information) Data Protection (Protection des données)
12.	Special data	Information Security (Sécurité de l'information) Data Protection (Protection des données)

Tableau 7. Correspondance entre les objectifs d'évaluation TISAX et les catalogues de critères ISA

Exemple : si vous avez sélectionné l'objectif d'évaluation « Protection des données », vous devrez répondre aux questions dans les catalogues de critères « Sécurité de l'information » ET « Protection des données ».

Vous aurez peut-être remarqué qu'il existe plus d'un objectif d'évaluation par catalogue de critères. Comment savoir quelles exigences sont applicables à quel objectif d'évaluation ?

Le tableau suivant vous indique quelles exigences sont applicables :

Nº	Objectif d'évaluation (Assessment objective)	Exigences applicables
1.	Info high	▪ Catalogue de critères "Information Security" (« Sécurité de l'information ») ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) ») ◦ Colonne "Additional requirements for high protection needs" (« Exigences supplémentaires pour des besoins de protection importants »)
2.	Info very high	▪ Catalogue de critères "Information Security" (« Sécurité de l'information ») ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) ») ◦ Colonne "Additional requirements for high protection needs" (« Exigences supplémentaires pour des besoins de protection importants ») ◦ Colonne ( ) « Exigences supplémentaires pour des besoins de protection très importants »
3.	Confidential	▪ Catalogue de critères "Information Security" (« Sécurité de l'information ») ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) ») ◦ Colonne "Additional requirements for high protection needs" (« Exigences supplémentaires pour des besoins de protection importants ») (mais uniquement celles marquées avec un « **C** » pour **C**onfidentiality (Confidentialité))

Nº	Objectif d'évaluation (Assessment objective)	Exigences applicables
4.	Strictly confidential	▪ Catalogue de critères "Information Security" (« Sécurité de l'information ») ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) ») ◦ Colonne "Additional requirements for high protection needs" (« Exigences supplémentaires pour des besoins de protection importants ») (mais uniquement celles marquées avec un « **C** » pour **C**onfidentiality (Confidentialité)) ◦ Colonne ( ) « Exigences supplémentaires pour des besoins de protection très importants » (mais uniquement celles marquées avec un « **C** » pour **C**onfidentiality (Confidentialité))
5.	High availability	▪ Catalogue de critères "Information Security" (« Sécurité de l'information ») ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) ») ◦ Colonne "Additional requirements for high protection needs" (« Exigences supplémentaires pour des besoins de protection importants ») (mais uniquement celles marquées avec un « **A** » pour **A**vailability (Disponibilité))

Nº	Objectif d'évaluation (Assessment objective)	Exigences applicables
6.	Very high availability	▪ Catalogue de critères "Information Security" (« Sécurité de l'information ») ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) ») ◦ Colonne "Additional requirements for high protection needs" (« Exigences supplémentaires pour des besoins de protection importants ») (mais uniquement celles marquées avec un « **A** » pour **A**vailability (Disponibilité)) ◦ Colonne ( ) « Exigences supplémentaires pour des besoins de protection très importants » (mais uniquement celles marquées avec un « **A** » pour **A**vailability (Disponibilité))
7.	Proto parts	▪ Catalogue de critères "Prototype Protection" (« Protection des prototypes ») Mais uniquement ces chapitres : 8.1 Physical and Environmental Security (8.1 Physical and Environmental Security (« Sécurité physique et environnementale »)) 8.2 Organizational Requirements (8.2 Organizational Requirements (« Exigences organisationnelles »)) 8.3 Handling of vehicles, components and parts (8.3 Handling of vehicles, components and parts (« Traitement des véhicules, composantes et pièces »)) ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) »)

Nº	Objectif d'évaluation (Assessment objective)	Exigences applicables
8.	Proto vehicles	▪ Catalogue de critères "Prototype Protection" (« Protection des prototypes ») Mais uniquement ces chapitres : 8.1 Physical and Environmental Security (8.1 Physical and Environmental Security (« Sécurité physique et environnementale »)) 8.2 Organizational Requirements (8.2 Organizational Requirements (« Exigences organisationnelles »)) 8.3 Handling of vehicles, components and parts (8.3 Handling of vehicles, components and parts (« Traitement des véhicules, composantes et pièces »)) ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) ») ◦ Colonne "Additional requirements for vehicles classified as requiring protection" (« Exigences supplémentaires pour des véhicules classés comme nécessitant une protection »)
9.	Test vehicles	▪ Catalogue de critères "Prototype Protection" (« Protection des prototypes ») Mais uniquement ces chapitres : 8.2 Organizational Requirements (8.2 Organizational Requirements (« Exigences organisationnelles »)) 8.3 Handling of vehicles, components and parts (8.3 Handling of vehicles, components and parts (« Traitement des véhicules, composantes et pièces »)) 8.4 Requirements for trial vehicles (8.4 Requirements for trial vehicles (« Exigences pour les véhicules de test »)) ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) »)

Nº	Objectif d'évaluation (Assessment objective)	Exigences applicables
10.	Proto events	▪ Catalogue de critères "Prototype Protection" (« Protection des prototypes ») Mais uniquement ces chapitres : 8.2 Organizational Requirements (8.2 Organizational Requirements (« Exigences organisationnelles »)) 8.3 Handling of vehicles, components and parts (8.3 Handling of vehicles, components and parts (« Traitement des véhicules, composantes et pièces »)) 8.5 Requirements for events and shootings (8.5 Requirements for events and shootings (« Exigences pour les événements et les shootings »)) ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) »)
11.	Data	▪ Catalogue de critères "Information Security" (« Sécurité de l'information ») ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) ») ◦ Colonne "Additional requirements for high protection needs" (« Exigences supplémentaires pour des besoins de protection importants ») (mais uniquement celles marquées avec un « **C** » pour **C**onfidentiality (Confidentialité)) ▪ Catalogue de critères "Data Protection" (« Protection des données ») ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) »)

Nº	Objectif d'évaluation (Assessment objective)	Exigences applicables
12.	Special data	▪ Catalogue de critères "Information Security" (« Sécurité de l'information ») ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) ») ◦ Colonne "Requirements (should)" (« Exigences (recommandées) ») ◦ Colonne "Additional requirements for high protection needs" (« Exigences supplémentaires pour des besoins de protection importants ») (mais uniquement celles marquées avec un « **C** » pour **C**onfidentiality (Confidentialité)) ◦ Colonne ( ) « Exigences supplémentaires pour des besoins de protection très importants » (mais uniquement celles marquées avec un « **C** » pour **C**onfidentiality (Confidentialité)) ▪ Catalogue de critères "Data Protection" (« Protection des données ») ◦ Colonne "Requirements (must)" (« Exigences (obligatoires) »)

Tableau 8. Applicabilité des exigences aux objectifs d'évaluation

Remarque :

Chaque exigence des colonnes « Exigences supplémentaires pour des besoins de protection importants » et « Exigences supplémentaires pour des besoins de protection très importants » est marquée par un « **C** » pour **C**onfidentiality (Confidentialité), un « **I** » pour **I**ntegrity (Intégrité) ou un « **A** » pour **A**vailability (Disponibilité) ou une combinaison de ces trois lettres.

Lorsque le tableau ci-dessous limite les exigences listées dans ces deux colonnes à celles marquées par l'*une* des lettres mentionnées ci-dessus, cela comprend toujours les exigences qui sont également indiquées par *les autres* lettres.

Exemple : toutes les exigences marquées « (C) », « (C, I, A) » ou « (C, I) » s'appliquent lorsque « C » est indiqué dans le tableau ci-dessus (par ex. dans l'objectif d'évaluation « Special data »).

La capture d'écran ci-dessous illustre les principaux éléments des questions de contrôle figurant dans le catalogue de critères « Sécurité de l'information ». (Les autres catalogues de critères possèdent uniquement un sous-ensemble de ces éléments.) Tous les éléments sont expliqués plus bas.

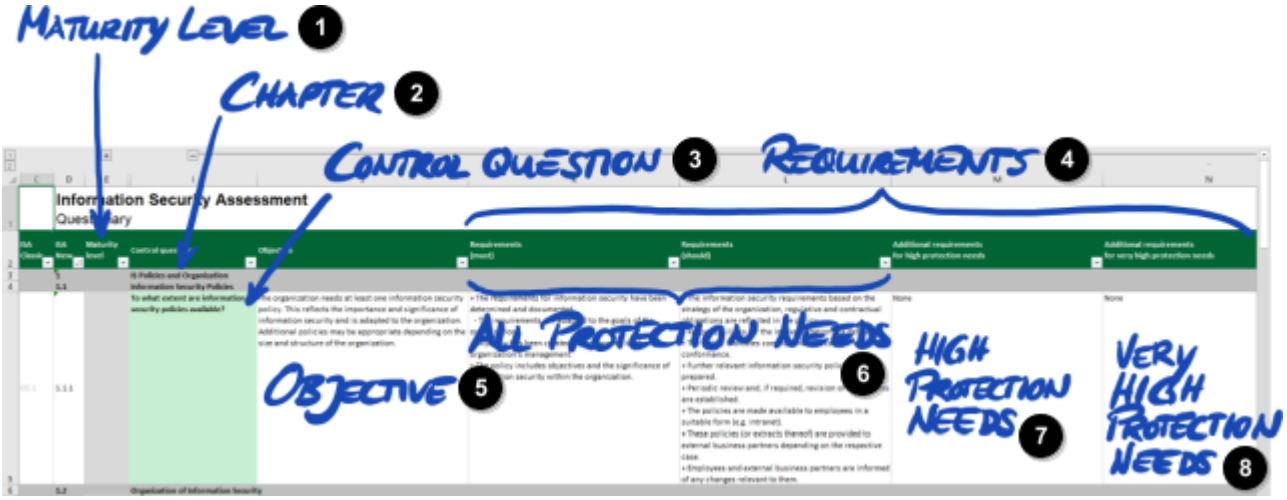


Illustration 11. Capture d'écran : principaux éléments des questions figurant dans le catalogue de critères ISA « Sécurité de l'information »

1. Niveau de maturité
2. Chapitre
3. Question de contrôle
4. Exigences
5. Objectif
6. Tous les besoins de protection
7. Besoins de protection importants
8. Besoins de protection très importants

5.2.2.2. Chapitres

Chaque catalogue de critères groupe les questions en chapitres.

Exemple : « 2 Human Resources »

Le regroupement repose sur les responsabilités traditionnelles dans une entreprise. Ces services sont indiqués dans la colonne « Usual person responsible for process implementation » (Personne habituellement responsable de la mise en œuvre du processus) (« HR » (« RH ») dans l'exemple ci-dessus).

5.2.2.3. Questions de contrôle

Vous trouverez les questions relatives à chaque catalogue de critères dans les feuilles Excel correspondantes.

Exemple : « 4.1.2 Dans quelle mesure l'accès utilisateur aux services en réseau, aux systèmes et applications informatiques est-il sécurisé ? »

Les questions de contrôle sont également désignées « contrôles ». Elles sont comparables à des questions d'audit. Les normes ISO sur lesquelles s'appuie l'ISA utilisent le terme de « contrôle ».

5.2.2.4. Champs du formulaire d'auto-évaluation

Entre les colonnes "Maturity level" (« Niveau de maturité ») et "Control question" (« Question de contrôle ») se trouvent les champs du formulaire que vous devez remplir lorsque vous effectuez une auto-évaluation :

Champ du formulaire	Objectif	Obligatoire ?
Implementation description (Description de la mise en œuvre) (colonne F)	Vous devez ici décrire brièvement ce que vous avez mis en œuvre pour traiter cette question de contrôle dans votre entreprise.	Oui
Reference Documentation (Documentation de référence) (colonne G)	Vous devez ici spécifier dans quel(s) document(s) vous attestez de la mise en œuvre.	Oui
Findings/Result (Constatations/résultat) (colonne H)	Vous pouvez ici prendre note de toutes les constatations pour lesquelles, selon vous, il existe un écart entre la situation telle qu'elle est et telle qu'elle devrait être.	Non

Tableau 9. Champs du formulaire d'auto-évaluation et leur objectif

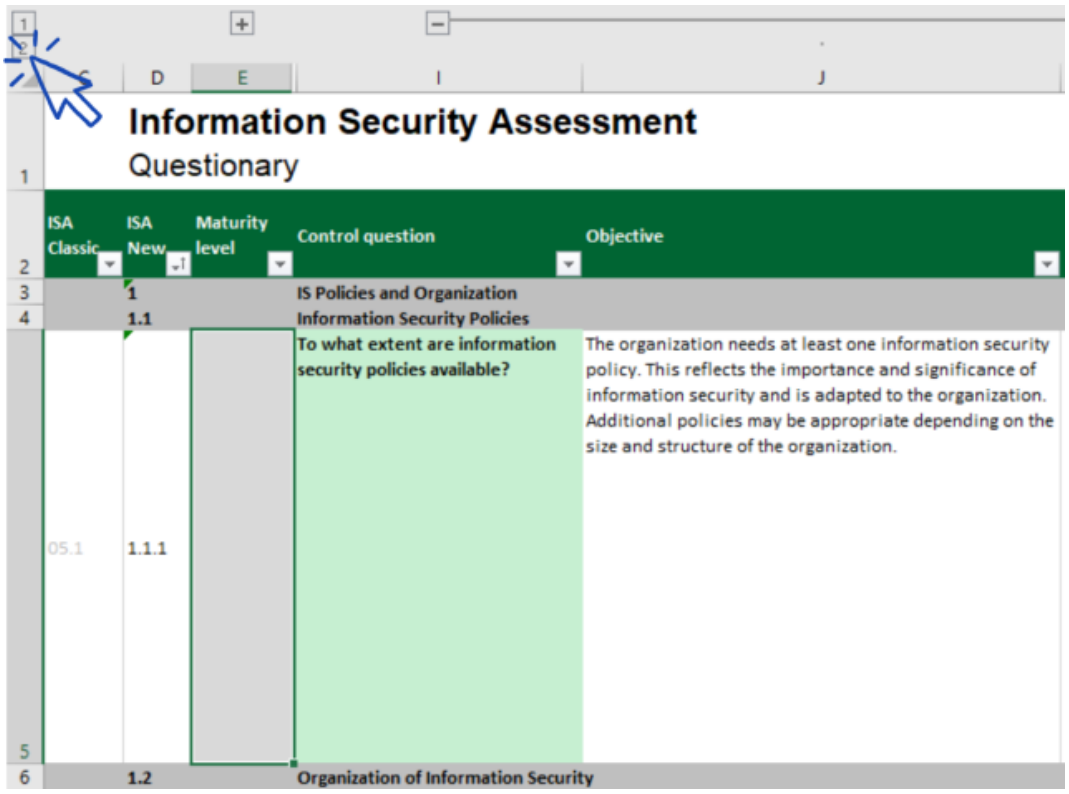
Seules la brève description de votre mise en œuvre et la référence à votre documentation sont obligatoires. Cette information aidera nos auditeurs TISAX à mieux comprendre votre entreprise et à préparer l'évaluation.

Il existe d'autres colonnes facultatives utiles à votre auto-évaluation :

- Measures/recommendations (Mesures/recommandations) (colonne R)
- Date of assessment (Date d'évaluation) (colonne S)
- Date of completion (Date d'achèvement) (colonne T)
- Responsible department (Service responsable) (colonne U)
- Contact (Contact) (colonne V)

Remarque importante :

Si vous ouvrez le fichier Excel téléchargé et sélectionnez l'une des feuilles de travail du catalogue de critères (p. ex. : Sécurité de l'information), il se peut que vous ne voyiez pas immédiatement les champs du formulaire d'auto-évaluation. Pour les afficher, vous devez cliquer sur le bouton de groupement de niveau « 2 »[14]. Le bouton se trouve en haut à gauche de la cellule C1. Vous agrandirez ainsi la zone de visualisation et afficherez les champs du formulaire d'auto-évaluation.



Vous pouvez aussi utiliser les touches fléchées de défilement vers le bas. En raison de la taille importante des cellules, il se peut que le défilement à l'aide de la barre nécessite une excellente motricité fine. Si vous utilisez la fonction de défilement de votre dispositif de pointage, vous risquez aussi de sauter par mégarde certaines des cellules de grande taille.

5.2.2.5. Objectif

La colonne « Objectif » (colonne J) se trouve à droite de la colonne « Question de contrôle ». Son contenu décrit ce que vous devez effectuer concernant cet aspect de votre gestion de la sécurité de l'information.

Exemple (pour la question de contrôle 4.1.2) : « Seuls des utilisateurs identifiés de manière fiable (authentifiés) peuvent accéder aux systèmes informatiques. Dans cette optique, l'identité d'un utilisateur est déterminée en toute fiabilité par l'intermédiaire de procédures adéquates. »

5.2.2.6. Exigences

Les exigences désignent les conditions que vous devez remplir pour atteindre l'objectif.

Les exigences sont réparties sur quatre colonnes :

1. Requirements (must) (Exigences (obligatoires)) (colonne K)
2. Requirements (should) (Exigences (recommandées)) (colonne L)
3. Additional requirements for high protection needs (Exigences supplémentaires pour des besoins de protection importants) (colonne M)
4. Additional requirements for very high protection needs (Exigences supplémentaires pour des besoins de protection très importants) (colonne N)

Vous devez répondre à toutes les exigences correspondant au besoin de protection à satisfaire (que vous pouvez trouver dans votre objectif d'évaluation).

Pour certains objectifs d'évaluation, seul un sous-ensemble des exigences s'applique. Pour de plus amples informations sur l'applicabilité des exigences, veuillez consulter le Tableau 8, "Applicabilité des exigences aux objectifs d'évaluation" dans la Section 5.2.2.1, "Catalogues de critères" et plus particulièrement la note à la fin de la section.

Pour de plus amples informations sur les définitions ISA des niveaux d'exigence « obligatoire » et « recommandée », veuillez consulter les « termes clés » dans la feuille Excel « Définitions ».

Remarque importante :

Il est très important que vous compreniez que vous devez interpréter chaque exigence dans le contexte et l'esprit de l'objectif. Le fait de remplir une exigence à la lettre ne vous garantit pas que l'auditeur confirmera que vous la remplissez dans le contexte et l'esprit de l'objectif (colonne J).

Les exigences et leur formulation sont basées sur une mise en œuvre théorique par une entreprise moyenne et fictive de taille inconnue.

L'auditeur doit toujours comparer l'objectif à la mise en œuvre particulière dans votre entreprise. Ce qui est approprié pour une entreprise moyenne ne l'est pas forcément dans votre situation.

Pour de plus amples informations, veuillez consulter la Section 5.2.5, "Traitement du résultat d'auto-évaluation".

5.2.2.7. Niveaux de maturité

L'ISA utilise le concept de "maturity levels" (« niveaux de maturité ») pour évaluer la qualité de tous les aspects de votre système de gestion de la sécurité de l'information. Plus votre

système est sophistiqué, plus votre niveau de maturité sera élevé.

L'ISA distingue six niveaux de maturité. Vous trouverez la définition détaillée dans la feuille Excel "Maturity levels" (« Niveaux de maturité »). Pour assurer une vision consolidée des niveaux de maturité, nous reprenons les descriptions informelles fournies dans l'ISA :

Maturity level (Niveau de maturité)	**En un mot**	**Description**
0	Incomplete (Incomplet)	Un processus n'est pas disponible, pas suivi ou pas adapté à la réalisation de l'objectif
1	Performed (Exécuté)	Un processus non documenté ou documenté de façon incomplète est suivi, et des indicateurs attestent qu'il atteint son objectif.
2	Managed (Géré)	Un processus atteignant ses objectifs est suivi. La documentation du processus et des preuves de sa mise en œuvre sont disponibles.
3	Established (Établi)	Un processus standard intégré dans un système global est suivi. Des dépendances à d'autres processus sont documentées et des interfaces adéquates sont créées. Il existe des preuves que le processus a été utilisé de manière durable et active sur une période prolongée.
4	Predictable (Prévisible)	Un processus établi est suivi. L'efficacité du processus est surveillée en permanence grâce à la collecte de données clés. Des valeurs limites sont définies auxquelles le processus est considéré comme insuffisamment efficace et nécessitant des ajustements. (Indicateurs clés de performance)
5	Optimizing (Optimisant)	Un processus prévisible est suivi, dont l'un des objectifs majeurs est l'amélioration continue. L'amélioration est promue de manière active par des ressources dédiées.

Tableau 10. Description informelle des niveaux de maturité

Vous devez évaluer le niveau de maturité de votre système de gestion de la sécurité de l'information par question. Saisissez votre niveau de maturité dans la colonne "Maturity level" (« Niveau de maturité ») (colonne E).

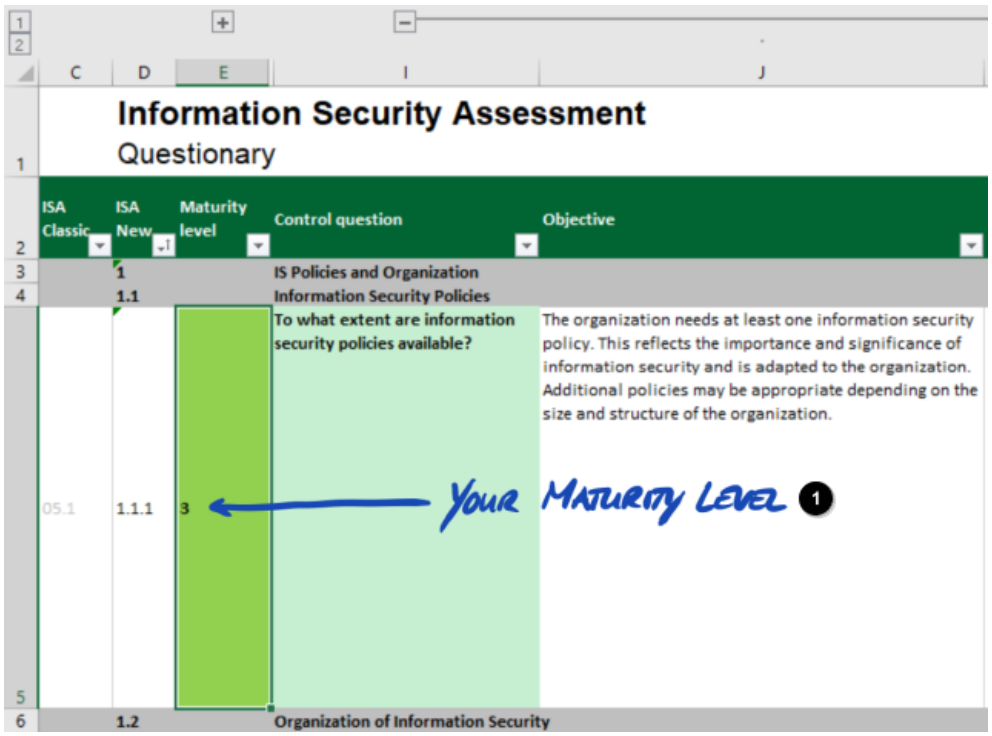


Illustration 12. Capture d'écran : exemple de sélection du niveau de maturité dans le document ISA (feuille Excel « Sécurité de l'information »)

1 Votre niveau de maturité

Pour de plus amples informations sur les niveaux de maturité cibles et leur impact sur le résultat de votre évaluation, veuillez consulter la Section 5.2.4, "Interprétation du résultat d'auto-évaluation".

Maintenant que vous avez une meilleure compréhension des choses, vous pouvez commencer votre auto-évaluation.

5.2.3. Réalisation de l'auto-évaluation

Ouvrez le fichier Excel, passez en revue toutes les questions de contrôle de chaque catalogue de critères applicable à votre/vos objectif(s) d'évaluation et déterminez le niveau de maturité qui correspond à l'état actuel de votre système de gestion de la sécurité de l'information. Faites-le sur la base de votre meilleur jugement. À ce stade, il n'y a pas de bon ou de mauvais jugement.

Une fois que vous avez rempli l'auto-évaluation, la colonne « Résultat » (H) dans la feuille Excel « Résultats (ISA5) » doit être intégralement complétée à l'aide de chiffres (0-5) ou avec la mention « n.a. » (non applicable).

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3
1.2.3	To what extent are information security requirements taken into account in projects?	3	3
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	3
1.3.1	To what extent are information assets identified and recorded?	3	3
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	3
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	3
1.4.1	To what extent are information security risks managed?	3	3
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	3
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	3
1.6.1	To what extent are information security events processed?	3	3

1 GREEN = ✓

Illustration 13. Capture d'écran : exemple de feuille « Résultats (ISA5) » dans le document ISA

1 Vert

Si vous avez des questions concernant l'ISA, veuillez nous contacter.

5.2.4. Interprétation du résultat d'auto-évaluation

Les cinq sous-sections suivantes expliquent comment analyser et interpréter le résultat de votre auto-évaluation. L'analyse vous dira si vous êtes prêt ou pas pour une évaluation TISAX.

5.2.4.1. Analyse

Votre note de résultat synthétise le résultat de l'auto-évaluation.

Vous trouverez la note du résultat (« Résultat réduit au niveau de maturité cible ») dans la feuille Excel « Résultats (ISA5) » (cellule D6). Nous expliquerons plus tard la notion de « réduction ».

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: YOUR RESULT SCORE 1 MAXIMUM RESULT SCORE 2

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Illustration 14. Capture d'écran : votre note de résultat et la note de résultat maximale (feuille Excel « Résultats (ISA5) », cellules D6 et G6)

1. Votre note de résultat
2. Note de résultat maximale

Afin de mieux comprendre et d'interpréter le résultat de votre auto-évaluation et votre note de résultat, vous devez distinguer deux niveaux d'analyse :

1. Niveau questions
   Ce niveau regroupe toutes les questions. Pour chaque question, on distingue le niveau de maturité cible et votre niveau de maturité.
2. Niveau note
   On trouve à ce niveau le résultat global synthétisant les résultats de toutes les questions. On distingue la note de résultat maximale et votre note de résultat.

L'illustration ci-dessous illustre les niveaux d'analyse :

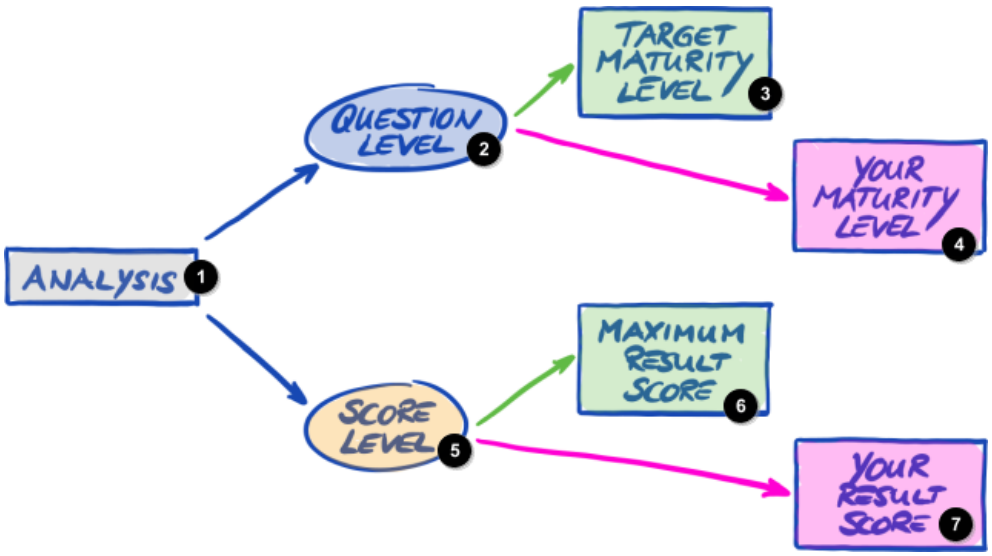


Illustration 15. Analyse du résultat d'auto-évaluation au niveau questions et au niveau note

1. Analyse
2. Niveau questions
3. Niveau de maturité cible
4. Votre niveau de maturité
5. Niveau note
6. Note de résultat maximale
7. Votre note de résultat

L'illustration ci-dessous vous montre où trouver les résultats au niveau note et au niveau questions :

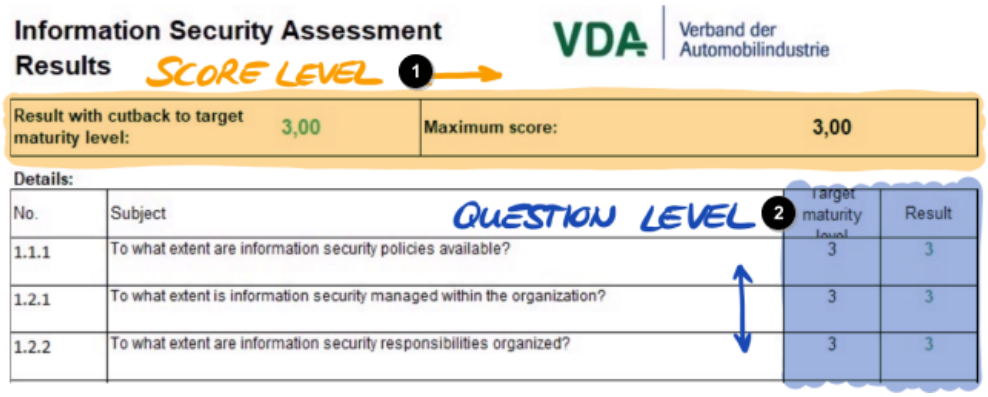


Illustration 16. Niveau note et niveau questions dans la feuille Excel « Résultats (ISA5) »

1. Niveau note
2. Niveau questions

L'illustration suivante offre une vue simplifiée des niveaux d'analyse, des définitions des cibles ISA et de vos propres résultats :

Illustration 17. Les cibles et vos résultats au niveau questions et au niveau note

1. Niveau de maturité cible
2. Votre niveau de maturité
3. Niveau questions
4. Q (Question)
5. TML (Niveau de maturité cible)
6. YML (Votre niveau de maturité)
7. Note de résultat maximale
8. Votre note de résultat
9. Niveau note

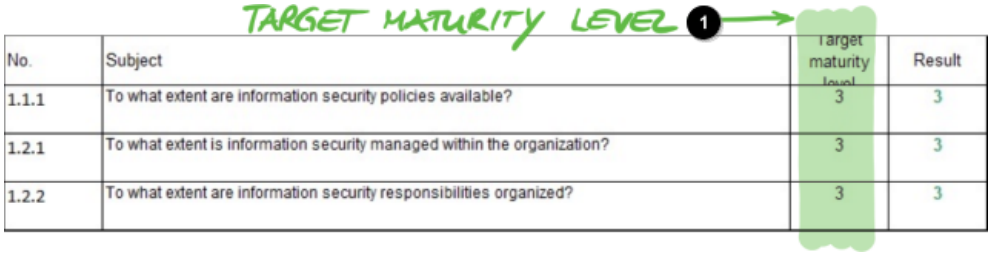
Les sections suivantes expliquent en détail le résultat et son analyse.

5.2.4.2. Le niveau de maturité cible (au niveau questions)

L'ISA définit un « niveau de maturité cible » de 3 pour chaque question.

Pour de plus amples informations sur la définition de chaque niveau de maturité, veuillez consulter la Section 5.2.2, "Compréhension du document ISA".

L'ISA définit les niveaux de maturité cibles dans la feuille Excel « Résultats (ISA5) » (en commençant par la colonne G, ligne 22 ; cf. l'illustration ci-dessous).



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Illustration 18. La définition du niveau de maturité cible dans la feuille Excel « Résultats (ISA5) »

1 Niveau de maturité cible

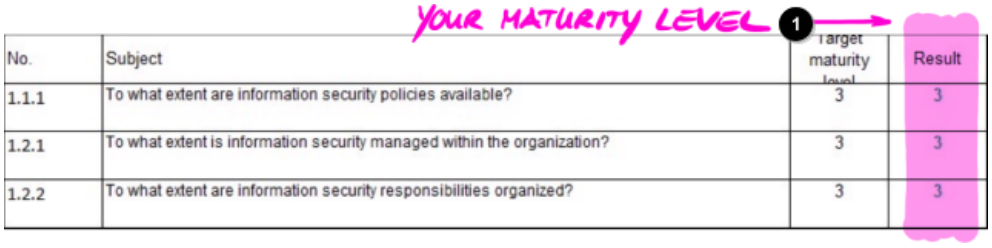
5.2.4.3. Votre résultat (au niveau questions)

Pour recevoir des labels TISAX, vous devez normalement avoir pour chaque question des niveaux de maturité égaux ou supérieurs au niveau de maturité cible.

Exemple : si le niveau de maturité cible pour la question X est de « 3 », votre niveau de maturité pour cette question doit être au moins égal à « 3 ». Si votre niveau de maturité pour cette question est inférieur à « 3 », il se peut que vous ne receviez pas de labels TISAX.

Il en va de même pour chaque question. Si le niveau de maturité cible pour deux questions est de « 3 », vous ne pouvez pas compenser le niveau de maturité de « 2 » obtenu pour une question avec un niveau de maturité de « 4 » obtenu pour l'autre.

Le document ISA transfère automatiquement vos niveaux de maturité de la feuille Excel « Sécurité de l'information » (colonne E) à la feuille Excel « Résultats (ISA5) (en commençant par la colonne H, ligne 23) :



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Illustration 19. Vos niveaux de maturité dans la feuille Excel « Résultats (ISA5) »

1. Votre niveau de maturité cible

Votre niveau de maturité fait l'objet d'un calcul avant que le document ISA le synthétise dans votre note de résultat. En fait, votre niveau de maturité est « réduit » au niveau de maturité cible. Cette réduction est effectuée de sorte que les questions pour lesquelles votre niveau de maturité est *supérieur* au niveau de maturité cible ne puissent pas compenser les questions pour lesquelles votre niveau de maturité est *inférieur* au niveau de maturité cible.

Voici comment l'ISA calcule votre résultat au niveau questions :

- Elle prend votre niveau de maturité et le compare au niveau de maturité cible de la question.
- Si votre niveau de maturité est supérieur au niveau de maturité cible, il est « réduit » au niveau de maturité cible.
- Si votre niveau de maturité est inférieur ou égal au niveau de maturité cible, il ne se passera rien pour cette question.

Exemple (cf. l'illustration ci-dessous) : le niveau de maturité cible est de « 3 ». Votre niveau de maturité est de « 4 ». Votre « résultat réduit » pour cette question sera de « 3 ».

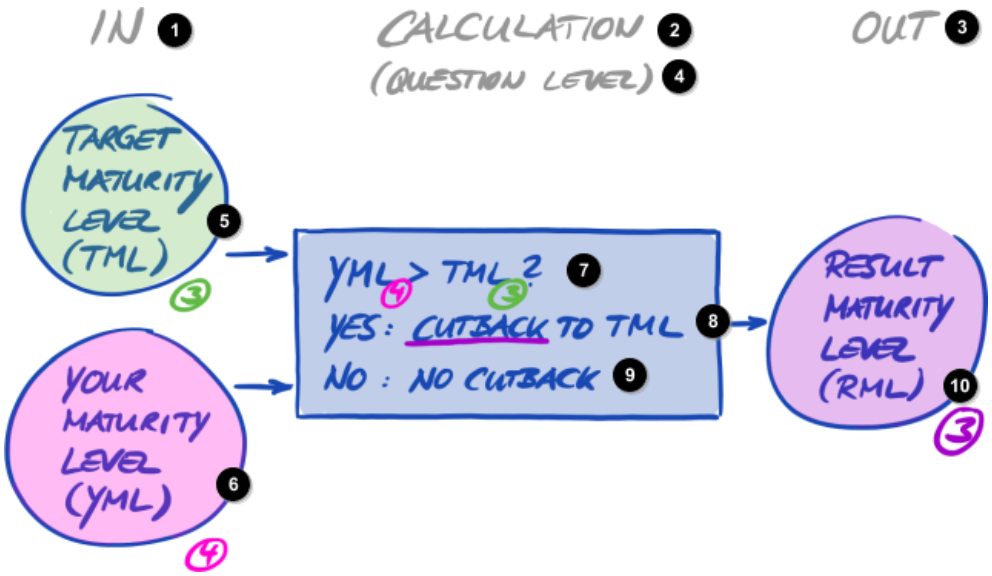


Illustration 20. Calcul de réduction du niveau de maturité du résultat

1. In
2. Calcul
3. Out
4. (Niveau questions)
5. Niveau de maturité cible (TML)

6. Votre niveau de maturité (YML)
7. YML > TML ?
8. Oui : réduction au TML
9. Non : pas de réduction
10. Niveau de maturité du résultat (RML)

L'illustration ci-dessous montre que si votre niveau de maturité est supérieur au niveau de maturité cible, l'ISA le réduira (les couleurs vert, orange et rouge correspondent aux couleurs utilisées dans la colonne « Résultat », cf. Illustration 19, "Vos niveaux de maturité dans la feuille Excel « Résultats (ISA5) »").

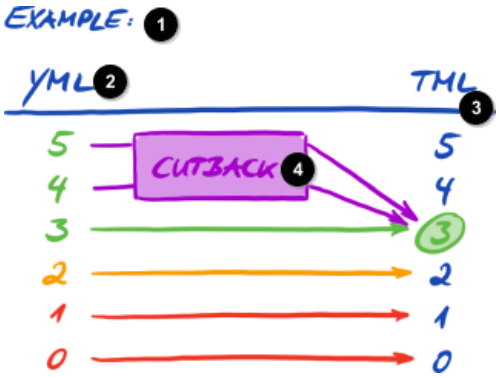


Illustration 21. Illustration de la réduction avec les couleurs utilisées dans la feuille Excel « Résultats (ISA5) »

1. Exemple :
2. YML
3. TML
4. Réduction

Une autre façon d'afficher les niveaux de maturité au niveau questions est illustrée ci-dessous. Les couleurs des cercles illustrent le niveau de maturité cible ou la « distance » par rapport à celui-ci (exemple : le cercle est orange si le niveau de maturité est de « -1 » par rapport au niveau de maturité cible). Les coches illustrent votre niveau de maturité.

Illustration 22. Niveaux de maturité au niveau questions

1. Niveau de maturité
2. Question
3. Réduction
4. Niveau de maturité cible (TML)
5. Un niveau ou plus au-dessus du TML
6. Un niveau en dessous du TML
7. Deux niveaux ou plus en dessous du TML
8. Votre niveau de maturité (YML)
9. Réduction au TML

Remarque :

Vous pouvez passer avec succès une évaluation TISAX, même si vous n'atteignez pas le niveau de maturité cible pour toutes les questions. La question principale dans ce genre de cas est de savoir si vous courez un risque important. Si votre niveau de maturité est inférieur à la valeur cible, mais qu'il n'existe aucun risque, ce niveau peut quand même être suffisant.

5.2.4.4. La cible (au niveau note)

L'ISA définit un niveau de maturité global « idéal » — la « note de résultat maximale » (ou la « note maximale », cellule G6).

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

MAXIMUM RESULT SCORE

Details:

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Illustration 23. Note de résultat maximale (feuille Excel « Résultats (ISA5) »)

1. Note de résultat maximale

En théorie, ce niveau de maturité global est la moyenne de tous les niveaux de maturité cibles (au niveau questions). Il s'agira d'une note de résultat maximale de « 3,0 ».

Toutefois, celle-ci est égale à « 3,0 » uniquement si toutes les questions s'appliquent à votre situation. Dès qu'une question ne s'applique pas à votre situation, la moyenne change et la note de résultat maximale descend en dessous de « 3,0 ».

Sur la base de ce qui a été illustré plus haut (Illustration 22, "Niveaux de maturité au niveau questions"), vous pouvez voir ci-dessous ce qui est pris en compte dans la moyenne pour la note de résultat maximale :

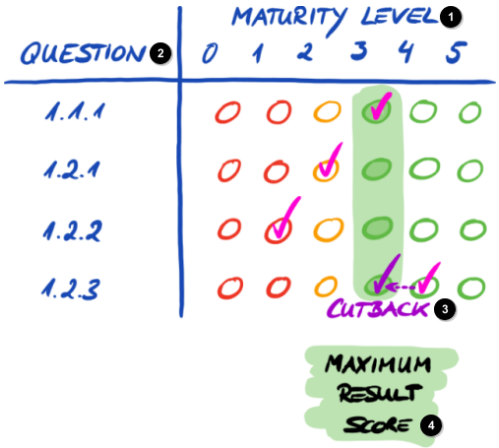


Illustration 24. La note de résultat maximale (au niveau note)

1. Niveau de maturité
2. Question
3. Réduction
4. Note de résultat maximale

5.2.4.5. Votre résultat (au niveau note)

Votre note de résultat globale (« Résultat réduit au niveau de maturité cible »,cellule D6) :

- synthétise le niveau de maturité global de votre système de gestion de la sécurité de l'information.
- est la moyenne de tous vos niveaux de maturité (au niveau questions).
- peut être inférieure ou égale à la note de résultat maximale.
- doit être la plus proche possible de la note de résultat maximale. Plus votre note de résultat est inférieure à la note de résultat maximale, plus la probabilité de bénéficier de labels TISAX sera faible.

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: YOUR RESULT SCORE ❶

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Illustration 25. Votre note de résultat (feuille Excel « Résultats (ISA5) »)

❶ Votre note de résultat

Sur la base de la même illustration que celle présentée plus haut (Illustration 22, "Niveaux de maturité au niveau questions"), vous pouvez voir ci-dessous ce qui est pris en compte dans la moyenne pour la note de résultat :

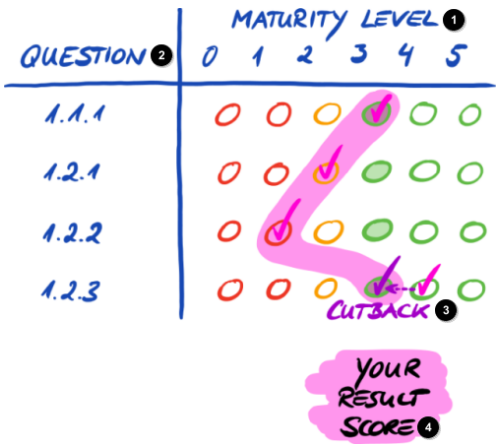


Illustration 26. Votre note de résultat (au niveau note)

❶ Niveau de maturité

2. Question
3. Réduction
4. Votre note de résultat

La note de résultat vous indique si :

- vous êtes prêt pour une évaluation TISAX.
- vous pouvez vous attendre à recevoir des labels TISAX.

Si votre note de résultat (« Résultat réduit au niveau de maturité cible ») est inférieure à « 3,0 », alors votre niveau de maturité ne correspond pas au niveau de maturité cible, du moins pour une question. Dans ce cas, vous devrez probablement améliorer votre système de gestion de la sécurité de l'information avant de pouvoir passer l'évaluation TISAX.

Remarque :

Concernant la note globale, il existe des limites formelles quant à une « distance » acceptable entre votre note de résultat et la note de résultat maximale (« Résultat réduit au niveau de maturité cible »).

Si votre note de résultat est de plus de :

- 10 % inférieure, le résultat global de l'évaluation sera « non conforme mineur ».
- 30 % inférieure, le résultat global de l'évaluation sera « non conforme majeur ».

Remarque importante :

Si votre note de résultat (« Résultat réduit au niveau de maturité cible ») est de « 3 », vous n'avez aucune garantie de passer l'évaluation TISAX sans constatations rédhibitoires. Gardez à l'esprit que l'auditeur peut avoir un point de vue différent du vôtre sur certains aspects.

5.2.4.6. Êtes-vous prêt ?

L'analyse ci-dessus vise à savoir si vous êtes prêt à passer une évaluation TISAX.

Vous êtes réellement prêt pour une évaluation TISAX si votre note de résultat (« Résultat réduit au niveau de maturité cible ») est (proche) de « 3,0 ». Dans ce cas, toutes les valeurs dans la colonne « Résultats » (H) sont vertes (aucune valeur orange ni rouge).

Si elles ne sont pas vertes, vous devez remédier au résultat de votre auto-évaluation (veuillez

consulter la Section 5.2.5, “Traitement du résultat d’auto-évaluation”).

L’illustration ci-dessous illustre le diagramme en forme de toile d’araignée de l’ISA dans la feuille Excel « Résultats (ISA5) ». La ligne verte marque le niveau de maturité cible par chapitre. Si vos niveaux de maturité sont sur ou au-dessus de cette ligne, vous êtes prêt pour une évaluation TISAX. S’ils sont sous cette ligne, il se peut qu’ils ne soient pas suffisants pour vous permettre de recevoir des labels TISAX.

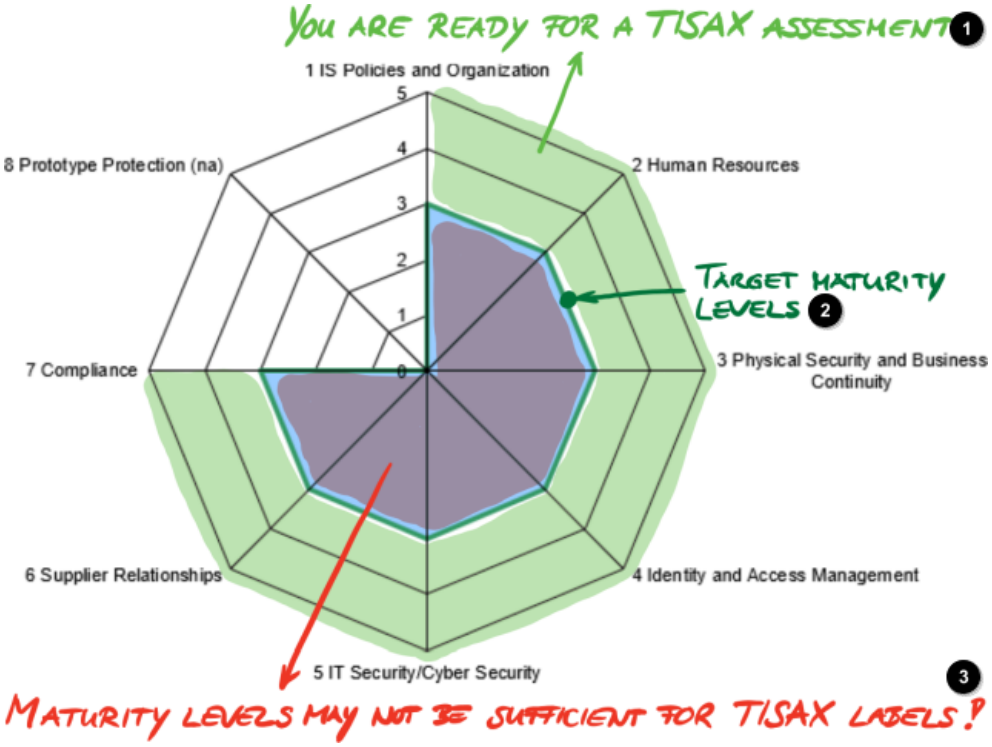


Illustration 27. Capture d’écran : réalisation du niveau de maturité cible sur le diagramme en toile d’araignée ISA (feuille Excel « Résultats (ISA5) »)

1. Vous êtes prêt pour une évaluation TISAX
2. Niveaux de maturité cibles
3. Il se peut que les niveaux de maturité ne suffisent pas pour permettre l’obtention de labels TISAX !

Si vous développez la toile ISA jusqu’au niveau questions, vous obtiendrez un affichage similaire vert/rouge au niveau questions :

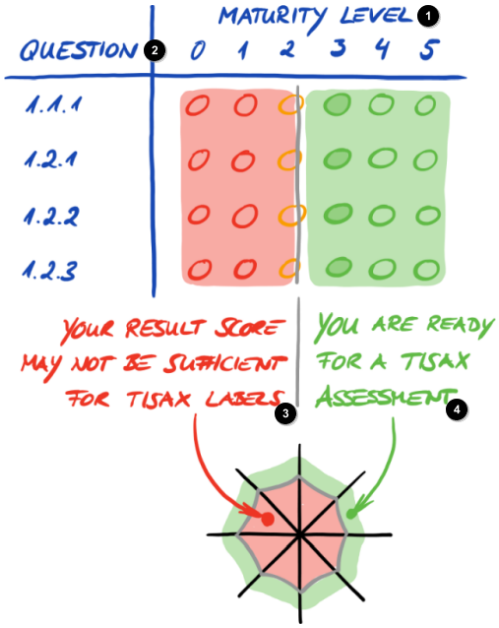


Illustration 28. Développement du diagramme en forme de toile d'araignée ISA

1. Niveau de maturité
2. Question
3. Il se peut que votre note de résultat ne suffise pas pour permettre l'obtention de labels TISAX
4. Vous êtes prêt pour une évaluation TISAX

5.2.5. Traitement du résultat d'auto-évaluation

Le résultat de votre auto-évaluation peut indiquer que vous devez améliorer votre système de gestion de la sécurité de l'information pour pouvoir recevoir des labels TISAX.

Il se peut que vous sachiez comment combler certains écarts entre votre niveau de maturité et le niveau de maturité cible. Concernant d'autres écarts, il est possible que vous ayez besoin de conseils externes. Dans ce cas, vous pouvez solliciter des services de conseil auprès de nos auditeurs TISAX. TISAX permet leur consultation sans l'exiger. Notez qu'un auditeur qui vous fournit des services de conseil ne peut plus effectuer d'évaluation TISAX pour vous.

Remarque importante :

À défaut de traitement adéquat du résultat d'auto-évaluation *avant* l'évaluation proprement dite, bon nombre d'entreprises se heurtent à un obstacle de taille. Ne sous-estimez pas les efforts nécessaires pour adapter votre système de gestion de la sécurité de l'information aux exigences. Dans beaucoup d'entreprises, un projet d'envergure devra être mis en place dans les règles pour se préparer à une évaluation TISAX.

Remarque :

Si vous cherchez une aide externe pour passer le processus TISAX, vous découvrirez que diverses entreprises offrent des services de conseil et de formation. Aucune de ces entreprises ne travaille avec nous.

Actuellement, nous :

- ne proposons pas de formations officielles, ni directement ni par l'intermédiaire de tiers.
- ne faisons aucune déclaration sur la qualité des services de tiers et invitons donc à la prudence.

Remarque :

Nous déconseillons de solliciter ou de commander des services tels qu'une « pré-évaluation » ou une « analyse de l'écart ». Nous comprenons que vous souhaitiez vous préparer à l'évaluation de cette façon, mais il est préférable dans la plupart des cas d'entamer l'évaluation sans attendre.

Pour de plus amples informations sur les raisons pour lesquelles nous déconseillons les pré-évaluations, veuillez consulter la Section 7.7, “Annexe : pourquoi nous déconseillons les « pré-évaluations » et les « analyses de l'écart »”.

5.3. Sélection de l'auditeur

Seuls des auditeurs que nous avons engagés peuvent mener des évaluations TISAX[15]. Les auditeurs TISAX sont autorisés à mener des évaluations TISAX pour vous, à la condition qu'ils n'aient jamais mené de missions de conseil auprès de vous par le passé.

Tous nos auditeurs TISAX sont tenus de mener les évaluations TISAX uniquement pour les entreprises inscrites comme participants TISAX.

Remarque importante :

Dès que vous avez inscrit un périmètre d'évaluation TISAX, vous *devez* commencer à contacter nos auditeurs. Il y a un certain délai quant à leur disponibilité. Le fait de les contacter *après* avoir terminé vos préparatifs pourrait rallonger inutilement ce délai.

Remarque :

Chaque périmètre d'évaluation a un cycle de vie. À ce stade, votre périmètre d'évaluation doit avoir le statut « approuvé » ou « inscrit »

Pour de plus amples informations sur le statut d'un périmètre d'évaluation, veuillez consulter la Section 7.5.5, "Assessment scope status "Awaiting your payment" (Statut du périmètre d'évaluation « En attente de votre paiement »)".

5.3.1. Informations de contact

Une fois que vous avez inscrit un périmètre d'évaluation TISAX, vous pouvez contacter tous les auditeurs TISAX et solliciter des offres. Leurs coordonnées figurent dans l'e-mail de confirmation d'inscription que vous avez reçu[16] (veuillez consulter la Section 4.5.8, "E-mail de confirmation").

Remarque :

Ne sollicitez des offres auprès de nos auditeurs TISAX qu'APRÈS votre inscription. Les auditeurs vérifieront que vous êtes bien inscrit. Ils sont tenus de rejeter toute demande sans inscription préalable.

C'est également la raison pour laquelle vous ne recevrez les coordonnées des auditeurs que dans l'e-mail de confirmation d'inscription et qu'elles ne figurent pas sur notre site Web public.

5.3.2. Couverture

Si actuellement, bon nombre de nos auditeurs se trouvent en Allemagne, tous sont en mesure de mener des évaluations TISAX partout dans le monde. La plupart d'entre eux ont même du personnel propre dans de nombreux pays.

Sur notre site Web, nous disposons d'une page sur laquelle vous pouvez sélectionner votre pays et voir ensuite quel auditeur a une équipe commerciale et/ou des auditeurs sur place (enx.com/en-US/TISAX/xap/).

5.3.3. Demande d'offres

Pour permettre à nos auditeurs TISAX de calculer précisément le travail à fournir pour l'évaluation, vous devez toujours inclure l'« extrait du périmètre TISAX ».

Illustration 29. Miniature d'un extrait de périmètre (première page)

Pour de plus amples informations, veuillez consulter la Section 4.5.8, "E-mail de confirmation".

Remarque :

L'impartialité est une caractéristique essentielle de nos auditeurs TISAX. Ils veilleront à ce qu'aucun conflit d'intérêts n'apparaisse. Peut-être souhaiterez-vous aborder le sujet lorsque vous les contacterez. Si votre entreprise est d'une quelconque manière liée à un auditeur, vous ne pouvez pas espérer être évalué par ce dernier.

5.3.4. Évaluation des offres

Vous pouvez librement choisir parmi tous nos auditeurs TISAX. Ils sont tous liés au même contrat. Ils mènent tous les évaluations sur la base des mêmes critères et utilisent tous les mêmes méthodes d'audit. En matière de résultat d'évaluation, vous n'observerez aucune différence selon l'auditeur choisi. Le résultat de votre évaluation sera accepté par tous les participants TISAX.

Outre des facteurs évidents tels que le prix, la réputation et l'amabilité, il existe d'autres aspects à prendre en considération dans une offre :

- Disponibilité :
  quand le processus d'évaluation peut-il débuter ? Cela peut être un aspect important si vous avez besoin rapidement de conclure l'évaluation TISAX.
- Frais de déplacement pour les rendez-vous sur site :
  les auditeurs qui ont des bureaux dans votre pays sont susceptibles d'avoir moins de frais de déplacement.
- Langue :
  est-ce que toute personne interrogée dans votre entreprise et vous-même serez en mesure de communiquer avec l'auditeur dans votre langue maternelle ?
- Périmètre de l'offre :
  Quelles sont les évaluations comprises ?

Pour de plus amples informations sur les évaluations, veuillez consulter la Section 5.4.3, “Types d’évaluation TISAX”.
Habituellement, les offres incluent l’évaluation initiale et l’évaluation du plan d’action corrective. Comme il est difficile de présumer du travail à fournir pour les évaluations de suivi, celles-ci font généralement l’objet d’une offre après la clôture des autres évaluations.

Enfin, il s’agit aussi de confiance. Vous devrez instaurer une relation de confiance avec votre auditeur, dans la mesure où il accédera à certains renseignements sur votre entreprise.

Remarque :

Nous déconseillons de solliciter ou de commander des services tels qu’une « pré-évaluation » ou une « analyse de l’écart ». Nous comprenons que vous souhaitiez vous préparer à l’évaluation de cette façon, mais il est préférable dans la plupart des cas d’entamer l’évaluation sans attendre.

Pour de plus amples informations sur les raisons pour lesquelles nous déconseillons les pré-évaluations, veuillez consulter la Section 7.7, “Annexe : pourquoi nous déconseillons les « pré-évaluations » et les « analyses de l’écart »”.

Remarque :

Nous voudrions pouvoir vous indiquer les montants facturés par nos auditeurs pour l’évaluation, mais nous ne sommes malheureusement pas en mesure de vous fournir cette information. Les coûts dépendent d’un trop grand nombre de facteurs. De plus, nos auditeurs peuvent calculer librement leurs tarifs.

Nous pouvons cependant vous fournir des estimations approximatives quant au nombre de jours-personnes que nos auditeurs vous factureront. Pour une petite entreprise moyenne disposant d’un seul site, attendez-vous à payer entre trois jours et demi et quatre jours-personnes pour une évaluation de niveau 2 et entre cinq et six jours-personnes pour une évaluation de niveau 3.

Remarque :

Chaque évaluation a un cycle de vie.

Pour de plus amples informations sur le statut d’une évaluation, veuillez consulter la Section 7.6, “Annexe : Assessment status (Statut de l’évaluation)”.

Une fois que vous avez choisi l’un de nos auditeurs TISAX, vous pouvez enfin entamer le processus d’évaluation TISAX.

5.4. Processus d’évaluation TISAX

5.4.1. Aperçu

Le processus d’évaluation TISAX comprend plusieurs types d’évaluation. Dans la plupart des cas, il y aura plus d’une évaluation.

Vous devez considérer le processus d’évaluation comme une suite d’étapes imbriquées les unes dans les autres où :

- Vous préparez votre système de gestion de sécurité de l’information pour le rendre excellent.
- L’auditeur vérifie si votre système de gestion de la sécurité de l’information répond à un ensemble prédéfini d’exigences. Il peut y trouver des lacunes.
- Vous comblez alors ces lacunes dans les délais impartis.
- Ensuite, l’auditeur vérifie une fois de plus si vous avez comblé les lacunes.

Ces étapes se succéderont jusqu’à ce que toutes les lacunes soient comblées.

Il est important de comprendre que *vous* êtes à l’initiative de chaque sous-étape dans le processus d’évaluation. Tout le processus d’évaluation est sous votre contrôle. Et bien entendu, vous seul décidez d’arrêter et d’abandonner le processus d’évaluation quand bon vous semble.[17]

Le processus d’évaluation TISAX possède la macrostructure suivante :

- Réunion de lancement
  Vous planifiez, avec l’auditeur, les détails du processus d’évaluation.
- Phase d’évaluation 1
  L’auditeur vérifie votre auto-évaluation.
- Phase d’évaluation 2
  L’auditeur réalise la/les évaluation(s).

5.4.2. Réunion de lancement

Le processus d’évaluation TISAX débute avec la réunion de lancement. Celle-ci permet de planifier les détails du processus d’évaluation. La réunion de lancement se déroule généralement par conférence téléphonique. L’auditeur vous guidera tout au long de la réunion.

Les thèmes suivants sont, entre autres, à l’ordre du jour :

- Qui participe à la réunion ?
- Qui est l’entreprise évaluée ?

- Comment fonctionne le processus d'évaluation TISAX ?
- Quel est le périmètre d'évaluation et est-il adapté ?
- Y a-t-il des conflits d'intérêts ?
- À quoi ressemble une bonne auto-évaluation ?
- Qui est responsable de quoi ?
- Comment communiquons-nous ?
- Quand l'évaluation aura-t-elle lieu (et autres éléments du calendrier) ?
- Qui doit participer à/aux évaluation(s) ?
- Qui pouvez-vous contacter en cas de réclamation ?

Le délai entre la fin de la réunion de lancement et la remise de votre auto-évaluation varie généralement entre un et trois mois. Mais il n'est pas rare que cela dure jusqu'à six mois. Cette période dépend du statut de votre préparation. TISAX ne fixe pas de limites pour cette période. Vous pouvez prendre tout le temps dont vous avez besoin pour préparer votre auto-évaluation et pour vous préparer pour l'évaluation.

5.4.3. Types d'évaluation TISAX

Le processus d'évaluation TISAX comprend trois types d'évaluation TISAX :

- Évaluation initiale (Initial assessment)
- Évaluation du plan d'action corrective (Corrective action plan assessment)
- Évaluation de suivi (Follow-up assessment) [18]

L'évaluation initiale est obligatoire. Les deux autres évaluations TISAX peuvent avoir lieu, et ce à plusieurs reprises. Elles interviendront soit :

- jusqu'à ce que vous ayez comblé toutes les lacunes
- ou jusqu'à ce que vous abandonniez le processus d'évaluation TISAX
- ou que vous atteigniez la durée maximale de neuf mois après la fin de la réunion de clôture de l'évaluation initiale (moment auquel une autre évaluation initiale est requise).

Toutes les évaluations TISAX seront décrites dans les sections suivantes.

Remarque :

Chaque évaluation a un cycle de vie.

Pour de plus amples informations sur le statut d'une évaluation, veuillez consulter la Section 7.6, "Annexe : Assessment status (Statut de

> l’évaluation)”.

5.4.4. Éléments de l’évaluation TISAX

Chaque évaluation TISAX comprend les éléments suivants :

- Réunion d’ouverture officielle[19][20]
  - Elle a pour objectif de traiter toutes les questions d’ordre organisationnel.
  - Il ne doit pas nécessairement s’agir d’une réunion physique.
  - Les sujets peuvent être traités simultanément ou répartis sur plusieurs sessions.
  - Il s’agit d’un « conteneur logique » pour l’ensemble des questions organisationnelles d’*avant* l’évaluation.
- Procédure d’évaluation
  - Votre auditeur vérifie toutes les exigences.
  - Les méthodes d’évaluation sont sélectionnées selon le niveau d’évaluation en question.
- Réunion de clôture officielle[21]
  - Elle conclut une évaluation TISAX.
  - L’auditeur y présente ses conclusions.
  - L’auditeur annonce le résultat de l’évaluation.
  - Il ne doit pas nécessairement s’agir d’une réunion physique.
  - Il s’agit d’un « conteneur logique » pour l’ensemble des questions organisationnelles d’*après* l’évaluation.

Après la « réunion de clôture », l’auditeur prépare et vous envoie une ébauche du « rapport d’évaluation TISAX » mis à jour. Vous pouvez faire part de vos objections si vous pensez que l’auditeur a mal compris quelque chose.[22] L’auditeur publie ensuite le « rapport d’évaluation TISAX » final.

Tous ces éléments seront décrits dans les sections suivantes.

5.4.5. À propos de la conformité

Avant de continuer à décrire le processus d’évaluation TISAX, nous souhaitons vous expliquer un concept clé, essentiel à la bonne compréhension des sections suivantes.

L’objectif d’une évaluation TISAX est de déterminer si votre système de gestion de la sécurité de l’information répond à un ensemble prédéfini d’exigences. L’auditeur vérifie si votre système de gestion de la sécurité de l’information « est conforme » (🇬🇧 “conforms”) aux exigences.

Étape 1 : les vérifications sont effectuées individuellement pour chaque exigence applicable.

Si votre approche « est conforme » à toutes les exigences, vous réussissez l'évaluation et recevez les labels TISAX correspondant à vos objectifs d'évaluation.

Tout ce qui est en-deçà d'une conformité complète ou idéale par rapport aux exigences est appelé une constatation (finding). TISAX distingue quatre types de constatation :

Nº	Type	Définition	Réaction	Exemples
1.	Non-conformité *majeure* (*Major* non-conformity)	Une non-conformité *majeure* : ▪ crée un risque immédiat important pour votre sécurité de l'information ▪ **ou** crée des doutes concernant l'efficacité globale de votre système de gestion de la sécurité de l'information.	Vous devez : ▪ résoudre immédiatement les non-conformités *majeures* grâce à des mesures compensatoires adaptées, ▪ mettre en œuvre les actions correctives dans les meilleurs délais.	▪ Non-conformités systématiques ▪ Déficits de mise en œuvre qui créent des risques critiques pour la sécurité des informations confidentielles ▪ Déficits de mise en œuvre qui ne sont pas résolus par une action corrective adaptée
2.	Non-conformité *mineure* (*Minor* non-conformity)	Une non-conformité *mineure* : ▪ ne crée *pas* de risque immédiat important pour votre sécurité de l'information ▪ **et** ne crée *pas* de doute concernant l'efficacité globale de votre système de gestion de la sécurité de l'information.	Vous devez : ▪ mettre en œuvre les actions correctives dans les meilleurs délais.	▪ Erreurs isolées ou sporadiques ▪ Non-conformité ou déficits dans la mise en œuvre des exigences ou de vos politiques

Nº	Type	Définition	Réaction	Exemples
3.	Observation (🇬🇧 Observation)	Une observation est une non-conformité avec les exigences de vos propres politiques qui ne crée pas de risque immédiat pour votre sécurité de l'information, mais pourrait en créer à l'avenir.	Vous devez : ▪ examiner, surveiller et évaluer soigneusement les risques possibles ▪ décider de la manière de traiter l'observation	n/a
4.	Marge d'amélioration (🇬🇧 Room for improvement)	Une variation qui n'appartient pas aux types mentionnés ci-dessus et qui ne crée pas de risque pour votre sécurité de l'information, mais offre une marge d'amélioration importante.	Vous pouvez choisir de traiter ou non ce type de constatation et la manière de le faire.	n/a

Tableau 11. Les quatre types de constatation

Étape 2 : tous les résultats de l'étape précédente « par exigence » sont fusionnés en un résultat global d'évaluation.

Le résultat global d'évaluation peut être :

a. Conforme (🇬🇧 Conform)
Le résultat global d'évaluation est « conforme ». Toutes les exigences sont satisfaites.

b. Non conforme mineur (🇬🇧 Minor non-conform)
Le résultat global d'évaluation est « non conforme mineur » si vous avez au moins une « non-conformité mineure » pour une exigence.

c. Non conforme majeur (🇬🇧 Major non-conform)
Le résultat global d'évaluation est « non conforme majeur » si vous avez au moins une « non-conformité majeure » pour une exigence.
(Sans plan d'action corrective approuvé, chaque non-conformité entraîne un résultat global d'évaluation « non conforme majeur ».)

Si le résultat global de votre évaluation est :

- « non conforme mineur », vous pouvez recevoir des labels TISAX *provisoires* jusqu'à ce que toutes les non-conformités soient résolues.
- « non conforme majeur », vous devez résoudre le problème en question avant de recevoir un label TISAX.
  À l'aide de mesures compensatoires appropriées et des actions correctives approuvées par l'auditeur, il est possible de changer le résultat global de votre évaluation de « non conforme majeur » en « non conforme mineur », et donc de recevoir des labels TISAX provisoires.

Il est important de comprendre que le résultat global de votre évaluation s'améliorera au cours de tout le processus d'évaluation TISAX.

Prenez cet exemple extrêmement simplifié : vous obtenez un résultat global d'évaluation correspondant à « non conforme majeur » après l'évaluation initiale. Ensuite, vous atténuez le risque correspondant. Votre démarche permet de modifier le résultat global de votre évaluation de « non conforme majeur » en « non conforme mineur ». Et une fois le risque éliminé, le résultat final de votre évaluation globale sera « conforme ».

Des explications plus détaillées à ce sujet sont données ci-dessous. Et vous trouverez davantage d'informations sur les labels TISAX plus loin à la Section 5.4.14, "Labels TISAX".

5.4.6. Votre préparation pour le processus d'évaluation TISAX

L'auditeur préparera l'évaluation sur la base de votre auto-évaluation. Par conséquent, pensez à mettre à temps votre auto-évaluation à la disposition de votre auditeur. Les échéances exactes de fourniture sont fixées lors de la réunion de lancement.

Un auditeur bien préparé abrégera le temps nécessaire à l'évaluation. Outre l'auto-évaluation, il demandera aussi de la documentation connexe avant l'évaluation. Il peut s'agir de documentation à laquelle vous avez fait référence dans l'auto-évaluation et d'autres documents que l'auditeur juge pertinents.

Sur la base de ces informations, votre auditeur planifiera la procédure d'évaluation.

5.4.7. Évaluation initiale

Cette première évaluation TISAX marque le début officiel du processus d'évaluation TISAX.

Remarque importante :

L'évaluation initiale marque le début de deux périodes importantes :

1. La période de validité maximale des labels TISAX est de trois ans.
2. Vous avez jusqu'à neuf mois pour résoudre les non-conformités. Si vous ne résolvez pas toutes les non-conformités dans le délai imparti, vous ne recevrez pas de labels TISAX. Si vous ne respectez pas ce délai, vous pouvez

néanmoins continuer en lançant une nouvelle évaluation initiale.

Les deux périodes commencent le jour de la réunion de clôture de l'évaluation initiale.

Remarque :

À l'exception des deux périodes décrites ci-dessus, il n'existe pas d'autre contrainte temporelle. Par exemple le fait de terminer le processus d'inscription en ligne, de contacter nos auditeurs ou même de participer à la réunion de lancement ne déclenche aucune échéance. C'est à vous de décider quand débuter l'évaluation initiale.

5.4.7.1. La première réunion d'ouverture officielle

Comme toutes les évaluations TISAX, l'évaluation initiale commence par une réunion d'ouverture officielle. La réunion d'ouverture officielle se tient généralement sous la forme d'une conférence téléphonique ou sur le Web. Pour les petites entreprises, qui ont déjà une certaine expérience des audits, cette réunion ne dure pas longtemps.

L'objectif de cette réunion est de :

- vérifier les conditions de l'évaluation
- présenter le chef de projet et l'équipe d'évaluation
- planifier l'évaluation

5.4.7.2. Procédure d'évaluation

Conformément au plan préparé, l'auditeur mène l'évaluation initiale. Sa mise en œuvre concrète dépend de vos objectifs d'évaluation. L'évaluation consiste principalement en des conférences téléphoniques, des entretiens et des inspections sur site plus ou moins approfondis[23].

L'auditeur présente l'ensemble de ses constatations durant l'évaluation initiale.

5.4.7.3. Réunion de clôture

Durant la réunion de clôture, votre auditeur synthétise à nouveau ses constatations.

5.4.7.4. Rapport d'évaluation TISAX

Après la réunion de clôture, l'auditeur prépare et vous envoie l'ébauche du « rapport d'évaluation TISAX ». Vous pouvez faire part de vos objections si vous pensez que l'auditeur a mal compris quelque chose.[24] L'auditeur publie ensuite le « rapport d'évaluation TISAX ».

À ce stade, le résultat global d'évaluation peut être :

- Conforme ou
- Non conforme majeur
  L'absence de traitement des non-conformités (mineures) entraîne toujours un résultat global d'évaluation « non conforme majeur ». Le résultat global de votre évaluation ne peut être « non conforme mineur » qu'une fois que vous avez défini des actions pour la mise en œuvre de mesures permettant de traiter les non-conformités.
  Pour de plus amples informations sur cette démarche, veuillez consulter la Section 5.4.9.4, "Labels TISAX provisoires".

Si le résultat global de votre évaluation est « conforme » au moment de l'évaluation initiale, vous pouvez passer le reste de la section concernant l'évaluation et aller à la section sur l'échange du résultat.

Si le résultat global de votre évaluation est « non conforme majeur », votre prochaine tâche consistera à élaborer un plan pour traiter les constatations et combler toute lacune identifiée par l'auditeur. Le plan est appelé officiellement « plan d'action corrective » (🇬🇧 "corrective action plan").

Remarque :

Si, avant le début de l'évaluation, vous avez connaissance d'une situation qui entraînera une non-conformité, et que vous ne pouvez pas la résoudre avant l'évaluation, vous pouvez planifier une action corrective (avec une date de mise en œuvre) et la présenter à l'auditeur au cours de l'évaluation. Cela devrait, en théorie, générer le résultat d'évaluation global « non conforme mineur ». Cette situation est cependant plutôt *rare*.

5.4.8. Préparation du plan d'action corrective

Votre « plan d'action corrective » (🇬🇧 "corrective action plan") définit la manière dont vous prévoyez de traiter les constatations de l'évaluation initiale. Votre auditeur évaluera l'adéquation de votre « plan d'action corrective » (cf. la section suivante).

Pour créer votre « plan d'action corrective », vous devez tenir compte des exigences suivantes :

- Constatation
  - Vous devez indiquer la constatation que l'action corrective doit résoudre.
- Cause profonde
  - Vous devez identifier et préciser la cause profonde de la constatation.
- Actions correctives
  - Pour chaque non-conformité, vous devez définir une ou plusieurs « actions correctives » prévoyant les mesures nécessaires au traitement de la non-conformité.

- Date de mise en œuvre
  - Vous devez définir une date de mise en œuvre pour chaque action corrective.
  - La période de mise en œuvre doit offrir suffisamment de temps pour appliquer intégralement les mesures.
- Mesures compensatoires
  - Pour l'ensemble des non-conformités qui créent des risques critiques, vous devez définir des mesures compensatoires qui traitent les non-conformités avant la mise en œuvre des actions correctives.
- Période de mise en œuvre
  - Pour toutes les actions correctives dont l'application prend plus de trois mois, vous devez justifier la période de mise en œuvre.
  - Pour toutes les actions correctives dont l'application prend plus de six mois, vous devez en plus fournir la preuve attestant qu'une mise en œuvre plus rapide n'est pas possible.
  - La période de mise en œuvre pour toute action corrective ne peut excéder neuf mois.

Une fois que votre plan d'action corrective est complet, vous pouvez demander l'« évaluation du plan d'action corrective ».

Remarque importante :

Nous recommandons de commencer la mise en œuvre le plus rapidement possible. Il n'est pas nécessaire d'attendre le résultat de « l'évaluation du plan d'action corrective ».
« L'évaluation du plan d'action corrective » intervient généralement une fois que vous avez présenté votre plan d'action corrective à votre auditeur.

Remarque :

Tisax a des exigences uniquement envers le contenu, pas envers la forme des plans d'action corrective.
La plupart de nos auditeurs proposent des modèles de plan d'action corrective.

5.4.9. Évaluation du plan d'action corrective

« L'évaluation du plan d'action corrective » vise à vérifier que votre « plan d'action corrective » (cf. ci-dessus) répond aux exigences TISAX.

Vous présentez votre « plan d'action corrective » à votre auditeur. Votre auditeur évalue le plan par rapport aux exigences (cf. ci-dessous). Si votre plan est conforme aux exigences, votre auditeur publiera le « rapport d'évaluation TISAX » mis à jour.

Cette évaluation ne prend habituellement pas beaucoup de temps. Dans la plupart des cas, elle prend la forme d'une conférence téléphonique ou d'une conférence sur le Web. Parfois, cela peut même se faire par e-mail.

5.4.9.1. Raisons d'une évaluation du plan d'action corrective

Les raisons d'une « évaluation du plan d'action corrective » sont :

- Non-conformités restantes après
  - une évaluation initiale
  - une évaluation de suivi
  - une évaluation d'extension du périmètre
- un « plan d'action corrective » qui a déjà été évalué, mais n'a pas répondu aux exigences
- Les facteurs déterminants qui servent de base au calcul des périodes de mise en œuvre d'un plan d'action corrective ont changé.

5.4.9.2. Combinaison avec l'évaluation initiale

« L'évaluation du plan d'action corrective » ne constitue pas forcément un événement indépendant. Vous avez déjà la possibilité de présenter votre « plan d'action corrective » lors de la réunion de clôture de l'évaluation initiale. L'auditeur peut alors mener directement « l'évaluation du plan d'action corrective ».

Si vous combinez « l'évaluation du plan d'action corrective » avec l'évaluation initiale, et que votre « plan d'action corrective » répond aux exigences, vous pouvez convenir avec votre auditeur que vous n'avez pas besoin d'un « rapport d'évaluation initiale ». Au lieu de cela, votre auditeur préparera uniquement le « rapport d'évaluation du plan d'action corrective ». Ce rapport vous permet de recevoir directement des labels TISAX provisoires.

5.4.9.3. Exigences concernant le plan d'action corrective

L'auditeur évalue votre « plan d'action corrective » sur la base des exigences suivantes :

- Les mesures sont appropriées
  - L'auditeur évaluera l'adéquation d'un plan d'action corrective en fonction de sa capacité à résoudre ou non la cause profonde de la non-conformité.
- Les risques critiques sont atténués par des mesures compensatoires appropriées[25]
- Les périodes de mise en œuvre sont appropriées
  - Les périodes de mise en œuvre commencent le jour où se termine l'évaluation initiale.
- Aucune période de mise en œuvre n'excède :
  - trois mois sans justification supplémentaire

- six mois sans justification et preuves supplémentaires
- neuf mois

5.4.9.4. Labels TISAX provisoires

Si le résultat global de votre évaluation est « non conforme mineur », vous recevez des labels TISAX provisoires.

L'avantage des labels TISAX provisoires est que votre partenaire les accepte généralement à la condition que vous receviez ultérieurement des labels TISAX permanents. Cela peut vous aider si vous devez prouver d'urgence l'efficacité de votre système de gestion de la sécurité de l'information à votre partenaire.

La condition pour l'obtention de labels TISAX provisoires est un rapport d'évaluation du plan d'action corrective présentant le résultat global d'évaluation « non conforme mineur ».

Les labels TISAX provisoires sont équivalents aux labels TISAX permanents. La seule différence concerne la durée de validité qui est plus courte pour les labels TISAX provisoires.

Les labels TISAX provisoires peuvent être valides jusqu'à neuf mois après la réunion de clôture de l'évaluation initiale. La période de validité des labels TISAX provisoires est déterminée par la période de mise en œuvre des actions correctives la plus longue.

Exemples :

- Vous n'avez qu'une seule non-conformité. Vous devez procéder à une révision de votre politique. La période de mise en œuvre associée est de *deux* mois.
  Dans ce cas, vos labels TISAX temporaires sont valides *deux* mois.
- Vous avez la non-conformité de la révision de politique mentionnée ci-dessus. À cela s'ajoute une non-conformité dont l'action corrective nécessite la construction d'un nouveau mur extérieur. Compte tenu du délai nécessaire pour obtenir les autorisations requises auprès de la municipalité, la période de mise en œuvre associée est de *huit* mois.
  Dans ce cas, vos labels TISAX temporaires sont valides *huit* mois.

Pour de plus amples informations sur les exigences des périodes de mise en œuvre, veuillez consulter la Section 5.4.9.3, "Exigences concernant le plan d'action corrective"

Remarque :

L'« évaluation du plan d'action corrective » est facultative.

Vous pouvez procéder directement à l'évaluation de suivi si vous :

- n'avez pas besoin de labels TISAX provisoires et
- êtes sûr de pouvoir mettre en œuvre toute action corrective sans que votre

plan soit approuvé par votre auditeur

Une fois que vous avez exécuté l'ensemble des actions correctives, vous devez demander une « évaluation de suivi ».

5.4.10. Évaluation de suivi

L'« évaluation de suivi » vise à évaluer si toutes les non-conformités préalablement identifiées sont résolues. Généralement, vous demandez l'évaluation de suivi lorsque vous êtes sûr que toutes les non-conformités sont résolues.

Mais vous pouvez passer autant d'évaluations de suivi que nécessaire. Si au cours d'une évaluation de suivi, votre auditeur atteste encore de non-conformités existantes ou même nouvelles, vous mettez simplement à jour votre plan d'action corrective et recommencez cette partie du processus d'évaluation.

Cette évaluation peut prendre la forme d'une réunion physique ou d'une conférence téléphonique ou sur le Web.

5.4.10.1. Calendrier

Votre auditeur peut mener l'/les évaluation(s) de suivi dans un délai de neuf mois après la conclusion de l'évaluation initiale[26].

5.4.10.2. Conditions préalables

Si vous n'avez pas besoin de labels TISAX provisoires, vous pouvez demander directement une évaluation de suivi. Vous ne devez pas avoir d'« évaluation du plan d'action corrective » avant l'évaluation de suivi.

5.4.10.3. Expiration des labels TISAX provisoires

Si vous avez besoin de labels TISAX provisoires, peut-être souhaiterez-vous vous assurer de ne pas devoir attendre vos labels TISAX permanents. Par conséquent, nous recommandons de demander votre évaluation de suivi bien avant la date limite[27]. Vous souhaitez en effet disposer d'une période tampon suffisante pour traiter toute constatation mineure identifiée durant une évaluation de suivi.

5.4.11. Diagramme du processus d'évaluation TISAX

Les précédentes sections sont à présent synthétisées dans le diagramme de processus suivant :

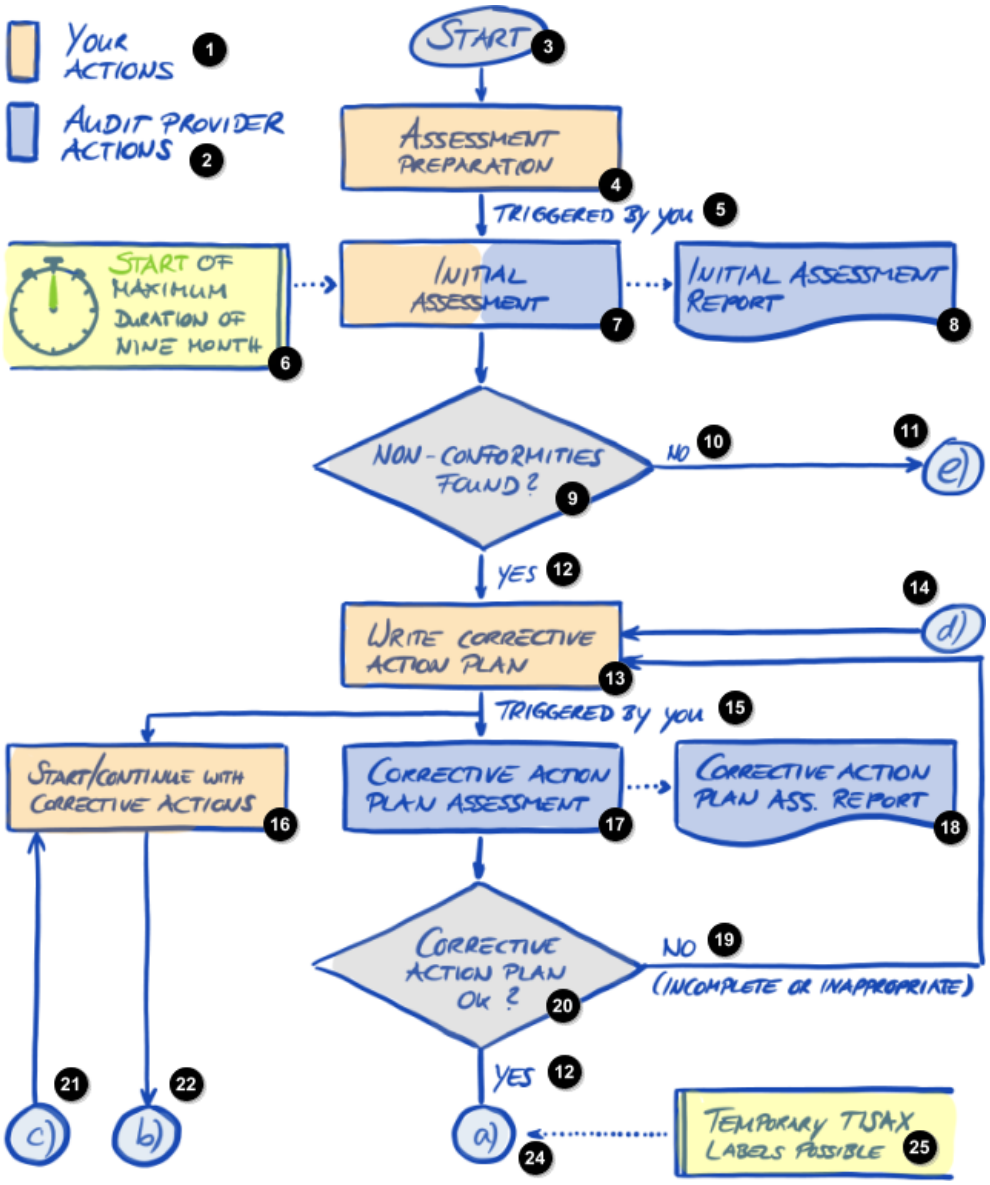


Illustration 30. Diagramme du processus d'évaluation TISAX (1/2)

1. Vos actions
2. Actions de l'auditeur
3. Début
4. Préparation de l'évaluation
5. Initié par vous
6. Début de la période maximale de neuf mois
7. Évaluation initiale
8. Rapport d'évaluation initiale
9. Non-conformités identifiées ?

10. Non
11. e)
12. Oui
13. Rédiger un plan d’action corrective
14. d)
15. Initié par vous
16. Début/poursuite des actions correctives
17. Évaluation du plan d’action corrective
18. Rapport d’évaluation du plan d’action corrective
19. Non (incomplet ou inapproprié)
20. Plan d’action corrective ok ?
21. c)
22. b)
24. a)
25. Labels TISAX provisoires possibles

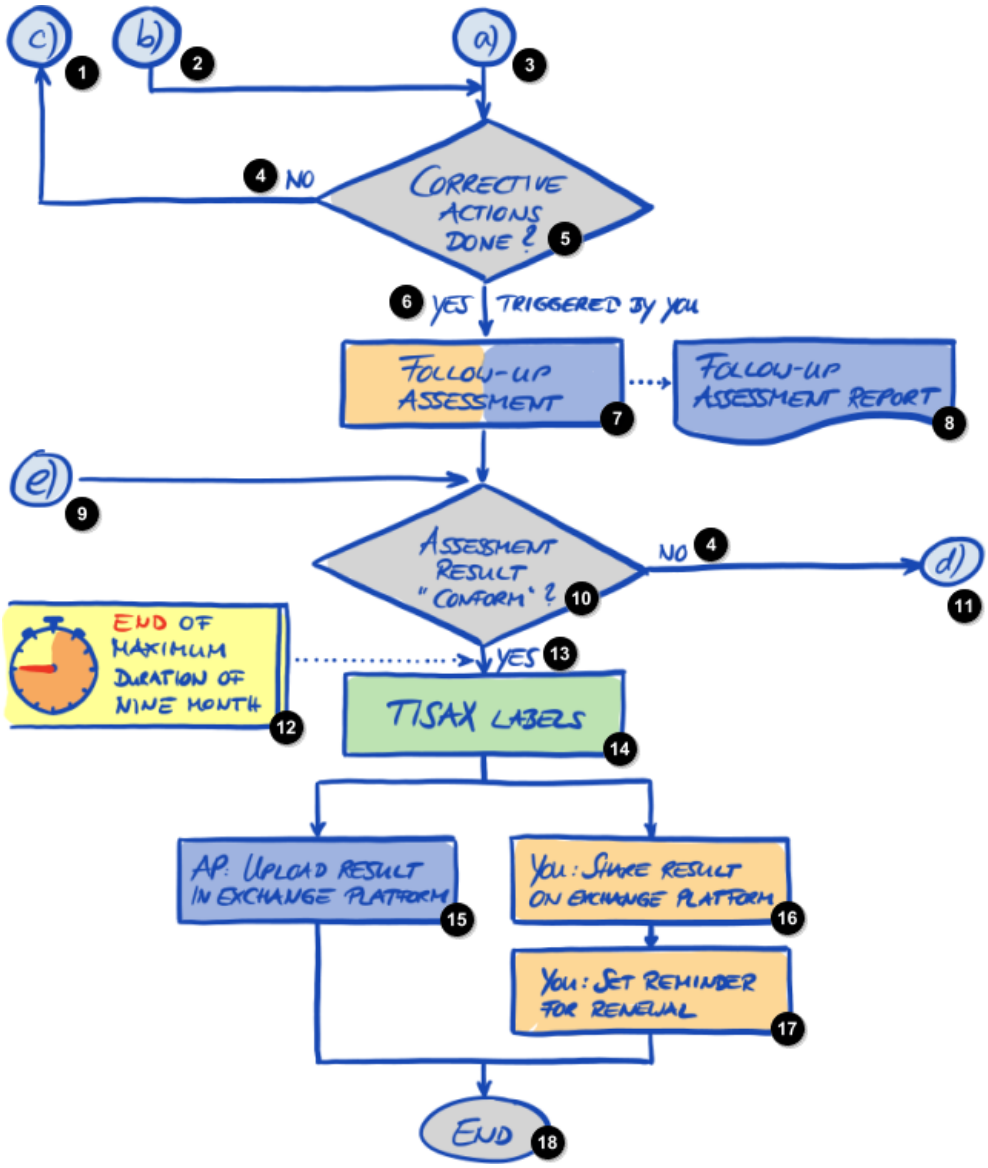


Illustration 31. Diagramme du processus d'évaluation TISAX (2/2)

1. c)
2. b)
3. a)
4. Non
5. Actions correctives réalisées ?
6. Oui, initiées par vous
7. Évaluation de suivi
8. Rapport d'évaluation de suivi
9. e)

10. Résultat d'évaluation « conforme » ?
11. d)
12. Fin de la période maximale de neuf mois
13. Oui
14. Labels TISAX
15. Auditeur : télécharger le résultat sur la plateforme d'échange
16. Vous : partager le résultat sur la plateforme d'échange
17. Vous : définir un rappel pour le renouvellement
18. Fin

5.4.12. Assessment ID (ID d'évaluation)

Chaque évaluation TISAX d'un périmètre d'évaluation est identifiée par un « ID d'évaluation ». Cet ID fait référence au résultat de votre évaluation et au rapport d'évaluation TISAX correspondant.

Voici à quoi ressemble l'ID d'évaluation :

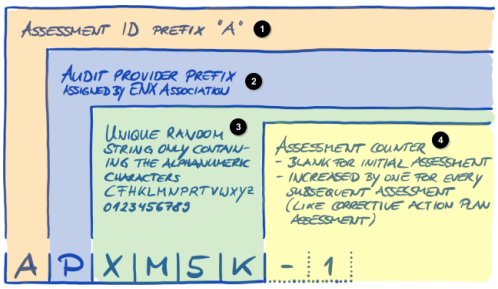


Illustration 32. Format de l'ID d'évaluation

1. Préfixe « A » (pour « Assessment ») de l'ID d'évaluation
2. Préfixe de l'auditeur attribué par ENX Association
3. Chaîne aléatoire unique contenant exclusivement des caractères alphanumériques :
   CFHKLMNPRTVWXYZ
   0123456789
4. Compteur d'évaluation
   – Vide pour l'évaluation initiale
   – Incrémenté de 1 pour chaque évaluation ultérieure (comme l'évaluation du plan d'action corrective)

L'ID d'évaluation est généralement utilisé lorsque votre auditeur communique avec vous.

5.4.13. Rapport d’évaluation TISAX

Le « rapport d’évaluation TISAX » (🇬🇧 “TISAX assessment report”) :

- est (mis à jour et) publié après chaque évaluation TISAX.
- documente les constatations de votre auditeur.
- contient le résultat global de votre évaluation (conforme, non conforme mineur, non conforme majeur).
- contient toutes les autres informations en lien avec votre évaluation TISAX (telles que l’objectif d’évaluation, le périmètre, les personnes impliquées et les sites).

Il existe différents types de « rapport d’évaluation TISAX » (selon le type d’évaluation) :

- Rapport d’évaluation *initiale* (🇬🇧 *Initial* assessment report)
- Rapport d’évaluation du *plan d’action corrective* (🇬🇧 *Corrective action plan* assessment report)
- Rapport d’évaluation de *suivi* (🇬🇧 *Follow-up* assessment report) [28]

Le « rapport d’évaluation TISAX » a toujours la même structure[29]. Votre auditeur l’étend simplement après chaque type d’évaluation. Ainsi, il vous suffit de vous reporter à la dernière version du rapport d’évaluation TISAX, car celle-ci reprend toujours le contenu de la/des version(s) antérieure(s).

Les premières sections du « rapport d’évaluation TISAX » constituent ce que vous partagez avec votre partenaire.

L’une des caractéristiques principales de TISAX est que vous êtes totalement libre de décider des parties du rapport d’évaluation TISAX que vous souhaitez partager avec votre partenaire ou tout autre participant. La structure du rapport d’évaluation TISAX est conçue pour permettre ce genre de partage sélectif. Chaque section accroît le niveau de détail.

Voici à quoi ressemble la structure du « rapport d’évaluation TISAX » :

- A. Informations sur l’évaluation
  Nom de l’entreprise, périmètre d’évaluation, ID de périmètre, ID d’évaluation, niveau d’évaluation, objectif(s) d’évaluation, date(s) d’évaluation, auditeur
  Cette section ne contient aucun résultat d’évaluation.
- B. Résumé des résultats
  Synthèse de gestion du résultat d’évaluation (conforme, non conforme mineur, non conforme majeur), nombre de constatations, brève classification des risques qui en résultent
- C. Résumé du résultat d’évaluation
  Résumé du résultat d’évaluation par chapitre (par exemple : « 9 Contrôle d’accès ») et par catalogue de critères (par exemple : « Sécurité de l’information »)

- D. Niveaux de maturité de l'ISA (onglet Résultat)
  Niveau de maturité pour chaque exigence
- E. Résultats détaillés de l'évaluation
  Description détaillée de toutes les constatations, résultats correspondants d'évaluation du risque, mesures requises, période de mise en œuvre

Lors de l'étape « d'échange » (détaillée ci-dessous), vous décidez du niveau de contenu maximal de votre rapport d'évaluation TISAX auquel votre partenaire aura accès.

5.4.14. Labels TISAX

Nous avons brièvement évoqué ce sujet dans la section de préparation de l'inscription. Comme nous l'avons déjà expliqué, ce qui initialement était un objectif d'évaluation devient à présent un label TISAX.

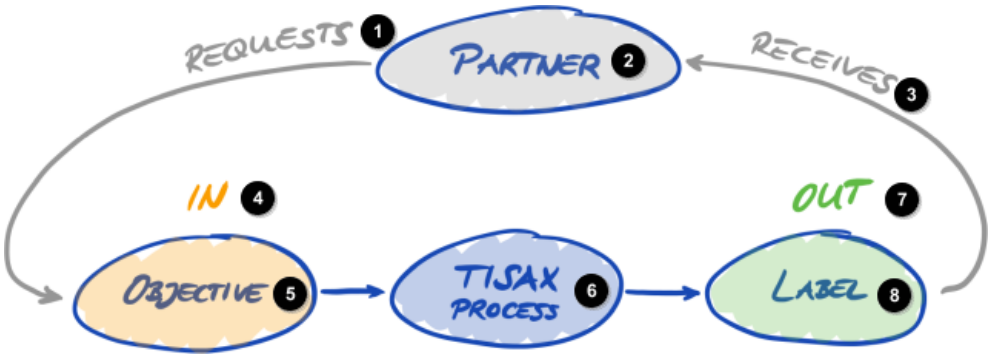


Illustration 33. Objectifs d'évaluation et labels TISAX

1. Demande
2. Partenaire
3. Reçoit
4. IN
5. Objectif
6. Processus TISAX
7. OUT
8. Label

Les labels TISAX :

- sont le fruit du processus d'évaluation TISAX.
- synthétisent votre résultat d'évaluation.
- sont la confirmation que votre système de gestion de la sécurité de l'information répond à

un ensemble prédéfini d'exigences.

L'utilisation des labels TISAX facilite la communication relative à TISAX avec votre partenaire et votre auditeur TISAX, car ils font référence à un output prédéfini du processus d'évaluation TISAX.

5.4.14.1. Hiérarchie des labels TISAX

La correspondance entre les objectifs d'évaluation et les labels TISAX associés est assez simple. Mais il faut tenir compte d'un autre aspect important : *certains* labels sont hiérarchiquement liés les uns aux autres. Cela signifie que si vous recevez un certain label TISAX, vous recevez automatiquement les labels TISAX « inférieurs » à ce label précis.

Exemple : si votre objectif d'évaluation était « Very high availability », vous recevrez le label TISAX correspondant « Very high availability ». Mais dans la mesure où l'objectif d'évaluation « Very high availability » est un surensemble de « High availability », vous recevrez également automatiquement le label TISAX « High availability ».

La hiérarchie suivante s'applique actuellement aux labels TISAX :

- « Info high » est un surensemble de « Confidential » et « High availability ».
- « Info very high » est un surensemble de « Strictly confidential » et « Very high availability ».
- « Strictly confidential » est un surensemble de « Confidential ».
- « Very high availability » est un surensemble de « High availability ».
- « Special data » est un surensemble de « Data ».

Remarque :

Vous pouvez également recevoir des labels TISAX rétroactivement. Lorsque nous lançons un nouveau label qui est un sous-ensemble de l'un des labels TISAX que vous avez déjà reçus, vous recevez automatiquement ce nouveau label.

Exemple : vous avez reçu le label TISAX « Info high » alors que le label « High availability » n'existait pas encore. Lorsque nous avons lancé le label High availability, notre système vous l'a automatiquement attribué.

Pour identifier ces relations hiérarchiques, vous pouvez comparer les exigences applicables définies dans la Tableau 8, “Applicabilité des exigences aux objectifs d'évaluation”.

Cela peut ne pas sembler important à tous les participants. Mais imaginez qu'un partenaire vous demande de lui montrer le label TISAX « Very high availability » et qu'un autre demande le label TISAX « High availability ». Disposer des deux labels rend les choses plus faciles pour tout le monde, car cela évite de devoir comprendre que « High availability » est un sous-ensemble de

« Very high availability ». Cela peut être particulièrement vrai pour les partenaires chez qui le fait d'avoir certains labels TISAX s'inscrit dans un processus d'achat assez rigoureux. Vous n'aurez certainement pas envie d'expliquer que « Very high availability » est « mieux » que « High availability ». Il vous suffira de montrer l'ensemble de vos labels TISAX, et la personne chargée de l'évaluation pourra simplement cocher l'exigence « doit avoir le label TISAX "High availability" ».

5.4.14.2. Période de validité des labels TISAX

Les labels TISAX sont généralement valables trois ans. La période de validité débute à la fin du processus d'évaluation (voire avant la publication du rapport d'évaluation TISAX).

Leur période de validité peut être plus courte si un élément significatif lié au périmètre d'évaluation TISAX est modifié.

Exemple : déménagement de votre entreprise, nouveaux sites. (Pour connaître les instructions sur les mesures à prendre en pareil cas, veuillez consulter la Section 7.9.3.2, "Comment demander la modification d'un site" et Section 7.9.3.4, "Comment ajouter un site supplémentaire".)

Remarque :

Vous ne pouvez voir vos labels TISAX que sur le portail ENX. Ils ne sont pas repris dans le rapport d'évaluation TISAX.

5.4.14.3. Renouvellement des labels TISAX

Pour conserver durablement vos labels TISAX, vous devez les renouveler[30] tous les trois ans.

Pour ce faire, vous devez en principe repasser le processus TISAX (enregistrer un périmètre d'évaluation, obtenir à nouveau l'évaluation TISAX, partager le résultat de votre évaluation). L'inscription est un peu plus facile, dans la mesure où vous ne devez pas recréer votre entreprise en tant que participant TISAX. Et vous pouvez bien entendu réutiliser tous vos contacts et sites déjà sauvegardés dans la base de données TISAX.

Remarque importante :

Veuillez enregistrer un NOUVEAU périmètre AVANT de contacter votre auditeur. Votre auditeur ne peut entamer un nouveau processus d'évaluation que si vous êtes en mesure de fournir un nouvel ID de périmètre.

Dans la plupart des cas, il est aisé d'enregistrer un nouveau périmètre. Il vous suffit de lui attribuer un nouveau nom, d'ajouter des contacts, de sélectionner l'/les objectif(s) d'évaluation et d'ajouter des sites. Vous pouvez réutiliser les contacts et les sites préalablement enregistrés dans le système pour tout autre

périmètre.

Remarque importante :

Veuillez réutiliser les enregistrements des sites existants que vous avez créés et utilisés lors de l'inscription de votre périmètre précédent. Ne créez pas de nouvel enregistrement de site avec la même adresse.

Voici la raison : certains participants TISAX traitent automatiquement les résultats d'évaluation de leurs partenaires. Ils synchronisent leur propre système avec le portail ENX. La moindre petite différence peut compromettre la synchronisation. De plus, ainsi, vous n'encombrez pas les données de vos participants avec des doublons inutiles.

Remarque importante :

S'il est nécessaire de toujours disposer de labels TISAX valables au cours de la relation avec votre partenaire, nous vous conseillons vivement de définir un rappel dans votre calendrier pour lancer le processus de renouvellement nécessaire.

Nous recommandons d'entamer les démarches de renouvellement au moins un an avant l'expiration de vos labels TISAX.

Maintenant que vous avez reçu vos labels TISAX, vous pouvez passer à la dernière étape et les partager avec votre partenaire.

6. Échange (étape 3)

Le temps de lecture estimé de la section consacrée à l'échange est de 7 minutes.

Vous avez à présent terminé le processus TISAX, mais votre partenaire n'a toujours pas vu de « preuve » que votre système de gestion de la sécurité de l'information est capable de protéger ses données confidentielles. La présente section décrit à présent comment partager le résultat de votre évaluation avec votre partenaire et lui présenter la preuve qu'il demande.

6.1. Principe

L'une des caractéristiques principales de TISAX est que le résultat de votre évaluation est intégralement sous votre contrôle. Sans votre permission explicite, toutes les informations relatives à votre évaluation ne sont partagées avec personne.

6.2. La plateforme d'échange

La plateforme d'échange se trouve sur le portail ENX.

Votre auditeur téléchargera les deux premières sections (A et B) de votre rapport d'évaluation TISAX. À ce stade, les informations ne sont disponibles pour personne sauf pour vous.

Vous pouvez vous servir du compte créé durant l'inscription pour accéder au portail et utiliser la plateforme d'échange.

Vous pouvez accéder au portail à l'adresse suivante :
enx.com/en-US/SignIn

6.3. Conditions générales

Vous ne pouvez partager le résultat de votre évaluation avec votre partenaire que si ces deux conditions sont remplies :

1. Votre auditeur a envoyé le résultat de l'évaluation sur la plateforme d'échange.
   D'ordinaire, le résultat de l'évaluation est disponible sur la plateforme d'échange entre 5 et 10 jours ouvrables après la publication du rapport d'évaluation TISAX.
2. Nous avons reçu de votre part le paiement des frais (le cas échéant).

Le statut de votre périmètre d'évaluation est « actif » lorsque les deux conditions sont remplies.

Remarque :

Chaque périmètre d'évaluation a un cycle de vie. À ce stade, votre périmètre d'évaluation doit avoir le statut « actif ».

> Pour de plus amples informations sur le statut d'un périmètre d'évaluation, veuillez consulter la Section 7.5.5, "Assessment scope status "Awaiting your payment" (🇫🇷 Statut du périmètre d'évaluation « En attente de votre paiement »)".

Pour vérifier si le résultat de votre évaluation est prêt à être partagé (statut du périmètre d'évaluation = actif), suivez les étapes suivantes :

1. Connectez-vous sur le portail ENX.
2. Allez dans la barre de navigation principale et sélectionnez "MY TISAX" (🇫🇷 « MON TISAX »).
3. À partir du menu déroulant, sélectionnez "SCOPES AND ASSESSMENTS" (🇫🇷 « PÉRIMÈTRES ET ÉVALUATIONS »).
4. Allez dans le tableau et identifiez-y la ligne contenant votre périmètre d'évaluation.
5. Vérifiez que votre périmètre d'évaluation a le statut "Active" (🇫🇷 « Actif ») (colonne "Scope Status" (🇫🇷 « Statut du périmètre »)).

6.4. Permanence des résultats échangés

Remarque importante :

Vous ne pouvez pas annuler les autorisations de publication ou de partage.

En effet, nous souhaitons que tous les participants passifs puissent compter sur un accès permanent à chaque résultat d'évaluation qu'ils reçoivent. Sans cet accès, ils devraient gérer et archiver eux-mêmes les résultats d'évaluation.

L'autorisation reste valable pour toute la période de validité de votre évaluation TISAX.

Si vous avez créé par erreur une autorisation de publication ou de partage, veuillez nous contacter immédiatement.

6.5. Niveaux de partage

Les niveaux de partage correspondent directement aux sections principales A-E du rapport d'évaluation TISAX.

	Principales sections du rapport d'évaluation TISAX	**Niveaux de partage sur la plateforme d'échange**
1	A. Informations sur l'évaluation (🇬🇧 Assessment Related Information)	
2	B. Résumé des résultats (🇬🇧 Summarized Results)	

	Principales sections du rapport d'évaluation TISAX	Niveaux de partage sur la plateforme d'échange
3	C. Résumé du résultat d'évaluation (Assessment result summary)	
4	D. Niveaux de maturité de l'ISA (onglet Résultat) (Maturity Levels of VDA ISA (Result Tab))	
5	E. Résultats détaillés de l'évaluation (Detailed Assessment Results)	

Tableau 12. Principales sections du rapport d'évaluation TISAX et niveaux de partage sur la plateforme d'échange

Plus le niveau de partage est élevé, plus le(s) participant(s) concerné(s) disposera/disposeront d'informations détaillées sur votre évaluation TISAX.

Pour plus de détails sur le contenu de chaque section du rapport d'évaluation TISAX, veuillez consulter la Section 5.4.7.4, "Rapport d'évaluation TISAX".

6.6. Publier le résultat de votre évaluation sur la plateforme d'échange

Vous pouvez partager le résultat de votre évaluation avec tous les autres participants TISAX en le publiant sur la plateforme d'échange. Ce faisant, vous autorisez tous les autres participants TISAX à accéder au résultat de votre évaluation dans les limites du niveau de partage que vous leur avez attribué.

Vous ne pouvez publier le résultat de votre évaluation que si le résultat global d'évaluation est « conforme ».

Les niveaux de partage pour la publication du résultat de votre évaluation sur la plateforme d'échange sont limités aux options suivantes :

- Do not publish (Default) (Ne pas publier (valeur par défaut))
- A. Assessment Related Information (A. Informations sur l'évaluation)
- A + Labels (A + Labels)
- A + Labels + B. Summarized Results (A + Labels + B. Résumé des résultats)

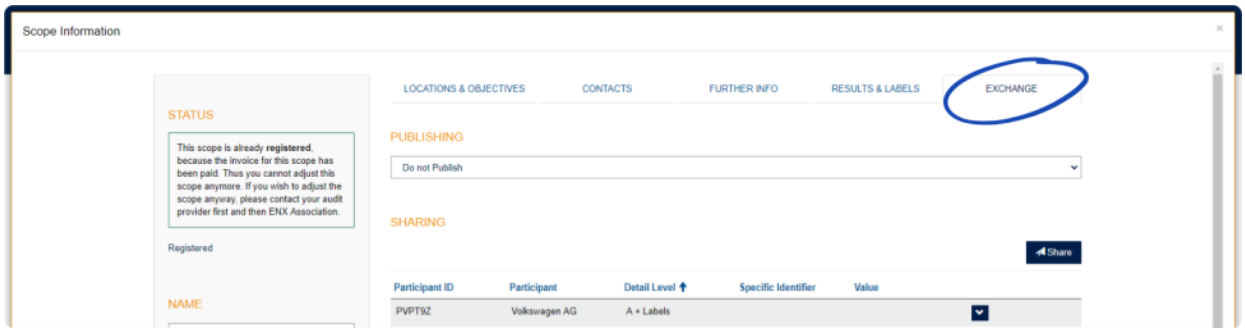
Nous recommandons le niveau de partage "A + Labels" (« A + Labels ») pour ce type général de publication.

Remarque importante :

Vous ne pouvez publier le résultat de votre évaluation que si les conditions préalables décrites à la Section 6.3, "Conditions générales" sont remplies.

Pour publier le résultat de votre évaluation sur la plateforme d'échange, suivez les étapes suivantes :

1. Connectez-vous sur le portail ENX.
2. Allez dans la barre de navigation principale et sélectionnez “MY TISAX” (« MON TISAX »).
3. À partir du menu déroulant, sélectionnez “SCOPES AND ASSESSMENTS” (« PÉRIMÈTRES ET ÉVALUATIONS »).
4. Allez dans le tableau et identifiez-y la ligne contenant votre périmètre d'évaluation.
5. Vérifiez que votre périmètre d'évaluation a le statut “Active” (« Actif ») (colonne “Scope Status” (« Statut du périmètre »)).
6. Allez au bout de la ligne de votre périmètre d'évaluation et cliquez sur le bouton avec la flèche vers le bas .
7. Sélectionnez “Scope Information” (« Informations sur le périmètre »).
8. Dans la nouvelle fenêtre (“Scope Information” (Informations sur le périmètre »), sélectionnez l'onglet “EXCHANGE” (« ÉCHANGE »).



9. Allez à la section “PUBLISHING” (« PUBLICATION »), ouvrez le menu déroulant et sélectionnez le niveau de partage souhaité (cf. la recommandation ci-dessus).

Remarque :

Les résultats d'évaluation ne sont publiés que sur la plateforme d'échange. Seuls les autres participants TISAX y ont accès. Il n'existe pas de listing public de tous les participants TISAX. Seul le numéro de ligne des participants TISAX peut être mentionné sur le site Web public de TISAX.

6.7. Partager le résultat de votre évaluation avec un partenaire particulier

Outre l'option ci-dessus pour la publication sur la plateforme d'échange, vous pouvez partager le résultat de votre évaluation TISAX avec des participants TISAX particuliers bénéficiant d'un niveau de partage plus élevé.

Contrairement à la publication susmentionnée, vous pouvez partager le résultat de votre

évaluation, même si le résultat global est non conforme (mineur/majeur).

Le partage des résultats d'évaluation fait partie intégrante de TISAX. Votre système de gestion de la sécurité de l'information a été évalué une seule fois, mais désormais, vous pouvez partager le résultat de votre évaluation avec autant de partenaires que vous le souhaitez.

Les options de partage du résultat de votre évaluation sur la plateforme d'échange sont :

1. A: Assessment Related Information (A : informations sur l'évaluation)
2. A + Labels (A + Labels)
3. A + Labels + B: Assessment Summary (A + labels + B : résumé de l'évaluation)
4. A + Labels + B + C: Summarized Results (A + labels + B + C : résumé des résultats)
5. A + Labels + B + C + D: Detailed Assessment Results (A + labels + B + C + D : résultats détaillés de l'évaluation)
6. A + Labels + B + C + D + E: Maturity Levels according to ISA (A + labels + B + C + D + E : niveaux de maturité selon l'ISA)

Nous recommandons le niveau de partage "A + Labels" (« A + labels ») pour le partage. Il est suffisant pour la majorité des partenaires. Vous pourrez toujours sélectionner un niveau de partage supérieur ultérieurement.

Remarque :

Certains participants TISAX traitent automatiquement les résultats d'évaluation de leurs partenaires. Ils synchronisent leur propre système avec le portail ENX. Seuls les résultats d'évaluation partagés spécifiquement avec ce participant sont synchronisés. Une publication seule, telle que décrite à la Section 6.6, "Publier le résultat de votre évaluation sur la plateforme d'échange", n'est pas reconnue.

Parmi les EOM qui utilisent TISAX, BMW, par exemple, adopte cette démarche. Si vous êtes un partenaire de BMW, veuillez vous assurer de partager (et pas uniquement de publier) le résultat de votre évaluation avec BMW.

6.7.1. Conditions préalables

Les conditions préalables au partage du résultat de votre évaluation avec votre partenaire (ou tout autre participant TISAX) sont les suivantes :

- Vous ne pouvez partager le résultat de votre évaluation TISAX qu'avec d'autres participants TISAX.
- Votre partenaire doit être un participant TISAX.

- Vous avez besoin de l'ID de participant de votre partenaire.[31]
- Vous devez payer les frais (le cas échéant).

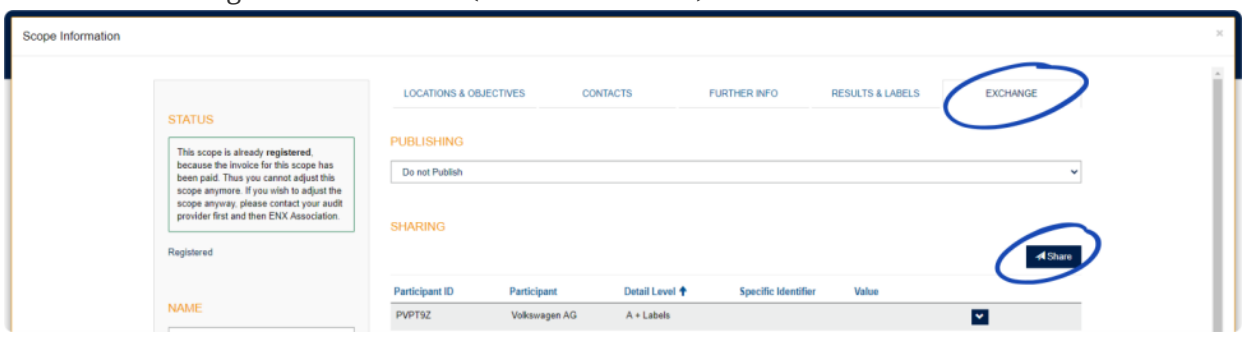
Remarque importante :

Vous ne pouvez partager le résultat de votre évaluation que si les conditions générales décrites à la Section 6.3, "Conditions générales" sont remplies.

6.7.2. Comment créer une autorisation de partage

Pour partager le résultat de votre évaluation avec un autre participant TISAX, suivez les étapes suivantes :

1. Connectez-vous sur le portail ENX.
2. Allez dans la barre de navigation principale et sélectionnez "MY TISAX" (« MON TISAX »).
3. À partir du menu déroulant, sélectionnez "SCOPES AND ASSESSMENTS" (« PÉRIMÈTRES ET ÉVALUATIONS »).
4. Allez dans le tableau et identifiez-y la ligne contenant votre périmètre d'évaluation.
5. Vérifiez que votre périmètre d'évaluation a le statut "Active" (« Actif ») (colonne "Scope Status" (« Statut du périmètre »)).
6. Allez au bout de la ligne de votre périmètre d'évaluation et cliquez sur le bouton avec la flèche vers le bas .
7. Sélectionnez "Scope Information" (« Informations sur le périmètre »).
8. Dans la nouvelle fenêtre ("Scope Information" (Informations sur le périmètre »), sélectionnez l'onglet "EXCHANGE" (« ÉCHANGE »).



9. Allez à la section "SHARING" (« PARTAGE ») et cliquez sur le bouton "Share" (« Partager »).
10. Dans la nouvelle fenêtre ("SHARE THIS SCOPE" (« PARTAGER CE PÉRIMÈTRE »)), saisissez l'ID de participant de votre partenaire (ou sélectionnez-le dans la liste de participants depuis la zone de recherche voisine).
11. Sélectionnez le niveau de partage souhaité.

12. Cliquez sur le bouton “Next” (« Suivant »).
13. Lisez attentivement les instructions concernant la permanence de l’autorisation de partage.
14. Cochez les deux cases “confirm” (« confirmer »).
15. Cliquez sur le bouton “Submit” (« Envoyer »).

Tout le reste est effectué sur la plateforme d’échange. Pour les niveaux de partage A et B, les informations sont disponibles sur la plateforme d’échange. Votre partenaire peut à présent se connecter sur le portail ENX et voir le résultat partagé de votre évaluation[32].

Pour les niveaux de partage supérieurs (C-E), la plateforme d’échange avise votre auditeur. Ensuite, votre auditeur envoie les informations (correspondant au niveau de partage sélectionné) au principal contact de participant de votre partenaire.

6.8. Partager le résultat de votre évaluation en dehors de TISAX

La règle[33] prévoit que vous pouvez utiliser la plateforme d’échange TISAX uniquement pour informer d’autres participants TISAX du résultat de votre évaluation.

6.8.1. Les raisons d’une gestion stricte du mécanisme d’échange

TISAX fournit un mécanisme d’échange standardisé pour les résultats d’évaluation. Celui-ci présente une valeur ajoutée par rapport à l’échange des résultats d’autres certifications (p. ex. : ISO), pour lesquelles l’échange se fait de diverses manières et ne comprend pas toujours toutes les informations nécessaires pour fournir une image complète.

Les OEM en particulier apprécient cette standardisation. Mais d’autres sociétés tirent également profit de procédures clairement définies.

6.8.2. Un guide concernant les références écrites publiques à TISAX

S’il vous est interdit d’écrire publiquement à propos du résultat d’évaluation, vous pouvez mentionner le travail que vous réalisez pour l’évaluation TISAX. Sur le portail ENX, nous prodiguons des conseils sur la manière d’aborder les déclarations publiques. Nous fournissons aussi les logos TISAX que vous pouvez utiliser.

Après vous être connecté sur le portail ENX, vous pouvez accéder aux informations suivantes :
enx.com/en-US/myenxportal/marketing/
Téléchargement direct de l’archive ZIP (document et logos) :
enx.com/en-US/myenxportal/marketing/TISAX-Trademark-and-Logos-Terms-and-Conditions.zip

Si vous vous demandez s’il existe un certificat que vous pourriez afficher sur votre mur :
En raison du processus d’échange standardisé mentionné ci-dessus, nous ne fournissons pas ce

genre de certificat.

6.8.3. Partage avec un partenaire qui n’est pas encore participant TISAX

Si vous souhaitez partager le résultat de votre évaluation TISAX avec un partenaire particulier qui a) n’est pas encore participant TISAX et b) n’a pas encore reçu de labels TISAX (après avoir passé le processus d’évaluation), vous pouvez suivre les étapes suivantes :

1. Dites à votre partenaire de s’inscrire en tant que participant TISAX.
   Il lui suffit de s’inscrire comme participant TISAX. Il n’a pas besoin de poursuivre le processus en enregistrant un périmètre d’évaluation.
2. Dites à votre partenaire de nous contacter.
   Habituellement, nous ne procédons à une nouvelle inscription que si l’entreprise enregistre également un périmètre d’évaluation. À la demande de votre partenaire, nous procédons à son inscription. Ainsi, il deviendra participant TISAX. Il peut désormais recevoir le résultat de votre évaluation TISAX par le biais du processus d’échange normal.

L’objectif de cette approche est de s’assurer que votre partenaire consent à respecter les « Conditions générales de participation TISAX » qui régissent l’échange des résultats d’évaluation TISAX.

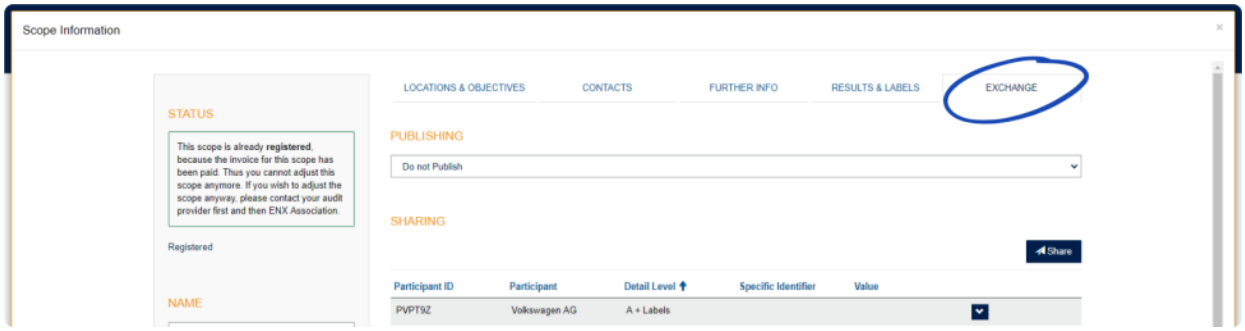
Seul l’inscription d’un périmètre d’évaluation implique des coûts. Comme l’inscription d’un participant TISAX est gratuite, votre partenaire peut recevoir gratuitement le résultat de votre évaluation. Toutefois, en l’absence d’un résultat d’évaluation propre, votre partenaire ne peut recevoir qu’un maximum de cinq résultats d’évaluation et ne peut voir aucune des publications.

6.8.4. Partage avec des salariés de votre partenaire qui n’ont pas d’accès direct au portail ENX

Seuls les salariés de votre partenaire qui ont un compte sur notre portail ENX peuvent voir directement votre résultat. Pour prouver vos labels TISAX à un salarié de votre partenaire qui n’a pas accès au portail, vous pouvez utiliser un document PDF particulier. Pour obtenir le document, veuillez suivre les étapes suivantes :

1. Partagez le résultat de votre évaluation avec votre partenaire comme décrit à la Section 6.7, “Partager le résultat de votre évaluation avec un partenaire particulier”.
2. Connectez-vous sur le portail ENX.
3. Allez dans la barre de navigation principale et sélectionnez “MY TISAX” (« MON TISAX »).
4. À partir du menu déroulant, sélectionnez “SCOPES AND ASSESSMENTS” (« PÉRIMÈTRES ET ÉVALUATIONS »).
5. Allez dans le tableau et identifiez-y la ligne contenant votre périmètre d’évaluation.
6. Vérifiez que votre périmètre d’évaluation a le statut “Active” (« Actif ») (colonne “Scope Status” (« Statut du périmètre »)).

7. Allez au bout de la ligne de votre périmètre d'évaluation et cliquez sur le bouton avec la flèche vers le bas .
8. Sélectionnez “Scope Information” (« Informations sur le périmètre »).
9. Dans la nouvelle fenêtre (“Scope Information” (Informations sur le périmètre »), sélectionnez l'onglet “EXCHANGE” (« ÉCHANGE »).



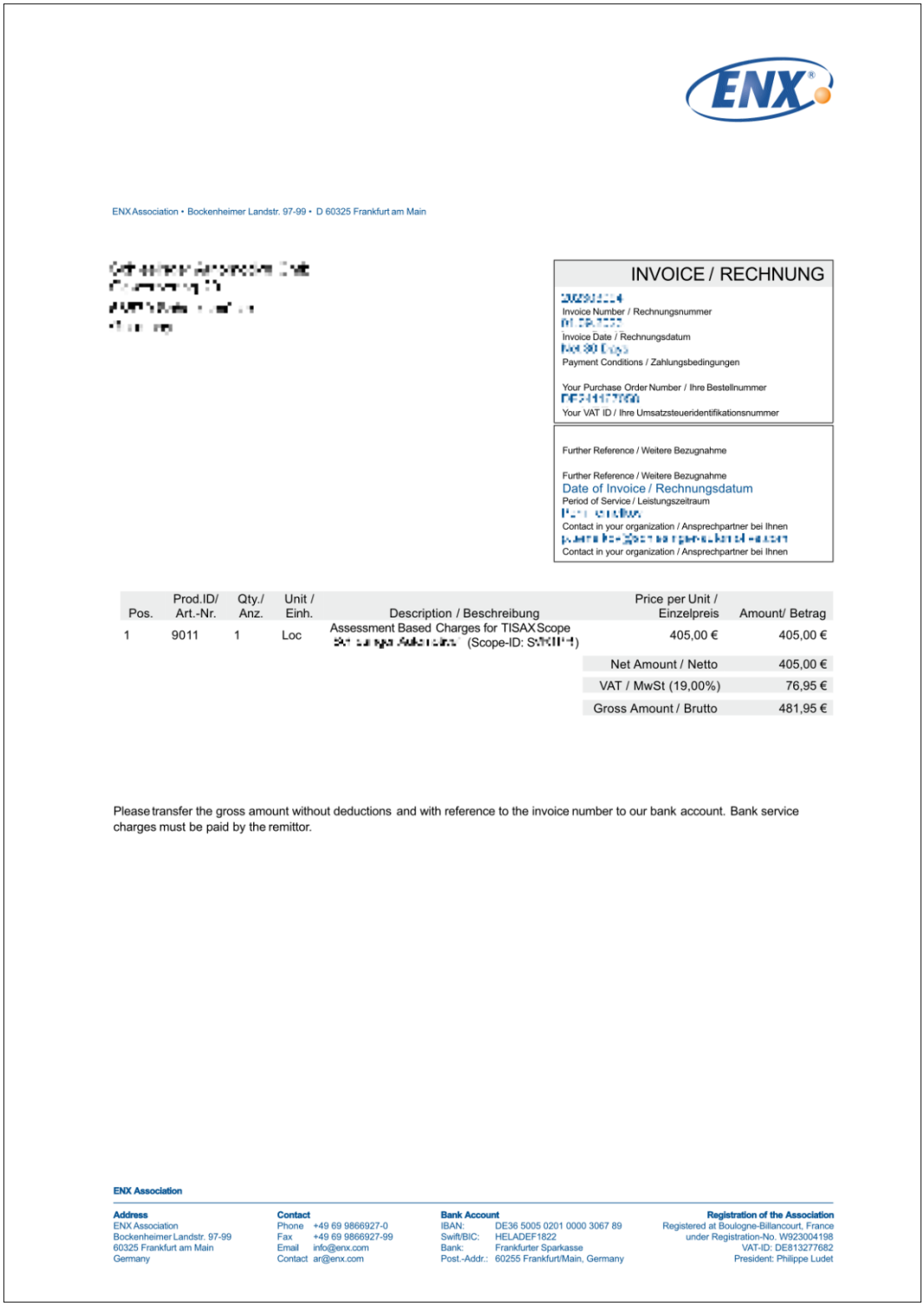
10. Allez à la section “SHARING” (« PARTAGE ») et identifiez la ligne du tableau contenant l'autorisation de partage (telle que créée à l'étape 1).
11. Allez au bout de la ligne du tableau de l'autorisation de partage et cliquez sur le bouton avec la flèche vers le bas .
12. Sélectionnez “Edit” (« Modifier »)
13. Dans la nouvelle fenêtre (“SHARE THIS SCOPE” (« PARTAGER CE PÉRIMÈTRE »)), faites défiler jusqu'en bas et sélectionnez “Request Shared Information as PDF” (« Demander des informations partagées en PDF »).
14. Attendez un moment que le document soit généré.
15. Téléchargez le document (“Copy of information shared with ACME.pdf (66.84 KB)” (« Copie des informations partagées avec ACME.pdf (66.84 KB) »))

7. Annexes

7.1. Annexe : exemple de facture

Voici un exemple de facture que nous envoyons.

Pour de plus amples informations, veuillez consulter la Section 4.3.4, “Frais”.



ENX Association • Bockenheimer Landstr. 97-99 • D 60325 Frankfurt am Main

[redacted]

INVOICE / RECHNUNG

[redacted]
Invoice Number / Rechnungsnummer
[redacted]
Invoice Date / Rechnungsdatum
[redacted]
Payment Conditions / Zahlungsbedingungen

Your Purchase Order Number / Ihre Bestellnummer
[redacted]
Your VAT ID / Ihre Umsatzsteueridentifikationsnummer

Further Reference / Weitere Bezugnahme

Further Reference / Weitere Bezugnahme
Date of Invoice / Rechnungsdatum
Period of Service / Leistungszeitraum
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen

Pos.	Prod.ID/ Art.-Nr.	Qty./ Anz.	Unit / Einh.	Description / Beschreibung	Price per Unit / Einzelpreis	Amount/ Betrag
1	9011	1	Loc	Assessment Based Charges for TISAX Scope [redacted] (Scope-ID: [redacted])	405,00 €	405,00 €
					Net Amount / Netto	405,00 €
					VAT / MwSt (19,00%)	76,95 €
					Gross Amount / Brutto	481,95 €

Please transfer the gross amount without deductions and with reference to the invoice number to our bank account. Bank service charges must be paid by the remittor.

ENX Association

Address	Contact	Bank Account	Registration of the Association
ENX Association Bockenheimer Landstr. 97-99 60325 Frankfurt am Main Germany	Phone +49 69 9866927-0 Fax +49 69 9866927-99 Email info@enx.com Contact ar@enx.com	IBAN: DE36 5005 0201 0000 3067 89 Swift/BIC: HELADEF1822 Bank: Frankfurter Sparkasse Post.-Addr.: 60255 Frankfurt/Main, Germany	Registered at Boulogne-Billancourt, France under Registration-No. W923004198 VAT-ID: DE813277682 President: Philippe Ludet

7.2. Annexe : exemple d’e-mail de confirmation

Nous envoyons l’e-mail de confirmation une fois que vous avez terminé toutes les étapes obligatoires au cours du processus d’inscription en ligne.

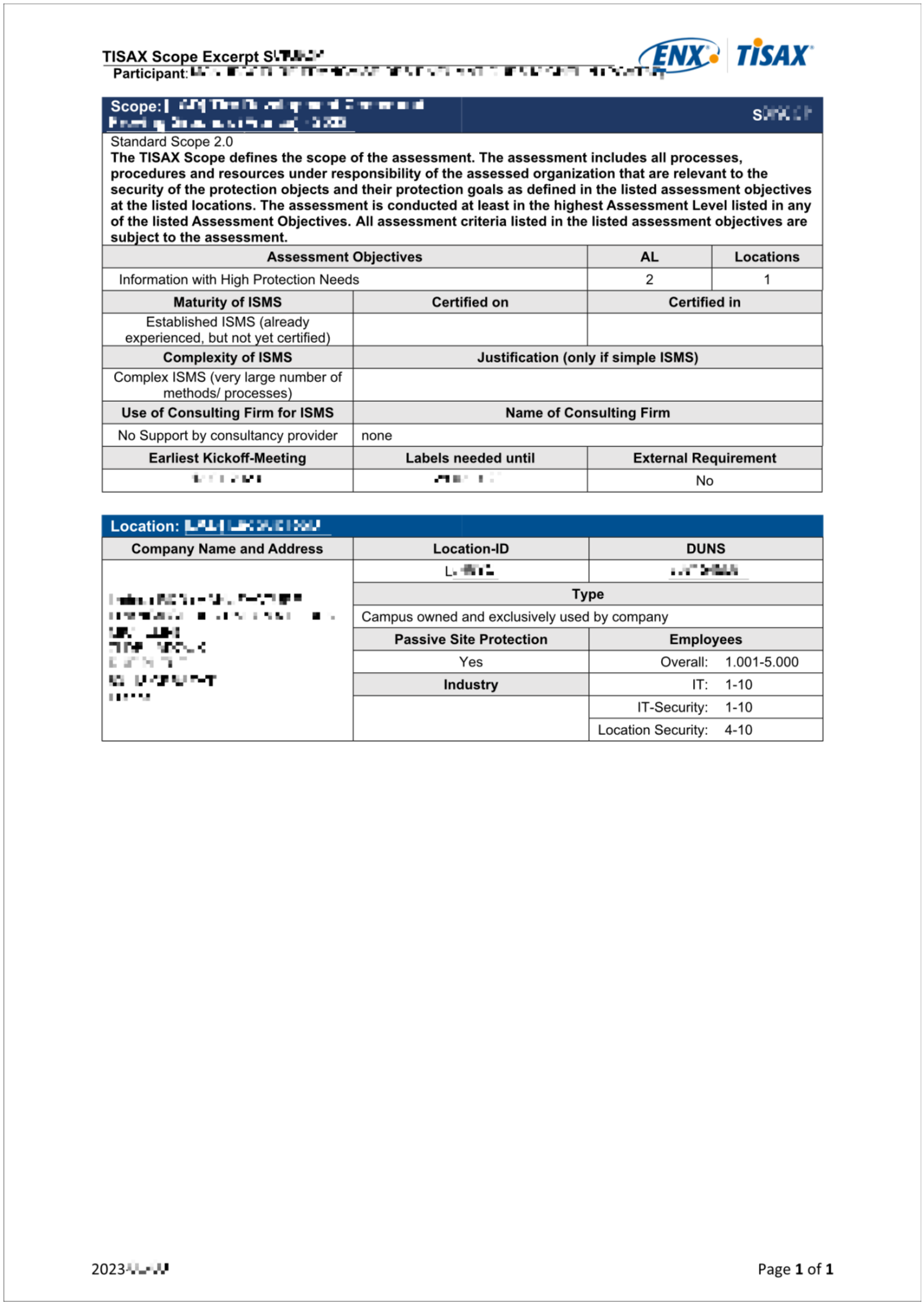
Pour de plus amples informations concernant le moment où nous envoyons cet e-mail de confirmation, veuillez consulter la Section 4.5.8, “E-mail de confirmation”.

```
Objet : [TISAX] périmètre S3ZY5V approuvé

Cher Jean Dupont,

Merci d'avoir inscrit le périmètre d'évaluation TISAX. J'ai procédé à l'inscription
de votre périmètre et ai approuvé ce dernier. Vous trouverez en pièce jointe
l'extrait de périmètre TISAX comprenant l'ensemble des informations sur le périmètre
et la liste actualisée des auditeurs TISAX.

Quelle est la prochaine étape ?

Avec l'extrait du périmètre TISAX en pièce jointe, vous pouvez désormais demander
des offres à tous les auditeurs TISAX pour votre périmètre.

Vous avez besoin d'aide ?

Pour toute autre question concernant TISAX, veuillez lire les FAQ TISAX ou le
manuel du participant TISAX  Si vous avez besoin d'une aide supplémentaire
concernant TISAX, n'hésitez pas à contacter la hotline TISAX par e-mail
(tisax@enx.com) ou par téléphone (+49 69 986692-777).

Sincères salutations,

Votre équipe TISAX
```

7.3. Annexe : exemple d’extrait de périmètre TISAX

Vous recevez « l’extrait de périmètre TISAX » joint à l’e-mail de confirmation.

Pour de plus amples informations, veuillez consulter la Section 4.5.8, “E-mail de confirmation”.



TISAX Scope Excerpt S[redacted]

Participant: [redacted]

Scope: [redacted]

Standard Scope 2.0

The TISAX Scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations. The assessment is conducted at least in the highest Assessment Level listed in any of the listed Assessment Objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

Assessment Objectives	AL	Locations
Information with High Protection Needs	2	1

Maturity of ISMS	Certified on	Certified in
Established ISMS (already experienced, but not yet certified)		

Complexity of ISMS	Justification (only if simple ISMS)
Complex ISMS (very large number of methods/ processes)	

Use of Consulting Firm for ISMS	Name of Consulting Firm
No Support by consultancy provider	none

Earliest Kickoff-Meeting	Labels needed until	External Requirement
[redacted]	[redacted]	No

Location: [redacted]

Company Name and Address	Location-ID	DUNS
[redacted]	[redacted]	[redacted]
	Type	
	Campus owned and exclusively used by company	
	Passive Site Protection	**Employees**
	Yes	Overall: 1.001-5.000
	Industry	IT: 1-10
		IT-Security: 1-10
		Location Security: 4-10

2023[redacted]

Page **1** of **1**

7.4. Annexe : Participant status (Statut du participant)

7.4.1. Aperçu : Participant status (Statut du participant)

Le « statut du participant » » définit à quel stade du processus TISAX vous (en tant qu'entreprise) vous trouvez.

Votre « statut du participant » peut être :

1. Incomplete (Incomplet)
2. Awaiting approval (En attente d'approbation)
3. Preliminary (Préliminaire)
4. Registered (Inscrit)
5. Expired (Expiré)

Les tableaux dans chaque section de statut ci-dessous décrivent :

- votre situation
  (telle qu'elle est actuellement alors que vous présentez ce statut)
- votre prochaine action
  (ce que vous devez faire pour progresser vers le prochain statut, le cas échéant)
- notre prochaine action
  (ce que nous devons faire pour faire passer votre statut au niveau supérieur, le cas échéant)
- le prochain statut
  (le cas échéant)

L'illustration suivante présente les actions qui permettent de progresser d'un statut à l'autre :

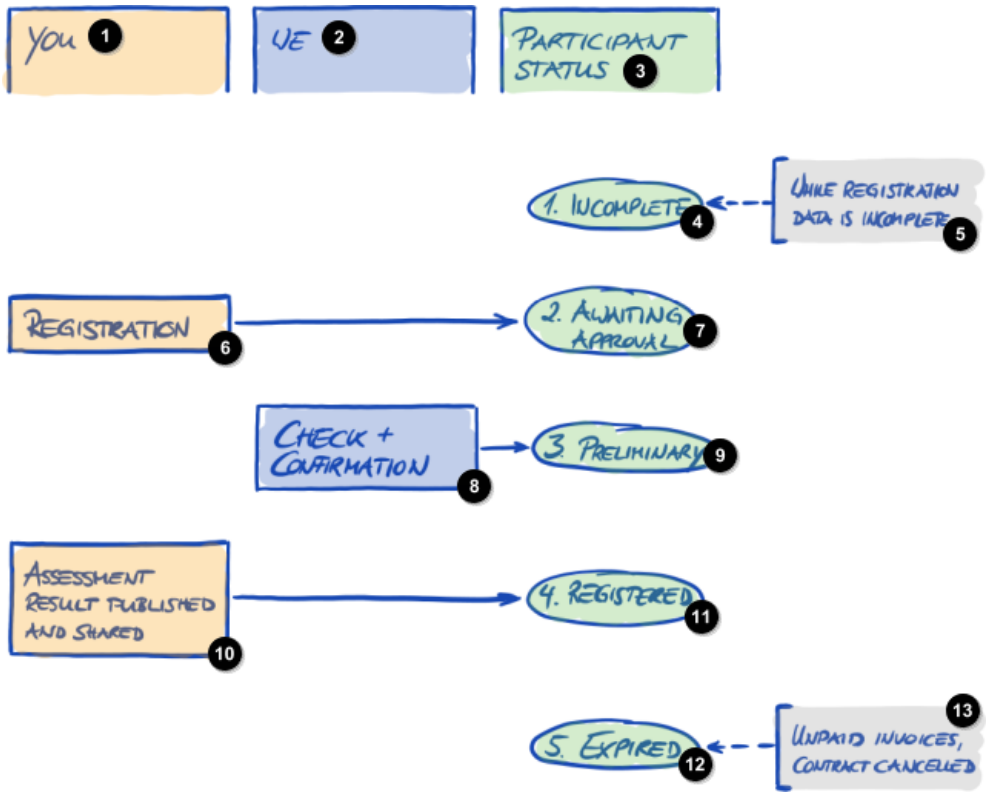


Illustration 34. Aperçu des statuts du participant

1. Vous
2. Nous
3. Statut du participant
4. 1. Incomplet
5. Tant que les données d’inscription sont incomplètes
6. Inscription
7. 2. En attente d’approbation
8. Vérifier + confirmation
9. 3. Préliminaire
10. Résultat d’évaluation publié et partagé
11. 4. Inscrit
12. 5. Expiré
13. Factures impayées, contrat annulé

7.4.2. Participant status “Incomplete” (Statut du participant « Incomplet »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
Incomplet	Vous n’avez pas terminé l’inscription TISAX. Vous n’avez pas accepté les conditions générales, ou vous n’avez pas spécifié le principal site du participant, ou vous n’avez pas spécifié le principal contact de participant, ou il manque d’autres informations requises.	Continuez sur enx.com/en-US/SignIn	Nous vous enverrons un rappel par e-mail (généralement sous quelques jours).	En attente d’approbation

7.4.3. Participant status “Awaiting approval” (Statut du participant « En attente d’approbation »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
En attente d’approbation	Votre inscription TISAX est complète. À ce stade, vous avez ou n’avez pas encore enregistré de périmètre d’évaluation.	Attendez notre prochaine action.	Nous vérifierons et en principe, nous approuverons votre demande. Toutefois, nos vérifications sont aussi généralement déclenchées par l’inscription d’un périmètre d’évaluation. Nous vous attribuerons un ID de participant et un/des ID de périmètre. Nous vous enverrons un e-mail de confirmation. « L’extrait de périmètre TISAX » en pièce jointe (PDF) résume les informations que nous avons dans notre base de données.	Préliminaire

7.4.4. Participant status “Preliminary” (Statut du participant « Préliminaire »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
Préliminaire	Vous avez terminé avec succès le processus d'inscription TISAX.	Payez les frais (le cas échéant). Suivez le processus d'évaluation TISAX. Publiez et partagez votre résultat d'évaluation.	Aucune	Inscrit

7.4.5. Participant status “Registered” (Statut du participant « Inscrit »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
Inscrit	Vous avez terminé avec succès le processus d’évaluation TISAX et avez reçu des labels TISAX. Vous avez publié et partagé le résultat de votre évaluation. Vous obtenez des labels TISAX uniquement si vous avez passé avec succès le processus d’évaluation TISAX. Dans le portail ENX, cela se traduit par un périmètre d’évaluation associé au statut « Actif ».	Aucune	Aucune	(Expiré)

Remarque :

Si vous souhaitez accéder aux résultats d’évaluation de votre/vos partenaire(s) :

Le prérequis conceptuel pour pouvoir recevoir des résultats d’évaluation d’autres participants est soit :

- Que vous partagiez le résultat de votre propre évaluation (cela « prouve » que vous êtes un participant TISAX sérieux et un membre de la communauté automobile) ;
- Que nous vous reconnaissions sur la base de votre réputation dans l’industrie automobile (p. ex. : en tant qu’OEM, fournisseur de premier

rang) ;

- Que vous prouviez que vous avez un intérêt légitime à recevoir les résultats d'évaluation d'autres participants. Nous devons le vérifier lors d'un processus élaboré susceptible d'impliquer des frais substantiels. Pour de plus amples détails, veuillez nous contacter.

7.4.6. Participant status "Expired" (Statut du participant « Expiré »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
Expiré	Vous n'avez pas payé les frais ou vous avez / nous avons annulé notre contrat mutuel (les CG).	Aucune	Aucune	n/a

7.5. Annexe : Assessment scope status (Statut du périmètre d'évaluation)

7.5.1. Aperçu : Assessment scope status (Statut du périmètre d'évaluation)

Le « statut du périmètre d'évaluation » définit à quel stade de son cycle de vie se trouve votre périmètre d'évaluation.

Notez que le « statut du périmètre d'évaluation » est différent du « statut de l'évaluation ». Pour de plus amples informations sur le « statut de l'évaluation », veuillez consulter la Section 7.6, "Annexe : Assessment status (Statut de l'évaluation)".

Le « statut de votre périmètre d'évaluation » peut être :

1. Incomplete (Incomplet)
2. Awaiting your order (En attente de votre commande)
3. Awaiting ENX approval (En attente d'approbation ENX)
4. Awaiting your payment (En attente de votre paiement)
5. Registered (Inscrit)
6. Active (Actif)
7. Expired (Expiré)

Les tableaux dans chaque section de statut ci-dessous décrivent :

- votre situation
  (telle qu'elle est actuellement alors que vous présentez ce statut)
- votre prochaine action
  (ce que vous devez faire pour progresser vers le prochain statut, le cas échéant)
- notre prochaine action
  (ce que nous devons faire pour faire passer votre statut au niveau supérieur, le cas échéant)
- le prochain statut
  (le cas échéant)

L'illustration suivante présente les actions qui permettent de progresser d'un statut à l'autre :

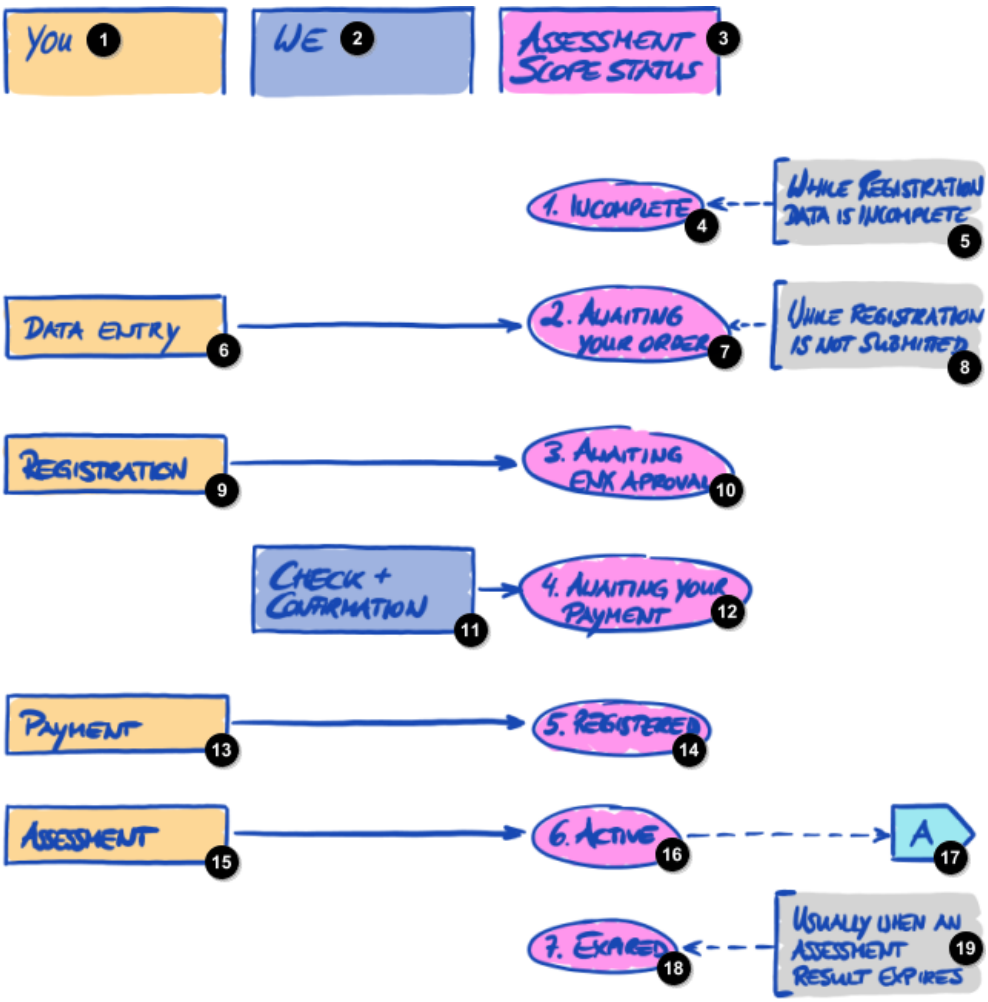


Illustration 35. Aperçu du statut du périmètre d'évaluation

1. Vous
2. Nous
3. Statut du périmètre d'évaluation

4. 1. Incomplet
5. Tant que les données d'inscription sont incomplètes
6. Saisie des données
7. 2. En attente de votre commande
8. Tant que l'inscription n'est pas envoyée
9. Inscription
10. 3. En attente d'approbation ENX
11. Vérifier + confirmation
12. 4. En attente de votre paiement
13. Paiement
14. 5. Inscrit
15. Évaluation
16. 6. Actif
17. A
18. 7. Expiré
19. Habituellement, lorsqu'un résultat d'évaluation expire

La référence hors page « A » dans l'illustration ci-dessus relie le statut du périmètre d'évaluation « Actif » au « statut de l'évaluation ». Pour de plus amples informations sur le « statut de l'évaluation », veuillez consulter la Section 7.6, "Annexe : Assessment status (Statut de l'évaluation)".

7.5.2. Assessment scope status "Incomplete" (Statut du périmètre d'évaluation « Incomplet »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
Incomplet	Vous n’avez pas terminé l’inscription du périmètre d’évaluation. ou vous n’avez pas fourni toutes les informations requises.	Continuez sur enx.com/en-US/SignIn	Nous vous enverrons un rappel par e-mail (généralement sous quelques jours).	En attente de votre commande

Pour de plus amples informations sur les circonstances dans lesquelles ce statut joue un rôle, veuillez consulter la Section 4.5.7, “Inscription du périmètre d’évaluation”.

7.5.3. Assessment scope status “Awaiting your order” (Statut du périmètre d’évaluation « En attente de votre commande »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
En attente de votre commande	Vous n’avez pas terminé l’inscription de votre périmètre.	Continuez sur enx.com/en-US/SignIn	Nous vous enverrons un rappel par e-mail (généralement sous quelques jours).	En attente d’approbation ENX

Pour de plus amples informations sur les circonstances dans lesquelles ce statut joue un rôle, veuillez consulter la Section 4.5.7, “Inscription du périmètre d’évaluation”.

7.5.4. Assessment scope status “Awaiting ENX approval” (Statut du périmètre d’évaluation « En attente d’approbation ENX »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
En attente d'approbation ENX	L'inscription de votre périmètre d'évaluation est terminée.	Attendez notre prochaine action.	Nous vérifierons et en principe, nous approuverons votre demande. Nous attribuerons l'/les ID de périmètre. Nous vous enverrons un e-mail de confirmation. « L'extrait de périmètre TISAX » en pièce jointe (PDF) résume les informations que nous avons dans notre base de données.	En attente de votre paiement

Pour de plus amples informations sur les circonstances dans lesquelles ce statut joue un rôle, veuillez consulter la Section 4.5.7, "Inscription du périmètre d'évaluation".

7.5.5. Assessment scope status “Awaiting your payment” (Statut du périmètre d’évaluation « En attente de votre paiement »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
En attente de votre paiement	L’inscription de votre périmètre d’évaluation est terminée et approuvée. Vous avez reçu notre e-mail de confirmation et l’« extrait de périmètre TISAX ».	Payez les frais (le cas échéant). Demandez des offres à nos auditeurs TISAX. À partir du statut « En attente de votre paiement », vous : ▪ pouvez commencer à partager certaines informations relatives à l’évaluation avec votre partenaire. [34] ▪ pouvez préconfigurer la publication du résultat de votre évaluation (elle ne sera effective que lorsque le statut de votre périmètre d’évaluation passera à « Actif ».	En attente de votre paiement.	Inscrit

Pour de plus amples informations sur les circonstances dans lesquelles ce statut joue un rôle, veuillez consulter la Section 4.5.8, “E-mail de confirmation”.

7.5.6. Assessment scope status “Registered” (Statut du périmètre d’évaluation « Inscrit »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
Inscrit	Votre périmètre d’évaluation est enregistré. Nous avons reçu l’intégralité de votre paiement ou votre statut commercial est « vert » en raison d’autres circonstances.	Suivez le processus d’évaluation TISAX.	Aucune	Actif

7.5.7. Assessment scope status “Active” (Statut du périmètre d’évaluation « Actif »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
Actif	Vous avez terminé avec succès le processus d’évaluation TISAX et avez reçu des labels TISAX.	Publiez et partagez le résultat de votre évaluation. Toute autorisation de publication et de partage préconfigurée à un statut inférieur devient à présent effective.	Aucune	Expiré

Pour de plus amples informations sur la publication et le partage, veuillez consulter la Section 6, “Échange (étape 3)”.

7.5.8. Assessment scope status “Expired” (Statut du périmètre d’évaluation « Expiré »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
Expiré	Soit : ▪ Vous n’avez pas terminé l’inscription de votre périmètre d’évaluation dans les 90 jours,	Démarrez une nouvelle inscription du périmètre d’évaluation.	Aucune	Incomplet ou En attente de votre commande ou En attente d’approbation ENX
	• ou il y a eu un retard excessif dans le paiement des frais,			
	• ou vous avez abandonné le processus d’évaluation TISAX,			
	• ou la validité du résultat de votre évaluation a expiré (trois ans),			

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
	• ou vous avez apporté des modifications majeures au périmètre d'évaluation (exemple : plus aucun site dans un périmètre d'évaluation n'appartient à votre entreprise).			

7.6. Annexe : Assessment status (🇫🇷 Statut de l'évaluation)

7.6.1. Aperçu : Assessment status (🇫🇷 Statut de l'évaluation)

Le « statut de l'évaluation » définit à quel stade du processus d'évaluation vous vous trouvez. Le statut change à mesure que vous progressez d'un type d'évaluation au suivant (comme « évaluation initiale » à « évaluation du plan d'action corrective »).

Notez que le « statut de l'évaluation » est différent du « statut du périmètre d'évaluation ». Pour de plus amples informations sur le « statut du périmètre d'évaluation », veuillez consulter la Section 7.5, "Annexe : Assessment scope status (🇫🇷 Statut du périmètre d'évaluation)".

Votre « statut de l'évaluation » peut être :

1. Initial assessment ordered (🇫🇷 Évaluation initiale commandée)
2. Initial assessment ongoing (🇫🇷 Évaluation initiale en cours)
3. Waiting for corrective action plan assessment (🇫🇷 En attente de l'évaluation du plan d'action corrective)
4. Waiting for follow-up (🇫🇷 En attente de suivi)
5. Finished (🇫🇷 Terminé)

Les tableaux dans chaque section de statut ci-dessous décrivent :

- votre situation

(telle qu'elle est actuellement alors que vous présentez ce statut)

- votre prochaine action
  (ce que vous devez faire pour progresser vers le prochain statut, le cas échéant)
- notre prochaine action
  (ce que nous devons faire pour faire passer votre statut au niveau supérieur, le cas échéant)
- le prochain statut
  (le cas échéant)

L'illustration suivante présente les actions qui permettent de progresser d'un statut à l'autre :

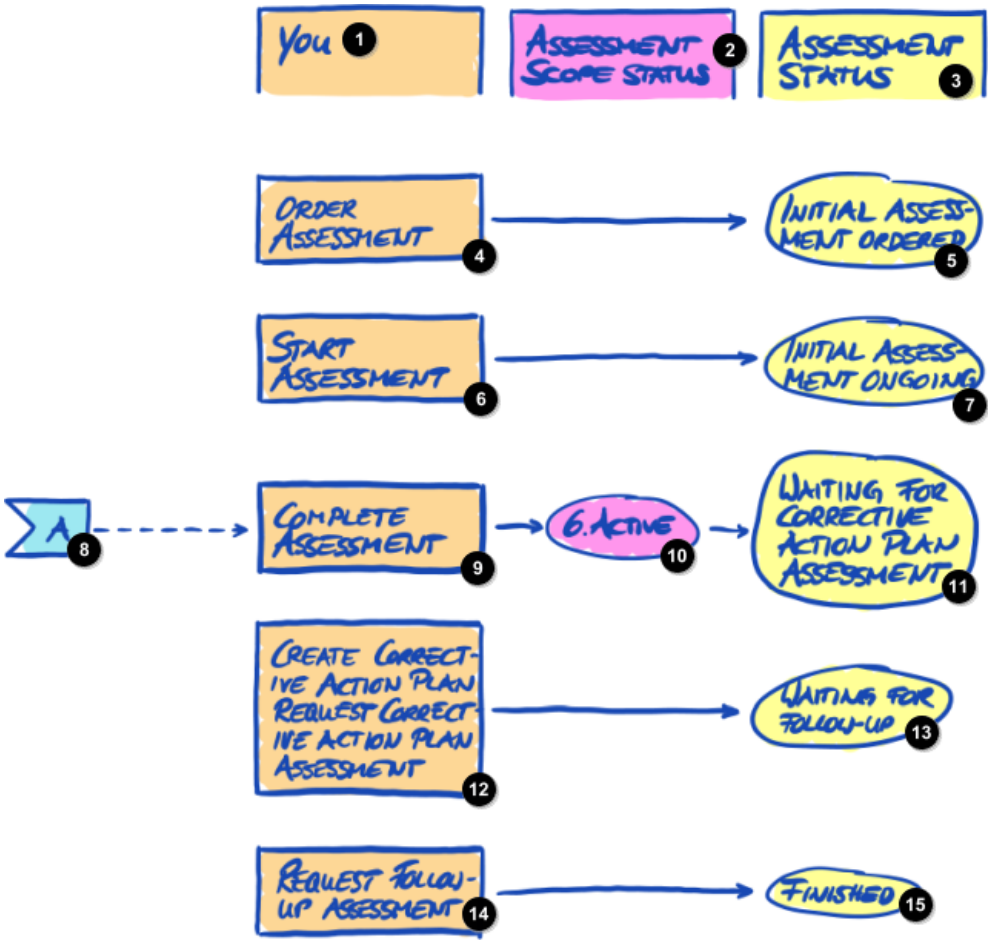


Illustration 36. Aperçu du statut de l'évaluation

1. Vous
2. Statut du périmètre d'évaluation
3. Statut de l'évaluation
4. Commandez l'évaluation
5. Évaluation initiale commandée

6. Débutez l'évaluation
7. Évaluation initiale en cours
8. A
9. Passez l'évaluation
10. 6. Actif
11. En attente de l'évaluation du plan d'action corrective
12. Créez un plan d'action corrective
    Demandez l'évaluation du plan d'action corrective
13. En attente de suivi
14. Demandez l'évaluation de suivi
15. Terminé

La référence hors page « A » dans l'illustration ci-dessus relie le statut du périmètre d'évaluation « Actif » au « statut de l'évaluation » « En attente de l'évaluation du plan d'action corrective ». Pour de plus amples informations sur le « statut du périmètre d'évaluation », veuillez consulter la Section 7.5, "Annexe : Assessment scope status (Statut du périmètre d'évaluation)".

7.6.2. Assessment status "Initial assessment ordered" (Statut de l'évaluation « Évaluation initiale commandée »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
Évaluation initiale commandée	Vous avez sélectionné l'un de nos auditeurs TISAX et avez commandé une évaluation initiale.	Poursuivez le processus d'évaluation TISAX.	Aucune	Évaluation initiale en cours

7.6.3. Assessment status "Initial assessment ongoing" (Statut de l'évaluation « Évaluation initiale en cours »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
Évaluation initiale en cours	Votre évaluation initiale : ▪ a commencé ▪ ou est terminée, mais votre auditeur n'a pas encore envoyé le rapport d'évaluation TISAX	Aucune	Aucune	En attente de l'évaluation du plan d'action corrective (le cas échéant)

7.6.4. Assessment status "Waiting for corrective action plan assessment" (Statut de l'évaluation « En attente de l'évaluation du plan d'action corrective »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
En attente de l'évaluation du plan d'action corrective	Votre auditeur a mené une évaluation initiale. Votre auditeur nous a envoyé le rapport d'évaluation TISAX. Le résultat de l'évaluation est non conforme (majeur/mineur).	Créez un plan d'action corrective. Entamez les actions correctives. Demandez une évaluation du plan d'action corrective.	Aucune	En attente de suivi (le cas échéant)

Le statut d'évaluation « En attente de l'évaluation du plan d'action corrective » est limité à neuf mois. Pour de plus amples informations, veuillez consulter la Section 5.4.9.3, "Exigences concernant le plan d'action corrective".

7.6.5. Assessment status “Waiting for follow-up” (Statut de l’évaluation « En attente de suivi »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
En attente de suivi	Votre auditeur a approuvé votre plan d’action corrective. Vous avez mis en œuvre les actions correctives.	Demandez une évaluation de suivi.	Aucune	Terminé

Le statut de l’évaluation « En attente de suivi » est limité à neuf mois. Pour de plus amples informations, veuillez consulter la Section 5.4.9.3, “Exigences concernant le plan d’action corrective”.

7.6.6. Assessment status “Finished” (Statut de l’évaluation « Terminé »)

Statut	Situation	Votre prochaine action	Notre prochaine action	Prochain statut
Terminé	Votre auditeur a mené une évaluation de suivi. Le résultat de l’évaluation ne présente aucune non-conformité. Votre auditeur nous a envoyé le rapport d’évaluation TISAX.	Publiez et partagez votre résultat d’évaluation.	Aucune	n/a

7.7. Annexe : pourquoi nous déconseillons les « pré-évaluations » et les « analyses de l’écart »

Nous déconseillons généralement de solliciter un auditeur pour qu’il réalise une « pré-évaluation » ou une « analyse de l’écart ». Dans la plupart des cas, il est préférable de commencer l’évaluation TISAX sans attendre.

Dans cette section, nous abordons les interrogations les plus fréquentes.

Envisagez-vous de demander une pré-évaluation parce que :

1. Vous craignez que votre client voie un résultat d'évaluation potentiellement défavorable ?

   Vous avez un contrôle total sur qui voit les résultats de votre évaluation. C'est vous qui décidez ce que l'auditeur télécharge sur le portail ENX. Si personne ne doit le voir, personne ne le verra (sauf l'auditeur bien évidemment).

   Par ailleurs, l'auditeur télécharge uniquement les deux premières sections du rapport d'évaluation TISAX et ne télécharge *jamais* les résultats détaillés de l'évaluation.

2. Vous pensez qu'une pré-évaluation peut vous faire économiser de l'argent ?
   - Avec une pré-évaluation, vous :
     - payez la pré-évaluation
     - pouvez payer des coûts internes pour résoudre les éventuelles non-conformités
     - payez l'évaluation TISAX complète (« évaluation initiale »)

     Même s'il n'y a *aucune* constatation, vous paierez *deux* évaluations complètes.

   - En commençant par l'évaluation TISAX, vous :
     - payez l'« évaluation initiale »
     - pouvez payer des coûts internes pour résoudre les éventuelles constatations
     - pouvez payer beaucoup moins (par rapport à l'évaluation initiale) pour ce que nous appelons l'« évaluation de suivi », au cours de laquelle l'auditeur veut uniquement savoir si vous avez résolu les non-conformités de l'évaluation initiale

     Même *avec* des constatations, vous payez uniquement une évaluation complète plus la brève évaluation de suivi.

3. Vous pensez que vous pourriez échouer à l'évaluation et que cela pourrait avoir des conséquences permanentes ?

   Vous ne pouvez pas échouer de manière permanente, car vous pouvez passer autant d'évaluations que vous le souhaitez. Si le résultat de l'évaluation ne satisfait pas vos attentes ou si vous ne parvenez pas à corriger les non-conformités à l'aide d'actions correctives au cours de la période de neuf mois requise, il vous suffit de considérer cet échec comme une pré-évaluation et de recommencer. De plus, personne n'a besoin de voir les résultats de votre première tentative. Vous partagez uniquement les résultats de l'évaluation que vous avez réussie.

Autres interrogations :

- Si le résultat de l'évaluation est meilleur que prévu, vous pouvez recevoir des labels TISAX provisoires. Vous pouvez les partager directement avec votre partenaire. Ceci est impossible avec une pré-évaluation.
- Si l'auditeur qui réalise la pré-évaluation doit également effectuer l'évaluation TISAX, il ne peux pas vous consulter. Sinon, vous devrez choisir un autre auditeur pour l'évaluation TISAX.

Si la plupart des entreprises auditées ne gagnent rien à réaliser une pré-évaluation, nous souhaitons mentionner les avantages suivants.

L'auditeur :

- peut se concentrer sur des aspects critiques lorsque vous manquez de confiance dans votre ISMS
- peut y consacrer plus de temps et approfondir les renseignements
- peut documenter les constatations différemment

Lorsque vous aurez lu les sections sur le processus d'évaluation TISAX, vous comprendrez plus facilement notre raisonnement.

7.8. Annexe : périmètres d'évaluation sur mesure

La quasi-totalité des participants TISAX choisissent le périmètre d'évaluation standard. Toutefois, dans certaines *rares* circonstances, vous pouvez être amené à choisir un périmètre d'évaluation sur mesure.

Il existe deux types de périmètres d'évaluation sur mesure :

7.8.1. Périmètre d'évaluation étendu sur mesure

Vous pouvez étendre le périmètre. Un périmètre d'évaluation étendu sur mesure contient PLUS que le périmètre d'évaluation standard. L'auditeur procédera à davantage de vérifications.

Objectif : un périmètre d'évaluation étendu sur mesure peut être pertinent si vous voulez utiliser votre évaluation TISAX à des fins internes ou en dehors de l'industrie automobile.

Labels TISAX et partage des résultats : un périmètre d'évaluation étendu sur mesure comprend toujours le périmètre d'évaluation standard. Par conséquent, un périmètre d'évaluation étendu sur mesure recevra des labels TISAX[35]. D'autres participants TISAX accepteront toutefois le résultat de l'évaluation.

Description : si le périmètre d'évaluation standard dispose d'une description prédéfinie, vous devez rédiger votre propre description du périmètre d'évaluation si vous avez besoin d'un périmètre d'évaluation étendu sur mesure.

7.8.2. Périmètre d’évaluation entièrement sur mesure

Vous pouvez définir entièrement votre périmètre.

Objectif : si certains de vos sites appartiennent à des périmètres d’évaluation différents et recourent à certains services sur un site particulier (tel qu’un centre de données), vous pouvez utiliser un périmètre d’évaluation entièrement sur mesure pour ces services. Ainsi, un auditeur TISAX peut aisément réutiliser le résultat d’évaluation correspondant au périmètre d’évaluation entièrement sur mesure du service.

Exemple : vous avez un grand nombre de sites (appartenant éventuellement à des périmètres différents) et disposez d’un département IT central sur l’un de ces sites. La définition d’un périmètre d’évaluation entièrement sur mesure pour ce seul département IT peut permettre de faciliter la réutilisation, dans les autres périmètres, du résultat d’évaluation correspondant.

Labels TISAX et partage des résultats : les périmètres d’évaluation entièrement sur mesure ne bénéficient pas de labels TISAX. Le résultat de votre évaluation est enregistré sur le portail ENX avec la date, la période de validité et l’indication de conformité ou non du résultat global de l’évaluation. Vous pourriez partager ce résultat d’évaluation. Mais si vous partagez un résultat d’évaluation sans labels TISAX, la plupart des destinataires pourraient considérer que vous avez « échoué ». Généralement, les autres participants TISAX n’acceptent pas les résultats d’évaluation basés sur un périmètre d’évaluation entièrement sur mesure.

Description : comme pour le périmètre d’évaluation étendu sur mesure, vous rédigerez votre propre description du périmètre si vous avez besoin d’un périmètre d’évaluation entièrement sur mesure.

Remarque importante :

Pour souligner la rareté des périmètres d’évaluation entièrement sur mesure, sachez que vous avez 98 % de chances que votre auditeur transforme votre périmètre d’évaluation entièrement sur mesure en un périmètre d’évaluation standard. Aucun participant n’a *jamais* choisi un périmètre d’évaluation entièrement sur mesure sans les conseils de son auditeur.

Une évaluation sur la base d’un périmètre d’évaluation entièrement sur mesure ne bénéficiera pas de labels TISAX. Ainsi, en règle générale, nous ne recommandons pas d’opter pour un périmètre d’évaluation entièrement sur mesure — en particulier parce que d’habitude, les autres participants n’acceptent pas les résultats d’évaluation basés sur un périmètre d’évaluation entièrement sur mesure.
Ne choisissez pas un périmètre d’évaluation entièrement sur mesure si vous n’avez pas la confirmation explicite que votre partenaire acceptera le résultat et a validé votre description du périmètre.

7.9. Annexe : gestion du cycle de vie des données du participant

Les sections suivantes décrivent ce que vous devez faire si un élément en lien avec vos données de participant est modifié.

7.9.1. Perte d'accès aux données du participant (portail ENX)

Si dans votre entreprise, plus personne n'a accès à votre portail ENX et par conséquent à vos données de participant, veuillez nous contacter. Nous tenterons de vous aider à accéder à nouveau aux données de participant de votre entreprise.

7.9.2. Administration des contacts

Les contacts principaux du participant de votre entreprise et tous les autres « contacts administratifs » ayant un compte sur le portail peuvent toujours se rendre sur le portail ENX et :

- ajouter de nouveaux contacts
- supprimer des contacts existants
- modifier les détails des contacts existants

7.9.2.1. Comment ajouter un nouveau contact

Pour ajouter un nouveau contact, suivez les étapes suivantes :

1. Connectez-vous sur le portail ENX.
2. Allez dans la barre de navigation principale et sélectionnez “MY TISAX” (« MON TISAX »).
3. À partir du menu déroulant, sélectionnez “ADMINISTRATORS” (« ADMINISTRATEURS »).
4. Cliquez sur le bouton “Create new TISAX Administrator” (« Créer un nouvel administrateur TISAX »).
5. Entrez les données du contact.
6. Cliquez sur le bouton “Save Contact” (« Enregistrer le contact »).
7. Allez dans le tableau et identifiez-y la ligne contenant le contact.
8. Allez au bout de la ligne du tableau du contact et cliquez sur le bouton avec la flèche vers le bas .
9. Sélectionnez “Edit TISAX Administrator” (« Modifier l'administrateur TISAX »).
10. Dans la nouvelle fenêtre (“Edit TISAX Contact” (« Modifier le contact TISAX »)), faites défiler jusqu'à la section “ENX PORTAL ACCESS” (« ACCÈS AU PORTAIL ENX »).
11. Sélectionnez “Yes” (« Oui »).
12. La section “WEB ROLES” (« RÔLES WEB ») apparaît. Cliquez sur le bouton “Add Role” (

« Ajouter un rôle »).

13. Sélectionnez le rôle que vous souhaitez attribuer (ex. “TISAX Administrator” (« Administrateur TISAX »)).
14. Cliquez sur le bouton « Ajouter le rôle ».
15. Cliquez sur le bouton « Enregistrer le contact ».

7.9.2.2. Comment supprimer un contact existant

Pour supprimer un contact existant, suivez les étapes suivantes :

1. Connectez-vous sur le portail ENX.
2. Allez dans la barre de navigation principale et sélectionnez “MY TISAX” (« MON TISAX »).
3. À partir du menu déroulant, sélectionnez “ADMINISTRATORS” (« ADMINISTRATEURS »).
4. Allez dans le tableau et identifiez-y la ligne contenant le contact.
5. Allez au bout de la ligne du tableau du contact et cliquez sur le bouton avec la flèche vers le bas .
6. Sélectionnez “Delete TISAX Administrator” (« Supprimer l’administrateur TISAX »).
7. Dans la demande de confirmation, cliquez sur le bouton “Delete” (« Supprimer »).

7.9.2.3. Comment modifier les détails d’un contact existant

Pour modifier les détails d’un contact existant, suivez les étapes suivantes :

1. Connectez-vous sur le portail ENX.
2. Allez dans la barre de navigation principale et sélectionnez “MY TISAX” (« MON TISAX »).
3. À partir du menu déroulant, sélectionnez “ADMINISTRATORS” (« ADMINISTRATEURS »).
4. Allez dans le tableau et identifiez-y la ligne contenant le contact.
5. Allez au bout de la ligne du tableau du contact et cliquez sur le bouton avec la flèche vers le bas .
6. Sélectionnez “Edit TISAX Administrator” (« Modifier l’administrateur TISAX »).
7. Modifiez les détails.
8. Cliquez sur le bouton “Save Contact” (« Enregistrer le contact »).

7.9.3. Administration des sites

Les contacts de participant principaux de votre entreprise et tous les autres « contacts administratifs » ayant un compte sur le portail peuvent toujours se rendre sur le portail ENX et demander :

- la modification du nom de l'entreprise
- la modification d'un site (déménagement)
- la modification d'un nom de rue
- l'ajout d'un nouveau site

Nous décrivons les étapes nécessaires dans les sections suivantes.

Remarque :

- Dans TISAX, la combinaison du nom d'une entreprise et d'une adresse définit un « site ».
- Chaque site possède un « ID de site » (les ID de site commencent toujours par un « L » et comptent six caractères ; exemple : L1L3XY).
- Si votre entreprise déménage de son adresse actuelle vers une nouvelle adresse, l'ancien site n'est plus un site valide.

Remarque importante :

Une fois que vous avez cliqué sur le bouton « Enregistrer le site » sur le portail ENX, vous ne pouvez plus le modifier vous-même. Vous pouvez demander des modifications dans les situations décrites ci-dessous.

7.9.3.1. Comment demander la modification du nom de votre entreprise

Votre situation :	Votre entreprise a changé de nom.
Exemple :	L'ancien nom de l'entreprise était « ACME Tires Corporation ». Le nouveau nom de l'entreprise est « ACME Corporation ».

Si vous souhaitez demander la modification du nom de votre entreprise, veuillez suivre les étapes suivantes :

1. Connectez-vous sur le portail ENX.
2. Allez dans la barre de navigation principale et sélectionnez "MY TISAX" (« MON TISAX »).
3. À partir du menu déroulant, sélectionnez "LOCATIONS" (« SITES »).
4. Allez dans le tableau et identifiez-y la ligne contenant votre site.
5. Allez au bout de la ligne du tableau de votre site et cliquez sur le bouton avec la flèche vers le bas .
6. Sélectionnez "Request Change" (« Demande de changement »).
7. Dans la nouvelle fenêtre ("Request Change" (« Demande de changement »)), rendez-vous

dans le champ du formulaire “Subject of the change” (« Objet du changement »), ouvrez le menu déroulant et sélectionnez “Company Name” (« Nom de l’entreprise »).

8. Remplissez le formulaire.
9. Envoyez le formulaire.

Nous étudierons votre demande, accepterons probablement de modifier le nom de l’entreprise, puis nous vous en informerons lorsque cela aura été fait.

7.9.3.2. Comment demander la modification d’un site

Votre situation :	Votre entreprise a déménagé.
Exemple :	L’ancienne adresse était : « ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Frankfurt, Allemagne ». La nouvelle adresse est : « ACME Corporation, Behrenstraße 35, 10117 Berlin, Allemagne ».

Remarque importante :

Si une autorité publique a modifié le nom de la rue de votre site, veuillez consulter la Section 7.9.3.3, “Comment demander la modification d’un nom de rue” pour en savoir plus.

Si l’un de vos sites a déménagé à une nouvelle adresse, veuillez suivre les étapes suivantes :

1. Créer un nouveau site :
   a. Connectez-vous sur le portail ENX.
   b. Allez dans la barre de navigation principale et sélectionnez “MY TISAX” (« MON TISAX »).
   c. À partir du menu déroulant, sélectionnez “Locations” (« Sites »).
   d. Cliquez sur le bouton “Create TISAX Location” (« Créer un site TISAX »).
   e. Dans la nouvelle fenêtre (“CREATE TISAX LOCATION” (« CRÉER UN SITE TISAX »)), remplissez le formulaire en indiquant les détails du nouveau site.
   f. Cliquez sur le bouton “Save Location” (« Enregistrer le site »).
2. Rappelez-vous le “Location ID” (« ID du site ») du nouveau site créé. L’« ID du site » apparaît dans la première colonne du tableau “MY LOCATIONS” (« MES SITES »). Votre auditeur a besoin de l’« ID du site » pour mettre à jour le périmètre d’évaluation sur le portail ENX.
3. Informez votre auditeur du changement d’adresse (fournissez-lui l’« ID du site » de l’ancien site ainsi que celui du nouveau site).
   Vous avez terminé l’évaluation ?

a. Si la réponse est NON, vous n'avez rien d'autre à faire concernant la modification du site.

b. Si la réponse est OUI, vous devez demander une « évaluation d'extension du périmètre » (“scope extension assessment”) à votre auditeur. Pour de plus amples informations, veuillez consulter la Section 7.10, “Annexe : évaluation d'extension du périmètre”.

Votre auditeur examinera votre demande et mettra à jour votre périmètre d'évaluation sur le portail ENX.

Remarque :

Un auditeur ne peut modifier votre périmètre d'évaluation que si vous lui avez déjà commandé l'évaluation.

7.9.3.3. Comment demander la modification d'un nom de rue

Votre situation :	Le nom de la rue de votre site a été changé. Votre entreprise occupe toujours le même site physique.
Exemple :	L'ancienne adresse était : « ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Frankfurt, Allemagne ». La nouvelle adresse est : « ACME Corporation, Behrenstraße 97-99, 60325 Frankfurt, Allemagne ».

Si une autorité publique a modifié le nom de la rue de votre site, veuillez suivre les étapes suivantes :

1. Connectez-vous sur le portail ENX.
2. Allez dans la barre de navigation principale et sélectionnez “MY TISAX” (« MON TISAX »).
3. À partir du menu déroulant, sélectionnez “Locations” (« Sites »).
4. Allez dans le tableau et identifiez-y la ligne contenant votre site.
5. Allez au bout de la ligne du tableau de votre site et cliquez sur le bouton avec la flèche vers le bas .
6. Sélectionnez “Request Change” (« Demande de changement »).
7. Dans la nouvelle fenêtre (“Request Change” (« Demande de changement »)), rendez-vous dans le champ du formulaire “Subject of the change” (« Objet du changement »), ouvrez le menu déroulant et sélectionnez “Address” (« Adresse »).
8. Remplissez le formulaire.
9. Envoyez le formulaire.

Nous étudierons votre demande, accepterons probablement de modifier le nom de la rue puis nous vous en informerons lorsque cela aura été fait.

Remarque importante :

Ces étapes s'appliquent uniquement lorsque votre entreprise occupe toujours le même site physique, mais qu'une autorité publique a modifié le nom de la rue.
Si vous avez déménagé dans un nouveau site, veuillez consulter la Section 7.9.3.2, "Comment demander la modification d'un site" pour en savoir plus.

7.9.3.4. Comment ajouter un site supplémentaire

Si vous inaugurez un site supplémentaire durant la période de validité de vos labels TISAX actuels, vous pouvez demander une « évaluation d'extension du périmètre » (🇬🇧 "scope extension assessment") à votre auditeur.

Pour de plus amples informations, veuillez consulter la Section 7.10, "Annexe : évaluation d'extension du périmètre".

7.10. Annexe : évaluation d'extension du périmètre

Outre les types d'évaluation standard décrits dans la Section 5.4.3, "Types d'évaluation TISAX", il existe un autre type d'évaluation spécial : l'« évaluation d'extension du périmètre » (🇬🇧 "scope extension assessment").

Vous pouvez étendre le périmètre d'une évaluation TISAX existante pour ajouter un ou plusieurs :

- objectifs d'évaluation, ou
- sites.

Vous ne pouvez pas sélectionner un autre auditeur pour mener une « évaluation d'extension du périmètre ». L'évaluation est similaire aux types d'évaluation standard. Toutefois, il est probable que votre auditeur envisagera de réutiliser les résultats applicables des précédentes évaluations.

Une fois que l'évaluation d'extension du périmètre sera terminée sans que des non-conformités soient identifiées, votre auditeur :

- mettra à jour votre périmètre d'évaluation sur le portail ENX.
- publiera un rapport d'évaluation d'extension du périmètre.

Une évaluation d'extension du périmètre ne prolonge pas la période de validité initiale de vos labels TISAX actuels.

Remarque :

> Si vous demandez une évaluation d'extension du périmètre suite à un déménagement ou à l'ajout d'un site supplémentaire, vous devez créer le nouveau site dans le portail ENX. Veuillez fournir l'« extrait de site »(« Location Excerpt ») ou au moins l'« ID de site » à votre auditeur.
> Chaque site possède un « ID de site » (les ID de site commencent toujours par un « L » et comptent six caractères ; exemple : L1L3XY). Votre auditeur a besoin de l'ID du site pour mettre à jour le résultat de votre évaluation sur le portail ENX.

7.11. Annexe : gestion du cycle de vie de l'ISA

Un groupe de travail ENX est chargé de maintenir l'ISA.

Les faits suivants peuvent vous intéresser :

- La VDA publie officiellement de nouvelles versions.
- L'auditeur utilise la version de l'ISA qui est valide au moment où vous *commandez* votre évaluation initiale.
- D'un commun accord, vous pouvez utiliser une nouvelle version de l'ISA si elle est publiée entre la commande et le début de l'évaluation initiale.
- Les dates de publication de chaque version de l'ISA sont indiquées dans la feuille Excel « Cover ».
  - Exemple :
    Version : 5.0 | Révision 4 | 16/04/2021

7.12. Annexe : documents utiles

La présente section énumère les documents que nous jugeons utiles.

- Livre blanc « Harmonization of classification levels » (« Harmonisation des niveaux de classification »)

  « Ce libre blanc décrit la proposition du groupe de travail sur la sécurité de l'information pour déterminer un programme centré sur l'objectif de protection de la confidentialité. Cela signifie qu'une information n'est accessible qu'aux personnes, organisations et processus autorisés. De plus, les objectifs de protection tels que la disponibilité, l'intégrité et la fiabilité ne font pas l'objet de ce livre blanc. »

  Éditeur : Verband der Automobilindustrie e.V. (« Association allemande de l'industrie automobile »)

  Langues disponibles : anglais, allemand

https://www.vda.de/en/news/publications/publication/harmonization-of-classification-levels
https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--harmonisierung-der-klassifizierungsstufen-

- Livre blanc « Information Security Risk Management » (« Gestion du risque en matière de sécurité de l'information »)

  « L'objectif de ce livre blanc est d'informer les entreprises actives dans l'industrie automobile sur la gestion du risque lié à la sécurité de l'information et de leur permettre d'instaurer une gestion efficace du risque en la matière. Il vise à aider les organisations à préparer ou mener une évaluation TISAX pour répondre aux exigences de la VDA associées à la question de contrôle 1.4.1 de l'ISA. Les informations qu'il contient doivent être considérées comme des recommandations de mise en œuvre, et non comme des exigences obligatoires. »

  Éditeur : Verband der Automobilindustrie e.V. (« Association allemande de l'industrie automobile »)

  Langues disponibles : anglais, allemand

  https://www.vda.de/en/news/publications/publication/white-paper--information-security-risk-management-
  https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--risikomanagement-in-der-informationssicherheit-

7.13. Annexe : gestion des réclamations

7.13.1. Causes de réclamation

Notre gestion des réclamations distingue les deux domaines suivants :

1. ENX Association — l'organisation responsable de TISAX
2. Auditeurs — les organisations qui réalisent les évaluations TISAX

7.13.1.1. Réclamations concernant ENX Association

Pour les réclamations concernant ENX Association, veuillez contacter notre « responsable TISAX de permanence » (voir les coordonnées ci-dessous).

7.13.1.2. Réclamations concernant les auditeurs

Dans un premier temps, vous devez essayer de résoudre le problème directement avec l'auditeur.

Vous pouvez ensuite contacter la personne responsable de TISAX chez l'auditeur.

Votre interlocuteur suivant sera la personne responsable de la gestion de la qualité chez l'auditeur.

Si le problème n'est toujours pas résolu, vous pouvez contacter notre « responsable TISAX de permanence » (voir les coordonnées ci-dessous).

Il existe des options au-delà du « responsable TISAX de permanence ». Le cas échéant, vous devez vous adresser au directeur général d'ENX Association.

La VDA n'intervient pas dans la gestion des réclamations.

Remarque :

L'auditeur doit vous informer de votre droit à faire des réclamations lors de la réunion de lancement. S'il ne le fait pas, cela peut constituer un motif de réclamation.

7.13.1.3. Conditions pour formuler une réclamation

Si vous voulez nous impliquer, nous aurons besoin des informations suivantes :

- Qui a des réclamations ?
  - Nom de l'entreprise
  - ID de participant TISAX
  - Coordonnées (nom, adresse e-mail, numéro de téléphone)
- De quelle évaluation s'agit-il ?
  - ID d'évaluation
  - Si l'évaluation n'est pas encore inscrite sur le portail ENX : ID de périmètre
- Qui est l'auditeur ?
  - Nom de la société de l'auditeur
  - Nom du/des auditeur(s)
- Sur quoi portent vos réclamations ?
  1. Réclamation générale sur la performance de l'auditeur
  2. Réclamation sur l'approche de l'auditeur
  3. Réclamation sur l'évaluation concernant son contenu
- Pour les réclamations concernant le contenu de l'évaluation : quelle constatation contestez-vous ?
  - Contrôle (ex. 1.6.1 "Dans quelle mesure les événements de sécurité de l'information sont-ils traités ?")

- Constatation (texte complet)
- Objection contre :
  - Interprétation du contrôle
  - Vérification du contenu (preuve disponible évaluée de manière incorrecte)
  - Évaluation du risque (adéquation non prise en compte)
- Raisons pour lesquelles vous évaluez les choses différemment

7.13.2. Contact pour les réclamations

Veuillez contacter le « responsable TISAX de permanence » :

Par e-mail :	tisax-complaints@enx.com
Ou par téléphone :	+49 69 9866927-79

Vous pouvez le joindre aux heures ouvrables normales en Allemagne (UTC+01:00).

Il parle anglais et allemand.

8. Historique du document

Version 2.7

- Ajout de quatre langues supplémentaires (japonais, portugais brésilien, italien, coréen)
- Ajout d'un commutateur de langues pour les versions HTML (dans l'angle supérieur droit)
- Amélioration de la mise en page des versions PDF
- Mise à jour de différentes sections avec les deux nouveaux objectifs d'évaluation relatifs à la confidentialité
- Mise à jour de la section « Liste des objectifs de l'évaluation » (correction de la formulation de l'objectif d'évaluation « Special data » ; ajout de la note relative à la transition des labels)
- Correction de fautes d'orthographe

Version 2.6

- Note générale concernant les objectifs d'évaluation et les labels que nous avons ajoutés dans cette version : dans les versions précédentes, les objectifs d'évaluation et les labels possédaient un « nom officiel » long et un « nom court » (exemple : « Traitement des informations présentant des besoins de protection importants » et « Info high »). Dans la mesure où la plupart des personnes utilisaient uniquement le nom court, la forme courte est devenue le « nom officiel ». L'ancienne version longue du nom correspond désormais à la « Description ». Par ailleurs, nous utilisons *uniquement* le nom officiel anglais sur le portail ENX et dans toutes les traductions du manuel du participant TISAX.
- Mise à jour de la section « Liste des objectifs de l'évaluation » avec les deux objectifs d'évaluation « haute disponibilité » et « très haute disponibilité » et suppression de l'« Illustration 6. Objectifs d'évaluation TISAX (tableau, versions longue et courte) »
- Mise à jour de la section « Objectifs d'évaluation et ISA » pour refléter le fait que seul un sous-ensemble du catalogue de critères « Sécurité de l'information » s'applique aux deux objectifs d'évaluation « haute disponibilité » et « très haute disponibilité »
- Suppression de la section « Les objectifs d'évaluation et leurs dépendances »
- Mise à jour de la section « Sélection de l'objectif d'évaluation » avec les deux objectifs d'évaluation « haute disponibilité » et « très haute disponibilité »
- Mise à jour de la section « Besoins de protection et niveaux d'évaluation » avec les deux objectifs d'évaluation « haute disponibilité » et « très haute disponibilité » et suppression du « Tableau 5. Correspondance entre catalogues de critères ISA, besoins de protection et objectifs d'évaluation TISAX »
- Mise à jour de la section « Catalogues de critères » avec les deux objectifs d'évaluation « haute disponibilité » et « très haute disponibilité »

- Mise à jour de la section « Exigences » pour refléter le fait que seul un sous-ensemble du catalogue de critères « Sécurité de l'information » s'applique aux deux objectifs d'évaluation « haute disponibilité » et « très haute disponibilité »
- Mise à jour de la section « Hiérarchie des labels TISAX » pour refléter le fait que la hiérarchie ne concerne plus que quelques cas et suppression de l'« Illustration 36. Objectifs d'évaluation et labels TISAX (dépendances et hiérarchie) »
- Mise à jour de la section « Annexe : documents utiles » pour refléter la modification des liens
- Plusieurs précisions mineures et petites corrections
- Correction de fautes d'orthographe

Version 2.5.1

- Réparation des liens rompus.

Version 2.5

- Ajout de la section « Administration des sites ».
- Mise à jour de la section « Annexe : documents utiles » pour refléter la modification des liens

Version 2.4

- Affirmation inexacte concernant la durée du processus d'évaluation TISAX supprimée de la Section 3.1, “Aperçu”
- « Rapport TISAX » renommé « rapport d'évaluation TISAX »
- Mise à jour de la note concernant les différences entre ISO 27001 et TISAX
- Mise à jour de la section « Description du périmètre » ; section sur le périmètre d'évaluation sur mesure déplacée en annexe
- Mise à jour de la « Description du périmètre d'évaluation standard » version 2.0
- Mise à jour de la section « Publication et partage » avec une remarque sur le partage du statut de l'évaluation
- Mise à jour de la section « Besoins de protection et niveaux d'évaluation » avec du contenu sur le « niveau d'évaluation 2.5 », la « méthode d'évaluation à distance par vidéo », les différences entre AL 2 et AL 3 et la différence entre test de plausibilité et vérification
- Mise à jour du lien vers le début du processus d'inscription
- Mise à jour de la section « Compte sur le portail » pour refléter la modification du processus d'invitation

- Modification des liens de téléchargement du document ISA (désormais également disponible sur enx.com)
- Mise à jour de la section « Évaluation des offres » avec une base pour l'estimation des coûts
- Ajout de la section « Réunion de lancement » (avec du contenu pris de la section « La première réunion d'ouverture officielle »)
- Mise à jour de la section « À propos de la conformité » avec un nouveau tableau sur les quatre types de constatation
- Mise à jour de la section « Évaluation initiale » avec une remarque sur les contraintes temporelles
- Mise à jour de la section « Rapport d'évaluation TISAX » avec une remarque sur le plan d'action corrective proactif
- Mise à jour de la section « Préparation du plan d'action corrective » avec les exigences de « constatation » et de « cause profonde » et une remarque sur les modèles de plan d'action corrective
- Mise à jour de la section « Évaluation du plan d'action corrective » avec une remarque sur l'e-mail comme seul mode de communication
- Section « Conditions préalables à une évaluation du plan d'action corrective » renommée « Raisons d'une évaluation du plan d'action corrective » et ajout de deux raisons
- Mise à jour de la section « Labels TISAX provisoires » avec des exemples et des précisions concernant la période de validité
- Section « Rapport TISAX » renommée « Rapport d'évaluation TISAX »
- Mise à jour de la section « Renouvellement des labels TISAX » avec une remarque concernant la réutilisation des enregistrements de sites sur le portail ENX
- Ajout de la section « Annexe : pourquoi nous déconseillons les "pré-évaluations" et les "analyses de l'écart" »
- Ajout de la section « Annexe : périmètres d'évaluation sur mesure » (« Périmètre d'évaluation étendu » et « Périmètre d'évaluation restreint » remplacés par « Périmètre d'évaluation étendu » et « Périmètre d'évaluation entièrement sur mesure »)
- Mise à jour de la section « Annexe : évaluation d'extension du périmètre » avec des raisons et une remarque concernant l'ajout des enregistrements de sites sur le compte du participant sur le portail ENX
- Mise à jour de la section « Annexe : gestion du cycle de vie de l'ISA » pour refléter la situation actuelle
- Mise à jour de la section « Annexe : documents utiles » pour refléter la modification des liens
- Ajout de la section « Annexe : gestion des réclamations »
- Les numéros de téléphone sont désormais cliquables

- Plusieurs précisions mineures et petites corrections
- Correction de fautes d'orthographe
- Remarque pour les auditeurs : cette mise à jour s'appuie sur le document ENX ID 612 version 2.1

Version 2.3

- Reformulation du sous-titre
- Changement de Word/PDF en HTML comme format primaire pour le manuel
- Autres traductions disponibles (chinois et français, cf. le point suivant)
- Ajout de la section « Le manuel du participant TISAX dans d'autres langues et formats »
- Tous les liens vers la page d'accueil d'ENX ont été modifiés de "https://portal.enx.com" en "https://enx.com" (les anciens liens fonctionnent toujours)
- « VDA ISA » devient « ISA »
- Mise à jour de la section Section 5.2, "Auto-évaluation basée sur l'ISA" pour refléter les modifications introduites dans la version 5 de l'ISA
- Les lignes de tous les tableaux énumérant les objectifs d'évaluation ont été réorganisées pour cadrer avec le nouvel ordre des catalogues de critères dans l'ISA 5
- Les illustrations énumérant les objectifs d'évaluation ont été mises à jour pour cadrer avec le nouvel ordre des catalogues de critères dans l'ISA 5
- Mise à jour de la section « Adaptation du périmètre » (illustration 6, faute de frappe corrigée, mise à jour des objectifs d'évaluation)
- Mise à jour de la section « Frais » avec des informations concernant les paiements par carte de crédit
- Mise à jour de la section « Diagramme du processus d'évaluation TISAX » (illustration 34, suppression de la référence aux fournisseurs de services gérés)
- Mise à jour de la section « Annexe : documents utiles » (ajout du livre blanc « Gestion du risque en matière de sécurité de l'information »)

Version 2.2.1

- Correction de fautes d'orthographe

Version 2.2

- Résolution du problème d'impression de la couverture

- Modification de tous les liens vers notre page d'accueil et les téléchargements
- Désormais, nous parlons aussi l'italien
- Extension de la section « Périmètre d'évaluation sur mesure »
- Mise à jour de la section « Sites du périmètre
- Suppression des objectifs d'évaluation « Lien avec des tiers » ; mise à jour des illustrations 7, 9 et 38 ; mise à jour des tableaux 4, 5, 6 et 8
- Formulation de l'anglais « *with* assessment level » (avec niveau d'évaluation) modifiée en « *in* assessment level » (correspondant au niveau d'évaluation)
- Suppression de la référence à la « liste d'activation TISAX » dans la section « Besoins de protection et niveaux d'évaluation »
  (plus applicable)
- Ajout de la section « Objectifs d'évaluation et vos propres fournisseurs »
- Mise à jour de la section « Contact de participant » avec des informations concernant les adresses e-mail de groupe et l'invitation des contacts à gérer les données de participant sur le portail ENX
- Mise à jour de la section « Inscription du périmètre d'évaluation » avec des informations sur les modifications apportées au périmètre d'évaluation
- Mise à jour de la section « Informations de statut » (illustration 12)
- Mise à jour de la section « Traitement du résultat d'auto-évaluation » avec des informations concernant l'aide externe apportée par des tiers
- Mise à jour de la section « Couverture » avec un lien vers la matrice de couverture des auditeurs
- Mise à jour de la section « Demande d'offres »
- Mise à jour de la section « Évaluation des offres » avec des informations concernant les « pré-évaluations »
- Mise à jour de la section « Renouvellement des labels TISAX » avec des informations sur la nécessité d'enregistrer un nouveau périmètre
- Mise à jour de diverses sous-sections de la section « Échange (étape 3) » pour refléter les changements sur le portail ENX
- Mise à jour de la section « Partager le résultat de votre évaluation avec un partenaire particulier » avec une recommandation concernant le niveau de partage et une remarque sur le traitement automatique des résultats d'évaluation partagés
- Ajout de la section « Partager le résultat de votre évaluation en dehors de TISAX »
- Ajout de la section « Gestion du cycle de vie de l'ISA »
- Mise à jour de la section « Annexe : statut du périmètre d'évaluation » (nouveau statut « En attente de votre commande », statut « En attente d'approbation » renommé « En attente

d’approbation ENX », statut « Approuvé » renommé « En attente de votre paiement », illustration 40).

- Mise à jour de la section « Annexe : exemple d’e-mail de confirmation »
- Mise à jour de la section « Annexe : exemple d’extrait de périmètre TISAX »
- Mise à jour de la section « Annexe : statut d’évaluation » (nouveau statut « Évaluation initiale en cours », statut « En attente d’évaluation de suivi » renommé « En attente de suivi », illustration 41).
- Suppression de la section « Annexe : évaluations antérieures de Volkswagen » (et des références à celle-ci) (plus de pertinence)

Version 2.1.2

- Limite formelle pour la « distance » entre la « note de votre résultat » et la « note maximale de résultat » corrigée de 25 % à 30 %

Version 2.1.1

- Correction de fautes d’orthographe

Version 2.1

- Suppression de la section « Fournisseurs de services gérés »
- Nouveaux objectifs d’évaluation/labels TISAX (labels de protection des données conformes au RGPD ; quatre labels de prototypes au lieu de deux ; « niveaux de protection » renommés « besoins de protection » ; mise à jour des conseils en matière de sélection)
- Mises à jour en raison de changements dans l’ISA (version 4.0 à 4.1)
- Référence au nouveau document « TISAX Simplified Group Assessment » (ajout au présent manuel)
- Ajout de suggestions concernant l’attribution de noms de sites et de noms de périmètres
- « Registration fee » (frais d’inscription) renommé « fee » (frais)
- Ajout d’une recommandation concernant les remplaçants des contacts
- Suppression de la sélection du modèle de tarification

Retour au début.

[1] Vous devriez envisager de réaliser le processus TISAX de manière préventive. Certaines entreprises procèdent de la sorte pour être mieux préparées. Le fait d'avoir déjà passé l'évaluation TISAX peut impliquer une période d'initiation plus courte et dès lors vous donner une longueur d'avance sur vos concurrents qui n'ont pas encore réalisé cette évaluation.

[2] Les « labels TISAX » désignent un concept visant à synthétiser le résultat de votre évaluation et constituent l'output du processus TISAX. Veuillez consulter la Section 5.4.14, "Labels TISAX" pour obtenir davantage de détails à ce sujet.

[3] Vous ne devez effectuer la plupart des étapes d'inscription qu'une fois lorsque vous débutez le processus en tant que participant TISAX. Si vous renouvelez le résultat de votre évaluation, vous devez uniquement mettre à jour et confirmer vos données d'inscription.

[4] Nous publierons les changements apportés à nos CG sur le portail ENX et en aviserons les contacts inscrits.

[5] Cela vaut aussi pour l'ensemble des autres accords supplémentaires (p. ex. : les codes de conduite).

[6] Veuillez noter qu'actuellement votre partenaire n'est pas informé automatiquement des nouvelles autorisations. Peut-être souhaiterez-vous informer votre partenaire une fois que le résultat de votre évaluation sera disponible pour lui.

[7] Si vous souhaitez figurer sur cette liste, veuillez nous contacter.

[8] Les données probantes désignent tout élément qui appuie votre affirmation selon laquelle vous répondez à une certaine exigence. Les données probantes sont généralement des documents. Les documents internes vous serviront certainement de données probantes.

[9] Les entretiens pour les évaluations de niveau d'évaluation 2 sont habituellement menés par conférence sur le Web. À votre demande, des entrevues peuvent avoir lieu sur site

[10] Le minimum théorique pour des évaluations de groupe simplifiées est de trois sites.

[11] Si vous savez déjà que vous devrez améliorer votre système de gestion de la sécurité de l'information, le minimum recommandé est d'au moins douze sites.

[12] Pour éviter tout risque de confusion entre les chiffres et les lettres (comme 8 et B), certaines lettres ne sont pas autorisées pour les ID de participant. Néanmoins, certains anciens ID de participant peuvent contenir la lettre « G ».

[13] Ces catalogues sont également appelés « modules » dans l'ISA

[14] Vous trouverez la fonction Excel sous-jacente dans le ruban « Données », section « Exposer »

[15] Disposez-vous pour votre entreprise d'auditeurs responsables d'évaluations similaires (comme pour la norme ISO 27001) et qui souhaitent également mener des évaluations TISAX ? Dans ce cas, partagez le présent manuel avec eux et dites-leur de nous contacter pour savoir comment devenir un auditeur TISAX

[16] Les auditeurs qui ne sont pas inclus dans notre listing ne sont pas autorisés à mener des évaluations TISAX.

[17] Si vous mettez un terme au processus d'évaluation, vous ne recevrez pas de labels TISAX.

[18] Il existe en fait un quatrième type : l'« évaluation d'extension du périmètre » (Scope extension assessment). Il s'agit d'un cas spécial décrit en détail en annexe dans la Section 7.10, "Annexe : évaluation d'extension du périmètre".

[19] La réunion *d'ouverture* officielle ne sera décrite en détail que pour l'évaluation initiale. Pour les autres évaluations TISAX, votre auditeur planifiera et organisera ces réunions.

[20] Certains auditeurs peuvent utiliser le terme de « réunion de lancement » au lieu de « réunion d'ouverture officielle ».

[21] La réunion de *clôture* officielle ne sera décrite en détail que pour l'évaluation initiale. Votre auditeur planifiera et organisera cette réunion pour les autres évaluations TISAX.

[22] Si un litige ne peut être résolu, vous pouvez faire remonter le problème. Pour de plus amples informations, veuillez consulter la Section 7.13, "Annexe : gestion des réclamations".

[23] Pour de plus amples informations sur les méthodes et l'intensité des audits, veuillez consulter la Section 4.3.3.5, "Besoins de protection et niveaux d'évaluation".

[24] Si un litige ne peut être résolu, vous pouvez faire remonter le problème. Veuillez nous contacter pour plus de détails.

[25] Veuillez noter que le résultat global de votre évaluation peut toujours être « non conforme majeur », même si vous avez défini des actions correctives appropriées. C'est le cas si vos mesures ne peuvent pas prendre effet/ne prennent pas effet immédiatement.

[26] Cela s'applique bien entendu uniquement à l'évaluation initiale qui a identifié des non-conformités. Vous n'avez pas besoin d'une évaluation de suivi pour une évaluation initiale présentant un résultat d'évaluation « conforme ».

[27] En théorie, il peut s'agir de neuf mois après la conclusion de l'évaluation initiale.

[28] Il existe en fait un quatrième type : le « rapport d'évaluation d'extension du périmètre ». Il s'agit d'un cas spécial décrit en détail à la Section 7.10, "Annexe : évaluation d'extension du périmètre".

[29] Le « rapport d'évaluation TISAX » est basé sur un modèle que tous les auditeurs TISAX sont tenus d'utiliser.

[30] Le terme de « renouvellement » peut prêter à confusion. Pour conserver un label TISAX plus de trois ans, vous devez repasser le processus TISAX. Cela commence par l'inscription d'un nouveau périmètre d'évaluation.

[31] Nous ne maintenons pas de liste « publique TISAX » des ID de participant. En effet, nous voulons éviter un partage accidentel fondé sur des noms d'entreprise similaires ou d'autres « erreurs humaines ». Par conséquent, vous devez toujours obtenir l'ID de participant de votre partenaire en le contactant directement.

[32] Votre partenaire doit se connecter sur le portail et rechercher activement le résultat partagé de votre évaluation. Votre partenaire ne reçoit pas de notification automatique concernant de nouveaux résultats d'évaluation partagés.

[33] La règle est définie dans les « Conditions générales de participation TISAX » (https://enx.com/tisaxgtcen.pdf).

[34] Au moment où le statut de votre périmètre d'évaluation est « En attente de votre paiement » ou « Inscrit », les « informations relatives à l'évaluation » comprennent le(s) site(s) du périmètre d'évaluation, le statut du périmètre d'évaluation et l'/les objectif(s) de l'évaluation. Elles n'incluent pas les résultats d'évaluation ou les labels TISAX.

[35] Les « labels TISAX » désignent un concept visant à synthétiser le résultat de votre évaluation et constituent l'output du processus TISAX. Veuillez consulter la Section 5.4.14, "Labels TISAX" pour obtenir davantage de détails à ce sujet.