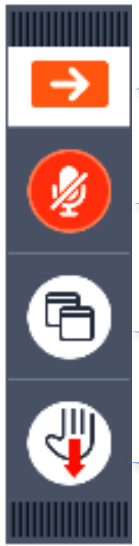
TISAX démystifié : Ce que vous devez savoir et comment vous y préparer

28 septembre 2023

Quelques infos pratiques sur l'outil GoToWebinar

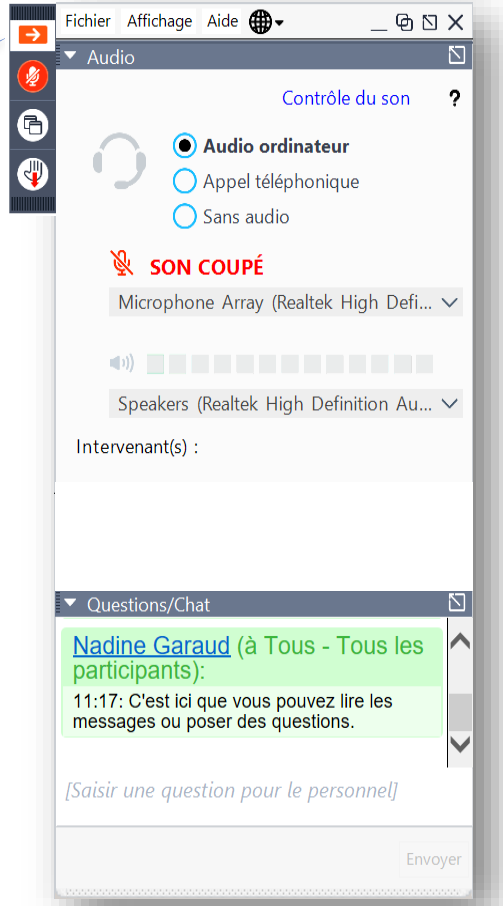


Ouvrir le panneau AUDIO, et accès l'espace QUESTIONS

Activer le MICRO pour parler (si autorisé par l'organisateur)

Mode FENETRE / PLEIN ECRAN

Demander la PAROLE



GALIA
Copyright © 29/09/2023

Agenda

- Introduction
- Qu’est-ce que TISAX® ?
- Les défis à relever
- TISAX® processus d'audit
- Quelle valeur apporte TISAX® ?
- Questions / réponses

Intervenantes

Nadine GARAUD
B2B & IS/IT Director
GALIA

Stéphanie HANTAT
Auditrice cybersécurité & TISAX
DNV Business assurance

Sarah VIRTUOSE
Directrice commerciale France
DNV Business assurance

Copyright © 29/09/2023

GALIA : Missions et domaines d’expertises

GALIA, au service de l'Industrie Automobile

- **GALIA** développe des **standards de processus et de communication** pour les constructeurs, équipementiers et sociétés prestataires du secteur automobile.
- GALIA est également organisme de **formation** (EDI, facture électronique, logistique…)
- GALIA représente la filière automobile Française au sein d’organisations européennes comme Odette et l’Association ENX.

GALIA
Copyright © 29/09/2023

Introduction - Contexte

La sécurité de l'information : au cœur des préoccupations de la Supply Chain automobile

- A l'ère de la **digitalisation massive**, la **cybercriminalité** est en augmentation exponentielle !
- Une Supply Chain **vaste et complexe** intégrant des acteurs de **toute taille**
- Une **maturité** cybersécurité variable
- Un risque accru également au niveau des **véhicules** de plus en plus **connectés**
- Des **règlementations** cybersécurité nationales et européennes à prendre en compte (Norme UNECE R155, Norme ISO/SAE 21434, Directive NIS2, Loi LOPMI, RGPD…)

GALIA
Copyright © 29/09/2023

Introduction - Objectifs

La filière automobile s'organise pour faire face aux enjeux liés à la sécurité de l'information

- Créer et maintenir un **niveau exigent de sécurité de l'information** parmi les entreprises de la filière automobile

- Un processus **commun** et **standard** pour accroître la robustesse et la résilience mondiale de notre filière

- Une **reconnaissance mutuelle** et des résultats comparables

GALIA
Copyright © 29/09/2023

Introduction – TISAX

TISAX (Trusted Information Security Assessment Exchange)

- Gouverné par l'association ENX
- Le label TISAX est le principal **standard international** d'audit
- Permet **d'évaluer le niveau de sécurité** de l'information des entreprises de la filière automobile
- En couvrant la sécurité de l'information et la cybersécurité des entreprises, TISAX :
  - **Protège** la confidentialité, l'intégrité et la disponibilité des informations de vos partenaires commerciaux
  - **Protège** vos partenaires commerciaux de l'impact des cyber-attaques sur votre entreprise

GALIA
Copyright © 29/09/2023

TISAX en termes de déploiement

ENX | TISAX

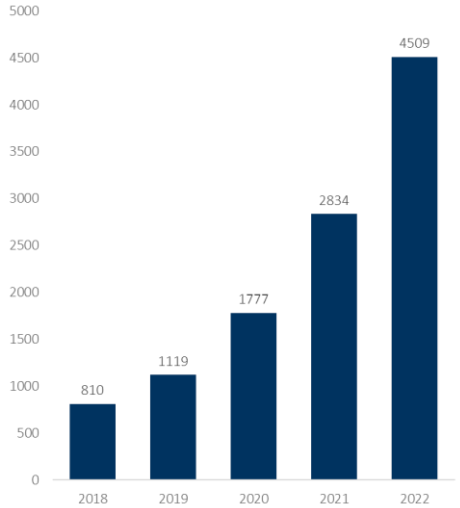
>10.000 **locations** in **77 countries** with valid labels

>1.000 **Improvements** every month

Strong growth of number of audits

International recognition

Nombre de sites évalués par an



TISAX Audit Providers (TISAX AP)

Operational: bsi. | Bureau Veritas | CIS | DEKRA | DNV | Deloitte. | dqs | EY | KPMG | Operational Services | pwc | SGS | TÜV NORD | TÜVRheinland | TÜV SÜD

Initialization Process: ssc | afnor | intertek | schellman | New in 2023

GALIA
Copyright © 29/09/2023

DNV

DNV ©

Qu’est-ce que TISAX® ?

Sécurité de l’information = Sécurité informatique ?

☐ Oui

☐ Non

Qu’est-ce que TISAX ?

TISAX est une labellisation portée par l’ENX

Permet d’évaluer le système de management de l’information des entreprises selon des niveaux de maturité prédéfinis

Basée sur le référentiel (catalogue) ISA créé par le VDA

Les principaux objectifs du label

INDUSTRIE

Création d'un niveau de sécurité des informations commun pour l'industrie automobile

QUALITÉ

Assurer la comparabilité et la qualité des tests/évaluations

VÉRIFICATION

Assurer une reconnaissance commune de l'audit et de ses résultats

RÉSULTATS

Échange de bonnes pratiques et d'expériences

COÛTS

Réduire les coûts, les efforts et la complexité

PARTAGER

L'audité peut choisir librement avec qui et avec quel niveau de détail il partage ses résultats

A quoi se rapporte TISAX ?

Pour les **informations confiées par les OEM** (Original Equipment Manufacturer) aux différents acteurs de la filière sur l'ensemble de la supply chain

3 thématiques :

1 obligatoire et 2 dépendantes de l'activité des acteurs de la filière

Couvre **7** domaines d'audit communs
+ 1 pour les prototypes
+ 1 pour les données personnelles

TISAX® exigences communes

Management de la sécurité de l'information

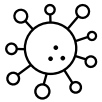
L'entreprise doit avoir mis en place un système de management de la sécurité de l'information (SMSI) conforme aux exigences de la norme internationale ISO/IEC 27001.

RH

L'entreprise doit avoir une bonne maîtrise de ses ressources humaines et fournir une formation suffisante au personnel et aux parties prenantes.

Sécurité physique et continuité des activités

L'entreprise doit mettre en place des mesures pour protéger ses actifs physiques, tels que les bâtiments, les équipements et les documents, contre l'accès non autorisé, le vol et les dommages. L'entreprise doit disposer de plans pour assurer la continuité de ses activités en cas d'incident de sécurité ou d'autre perturbation.



Gestion des incidents

L'entreprise doit avoir mis en place des procédures pour détecter, signaler et réagir aux incidents et aux violations de la sécurité.

Contrôles d'accès

L'entreprise doit mettre en place des contrôles pour s'assurer que seules les personnes autorisées ont accès à ses systèmes d'information et à ses données.

Gestion des fournisseurs et prestataires

L'entreprise doit disposer de processus pour gérer la sécurité de ses fournisseurs et prestataires de services tiers.

Conformité juridique et protection des données

L'entreprise doit avoir mis en place des mesures pour protéger les données personnelles conformément au GDPR et aux autres lois applicables en matière de protection des données.

DNV ©

TISAX concerne…

- ☐ Un site
- ☐ Une activité

Différences entre TISAX et ISO/IEC 27001

	ISO/IEC 27001	TISAX
Exigences spécifiques à l'industrie	**Générique** qui peut être appliquée à n'importe quel secteur	**Spécifique** qui comprend des exigences spécifiques à l'industrie
Évaluation et certification	Exige une **certification** pour 3 ans par un organisme de certification accrédité avec une **visite annuelle**	Exige une **évaluation** par un prestataire accrédité par ENX réalisé tous les **3 ans**
Périmètre	**Activités** choisies par l'entreprise en fonction des risques prépondérants	Toutes les activités réalisées sur **un site**
Partage d'informations sur la certification/la labélisation	Ne prévoit **pas de cadre**	Comprend un **cadre pour le partage d'informations** entre les organisations
L'accent mis sur la chaîne d'approvisionnement	Ne comporte pas d'exigences spécifiques de ce type	Met fortement **l'accent sur la maîtrise de la chaîne d'approvisionnement**
Type d'audit	Audit sur site	Audit sur site **ou à distance** en fonction de l'objectif de l'audit

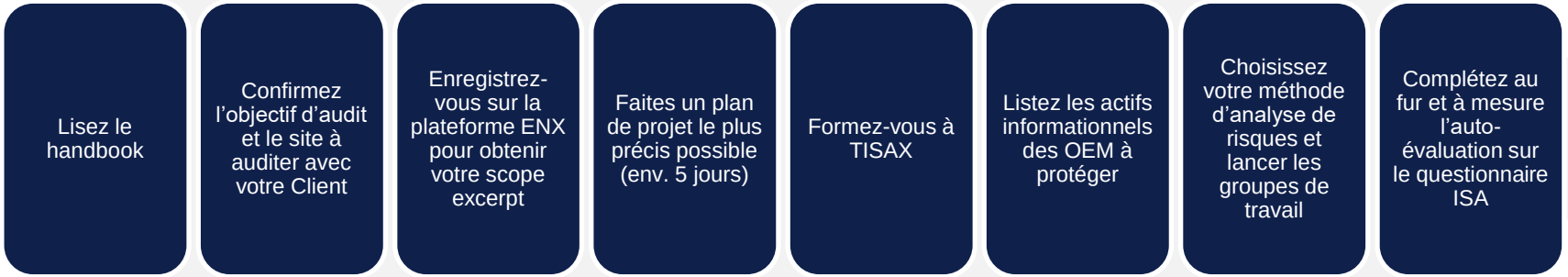
Est-il difficile de mettre en œuvre TISAX si j'ai la norme ISO 27001 ?

Si votre organisation dispose déjà d'un système de management de la sécurité de l'information (SMSI) certifié ISO 27001, vous êtes en **bonne position pour mettre en œuvre TISAX**.

TISAX s'appuie sur la norme ISO 27001 et inclut des **exigences supplémentaires spécifiques** à l'industrie automobile.

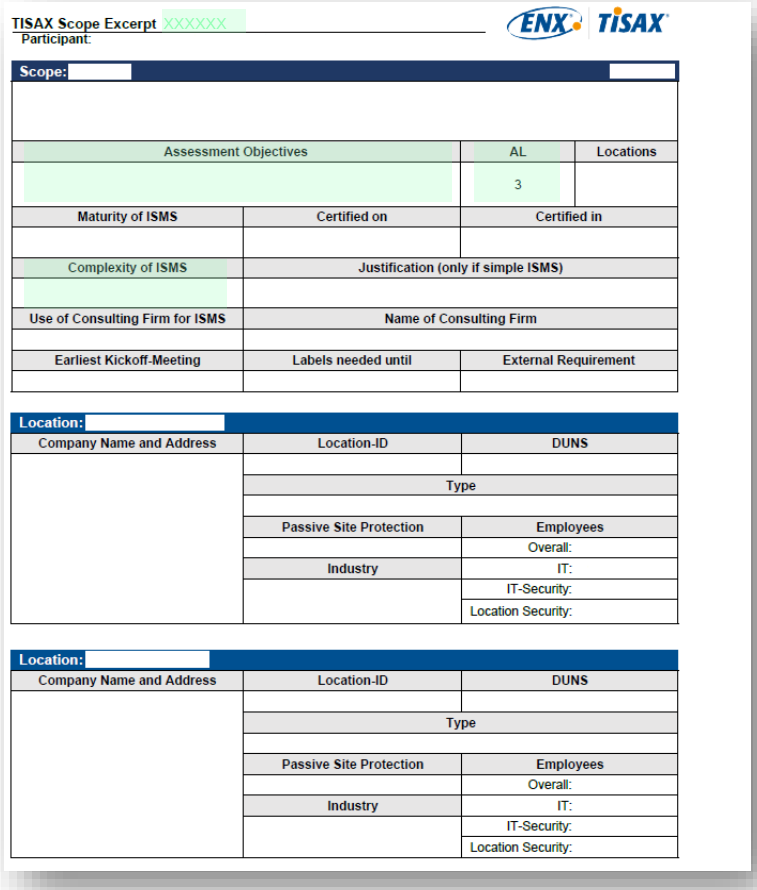
Pour garantir la réussite de la labellisation TISAX, il est important de bien comprendre les exigences TISAX et leurs différences par rapport à la norme ISO 27001, ainsi que d'effectuer un **Gap Analysis** afin d'identifier les contrôles ou processus supplémentaires qui pourraient être nécessaires pour répondre aux exigences TISAX.

Les premières étapes



DNV ©

Focus sur le scope excerpt



TISAX Scope Excerpt XXXXXX

Participant:

Scope:		
Assessment Objectives	AL	Locations
	3	
Maturity of ISMS	Certified on	Certified in
Complexity of ISMS	Justification (only if simple ISMS)	
Use of Consulting Firm for ISMS	Name of Consulting Firm	
Earliest Kickoff-Meeting	Labels needed until	External Requirement

Location:		
Company Name and Address	Location-ID	DUNS
	Type	
	Passive Site Protection	Employees
		Overall:
	Industry	IT:
		IT-Security:
		Location Security:

Location:		
Company Name and Address	Location-ID	DUNS
	Type	
	Passive Site Protection	Employees
		Overall:
	Industry	IT:
		IT-Security:
		Location Security:

Planning

Objectif de labellisation en juin 2024

Il y a un délai maximum de 9 mois à partir de l'évaluation TISAX pour obtenir le label définitif

Les points importants à retenir

Cette labellisation est **stratégique** pour l'entreprise, **investissez** les ressources adéquates

Les réflexions vont conduire à des **changements** qu'il est important d'**accompagner** pour assurer la pérennité de la démarche

Comptez a minima

120 jours

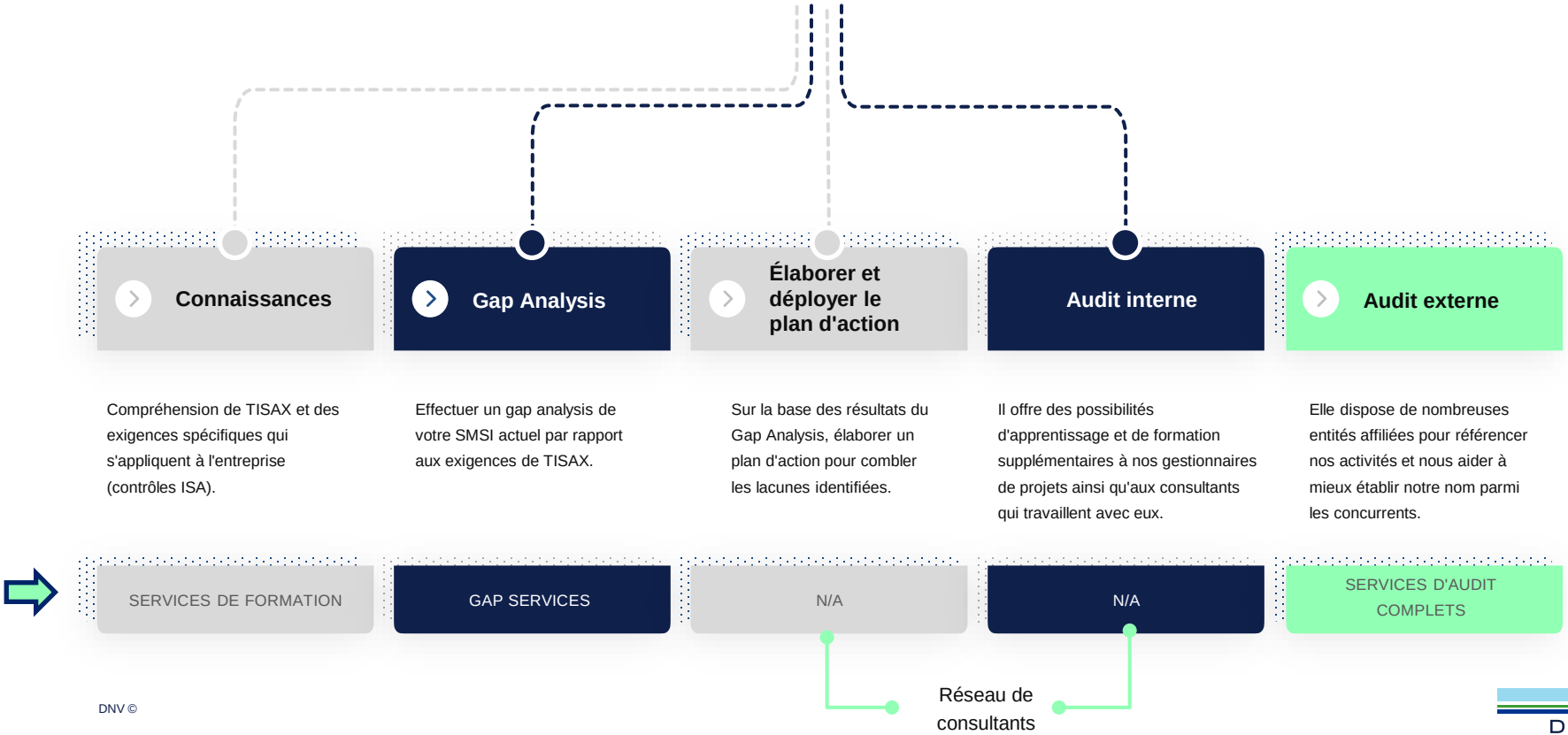
de travail de mise en conformité, dont la moitié est concentrée sur la personne en charge du projet

Il s'agit d'un référentiel complexe à comprendre de prime abord, n'hésitez pas à **faire appel à des professionnels**

Les défis à relever

DNV ©

Quelles étapes peuvent être externalisées ?



DNV ©

Vos 3 principaux défis

1. APPREHENDER L’OBJECTIF

TISAX se concentre sur la sécurité des informations confiées par les donneurs d’ordre sur toute la chaîne d’approvisionnement.

2. COMPRENDRE LES EXIGENCES

Certaines entreprises ont fait part de leurs difficultés à interpréter les exigences de TISAX et à déterminer les mesures spécifiques à prendre pour s'y conformer.

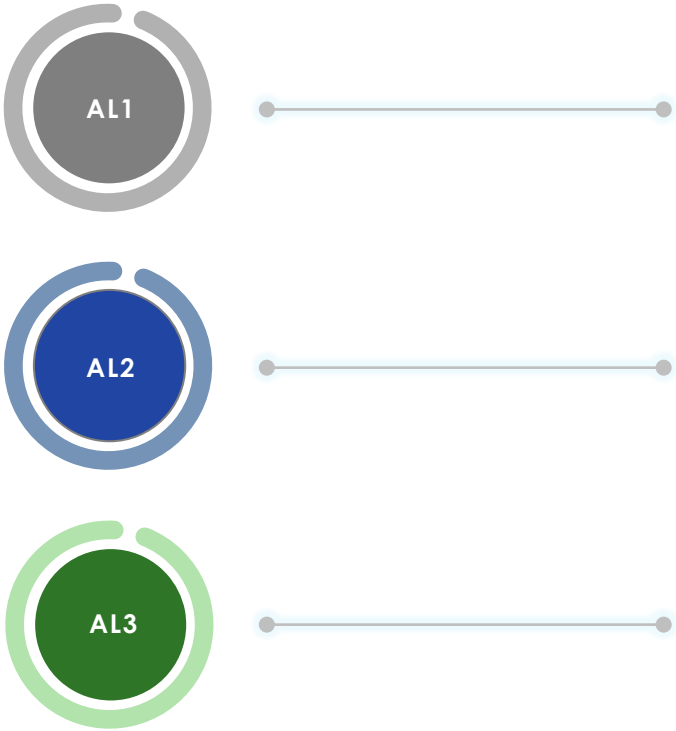
3. DÉFINIR L’ÉCHÉANCIER

Le processus d'évaluation de TISAX peut être long et complexe.

TISAX® processus d'audit

Niveaux d'évaluation

AL = Assessment Level



Les évaluations du niveau d'évaluation 1 sont principalement destinées à des fins internes, au sens propre d'une auto-évaluation.

Pour une évaluation de niveau 2, le prestataire d'audit effectue un contrôle de plausibilité de l'auto-évaluation du client. Le prestataire de services d'audit mène l'entretien généralement par conférence web.

Pour une évaluation de niveau 3, le prestataire d'audit procède à une vérification complète de la conformité de votre entreprise aux exigences applicables. Audit sur site et entretiens.

DNV ©

Niveaux d'évaluation

	Évaluation - Niveau 1 (AL 1)	Évaluation-Niveau 2 (AL 2)	Évaluation-Niveau 3 (AL 3)
Auto-évaluation	✓	✓	✓
Les preuves	✗	Contrôle de plausibilité	Plongée profonde
Interviews	✗	A distance	Sur place
Audit sur place	✗	*si l'audité le souhaite*	✓

Quelle valeur apporte TISAX® ?

Pourquoi TISAX ® crée de la valeur

1. Développer la **culture de sécurité** des informations de l'entreprise

2. Prendre conscience de la **valeur de l'information**

3. Permettre de gagner en **visibilité** via l'ENX

4. Facilite au travers du principe de **standardisation**

5. Permet **d'inspirer confiance** pour les clients d'autres industries

DNV ©

Seriez-vous intéressé par les services d’un prestataire comme DNV ?

☐ Oui

☐ Non

Questions / réponses

GALIA
Copyright © 29/09/2023

Nos coordonnées

Nadine GARAUD
B2B & IS/IT Director
garaud@galia.com

Stéphanie HANTAT
Auditrice cybersécurité & TISAX
DNV Business assurance
France.business-assurance@dnv.com

Sarah VIRTUOSE
Directrice commerciale France
DNV Business assurance
France.business-assurance@dnv.com

Copyright © 29/09/2023