FORMATION MISE EN ŒUVRE PART IS

REF : CYB-PARTIS-002-6

Formation à la mise en œuvre du PART IS
Durée : 3.0 jours / 21 heures - Réf. Réf. : CYB-PARTIS-002-6

L'objectif de la règlement PART IS est d'assurer que le secteur aéronautique dispose des compétences nécessaires pour identifier et gérer les risques liés à la sécurité de l'information, susceptibles d'avoir un impact sur la sûreté aérienne.
Une compréhension approfondie du **Part-IS** est essentielle pour sa mise en œuvre efficace et pour se préparer aux audits de conformité. Grâce à une explication détaillée des exigences, cette formation vous permettra :

- d'identifier les principaux leviers de conformité,
- de comprendre les impacts sur votre organisation et vos processus,
- et de vous préparer efficacement à la mise en œuvre de PART IS

Cette formation constitue un élément clé dans le processus de conformité au Part-IS.

Durée

21 heures

Public concerné

- Responsable de projet sécurité industrielle
- Responsable de gestion de la sécurité
- Responsable de la surveillance de la conformité
- Professionnel SI
- Responsable SMSI

Objectifs

1. Enregistrer les fondements du Part-IS : son cadre réglementaire, ses objectifs et les documents d'orientation associés.
2. Appréhender la complémentarité entre sécurité de l'information et sûreté aérienne
3. Assimiler le modèle de gouvernance attendu, en particulier l'articulation entre le SMSI (Système de Management de la Sécurité de l'Information) et le SMS (Safety Management System).
4. Identifier les actifs critiques, les parties prenantes internes et externes, ainsi que les fournisseurs à mobiliser pour répondre aux exigences du Part-IS.
5. Savoir construire une analyse de risque cyber
6. Être en capacité de structurer un projet de mise en œuvre du Part-IS, adapté au contexte et aux enjeux de votre organisation.

Programme

I. Fondamentaux et cadre réglementaire

- Contexte réglementaire européen (EASA, règlements 2022/1645 et 2023/203)
- Objectifs du Part-IS et articulation avec la sécurité aérienne
- Présentation du Cadre de Conformité Cyber France (3CFv3)
- Documents d'orientation et AMC associés
- Notification des incidents (Autorité, interne et externe)
- Notification de changement de SMSI à l'autorité

II. Complémentarité entre sécurité de l'information et sûreté

- Définitions : sécurité, sûreté, SMSI, SMS
- Cas concrets d'interdépendance (ex : compromission d'un système critique)
- Enjeux de la cybersécurité pour la sûreté aérienne

Étude de cas : Analyse d'un incident cyber ayant un impact sur la sûreté

III. Gouvernance, actifs et parties prenantes

- Rôle du Dirigeant Responsable, du Responsable de la mise en œuvre et du responsable de la conformité
- Articulation SMSI / SMS
- Organisation cible, rôles et responsabilités
- La matrice RASCI
- Définition des fonctions critiques
- Cartographie des actifs (systèmes, données, équipements)
- Identification des parties prenantes internes et externes
- Externalisation d'une partie du SMSI
- Gestion des tiers, sous-traitants et salariés
- Système de management : PDCA, revue de direction, amélioration continue …

IV. Analyse de risque

- Les méthodologies d'analyse de risque : ISO 27005, EBIOS RM
- Identification des événements redoutés
- Évaluation de la gravité et de la vraisemblance
- Plan de traitement des risques et risque résiduel
- Gestion des risques : ISO 27002 – Guide hygiène numérique de l'ANSSI – ISO 62443

Atelier : Réalisation d'une mini-analyse de risque sur une fonction critique

V. Structurer le projet de mise en œuvre du PART IS

- Étapes clés de la mise en conformité
- Intégration dans les processus existants
- Pilotage, indicateurs, tableaux de bord

Atelier : Élaboration d'un plan de mise en œuvre

VI. Test de connaissance

Méthodes et supports

Enseignement théorique
Exposés avec illustrations
Pédagogie active
Études de cas
Atelier pédagogique
La formation est animée par un formateur :
- disposant d'une qualification spécifique de formateur selon les procédures de qualification de Bureau Veritas
- justifiant d'une expérience terrain confirmée dans le domaine concerné

Prérequis

Connaissance de base dans les systèmes de management et les bases en sécurité de l'information

Modalités d'évaluation

EXAMEN : QCM

La note minimale de réussite est fixée à 75 %.