Formation « PART-IS Lead Implementer »

Réf : PARTIS

Dans un contexte aéronautique où la cybersécurité devient un enjeu majeur pour la sécurité des vols, la réglementation Part-IS impose aux acteurs du secteur de mettre en œuvre un système de management de la sécurité de l'information en cohérence avec les exigences de l'EASA. La formation « Part-IS Lead Implementeor » a pour objectif d'accompagner les professionnels dans la compréhension, l'intégration et le déploiement opérationnel de cette réglementation au sein de leur organisation.

Conçue pour les responsables sécurité, qualité, conformité, ou encore les chefs de projet SMSI/SGS, cette formation immersive de cinq jours articule apports théoriques, études de cas réalistes et ateliers pratiques. Elle permet aux participants d'acquérir les compétences nécessaires pour piloter efficacement une démarche de conformité Part-IS, depuis la cartographie des risques critiques jusqu'à la production de preuves de conformité et l'élaboration d'un plan d'action structuré.

Objectifs

- **Permettre aux participants de comprendre, intégrer et mettre en œuvre la réglementation Part-IS au sein de leur organisation, en assurant la convergence entre cyber sécurité et sécurité des vols.**
  - **Expliquer les exigences de la réglementation Part-IS et son articulation avec l'ISMS et le SMS.**
  - **Cartographier les processus critiques et évaluer les risques cyber impactant la sécurité des vols.**
  - **Construire une matrice de conformité et produire des preuves de conformité (registre, grille de traçabilité).**
  - **Identifier les écarts et définir un plan d'action réaliste dans leur contexte professionnel.**
  - **Adopter une posture collaborative et systémique pour piloter la mise en œuvre de Part-IS.**

Durée & horaires

- **5 jours soit 35 heures réparties comme suit :**

Phase pédagogique	Temps alloué	Modalité dominante
Apport théorique ciblé	30 % (10,5 h)	Présentation interactive
Études de cas concrètes	20 % (7 h)	Analyse collective
Travaux pratiques encadrés	30 % (10,5 h)	Atelier pratique guidé
Échanges et retours d'expérience	10 % (3,5 h)	Ateliers / tables rondes
Synthèse + plan d'action individuel	10 % (3,5 h)	Coaching / restitution

- **Du lundi au vendredi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 15 participants**

Public visé

- **RSSI, responsable qualité, sécurité aérienne**
- **Responsable conformité ou juridique**
- **Chefs de projet SMSI ou SGS**
- **Auditeurs, formateurs, consultants aéronautiques**

Pré-requis

- **Connaissance de base en sécurité de l'information**
- **Familiarité avec le secteur aérien ou les normes ISO 27001/27002 est un plus**

Méthode pédagogique

- **Alternance théorie / pratique**

- **Pédagogie inductive et collaborative**
- **Approche par compétences métier**
- **Cas simulés réalistes et ancrés dans les pratiques aéronautiques**

Supports

- **Fiches théoriques**
- **Trames de registre Part-IS, analyse de risques, plan d'action**
- **Outils de suivi de conformité**
- **Grille d'auto-diagnostic Part-IS**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation prépare à l'examen de certification PART-IS Lead Implementer. A l'issue de cette formation, le stagiaire passe l'examen en français. L'examen est constitué d'un QCM.**

Programme

- **Phase 1 – Apport théorique ciblé**
  - Part-IS : le Cadre réglementaire (définition, scope, articles, rôle de l'EASA…).
  - Part-IS en tant que Système de management de la sécurité de l'information, intégré au SMS de l'entreprise : Méthode d'Implémentation, Livrables.
  - Part-IS et la maîtrise du risque (réactive, proactive, prédictive) intégrée à l'iso27001.
  - Focus outils : BowTie, AMDEC, Modélisation de processus, ADC, Matrices (SIRA/ERC).
  - Référentiels complémentaires : ISO 27001 / 27002/ 27005
    - Supports : Diaporama, schémas, quiz d'ancrage

- **Phase 2 – Études de cas concrètes**
  - Analyse de scénarios réalistes : intrusion IT impactant un vol, attaque par rançongiciel, données interfaces corrompues, etc.
  - Identification des défaillances systémiques
  - Élaboration de barrières de sécurité
  - Constitution d'un registre de dangers Part-IS
  - Supports : Fiches scénarios, outils collaboratifs (tableaux, post-it digitaux)

- **Phase 3 – Travaux pratiques encadrés**
  - Cas simulé : compagnie aérienne fictive et son écosystème
  - Cartographie des processus critiques
  - Évaluation des risques selon l'exigence Part-IS
  - Élaboration d'un plan de sécurité et de conformité
  - Rédaction des preuves attendues par Part-IS
    - Supports : Trames vierges (registre, SoA, analyse de risques), canevas de présentation

- **Phase 4 – Échanges et retours d'expérience**
  - Ateliers collaboratifs : facteurs de succès/échec
  - Freins à l'implémentation & leviers d'engagement
  - Retour d'expériences croisées entre métiers
    - Supports : Tableau des freins/leviers, grille de synthèse collective

- **Phase 5 – Synthèse + plan d'action individuel**

- Élaboration d'un plan d'implémentation personnalisé
- Identification des parties prenantes, étapes clés, KPI
- Restitution volontaire devant les pairs
    - Supports : Fiche de plan d'action guidée, modèle de tableau de bord