Pour toute question, contacter l'ANSSI :

- Par e-mail : support@anssi.etat.lu
- Par téléphone : 247-88930

Réunion de lancement du Comité de Sécurité de l'Information (CSI)

Sommaire

1. Le DSI – Rôle et Missions

1. Le DSI – Présentation

- Présentation du DSI nommé

1. Le DSI – Rôle et Missions

Le Délégué à la Sécurité de l'Information (DSI) agit comme un chef d'orchestre, s'assurant que l'ensemble des mesures techniques, organisationnelles et humaines sont implémentées pour maintenir la confidentialité, l'intégrité et la disponibilité des actifs numériques.

Quatre aspects principaux :

1. Gouvernance de sécurité de l'information.
2. Gestion des risques.
3. Gestion de la sensibilisation et de la formation.
4. Gestion des incidents de sécurité de l'information.

1. Le DSI – Rôle et Missions

- Gouvernance de sécurité de l'information

  - Définir, superviser et coordonner la mise en œuvre de la stratégie de la sécurité de l'information.
  - Implémenter / piloter et maintenir le Système de Management de la Sécurité de l'Information (SMSI).
  - Définir et mettre en œuvre la PGSI de l'entité.
  - Conseiller la Direction sur les mesures de sécurité de l'information à mettre en œuvre.
  - S'assurer de l'implémentation des fonctions et organes nécessaires à la gouvernance de sécurité de l'information (p.ex. Comité de Sécurité de l'Information).

- Gestion des risques

  - Définir et implémenter une approche structurée de gestion des risques liés à la sécurité de l'information.
  - Collaborer avec les responsables de projets pour intégrer la sécurité dès la conception (Security by Design) dans les applications informatiques et les processus métiers.

1. Le DSI – Rôle et Missions

- Gestion de la sensibilisation et de la formation

  - Diffuser une culture de sécurité des systèmes d'information au sein de l'entité.
  - S'assurer que les collaborateurs sont sensibilisés (règles de sécurité, enjeux de sécurité, etc.) et formés en matière de sécurité de l'information.

- Gestion des incidents de sécurité de l'information

  - Prendre les mesures techniques et/ou organisationnelles permettant la surveillance des événements de sécurité de l'information.
  - Contribuer au pilotage des incidents de sécurité de l'information, le cas échéant en lien avec le DPO et/ou avec le GOVCERT.
  - S'assurer que les autorités compétentes soient notifiées en cas d'incident de sécurité.

1. Le DSI – Rôle et Missions

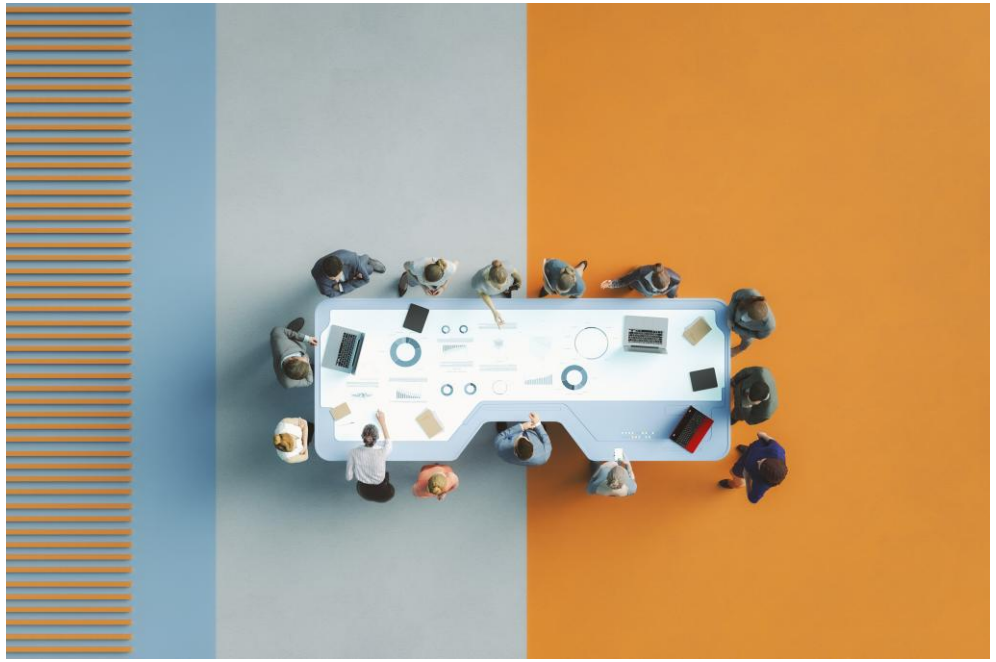
Deux piliers optionnels supplémentaires :

- Gestion de la continuité des activités
  - Définir, mettre en œuvre et maintenir le plan de continuité des activités (« Business Continuity Plan »).
  - Sensibiliser et former les collaborateurs au plan de continuité des activités.
  - Coordonner les exercices en matière de continuité des activités.
- Gestion de la conformité
  - Evaluer le niveau de sécurité, notamment à travers la réalisation d'audits / revues de sécurité.
  - S'assurer que la sécurité de l'information est intégrée dans le dispositif de contrôle interne, et réaliser des contrôles clés si nécessaire.

2. Le CSI - Rôle et Missions

2.1 Pourquoi instaurer un CSI ?

- **Alignement Stratégique :** Assurer que la sécurité soutient directement les objectifs opérationnels et métiers de l'entité.
- **Gouvernance Structurée :** Créer un espace formel pour coordonner les rôles et valider les décisions critiques.
- **Gestion des Risques :** Prioriser les investissements et les actions basés sur une analyse de risque validée par la direction.
- **Conformité Réglementaire :** Répondre aux exigences formelles (NIS2, et standards ENISA).



2.2 Le Reporting

Ce qu’il est

- Une vue d’ensemble claire
- Un outil pour prioriser
- Un suivi dans le temps

Ce qu'il n'est pas

- Une liste technique illisible
- Un export brut d'outil de sécurité
- Un rapport de conformité exhaustif

Fréquence des réunions : X réunions par an

+ Réunion en cas d’urgence

2.3 Structure du reporting au CSI

1. Nouveautés & Points d'attention

Changements notables depuis le dernier reporting (incidents majeurs, évolutions réglementaires, audits, initiatives clés).

2. Synthèse du niveau de risques

Scénarios de la macro-cartographie des risques et dérogations présentant un niveau de risque significatif

3. Suivi du plan d'action pluriannuel

État d'avancement des actions de sécurité et identification des retards, difficultés et besoin.

4. Indicateurs clés

Évolution de la maturité, tendances des incidents et des dérogations, efficacité des contrôles clés.

5. Arbitrages attendus

Décisions attendues sur les priorités, l'adaptation du plan d'action, les risques résiduels critiques et les dérogations.

2.4 Le Règlement d’organisation intérieure du CSI

Le règlement du CSI présente :

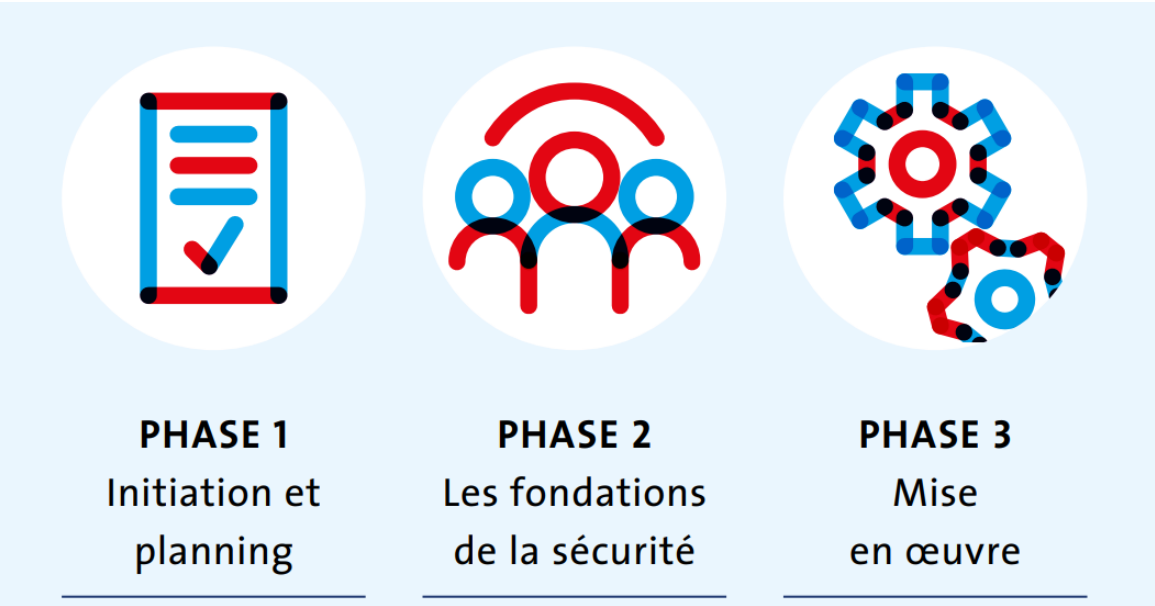
- **Rôles et missions**
- **Composition**
- **Fonctionnement**

Il sera transmis après la réunion et ajusté si nécessaire en fonction de vos commentaires

3. Approche du guide de l’ANSSI

3. Approche du guide de l'ANSSI

Nous allons suivre l'implémentation de la sécurité de l'information de l'ANSSI:



Ces étapes sont détaillées dans le « Guide pratique – Mettre en place la sécurité de l'information: les étapes clés pour bien débuter »

3. Approche du guide de l'ANSSI

Initiation et planning : définition du périmètre

- **Identification des services métiers vitaux :** lister les services, comprendre les interdépendances et évaluer la criticité

- **Inventaires des prestataires :** lister les prestataires et évaluer la criticité

3. Approche du guide de l'ANSSI

Initiation et planning : auto-évaluation

- **Évaluation de la maturité actuelle :** réaliser une autoévaluation à l'aide des objectifs de sécurité
- **Définir le niveau cible :** en tenant compte de la maturité actuelle, des enjeux de sécurité, des exigences réglementaires et des ressources disponibles
- **Identifier les écarts :** comparer la situation actuelle avec le niveau cible afin d'établir un plan d'action priorisé

3. Approche du guide de l'ANSSI

Initiation et planning : macro-cartographie des risques et plan d'action

- **Macro-cartographie des risques :**
- offre une vue d'ensemble des risques pouvant affecter les services vitaux d'une entité
- elle repose sur des scénarios types, adaptés au contexte de l'organisation, pour identifier, évaluer et prioriser les risques

- **Définition d'un plan d'action sécurité sur la base :**
- des écarts identifiés lors de l'auto-évaluation
- de la macro-cartographie des risques
- et des quick wins permettant des améliorations rapides et visibles

3. Approche du guide de l'ANSSI

Mise en place des fondations de la sécurité :

- **Référentiel de sécurité** : formalisation de la PGSI de l'entité, élaboration des politiques et procédures, en cohérence avec NIS2 ;
- **Organisation de la sécurité** : désignation et formation d'un Délégué à la Sécurité de l'Information (DSI), mise en place éventuelle d'un Comité de Sécurité de l'Information, clarification des rôles et responsabilités ;
- **Gestion des risques** : mise en œuvre d'un processus structuré d'analyse, d'évaluation et de traitement des risques, incluant la gestion des dérogations et des risques résiduels ;
- **Intégration de la sécurité dans les projets** : information précoce du DSI sur les projets, suivi des étapes clés et définition des exigences de sécurité pour chaque projet ;
- **Préparation à la gestion des incidents** : désignation d'une instance gestionnaire, mise en place de procédures de détection et de réponse, vérification de la journalisation et de la traçabilité pour assurer la conformité et la notification dans les délais prévus par NIS2.

HUTT DIR FROEN ?