Pour toute question, contacter l'ANSSI :
- Par e-mail : support@anssi.etat.lu
- Par téléphone : 247-88930

Comité de Sécurité de l'Information de [nom de l'entité]

Modèle Règlement d'organisation interne

1) Objet

Il est créé un Comité de Sécurité de l'Information (CSI) qui peut être consulté concernant les aspects sécurité de l'information par le *[chef d'administration]* en cohérence notamment avec les obligations prévues par la Directive (UE) 2022/2555, dite « NIS2 », applicables aux entités essentielles du secteur « Administration publique » (Annexe I) et couvrant la protection des réseaux et systèmes d'information qui supportent les informations de l'entité.

2) Rôle et positionnement du CSI

Le Comité de Sécurité de l'Information (CSI) constitue une instance transversale de gouvernance visant à appuyer la coordination, l'analyse et la préparation des décisions en matière de sécurité de l'information. Il réunit les parties prenantes concernées, incluant notamment un représentant de l'organe de direction.

Le CSI agit comme une instance d'appui à la décision et de suivi, sur la base d'un reporting consolidé, factuel et orienté risques, préparé notamment par le Délégué à la Sécurité de l'Information (DSI). À ce titre, il contribue à l'instruction des sujets stratégiques et à la priorisation des actions en matière de sécurité de l'information.

Le CSI ne se substitue pas à l'organe de direction, qui demeure responsable des décisions en matière de sécurité de l'information. Le DSI rend compte directement à l'organe de direction, le cas échéant en s'appuyant sur les travaux et analyses réalisés dans le cadre du CSI.

Le CSI assure également un rôle de suivi du dispositif de sécurité, notamment à travers l'examen des indicateurs, des risques, des incidents significatifs et de l'avancement des plans d'action, afin de soutenir une prise de décision éclairée et une supervision effective par l'organe de direction.

Le CSI exerce une fonction de gouvernance et n'assure pas la gestion opérationnelle des situations de crise.

3) Missions du CSI

Le CSI a pour missions principales de :
- Améliorer durablement la résilience de *[nom de l'entité]* en matière de sécurité de l'information ;

- Maintenir un niveau de risque maîtrisé et acceptable, en disposant d'une vision consolidée des risques, incidents, vulnérabilités et dérogations ;
- Prioriser et arbitrer les actions de sécurité, en tenant compte des analyses de risques, des ressources disponibles et des obligations réglementaires, dont NIS2 ;
- Assurer le suivi de la conformité aux normes et exigences réglementaires applicables ;
- Structurer et formaliser la prise de décision, en impliquant les parties prenantes concernées dans un pilotage concerté.

4) Réunion du CSI

Les réunions du CSI ont pour objectif de permettre à la Direction et aux parties prenantes de disposer d'une vision consolidée, actualisée et orientée décision de la sécurité de l'information de l'entité.

Le reporting présenté au CSI est structuré afin de permettre notamment, lors de chaque réunion, de :

- Prendre connaissance des nouveautés et événements marquants intervenus depuis la dernière réunion, notamment les incidents de sécurité significatifs, les évolutions réglementaires, les résultats d'audit ou de contrôle ;
- Examiner les risques pour l'entité, leur évolution dans le temps et leur niveau de maîtrise ;
- Suivre l'avancement du plan d'action pluriannuel en sécurité de l'information, identifier les retards, difficultés ou besoins d'ajustement, et valider les mesures correctrices nécessaires ;
- Analyser les éléments de suivi relatifs à la maturité, aux incidents, et aux dérogations afin d'apprécier l'évolution globale du dispositif ;
- Arbitrer et décider sur les priorités, les adaptations du plan d'action, l'acceptation des risques résiduels et les demandes de dérogation.

5) Composition

a) Membres

Font partie du CSI :

- un représentant de la direction
- le ou la délégué(e) à la sécurité de l'information,
- le ou la référent(e)/délégué(e) à la protection des données,
- *[des représentant des fonctions métiers],*
- le cas échéants :
    - gestionnaire des risques.
    - gestionnaire de la continuité des activités.

b) Présidence

La présidence du CSI est exercée par *[un représentant de la direction]*.

c) Bureau

Le président et le secrétaire constituent le bureau du comité et sont désignés par *[le chef d'administration]*.

Le bureau du comité se réunit à la demande du président et a pour mission de préparer les réunions du comité.

d) Secrétariat

Le secrétariat du CSI est exercé par le délégué à la sécurité de l'information.

6) Fonctionnement

a) Convocation et ordre du jour

Le CSI se réunit périodiquement, avec une fréquence minimale de *X [X entre 2 et 4]* réunions par an. Les convocations sont adressées au moins cinq jours à l'avance.

Un CSI extraordinaire peut être convoqué lorsqu'un événement, une évolution ou une décision requiert une prise de position rapide au niveau de la gouvernance de la sécurité de l'information, en dehors du cycle normal des réunions.

Le secrétariat prépare l'ordre du jour d'un commun accord avec le président. L'ordre du jour fait partie intégrante de la convocation et il est approuvé en début de chaque séance.

En cas d'urgence et dans l'impossibilité de se réunir dans un délai raisonnable, le président peut décider d'avoir recours à la procédure écrite.

Si un membre effectif ne peut pas assister à la réunion du comité, il en informe le président et le secrétaire.

b) Compte rendu

Le secrétariat établit le compte rendu en coordination avec le président. Le document reprend l'ensemble des décisions arrêtées lors de la réunion. Une fois rédigé, il est soumis à l'approbation des membres du CSI.

c) Experts

À la demande d'un membre du CSI et avec l'accord du CSI, des experts peuvent être consultés concernant certains dossiers à l'ordre du jour et assister à la réunion. Ces experts sont tenus de garder le secret des délibérations et de ne pas divulguer les données inhérentes aux dossiers traités.

d) Délibérations

Le CSI ne délibère valablement qu'en présence de la majorité des membres. Les avis sont adoptés à la majorité simple des voix des membres présents. Les avis mentionnent le nombre de voix en faveur, en défaveur et les abstentions. L'avis peut être accompagné d'avis séparés émis par un ou plusieurs membres du CSI.

Le président et le délégué à la sécurité de l'information veillent à la mise en œuvre des avis adoptés.