HCPN
ANSSI

Mettre en place la sécurité de l’information, dans le contexte de NIS2

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Plan

1. Missions du HCPN-ANSSI
2. Eléments clés de l'approche « sécurité de l'information »
   A. Responsabilités d'une entité
   B. Approche recommandée
3. Initiatives principales
   A. Mise à disposition de politiques et lignes directrices
   B. Sensibilisation et formation
   C. Réalisation d'analyses de risques
4. Echange et communications

1. Missions du HCPN-ANSSI

1. Missions du HCPN-ANSSI

Suivant la loi du 23 juillet 2016 portant création du HCPN telle que modifiée par la loi du 17 juin 2022, le HCPN, dans sa fonction d'ANSSI, a notamment pour missions :

- de contribuer à la mise en œuvre de la politique générale de sécurité de l'information de l'État ;
- de contribuer à la mise en œuvre, en concertation avec les administrations et services de l'État, des politiques et lignes directrices de SI portant sur les domaines de la PGSI de l'État et des nouvelles technologies de l'information et de la communication ;
- d'émettre des recommandations d'implémentation des politiques et lignes directrices de SI et d'assister les administrations et services de l'État au niveau de l'implémentation des mesures proposées ;

1. Missions du HCPN-ANSSI

- de définir, en concertation avec les administrations et services de l'État, une approche de gestion des risques, en vue de constituer un plan d'évaluation et d'identification des risques concernant la sécurité de l'information et d'accompagner, à leur demande, les administrations et services de l'État dans l'analyse et la gestion des risques ;
- de conseiller l'INAP, respectivement, à leur demande, les administrations et services de l'État dans la définition d'un programme de formation dans le domaine de la sécurité de l'information ;
- de promouvoir la SI par le biais de mesures de sensibilisation ;
- de conseiller, à leur demande, les établissements publics et les infrastructures critiques en matière de sécurité des réseaux et systèmes d'information et des risques y liés ; […]

2. Eléments clés de l'approche SI

A. Responsabilités d'une entité

2A. Responsabilités d'une entité

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Selon la Politique générale de la sécurité de l'information de l'État luxembourgeois (version 2.0) :

> « Les entités sont responsables de la sécurité de l'information dans leur champ d'attribution et, à cette fin, elles prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité de l'information. »

- Chaque entité est donc responsable de sa propre gestion des risques en matière de sécurité de l'information

2A. Responsabilités d’une entité

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Une idée reçue potentiellement dangereuse :

« Le CTIE prend entièrement en charge ma sécurité informatique »

2A. Responsabilités d'une entité

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Une entité doit se concentrer en interne sur plusieurs aspects clés de la sécurité de l'information, indépendamment de ses prestataires :

- **Gouvernance sécurité**
  - Politiques et procédures de sécurité
  - Désignation des rôles (DSI, comité de sécurité, etc.)
- **Gestion des Risques**
  - Évaluation des risques
  - Plans d'action
- **Gestion des tiers et relations contractuelles**
- **Gestion des incidents internes**
  - Plan de réponse aux incidents
  - Équipe de réponse aux incidents
- **Sensibilisation et formation**
  - Formation des cadres dirigeants et employés
  - Sensibilisation des agents

2A. Responsabilités d'une entité

Une entité doit se concentrer en interne sur plusieurs aspects clés de la sécurité de l'information, indépendamment de ses prestataires (suite) :

- **Protection de l'information**
  - Classification des informations
  - Règles de manipulation
- **Accompagnement des projets**
  - Identification des besoins en sécurité
  - Mesures de sécurisation
- **Gestion de la continuité des activités**
  - Plan de continuité des activités
  - Exercices
- **Gestion des accès logiques**
- **Sécurité physique**
- **…**

2. Eléments clés de l'approche SI

B. Approche recommandée

2B. Recommandation d'implémentation

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Nous recommandons aux entités de procéder à l'implémentation de la sécurité de l'information par phases :

INITIATION ET PLANNING

FONDATIONS DE LA SÉCURITÉ

IMPLÉMENTATION

Ces étapes seront détaillées dans le guide « Poser les bases de la sécurité de l'information » (échéance Q4 2025)

2B. Recommandation d'implémentation

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

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 prestataire et évaluer la criticité

2B. Recommandation d'implémentation

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

2B. Recommandation d'implémentation

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

2B. Recommandation d'implémentation

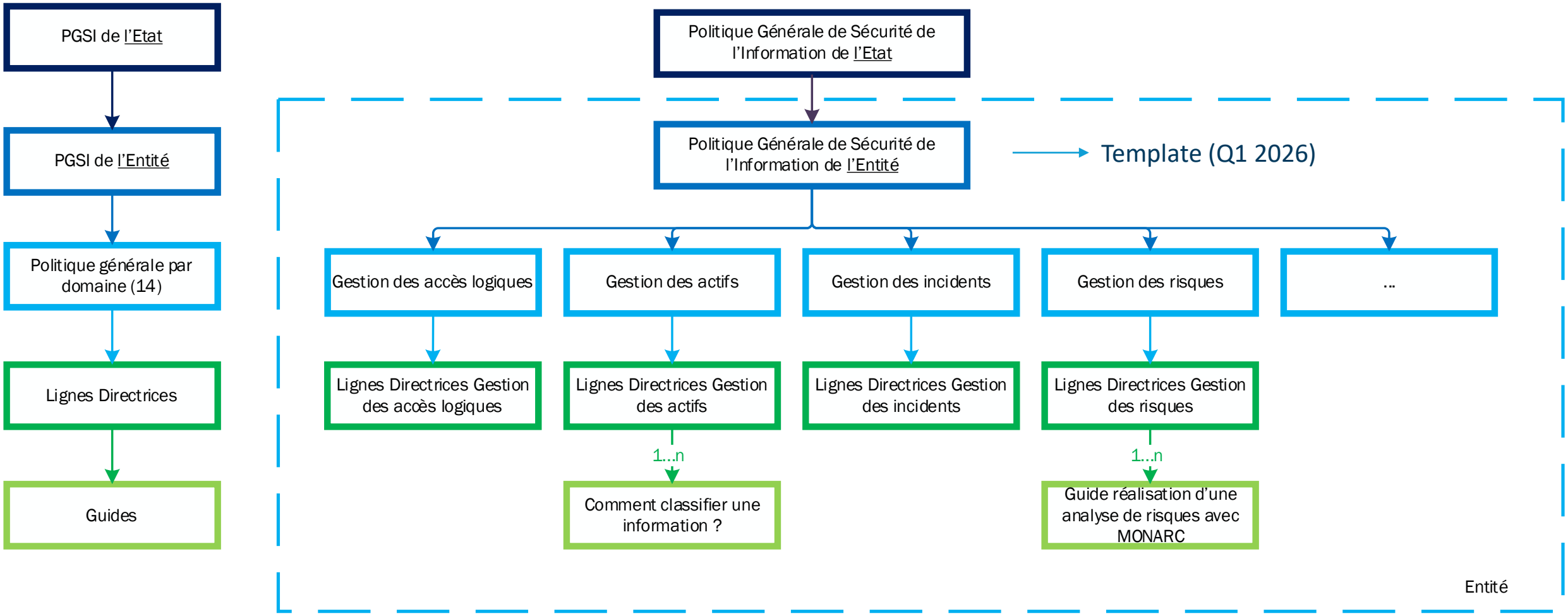
Mise en place des fondations de la sécurité :

- **Référentiel de sécurité** : formalisation de la PGSSI 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.

3. Initiatives en relation avec NIS2

A. Mise à disposition de politiques et lignes directrices

3A.2 . Structure du référentiel



3A.1 . Approche générale

- Mise à disposition par le HCPN/ANSSI de politiques thématiques et lignes directrices :
  - Approche “boîte à outils” : documents courts, clairs et directement exploitables.
  - Contenu pragmatique et réaliste, facilitant l’application sur le terrain.
  - Plusieurs niveaux d’exigences, permettant une adaptation selon la taille et la maturité des entités.
  - Alignement avec le contexte luxembourgeois et les spécificités du secteur public.
  - Basés sur les référentiels ISO et NIS2.
  - Mise à disposition sans caractère obligatoire, l’entité restant seule responsable de décider si elle rend ces documents contraignants dans son organisation.

3.3 . Planning : 2025

Politiques	Aspects couverts	Livraison
Gestion des risques	• Analyses des risques SI • Traitement des risques SI • Gestion des menaces	Livré
Organisation de la sécurité de l'information	• Responsabilités de la direction • Politiques de sécurité de l'information • Fonctions et responsabilités liées à la sécurité de l'information • Gestion des dérogations	Q4 2025
Gestion des actifs	• Classification des informations • Manipulation des informations • Gestion des médias amovibles • Gestion de l'inventaire des actifs	Q4 2025

3.3 . Planning : 2026 (1er semestre)

Politiques	Aspects couverts	Livraison
Gestion des événements et incidents liés à la sécurité de l'information	• Planification et préparation • Surveillance et journalisation • Evaluation et classification des événements • Réponse aux incidents • Examens post-incident	Q1 2026
Relation avec les fournisseurs	• Gestion des fournisseurs et prestataires de services • Inventaire des fournisseurs et prestataires de services	Q1 2026
Gestion des accès logiques	• Gestion des accès logiques • Gestion des droits d'administration • Gestion de l'identification et de l'authentification • Gestion de l'authentification forte	Q1 2026
Acquisition, développement et de la maintenance des systèmes d'information	• Sécurité lors de l'acquisition de services, de systèmes ou de produits TIC • Cycle de vie du développement sécurisé	Q2 2026
Sécurité physique et environnementale	• Sécurité physique et environnementale • Protection contre les menaces physiques et environnementales	Q2 2026
Sécurité des ressources humaines	• Sécurité des ressources humaines • Recrutements • Procédure de gestion des départs et des mutations • Sensibilisation & formation	Q2 2026

3.3 . Planning : 2026 (2eme semestre)

Politiques	Aspects couverts	Livraison
Gestion de la continuité des activités	• Gestion de la continuité des activités • Gestion du plan de reprise d'activités (DRP) • Gestion de crises • Gestion des sauvegardes et des redondances	2eme semestre 2026
Gestion de la conformité	• Surveillance de la conformité • Evaluation des mesures de sécurité • Revue indépendante de la sécurité	2eme semestre 2026
Cryptographie	• Gestion de la cryptographie	2eme semestre 2026
Sécurité des réseaux	• Sécurité des réseaux • Segmentation des réseaux	2eme semestre 2026
Sécurité liée à l'exploitation	• Systèmes d'administration • Gestion des configurations • Gestion et divulgation des vulnérabilités et correctifs de sécurité • Tests de sécurité • Protection contre les logiciels malveillants et non autorisés	2eme semestre 2026

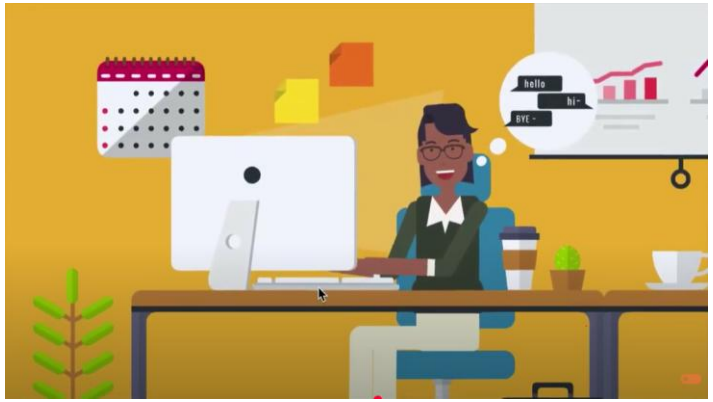
3. Initiatives en relation avec NIS2

B. Sensibilisation et formation

3B. La sensibilisation et formation

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

- **Nouveaux contenus de sensibilisation à destination des agents de l'Etat :**
  - Un « Cybersecurity Escape Room » a été ajouté au catalogue de l'INAP ;
  - Un nouveau cours de sensibilisation (3 heures) sera ajouté au catalogue de l'INAP (échéance Q4 2025);



Ce contenu sera également mis à disposition sous forme de vidéos utilisables pour les DSIs dans le cadre de leur campagnes de sensibilisation (échéance Q4 2025).

4. La sensibilisation et formation

- **Nouvelles formations au catalogue de l'INAP :**

  - **A destination des cadres dirigeants :** comprendre les enjeux, responsabilités et décisions clés en matière de cybersécurité (échéance Q1 2026);

  - **A destination des DSIs :** acquérir les connaissances et compétences pratiques pour piloter efficacement la sécurité des systèmes d'information (échéance Q1 2026).

3. Initiatives en relation avec NIS2

C. Réalisation d’analyses de risques

3C.1. Concepts clés de l'approche

Notre approche est basée sur la méthodologie d'analyse de risques MONARC, qui s'appuie sur une méthodologie orientée « service » :

1 - Actifs primaires

- Services métier
- Processus internes

supporté par

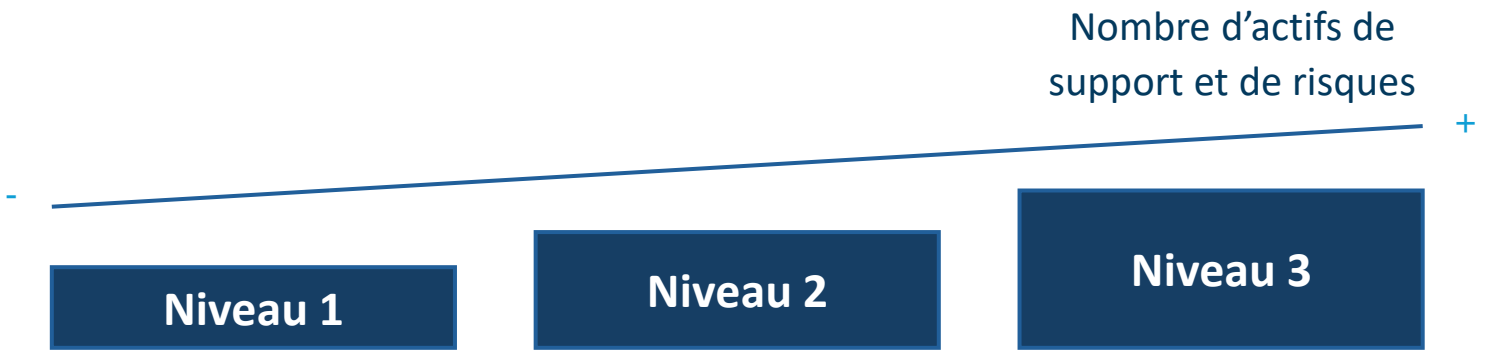
2 - Actifs de support

- Actifs (applications, réseaux, personnel, etc.) supportant les actifs primaires
- Les risques sont associés à ces actifs

3C.1. Concepts clés de l’approche

Pour faciliter la réalisation d’une analyse de risques, nous avons conçu une bibliothèque d’actifs de support prédéfinis, organisée en trois niveaux progressifs :

- Elle contient des actifs, où le nombre d’actifs de support et de risques associés augmente progressivement ;



- Les risques les plus significatifs sont couverts, tout en limitant la charge de travail nécessaire.

3C.2. Comment procéder ?

Par où commencer ?

- Lancez une analyse de risques sur un périmètre restreint, en vous concentrant d'abord sur quelques services métiers.
- Choisissez avec attention le processus métier pilote, qui servira d'exemple pour déployer la méthode progressivement.

Nous vous accompagnons tout au long du processus :

- Coaching gratuit pendant les différentes phases de l'analyse.
- Hébergement d'une instance MONARC dédiée et sécurisée.
- Accès à un guide utilisateur détaillé pour vous guider pas à pas.

4. Echange et communications

4. Groupe d’échanges informels

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

- Création d’un groupe d’échanges informels (« ISAC Administrations ») destinés aux DSIs, afin de partager les bonnes pratiques, discuter des problèmes rencontrés et identifier des solutions communes : à partir de Q1 2026.

4. Où nous contacter ?

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

- **Besoin d'aide ou de conseils ?**
- Notre équipe est à votre disposition pour vous accompagner et vous soutenir.

- **Par e-mail :** support@anssi.etat.lu

- **Par téléphone :** 247 - 88930

4. Où trouver nos informations ?

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

- **Retrouvez toutes nos ressources en ligne :**
- **Extranet ANSSI** : anssi.extranet.etat.lu
- **GovSpace ANSSI** : govspace.msp.etat.lu/gs/anssi/default.aspx

HUTT DIR FROEN ?

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale