INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

GUIDELINES NIS2 - ORGANES DE DIRECTION

17, rue du Fossé
Adresse postale
L-2922 Luxembourg

T +352 28 228 228
F +352 28 228 229
info@ilr.lu

www.ilr.lu

1. Obligations des organes de direction dans le cadre de NIS2

La directive européenne NIS2 marque un tournant significatif dans la gouvernance de la cybersécurité au sein des entités considérées comme essentielles ou importantes. L'un des apports majeurs est l'insistance sur la responsabilité **directe et explicite** des organes de direction dans la **gestion des risques en matière de cybersécurité.**

Cette implication ne se limite plus à une simple supervision ponctuelle ou à une délégation technique. Elle implique un engagement actif et démontrable des dirigeants. Les organes de direction sont ainsi renforcés dans leur rôle d'acteurs clés de la cybersécurité au sein de l'organisation.

Concrètement, cela signifie que les membres des organes de direction doivent non seulement valider les grandes orientations stratégiques en matière de cybersécurité (notamment au travers d'une politique générale en matière de sécurité de l'information), mais également veiller à leur mise en œuvre effective. Conformément **à l'article 20 de la directive NIS2**, les membres des organes de direction doivent :

- suivre les formations nécessaires afin d'acquérir les connaissances et compétences suffisantes pour **évaluer les risques** en cybersécurité**, comprendre les impacts** sur les services fournis**, prendre des décisions** éclairées, notamment pour la **gestion des ressources**, et assumer pleinement leurs **responsabilités** ;
- veiller à ce que des **formations** similaires soient régulièrement proposées aux **membres du personnel**, afin d'acquérir les bonnes pratiques pour la gestion des risques et garantir une formation continue et adaptée à tous les niveaux de l'organisation ; et
- **approuver les mesures de gestion des risques en matière de cybersécurité** et superviser leur mise en œuvre, ce qui inclut la validation des résultats des évaluations de risques ainsi que des plans de remédiation associés.

Dans un contexte où les menaces cyber augmentent se multiplient en fréquence, en complexité et en impact, le rôle des organes de direction devient un pilier incontournable de la sécurité organisationnelle. La directive NIS2 en fait une exigence réglementaire, mais peut être également une opportunité stratégique : celle de positionner la cybersécurité comme un enjeu de gouvernance porté au plus haut niveau de l'entité.

2. Thématiques à intégrer dans la formation des organes de direction

Avec l'arrivée de la directive européenne **NIS2,** la cybersécurité n'est plus uniquement l'affaire des équipes techniques. Elle devient un sujet stratégique, qui concerne directement les **organes de direction**. La **formation** des organes de direction est un **levier de cybersécurité**, et même un accélérateur de **maturité numérique**.

Voici les sujets que toute formation destinée aux organes de direction devrait intégrer :

1. **<u>Comprendre la directive NIS2 et ses implications pour la gouvernance :</u>**

   Permettre aux dirigeants de comprendre les principes fondamentaux de la directive NIS2, son périmètre d'application et les obligations précises qui leur sont assignées. L'accent est à mettre sur le fait que la cybersécurité relève désormais pleinement de la responsabilité stratégique de l'organe de direction et ne peut pas être seulement considérée comme un simple enjeu technique dont la responsabilité est du ressort du responsable informatique ou de la personne en charge de la sécurité de l'information.

2. **Identification des risques et gestion de la sécurité des réseaux et des systèmes d'information :**

   Les dirigeants ont la responsabilité de valider l'identification, l'évaluation et le traitement des risques liés à la sécurité des réseaux et des systèmes d'information. Ils doivent disposer d'une compréhension claire de ces risques, déterminer l'appétence au risque de l'entité et prendre les arbitrages stratégiques nécessaires pour concilier sécurité, performance et continuité d'activité.

   Une analyse de risques efficace repose sur le recensement des actifs critiques et des scénarios, l'évaluation des menaces et vulnérabilités, puis la mise en œuvre de mesures techniques et organisationnelles adaptées pour en réduire l'impact et la probabilité.

3. **Notification des incidents de sécurité :**

   Les dirigeants veillent au respect des obligations de notification imposées par la directive NIS2. En cas d'incident important, l'entité est tenue d'alerter dans les délais prescrits et, si la situation l'exige, d'informer également les utilisateurs concernés.

4. **Mise en place de mesures de sécurité appropriées :**

   Les dirigeants veillent au respect des obligations imposant la mise en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité proportionné aux risques liés aux activités de l'entité. Ces mesures doivent permettre de prévenir, détecter et atténuer les menaces et les vulnérabilités, tout en assurant la continuité et la résilience des opérations.

5. **Principes de sécurité de l'information et veille sur les menaces :**

   Il est essentiel que les dirigeants comprennent les principes fondamentaux de la sécurité de l'information couverts par la directive NIS 2 — confidentialité, intégrité, disponibilité et authenticité des données et systèmes — ainsi que les menaces et vulnérabilités actuelles pouvant les affecter, et qu'ils en mesurent les impacts potentiels sur l'entité en cas d'incident. Cela inclut la connaissance des cyberattaques les plus répandues, telles que le ransomware, le phishing ou les attaques sur la chaîne d'approvisionnement, ainsi que l'analyse de cas concrets touchant leur secteur d'activité. Ils doivent également être informés des tendances émergentes en matière de cybercriminalité afin d'anticiper les évolutions des risques et d'adapter en conséquence la posture de cybersécurité de l'entité.

6. **Coopération avec les autorités compétentes :**

   Les dirigeants veillent à ce que l'entité coopère pleinement avec les autorités compétentes. Cette coopération inclut la fourniture des informations nécessaires pour évaluer la conformité réglementaire et pour faciliter la gestion et la résolution des incidents de sécurité.

NIS2 ne demande pas aux dirigeants de devenir des experts techniques. Mais elle exige qu'ils soient éclairés, impliqués et responsables en matière de cybersécurité. Une bonne formation donne les clés pour comprendre, décider, et piloter la sécurité numérique comme un vrai sujet stratégique. Car aujourd'hui, **diriger**, c'est aussi **sécuriser**.