Registre de formation NIS2 de l'organe de direction

Article 20, paragraphe 2, directive (UE) 2022/2555 · transpositions nationales

MODÈLE GRATUIT — XLSX · PDF · MD | Version 1.0 · Mis à jour 2026-07-21

Ce que contient le classeur

Registre de l'organe de direction	Une ligne par membre : nom, rôle, organe, date de nomination, applicabilité du devoir de l'article 20 (avec justification), statut, et deux colonnes calculées — dernière session accomplie et prochaine échéance. Les auditeurs échantillonnent les preuves contre cette liste ; les membres en retard sont signalés automatiquement.
Journal des formations	Une ligne par membre et par session : intitulé, prestataire et type, date, durée en heures, format, objectifs de l'article 20(2) couverts (identifier les risques / évaluer les pratiques / impact sur les services), intervalle de renouvellement, échéance calculée, référence de preuve (certificat, feuille de présence, export LMS) et statut.
Catalogue des sessions	Le programme de formation : sessions prévues avec public, objectifs, fréquence, modalité, prestataire et — de plus en plus demandé — une mesure d'efficacité par session. Le document programme attendu en plus des preuves individuelles.
Référence par juridiction	Comment le devoir de formation est quantifié là où vous opérez : base UE, France (transposition en cours, guichet MonEspaceNIS2 de l'ANSSI), § 38 BSIG allemand avec le repère ~4 h tous les 3 ans, règle lettone, devoir tchèque, modèle discrétionnaire belge (CCB), Digitalsikkerhetsloven norvégienne et le code volontaire britannique.

L'échelle juridique

Art. 20(1)	Les organes de direction des entités essentielles et importantes doivent **approuver** les mesures de gestion des risques de l'article 21, **superviser** leur mise en œuvre et **peuvent être tenus responsables** des violations. L'approbation suppose une compréhension documentée — c'est précisément ce que le devoir de formation vise à créer.
Art. 20(2)	Les membres des organes de direction **sont tenus de suivre une formation** afin d'acquérir des connaissances et compétences suffisantes pour identifier les risques et évaluer les pratiques de gestion des risques et leur impact sur les services. La formation des salariés est ici seulement *encouragée* — l'obligation de formation du personnel figure à l'article 21(2)(g) et se suit séparément.
France	La transposition n'est pas achevée : la Commission a renvoyé la France devant la **CJUE le 8 juillet 2026** pour défaut de notification. Le guichet MonEspaceNIS2 de l'ANSSI annonce néanmoins déjà les exigences de l'article 20 — approbation, supervision et formation de l'organe de direction. Constituer le registre dès maintenant évite de courir après les preuves quand la loi arrivera.
Preuve	Les autorités échantillonnent des **preuves individuelles**, pas des tableaux de bord : nom, rôle, date, durée, contenus rattachés aux objectifs de l'article 20(2), prestataire, preuve d'achèvement, prochaine échéance — plus le document programme et les procès-verbaux montrant l'organe formé approuvant le jeu de mesures de l'article 21.

À quelle fréquence « régulièrement » ? — quantifications nationales

Juridiction	Règle	Quantification
Base UE	Art. 20(2) : les membres des organes de direction sont tenus de suivre une formation	Aucune — définie par l'objectif
France	Transposition en cours (renvoi CJUE 8.7.2026) ; MonEspaceNIS2 (ANSSI) annonce les devoirs de l'art. 20	Aucune fixée à ce stade
Allemagne	§ 38 al. 3 BSIG : régulier, personnel, non délégable ; en vigueur depuis le 6.12.2025	~4 h au moins tous les 3 ans (repère des travaux préparatoires)
Lettonie	Loi (1.9.2024) + règlement 397 (2.7.2025) : formation de la direction obligatoire ; contenus revus au moins annuellement	Régulière — le plus souvent annuelle

Belgique	Loi du 26.4.2024 art. 31 §2 + CCB : formation régulière, modalités à la discrétion de l'entité	Aucune — attentes plus élevées pour les entités essentielles
Norvège	Digitalsikkerhetsloven (1.10.2025) : la direction approuve le SMSI, revue annuelle ; formation attendue	Aucune fixée
Royaume-Uni	Cyber Security and Resilience Bill : pas d'obligation légale ; code de gouvernance volontaire	Aucune

Le dossier de preuves prêt pour l'inspection

Le registre est une pièce d'un dossier en cinq éléments vers lequel convergent les autorités : **(1)** le registre nominatif de l'organe de direction ; **(2)** les preuves de formation individuelles — ce classeur ; **(3)** le document programme — la feuille Catalogue des sessions ; **(4)** les procès-verbaux montrant l'organe formé approuvant les mesures de l'article 21 (version, date, participants nommés) ; et **(5)** les preuves d'efficacité — rapports d'exercices sur table, briefings actés avec actions de suivi. Faites pointer les références de preuve vers des artefacts réellement archivés : un certificat introuvable sur demande n'existe pas, du point de vue d'un audit.

Pourquoi c'est important maintenant : l'article 20 lie la formation à la responsabilité. Un organe de direction qui approuve des mesures de gestion des risques sans pouvoir prouver sa propre formation offre à l'autorité un constat facile — et les entités françaises opérant en Allemagne relèvent déjà du § 38 BSIG, personnel et sans renonciation possible. Ce registre est l'assurance la moins chère de la pile de preuves NIS2.

> **Du registre de formation à la preuve visible par vos clients.** Les preuves de gouvernance que votre autorité échantillonne sont celles que les acheteurs B2B demandent dans leurs questionnaires de sécurité (« la direction reçoit-elle une formation cybersécurité ? »). Orbiq publie ces preuves dans un Trust Center gouverné — un seul enregistrement répond au régulateur et au client. Bibliothèque complète de modèles gratuits : orbiqhq.com/fr/modeles.