Checklist de conformité NIS2

Vingt-huit points pour vérifier votre conformité à la loi NIS2 belge : champ d'application, enregistrement, gouvernance, les dix mesures de gestion des risques, notification des incidents et preuves.

NIS2 Aware · nis2aware.eu · novembre 2026

1. Champ d'application et enregistrement

- [ ] **Évaluez si votre organisation est concernée**
  Vérifiez votre secteur (annexe I ou II) et votre taille (50 travailleurs ou plus, ou plus de 10 M€ de chiffre d'affaires et de bilan), entreprises partenaires et liées comprises. Documentez l'analyse.
- [ ] **Déterminez votre catégorie : essentielle ou importante**
  Les grandes organisations des secteurs hautement critiques sont en général essentielles ; les autres organisations concernées sont en général importantes. Votre régime de supervision en dépend.
- [ ] **Enregistrez-vous sur Safeonweb@Work**
  L'enregistrement auprès du CCB est obligatoire. Tenez à jour les coordonnées de vos représentants.
- [ ] **Vérifiez si une autorité sectorielle ou d'autres règles s'appliquent**
  Certains secteurs ont une autorité sectorielle aux côtés du CCB. Les entités financières relèvent principalement de DORA pour le risque TIC.

2. Gouvernance

- [ ] **L'organe de direction a approuvé les mesures de cybersécurité**
  Actez l'approbation dans le procès-verbal d'une réunion du conseil.
- [ ] **L'organe de direction supervise la mise en œuvre**
  Prévoyez un reporting régulier (par exemple trimestriel) avec quelques indicateurs clairs.
- [ ] **Les membres de l'organe de direction ont suivi une formation**
  C'est une obligation légale. Conservez les listes de présence et prévoyez des remises à niveau.
- [ ] **Une personne est responsable de la cybersécurité**
  Désignez un responsable (interne ou externe) avec du temps, de l'autorité et un suppléant.

- [ ] **Un budget et une feuille de route à 12 mois sont approuvés**
  Fixez un objectif, comme un niveau d'assurance CyberFundamentals, et les moyens de l'atteindre.

3. Mesures de gestion des risques

Les dix domaines que la loi impose au minimum, selon une approche « tous risques ».

- [ ] **Analyse des risques et politiques de sécurité des systèmes d'information**
  Identifiez vos actifs critiques et vos risques, et approuvez une politique de sécurité qui en découle.
- [ ] **Gestion des incidents**
  Détecter, analyser, contenir les incidents et s'en rétablir, avec des rôles définis.
- [ ] **Continuité des activités : sauvegardes, reprise après sinistre, gestion de crise**
  Gardez au moins une sauvegarde hors ligne ou immuable, testez les restaurations et rédigez un plan de crise.
- [ ] **Sécurité de la chaîne d'approvisionnement**
  Identifiez les fournisseurs critiques et fixez des exigences de sécurité dans les contrats.
- [ ] **Sécurité de l'acquisition, du développement et de la maintenance, y compris la gestion des vulnérabilités**
  Appliquez les correctifs dans des délais définis, recherchez les vulnérabilités et traitez les signalements de vulnérabilités.
- [ ] **Évaluation de l'efficacité des mesures**
  Utilisez des audits, des tests et des indicateurs pour vérifier que les mesures fonctionnent.
- [ ] **Cyberhygiène de base et formation à la cybersécurité**
  Formez tout le personnel au moins une fois par an : hameçonnage, mots de passe, signalement.
- [ ] **Cryptographie et chiffrement**
  Chiffrez les ordinateurs portables, les données sensibles et les communications, et gérez correctement les clés.
- [ ] **Sécurité des ressources humaines, contrôle d'accès et gestion des actifs**
  Tenez un inventaire des actifs, n'accordez que les droits nécessaires et gérez les arrivées, mutations et départs.
- [ ] **Authentification multifacteur et communications sécurisées**
  MFA sur la messagerie, l'accès à distance, le cloud et les comptes administrateurs ; communications vocales, vidéo, texte et d'urgence sécurisées.

4. Notification des incidents

- [ ] **Les critères d'un incident significatif sont définis**
  Perturbation opérationnelle grave, pertes financières ou dommages considérables à des tiers.
- [ ] **La procédure 24 h / 72 h / un mois est écrite**
  Qui décide, qui notifie le CCB, avec quelles informations. Gardez-en une copie hors ligne.
- [ ] **Les canaux de notification et les contacts sont connus et testés**
  Sachez comment notifier le CCB et tenez à jour la liste des contacts de la cellule de crise.
- [ ] **Vous savez quand informer les destinataires de vos services**
  Préparez des messages pour informer les clients touchés par un incident significatif.
- [ ] **Les incidents sont consignés et les leçons tirées**
  Tenez un registre des incidents et mettez à jour votre analyse des risques après chaque incident.

5. Preuves et conformité

- [ ] **Un cadre de référence est choisi**
  CyberFundamentals (Basic, Important, Essential) ou ISO/IEC 27001.
- [ ] **Une analyse des écarts est faite et un niveau cible fixé**
  Mesurez où vous en êtes par rapport au cadre et planifiez les améliorations.
- [ ] **Entités essentielles : l'évaluation de la conformité est planifiée**
  Planifiez la vérification ou la certification avec un organisme accrédité et vérifiez les échéances du CCB qui s'appliquent à vous.
- [ ] **Les preuves sont conservées et organisées**
  Procès-verbaux du conseil, politiques, listes de formation, rapports de tests et d'audit, registre des incidents.

> **Une checklist n'est pas la conformité.** NIS2 demande une approche fondée sur les risques, tenue à jour. Utilisez cette liste pour structurer le travail, pas pour cocher des cases une fois pour toutes.

Information générale sur le cadre NIS2 belge en date de novembre 2026, pas un avis juridique. Consultez toujours les dernières informations du CCB (ccb.belgium.be et atwork.safeonweb.be).