

Les 11 mesures de l'article 30

Loi belge du 26 avril 2024 transposant la directive (UE) 2022/2555. Chaque mesure est mise en regard des contrôles ISO 27001:2022 et des sous-catégories NIST CSF sur lesquelles CyFun est bâti.

N°	MESURE	ISO 27001:2022	CYFUN (NIST CSF)	ART. 21 §2
1	Analyse des risques et politiques de sécurité des systèmes d'information Disposer d'une méthodologie d'analyse des risques documentée, d'un registre des risques tenu à jour et d'une politique de sécurité approuvée par la direction.	5.1 · 5.7 · 5.31 · 5.35 · 5.36	GV.OC-03 · GV.OV-01 · GV.PO-01 · ID.RA-01	a
2	Gestion des incidents Détecter, qualifier, traiter et capitaliser sur les incidents, avec les délais de notification réglementaires (24 h / 72 h / 1 mois).	5.24 · 5.25 · 5.26 · 5.27 · 5.28 · 6.8 · 8.15 · 8.16	RS.MA-01 · DE.AE-02 · RS.MA-03 · RS.CO-02 · RS.MA-05 · PR.PS-04	b
3	Continuité des activités, sauvegardes, reprise après sinistre et gestion de crise BIA, PCA/PRA testés, sauvegardes restaurables et hors ligne, cellule de crise entraînée.	5.29 · 5.30 · 8.13 · 8.14 · 7.11	ID.AM-05 · PR.IR-03 · RC.RP-01 · ID.IM-02 · PR.DS-11 · PR.IR-02	c
4	Sécurité de la chaîne d'approvisionnement Cartographie des fournisseurs critiques, exigences contractuelles de sécurité, surveillance dans la durée.	5.19 · 5.20 · 5.21 · 5.22 · 5.23	GV.SC-04 · GV.SC-05 · GV.SC-07	d
5	Sécurité de l'acquisition, du développement et de la maintenance, traitement des vulnérabilités SDLC sécurisé, gestion des vulnérabilités et des correctifs, divulgation coordonnée.	8.8 · 8.9 · 8.25 · 8.26 · 8.27 · 8.28 · 8.29 · 8.30 · 8.31 · 8.32 · 8.19	PR.PS-06 · GV.SC-07 · PR.PS-01 · ID.RA-01 · ID.RA-06 · GV.SC-04	e
6	Évaluation de l'efficacité des mesures de gestion des risques Programme d'audit interne, indicateurs, revue de direction — c'est la mesure que les inspections du CCB regardent en premier.	5.35 · 5.36 · 8.29 · 8.34	GV.OV-01 · PR.PS-06	f
7	Pratiques de cyber-hygiène et formation à la cybersécurité Socle d'hygiène (mises à jour, moindre privilège, sauvegardes) et sensibilisation régulière, dirigeants inclus.	6.3 · 5.10 · 8.1 · 8.7	PR.PS-05 · PR.AT-01 · GV.RR-04 · PR.PS-01	g
8	Politiques et procédures de cryptographie et de chiffrement Politique cryptographique, algorithmes et longueurs de clés approuvés, gestion du cycle de vie des clés.	8.24 · 5.14	PR.DS-01 · PR.DS-02 · PR.AA-01	h
9	Sécurité des ressources humaines, contrôle d'accès et gestion des actifs Filtrage à l'embauche, départs, inventaire des actifs, revue périodique des droits.	6.1 · 6.2 · 6.4 · 6.5 · 6.6 · 6.7 · 5.9 · 5.10 · 5.11 · 5.12 · 5.15 · 5.16 · 5.17 · 5.18 · 8.2 · 8.3	PR.AA-05 · PR.AA-01 · PR.AA-03 · ID.AM-01 · ID.AM-05 · GV.RR-04	i

N°	MESURE	ISO 27001:2022	CYFUN (NIST CSF)	ART. 21 §2
10	Authentification à plusieurs facteurs ou authentification continue MFA sur les accès distants, les comptes à privilèges et les applications critiques.	5.17 · 8.5 · 8.2	PR.AA-03 · PR.AA-05	j
11	Communications vocales, vidéo et textuelles sécurisées, et communications d'urgence Canaux de communication protégés, y compris un moyen de secours utilisable si le SI principal est indisponible.	5.14 · 8.20 · 8.21 · 8.22	PR.AA-05 · PR.IR-01 · PR.DS-02	j

Dix ou onze mesures ?

L'article 21 §2 de la directive énumère dix points, de (a) à (j). La loi belge les transpose en onze mesures à son article 30 §3, en scindant le point (j) — authentification à plusieurs facteurs d'un côté, communications sécurisées de l'autre. Devant le CCB, c'est la numérotation belge qui fait foi.