flowlysis.

TRAVAILLER AVEC SON CISO

Dans une entité soumise à NIS2, la direction approuve les mesures de gestion des risques de cybersécurité et supervise leur mise en œuvre. Dans une entité financière, DORA lui confie le cadre de gestion du risque lié aux TIC. Le CISO prépare et fait vivre ces mesures. Ce qui touche au service reste au métier : durée d'arrêt, mode dégradé, accès, fournisseurs.

POUR QUI COO et comités de direction **SERT À** partager les décisions avec le CISO **SE LIT EN** 8 minutes **À LIRE AVEC** P-14, O-30 et C-08

CE QUI RESTE AU COO		CE QUE PORTE LE CISO	
1	Combien de temps chaque service peut s'arrêter	1	L'analyse des risques et les mesures techniques
2	Les risques métier acceptés, signés et datés	2	La détection et la coordination de la réponse
3	Les accès et les fournisseurs, côté métier	3	Le rapport à la direction, qui décide

Le CISO éclaire les décisions de risque. Il ne les prend pas à la place du métier.

1 Ce qui retombe sur la direction

« La cyber, c'est le sujet du CISO. » Les textes nomment la direction.

Approuver, superviser, se former

Chaque État veille à ce que les organes de direction approuvent les mesures de gestion des risques de cybersécurité, supervisent leur mise en œuvre et puissent être tenus responsables si l'entité viole l'article 21, qui fixe ces mesures. Il veille aussi à ce que leurs membres suivent une formation.

NIS2, art. 20.1 et 20.2

Notifier un incident important

Au CSIRT ou, selon le cas, à l'autorité compétente : alerte précoce sans retard injustifié et, en tout état de cause, dans les 24 h après en avoir eu connaissance ; notification d'incident dans les 72 h ; rapport final au plus tard un mois après cette notification. Si l'incident est encore en cours, rapport d'avancement, puis rapport final un mois après son traitement.

NIS2, art. 23.1 et 23.4 · fiche O-69

Secteur financier : porter le risque lié aux TIC

L'organe de direction définit, approuve, supervise le cadre de gestion du risque lié aux TIC et est responsable de sa mise en œuvre. Il assume la responsabilité ultime de la gestion de ce risque, approuve la politique de continuité TIC et alloue le budget de la résilience opérationnelle numérique.

DORA, art. 5.2 a), e) et g)

En Belgique

Toute personne physique responsable de l'entité, ou qui la représente légalement, est responsable des manquements à son devoir de veiller au respect de la loi. La loi dit incident « significatif », notifié au CCB.

Loi du 26 avril 2024, art. 8, 16, 34 et 61 ; AR du 9 juin 2024, art. 3

2 Qui est concerné

Qualification à faire vérifier par un juriste, et à écrire avec sa date

Entité essentielle

Une entité de l'annexe I, au-delà de la taille d'une moyenne entreprise, et d'autres cas prévus.

NIS2, art. 3.1

Entité importante

Les autres entités des annexes I ou II, dès la taille d'une moyenne entreprise. Certains acteurs sont concernés quelle que soit leur taille.

NIS2, art. 2 et 3.2

Entité financière

Pour une entité financière essentielle ou importante au sens de NIS2, DORA est l'acte sectoriel qui s'applique à sa place : risque lié aux TIC, incidents, tests, partage d'informations, prestataires tiers de services TIC.

DORA, art. 1.2 ; NIS2, art. 4 et considérant 28

Hors périmètre, mais fournisseur d'une entité soumise

Les mesures de vos clients soumis comprennent la sécurité de leur chaîne d'approvisionnement, y compris leurs relations avec leurs fournisseurs directs.

NIS2, art. 21.2 d)

En Belgique

Entités essentielles : deux échéances, 18 et 30 mois après l'entrée en vigueur de la loi (le 18 avril 2026, passée, et le 18 avril 2027) ou, pour une entité identifiée par le CCB, après cette identification. Ce qui est dû à chaque échéance dépend de la voie choisie, certification ou inspection. Entités importantes : pas d'échéance d'évaluation obligatoire.

AR du 9 juin 2024, art. 22 et 23 ; loi, art. 11, 39 et 41

3 Quelle fiche ouvrir

Selon la phrase qu'on entend en comité

Chaque fiche part d'un flux que le COO possède déjà.

« On a accepté ce risque l'an dernier. Qui l'a signé ? »
Fiche P-14 · le risque a un propriétaire métier

« Si on se fait chiffrer demain, qui appelle qui ? »
Fiche O-69 · les premières heures d'un incident

« Si l'outil est indisponible trois jours, on fait comment ? »
Fiche O-70 · le mode dégradé

« Il est parti depuis des mois et il a encore accès au partage. »
Fiche O-71 · le cycle des accès

« Le fournisseur nous a envoyé son nouveau RIB par mail. »
Fiche O-72 · le changement de coordonnées bancaires

« On ne sait pas lesquels de nos prestataires peuvent nous arrêter. »
Fiche O-73 · les fournisseurs critiques

« Il y a des milliers de vulnérabilités ouvertes. »
Fiche O-75 · le stock de vulnérabilités

« C'est rouge. Je ne sais pas quoi arbitrer. »
Fiche O-74 · chiffrer un risque en euros

LE CAS TYPE

Une société de services financiers, entité financière au sens de DORA selon ses juristes. Les chiffres sont des hypothèses du cas.

Le déclencheur

Le comité prépare la revue de la politique de continuité TIC, que l'organe de direction approuve. Elle fixe un délai de reprise de 48 h pour six services, choisi par l'IT seule. Aucun responsable métier n'a dit combien de temps son service peut s'arrêter.

Le geste

Le COO demande à chaque responsable sa durée d'arrêt tolérable et le coût d'une heure d'arrêt. L'IT, avec le CISO, chiffre ce que coûte de tenir chaque durée.

Ce qu'ils ont vu

Deux services sur six ne tolèrent pas 48 h : les paiements des clients (4 h) et le centre de contact (24 h).

La décision

Reprise des paiements en moins de 4 h, financée. Mode dégradé pour le centre de contact au-delà de 24 h, risque résiduel signé par sa directrice, révisé dans un an.

Refaites-le : une ligne par service, sa durée tolérable face au délai de l'IT

QUI TRANCHE QUOI

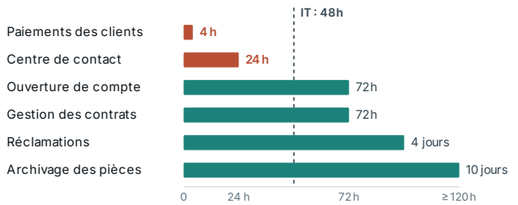
À droite, le cas type chiffré.

UNE LIGNE PAR DÉCISION

LE COO TRANCHE, AVEC LES RESPONSABLES MÉTIER		
La durée d'arrêt tolérable de chaque service Le CISO apporte : avec l'IT, ce que coûte le délai de reprise qui la tient	O-70
Le mode dégradé, et le moment où l'on y passe Le CISO apporte : les systèmes touchés et leur état	O-70
L'acceptation d'un risque métier, signée et datée Le CISO apporte : le scénario, l'estimation, le coût de la mesure écartée	P-14
Le circuit des accès, côté RH et managers Le CISO apporte : la liste des droits sensibles et le rythme de leur revue	O-71
Le choix et le contrat des fournisseurs Le CISO apporte : les exigences de sécurité, pour les seuls critiques	O-73
LE CISO TRANCHE, ET REND COMPTE	
L'analyse des risques Le COO apporte : les services, leurs volumes, le coût d'une heure d'arrêt	O-74
Les mesures techniques Le COO apporte : les fenêtres de maintenance et la capacité de correction	O-75
La détection Le COO apporte : ce qui paraît anormal dans le métier, un paiement, un accès	
La coordination de la réponse à un incident Le COO apporte : les décisions de crise métier, nommées d'avance	O-69
Le rapport à la direction Le COO apporte : une place fixe à l'ordre du jour du comité	O-11

LE CAS · DURÉE D'ARRÊT TOLÉRABLE

Fixée par le métier, face au délai de reprise de 48h choisi par l'IT.



CE QUE LE COMITÉ EN A FAIT

Paiements : une heure d'arrêt coûte 6 000 €.
Arrêt de 48 h au lieu de 4 h : (48 − 4) × 6 000 € = 264 000 €.
Reprendre en moins de 4 h, chiffré par l'IT : 120 000 € par an, 45 % d'un seul arrêt de 48 h. Financé.

Centre de contact : une heure d'arrêt coûte 800 €.
(48 − 24) × 800 € = 19 200 €. Mode dégradé, risque signé.

Quatre services sur six : 48 h suffisent, rien ne change.

Le délai de reprise doit normalement être plus court que la durée tolérable.

À gauche, le partage des décisions entre COO et CISO, sur le principe de la fiche O-30. À droite, chaque barre est la durée d'arrêt tolérable fixée par le métier ; le trait, le délai de reprise fixé par l'IT.

Les trois pièges

Et ce qu'on fait à la place

CONFONDRE CONFORMITÉ ET SÉCURITÉ
Le dossier d'évaluation est complet, et personne n'a vérifié que le service repart dans le délai voulu. Une case cochée ne dit rien de la capacité à tenir le service. On teste la reprise, en vrai.

CONCLURE SOI-MÊME SUR LE PÉRIMÈTRE
« Nous ne sommes pas concernés » se dit en comité, sans texte en main. La qualification se fait vérifier, s'écrit, se date, et se revoit quand l'activité change.

FAIRE DU CISO LE PROPRIÉTAIRE DE TOUS LES RISQUES
Il signe les acceptations à la place du métier, et personne ne répond du service. Le risque appartient au responsable du processus concerné (fiche P-14).

LA PHRASE À RETENIR
Le CISO dit ce que coûte un risque. Le COO décide combien de temps son service peut s'arrêter.