flowlysis.

LE RISQUE A UN PROPRIÉTAIRE MÉTIER

Garder un risque est une décision de gestion, prise par le responsable du processus qui subirait la perte. Il la signe, chiffrée et datée ; le CISO l'éclaire, il ne la prend pas.

AUSSI APPELÉ propriétaire du risque, risk owner, acceptation formelle du risque **S'APPLIQUE À** tout risque qu'on garde : outil hors support, mesure reportée, exception

SE VÉRIFIE EN une heure, en lisant le registre des risques acceptés **OUTIL QUI L'APPLIQUE** chiffrer un risque en euros, fiche O-74

CE QUE ÇA RAPPORTE	
Impact sur le TTM	Faible
Impact sur la qualité (FTR)	Faible
Impact sur l'Opex / Capex	Moyen

CE QUE ÇA EXIGE	
Ce que ça invalide dans la pratique actuelle	Moyen
Délai avant effet visible	Faible
Difficulté à tenir dans la durée	Élevé

Faible · Moyen · Élevé · N/A (sans objet)

1 Ce que dit le principe
Et pourquoi c'est vrai

LA RÈGLE

Chaque risque gardé a un propriétaire nommé : le responsable du processus qui subirait la perte. Il signe une ligne du registre avec le scénario, une fourchette en euros, le coût de la mesure écartée, une date de révision et ce qui rouvre la décision. Le CISO donne son avis par écrit.

POURQUOI ÇA MARCHE

Le mécanisme. Une chaîne de causes que le lecteur peut refaire dans sa tête.

SI CELUI QUI SUBIRAIT LA PERTE SIGNE	ALORS	DONC
il compare la perte possible au coût de la mesure, avec ses chiffres.	la décision se défend en comité, et quelqu'un sait quand la relire.	un risque gardé reste un choix daté, pas un oubli.

L'IDÉE REÇUE QUE ÇA RENVERSE

Écrite telle qu'on l'entend vraiment en comité : c'est une croyance raisonnable qui a cessé d'être vraie.

"Le CISO connaît les risques mieux que nous. S'il juge celui-ci acceptable, c'est à lui de signer."

OÙ ÇA NE S'APPLIQUE PAS

Quand un texte ou un contrat impose la mesure : il n'y a plus d'arbitrage, seulement un plan. Un risque qui touche tous les processus remonte au comité de direction, qui nomme un seul propriétaire.

2 Est-ce respecté chez vous ?
Des tests qu'on fait en marchant

Cinq vérifications observables. Chacune dit où aller regarder, et à quoi on voit que ce n'est pas respecté.

LE PLUS RAPIDE **Lisez les signataires du registre des risques acceptés.**
Un responsable métier nommé par ligne.
× Le CISO partout, ou « la direction informatique ».

Cherchez la date de révision de la plus ancienne acceptation.
Une date, et une revue tenue à cette date.
× Pas de date, ou une date passée sans revue.

Demandez au propriétaire ce que coûterait le risque s'il arrivait.
Une fourchette en euros, et le coût de la mesure écartée.
× « Il est en orange. »

Cherchez sur la ligne ce qui rouvre la décision.
Une condition écrite : incident, changement de fournisseur, nouvelle obligation.
× Rien : la décision ne bouge qu'à la date, ou jamais.

DANS LA DURÉE **Suivez le dernier incident jusqu'au registre.**
Les lignes touchées sont revenues au comité suivant.
× Le registre n'a pas bougé depuis l'incident.

3 Les confusions courantes
Ce que le principe n'est pas

Quatre faux amis. Ce sont eux qui font croire qu'on applique le principe en faisant l'inverse.

Ce n'est pas une acceptation sans échéance
Les deux portent une signature.
→ Sans date, l'acceptation devient l'état normal. Elle porte une date de révision ; ce jour-là, on la renouvelle ou on traite le risque.

Ce n'est pas la signature du CISO
Le CISO connaît les menaces et les failles mieux que personne.
→ Il analyse, chiffre les options et donne son avis. En général, il ne finance pas la mesure et ne porte pas la perte : la signature revient au métier.

Ce n'est pas un risque en couleur
La matrice rouge, orange, vert dit aussi qu'un risque est grave.
→ Une couleur ne se compare pas au coût d'une mesure. Une fourchette en euros, avec sa probabilité, se compare (fiche O-74).

Ce n'est pas désigner un coupable
Les deux mettent un nom sur un risque.
→ Le propriétaire répond de son choix, pas de l'incident. Si le risque arrive, on rouvre la décision sur ses chiffres (fiche P-11).

4 D'où ça vient, et un exemple
L'origine, puis le principe à l'œuvre

ORIGINE

Un seul nom par décision (fiche P-09). Le NIST réserve l'acceptation explicite d'un risque à celui qui autorise le système, en général le titulaire du budget ou de la mission, sans délégation ; le CISO l'appuie (SP 800-37 rév. 2, tâche R-4).

IMAGINONS… Un assureur garde un an de plus son outil des sinistres hors support : la migration (380 k€) est reportée.

SANS LE PRINCIPE Le CISO note le risque en rouge et signe. Un an après, nul ne sait ce qu'il coûterait.

AVEC LE PRINCIPE La directrice des sinistres chiffre : arrêt de 5 à 10 jours, 225 à 450 k€ (45 k€ par jour). Elle paie 40 k€ pour isoler l'outil et préparer sa restauration, puis signe le reste : 2 à 4 jours, 90 à 180 k€.

POUR ALLER PLUS LOIN

fiche O-74, Chiffrer un risque en euros
fiche O-30, Le RACI, et ce qu'il ne règle pas

LE MOT JUSTE

Accepter un risque, pas le valider : on valide une analyse.

CE QUE ÇA CHANGE, CONCRÈTEMENT

L'outil de gestion des sinistres d'un assureur, hors support : la ligne du registre, avant et après.

AVANT · UNE LIGNE QUE PERSONNE NE RELIT

RISQUE	NIVEAU	ACCEPTÉ PAR	RÉVISION
Outil sinistres hors support	ROUGE	le CISO	aucune

Ni montant, ni propriétaire métier, ni échéance : rien ne dit quand ni pourquoi la relire.

APRÈS · LA MÊME LIGNE, SIX CHAMPS REMPLIS

Scénario	faille exploitée (10 % de chances par an), outil arrêté 5 à 10 jours
Estimation	225 à 450 k€ (45 k€ par jour d'arrêt × 5 à 10 jours)
Mesure écartée	migration avancée à cette année : 380 k€ sur ce budget
Propriétaire	la directrice des sinistres, qui signe ; avis du CISO joint
Révision	30 juin, en comité, sur une page A3 (fiche O-11)
Rouvre si	incident, faille exploitée chez d'autres, changement d'hébergeur

Décision : payer 40 k€ pour isoler l'outil et préparer sa restauration, garder le reste
risque gardé : arrêt de 2 à 4 jours, 90 à 180 k€ (45 k€ × 2 à 4 jours)

QUI FAIT QUOI



Chiffres du cas : hypothèses. 45 k€ par jour d'arrêt : rattrapage, renforts, réclamations.

QUAND LE PRINCIPE EST TENU

QUI SIGNE
le responsable du processus qui subirait la perte.
CE QUE DIT LA LIGNE
un scénario, une fourchette en euros, le coût de la mesure.
QUAND ON LA RELIT
à la date fixée, ou dès qu'une condition se réalise.
LE CISO
analyse et donne son avis par écrit.

QUAND IL NE L'EST PAS

QUI SIGNE
le CISO, ou personne.
CE QUE DIT LA LIGNE
une couleur.
QUAND ON LA RELIT
à l'audit suivant, ou après l'incident.
LE CISO
porte seul des risques qu'il ne finance pas.

Ce qu'il faut accepter de perdre
Le prix du principe, dit franchement

CE QU'ON ABANDONNE
Le confort de laisser la sécurité au CISO. Le responsable métier signe un risque à son nom, avec un montant, et le défend en comité.

L'INDICATEUR QUI VA SE DÉGRADER
Le nombre de risques ouverts présentés au comité. Les acceptations anciennes, sans date ni montant, ressortent toutes à la première revue.

CE QUI CASSE SI ON L'APPLIQUE À MOITIÉ
Un propriétaire nommé, sans date de révision. Sa signature couvre le risque pour toujours, et l'incident tombe sur une décision que personne n'a relue.

LA PHRASE À RETENIR
Celui qui subirait la perte signe. Avec un montant, une date, et ce qui rouvre la décision.