flowlysis.

LA SÉCURITÉ INTÉGRÉE AU FLUX

Le contrôle de sécurité tourne là où naît le risque, à chaque changement. La sécurité écrit les règles et les modèles approuvés ; la revue manuelle ne garde que ce qui en sort.

AUSSI APPELÉ sécurité intégrée au développement ; DevSecOps, shift left

S'APPLIQUE À tout changement d'un service numérique ou d'un outil interne : code, configuration

SE VÉRIFIE EN une heure, en suivant la dernière mise en production jusqu'à l'avis sécurité

OUTIL QUI L'APPLIQUE l'avis sécurité de la demande IT comme un flux, fiche O-58

CE QUE ÇA RAPPORTE

Impact sur le TTM	Élevé
Impact sur la qualité (FTR)	Moyen
Impact sur l'Opex / Capex	Moyen

CE QUE ÇA EXIGE

Ce que ça invalide dans la pratique actuelle	Élevé
Délai avant effet visible	Moyen
Difficulté à tenir dans la durée	Moyen

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

1 Ce que dit le principe

Et pourquoi c'est vrai

LA RÈGLE

Le contrôle tourne à chaque changement, là où le risque naît. La sécurité écrit les règles, les modèles approuvés et les contrôles ; le CISO les arrête. Ce qui reste dans un modèle passe sans revue séparée ; le reste est revu dès la conception, puis visé avant la production. Un risque gardé se signe au métier (fiche P-14).

POURQUOI ÇA MARCHE

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

SI modèles et contrôles sont écrits d'avance — l'auteur du changement voit son défaut le jour même.
▶ **ALORS** il le corrige en heures, et apprend à ne plus le faire.
▶ **DONC** la revue manuelle ne garde que ce qui sort des modèles, et sa file se vide.

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.

« Rien ne part en production sans l'avis de la sécurité. C'est ce qui nous protège. »

OÙ ÇA NE S'APPLIQUE PAS

Ce qu'aucun modèle ne couvre, un nouveau prestataire, une donnée sensible nouvelle, passe en revue complète. Une revue indépendante imposée par un texte ou un contrat reste, comptée dans le flux ; le juriste dit laquelle (fiche C-15). Aucun contrôle ne voit tout : la surveillance en production reste.

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 **Suivez la dernière mise en production.**
Aucune attente, si elle restait dans un modèle.
× « Huit jours. Ils sont débordés. »

Demandez la liste des modèles approuvés.
Authentification, chiffrement, configuration : publiés, datés.
× « On demande au CISO, au cas par cas. »

Ouvrez le dernier défaut de sécurité trouvé.
Signalé au développeur, dans son outil, au moment du changement.
× Un rapport de cinquante pages, après la recette.

Demandez ce qui déclenche une revue manuelle.
Un critère écrit : hors modèle, ou première utilisation.
× Tout passe en revue, « par prudence ».

DANS LA DURÉE **Prenez le dernier défaut qui revenait.**
Il a produit un contrôle partagé, pour toutes les équipes.
× Une ligne de plus dans la liste de la revue.

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 automatiser la revue de fin
Les deux raccourcissent l'attente.
→ En fin de chaîne, l'outil trouve le défaut aussi tard. Une revue qui n'arrête rien, hors obligation, se retire (fiche P-25).

Ce n'est pas supprimer la revue de sécurité
Les deux allègent la fin du circuit.
→ Elle garde ce qui sort des modèles : revue dès la conception, visa avant la mise en production.

Ce n'est pas laisser la sécurité aux développeurs
Les deux mettent le contrôle dans l'équipe.
→ La sécurité écrit les contrôles, forme, revoit les écarts. Le risque hors modèle se chiffre (fiche O-74) et se signe au métier.

Ce n'est pas cocher une liste de conformité
Les deux s'appuient sur des règles écrites.
→ La case cochée déclare la règle. Le contrôle s'exécute sur le changement, et laisse sa trace (fiche P-28).

4 D'où ça vient, et un exemple

L'origine, puis le principe à l'œuvre

ORIGINE

Deming : bâtir la qualité dans le processus plutôt que la contrôler après coup. Les équipes du logiciel l'étendent à la sécurité.

> **IMAGINONS…** Un établissement de crédit met en production son espace client 120 fois par an, chaque fois après revue de la sécurité.
>
> **SANS LE PRINCIPE** L'avis attend 8 jours ; une fois sur quatre, un défaut : 4 jours de plus. 9 jours ajoutés en moyenne.
>
> **AVEC LE PRINCIPE** 90 restent dans les modèles ; 30 sont revus, puis visés. 1 jour ajouté ; 400 h au lieu de 1 020.

POUR ALLER PLUS LOIN

fiche P-22, Ne pas transmettre un défaut
fiche P-14, Le risque a un propriétaire métier

LE MOT JUSTE

Dire écrire la règle, et non valider la livraison.

CE QUE ÇA CHANGE, CONCRÈTEMENT

Les mises en production de l'espace client d'un établissement de crédit, sans et avec le principe.

SANS LE PRINCIPE · UN AVIS MANUEL AVANT CHAQUE MISE EN PRODUCTION

Conception	Développement	Avis sécurité	Mise en production
par l'équipe **sans modèle écrit**	et recette **le défaut naît ici**	revue de 4 h **8 j de file**	après le visa **120 par an**
aucune règle partagée	vu par personne	1 sur 4 revient : 4 j	9 j de plus en moyenne

30 sur 120 reviennent avec un défaut ; l'avis attend dans une file commune à six équipes

AVEC LE PRINCIPE · LE CONTRÔLE TOURNE À CHAQUE CHANGEMENT

Modèles approuvés et contrôles partagés : écrits par la sécurité, arrêtés par le CISO

Conception	Développement	Recette	Mise en production
dans un modèle ? **90 oui · 30 non**	contrôles automatiques **défaut vu le jour même**	mêmes contrôles **aucune file**	90 sans visa séparé **30 visées, toutes tracées**
30 revues tôt	défaut corrigé en 2 h	par l'équipe elle-même	1 j de plus en moyenne

Hors modèle, nouveau prestataire ou donnée sensible : revue dès la conception, visa avant production
Le risque qu'on garde, la directrice de l'espace client le signe (fiche P-14)

MÊMES 120 MISES EN PRODUCTION PAR AN	SANS	AVEC
Jours ajoutés par la sécurité, par mise en production	9 j	1 j
Heures de la sécurité, par an	540 h	340 h
Reprise des défauts par l'équipe, par an	480 h	60 h
Temps total, par an	1020 h	400 h

Sans : 8 j + 1 sur 4 × 4 j = 9 j ; 120 × 4 h + 30 × 2 h de nouvelle revue = 540 h ; 30 × 16 h = 480 h.
Avec : 30 × 4 j d'attente ÷ 120 = 1 j ; 30 × 6 h de revue et visa + 160 h d'entretien = 340 h ; 30 × 2 h = 60 h.
Hypothèses : mêmes 30 défauts, trouvés plus tôt ; jours ouvrés ; 300 h pour écrire les modèles, non comptées.

QUAND LE PRINCIPE EST TENU

LE CONTRÔLE
à chaque changement, dans la chaîne.
LA REVUE MANUELLE
pour ce qui sort des modèles, dès la conception.
LA SÉCURITÉ
écrit les règles, les modèles et les contrôles.

QUAND IL NE L'EST PAS

LE CONTRÔLE
un visa, juste avant la mise en production.
LA REVUE MANUELLE
pour tout, en fin de chaîne.
LA SÉCURITÉ
inspecte chaque livraison, et devient la file.

Ce qu'il faut accepter de perdre

Le prix du principe, dit franchement

CE QU'ON ABANDONNE

Le visa sur chaque mise en production, et l'impression qu'il couvre tout. La sécurité écrit d'abord : 300 h, puis 160 h par an pour tenir les modèles à jour.

L'INDICATEUR QUI VA SE DÉGRADER

Le nombre de revues, de 120 à 30 : lu seul en comité, il ressemble à moins de sécurité. Les alertes se voient chaque jour, fausses comprises ; la sécurité corrige la règle qui se trompe.

CE QUI CASSE SI ON L'APPLIQUE À MOITIÉ

Garder la revue de fin pour tout, en plus des contrôles : deux attentes. Ou la retirer avant que les contrôles existent : plus rien n'arrête le défaut.

LA PHRASE À RETENIR

Une revue en fin de chaîne trouve le défaut quand il coûte le plus cher. Une règle écrite d'avance sert à chaque changement.