flowlysis.

LE CYCLE DES ACCÈS

L'arrivée, la mobilité ou le départ, saisi une fois dans l'outil RH, lance toutes les demandes d'accès. On mesure le délai jusqu'au retrait, et chaque responsable relit les droits de son équipe.

AUSSI APPELÉ joiner-mover-leaver, gestion des habilitations **PRINCIPE QU'IL APPLIQUE** un seul point de lancement, fiche P-13 **SE PRÉPARE EN** 2 à 3 semaines

SE FAIT EN un déclencheur RH, une revue à date fixe **VOIR AUSSI** fiche O-59 **LEVIER PRINCIPAL** Qualité (FTR)

CE QUE ÇA RAPPORTE		CE QUE ÇA COÛTE	
Impact sur le TTM	Moyen	Coût d'implémentation	Moyen
Impact sur la qualité (FTR)	Élevé	Difficulté d'implémentation	Moyen
Impact sur l'Opex / Capex	Faible	Difficulté de maintien	Moyen

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

1 Le problème auquel ça s'applique

Et ce qu'il vous coûte chaque année

CE QUE VOUS VOYEZ DÉJÀ

- « Il est parti depuis des mois et il a encore accès au partage. »
- Un collaborateur change de service, et garde ses anciens droits.
- La revue annuelle des droits revient signée partout, sans un seul droit retiré.

OÙ PART L'ARGENT

Chaque droit de trop est une porte ouverte : le compte d'un salarié parti, ou une même personne qui saisit et valide. Il ne coûte rien jusqu'à la fraude ou au constat d'audit. NIS2 range la sécurité des ressources humaines, les politiques de contrôle d'accès et la gestion des actifs parmi les mesures minimales (art. 21, par. 2, point i).

L'ORDRE DE GRANDEUR, À LA LOUCHE

Comptez-le sur vos chiffres. Un ordre de grandeur suffit pour décider d'essayer.

COMBIEN DE FOIS / AN		CE QUE ÇA COÛTE À CHAQUE FOIS		PART QU'ON ÉVITE		GAIN / AN
arrivées, mobilités et départs de l'année	×	transcriptions et relances × durée × coût horaire	×	transcriptions supprimées par le lancement unique	=	**au crayon. Le risque se compte à part, en jours de droits ouverts**

QUAND ÇA NE SERT À RIEN

Pour décider qui a droit à quoi selon le poste. C'est le travail du métier avec le CISO, en amont. Cette fiche fait circuler la décision, elle ne la prend pas.

2 Comment ça marche

La mécanique, en clair

L'IDÉE EN UNE PHRASE

L'événement saisi une fois dans l'outil RH lance toutes les demandes. Le retrait se mesure comme un délai.

LES GESTES, DANS L'ORDRE

1. Suivre trois départs et trois mobilités jusqu'au retrait, en comptant les transcriptions (fiche O-37).
2. Faire de l'événement RH le seul point de lancement : il prévient chaque gestionnaire de comptes d'un départ ou d'une mobilité (NIST SP 800-53, AC-2 h).
3. Traiter la mobilité comme un départ suivi d'une arrivée.
4. Mesurer chaque mois le délai entre la date de départ et le retrait effectif.
5. Faire relire à chaque responsable les droits de son équipe, plus souvent les droits sensibles.
6. Y faire entrer intérimaires, prestataires et comptes partagés, chacun avec un responsable et une date de fin.

CE QU'IL FAUT AVOIR SOUS LA MAIN

Les événements RH de trois mois, les comptes de chaque application, et quelqu'un de l'IT qui sait dater un retrait.

LE SIGNE QUE ÇA A MARCHÉ

À la revue, un responsable retire des droits sans qu'on le lui demande.

3 Les pièges de l'implémentation

Ce qui fait rater, et ce qu'on fait à la place

AU LANCEMENT — Commencer par acheter l'outil
Le nouvel outil de gestion des accès reprend toutes les ressaisies de l'ancien circuit.
→ Cartographier le circuit, supprimer les transcriptions, puis automatiser ce qui reste.

AU LANCEMENT — Laisser les prestataires hors circuit
Ils n'existent pas dans l'outil RH. Leur compte vit jusqu'à ce que quelqu'un le remarque.
→ Pour chacun, un responsable interne et une date de fin.

PENDANT — La revue signée sans lecture
Trois cents lignes envoyées au responsable, signées en deux minutes, aucun droit retiré.
→ Peu de lignes, en clair, les droits sensibles en tête. Suivre la part de droits retirés.

PENDANT — La mobilité traitée comme un ajout
Le nouveau service demande ses droits. Personne ne demande de retirer les anciens.
→ Retirer les droits de l'ancien poste à la date du changement, puis ouvrir ceux du nouveau.

DANS LA DURÉE — Les comptes génériques partagés
Cinq personnes sur « accueil1 » : un départ ne retire rien, et personne ne sait qui a fait quoi.
→ Un compte par personne. Pour un compte partagé qui reste, un responsable et un secret changé à chaque départ.

4 Exemple

Cas type du tertiaire, du constat au résultat

LA SITUATION DE DÉPART

L'OBJET
Les droits d'accès d'une banque régionale, du siège aux soixante agences.

CE QUI CLOCHE
Un chargé de clientèle passé du crédit à l'épargne a gardé ses droits de validation crédit. L'audit interne le découvre huit mois après.

CE QU'ILS REGARDAIENT AVANT
La part de revues retournées signées : 100 % chaque année, sans un droit retiré. Elle ne disait pas combien de droits étaient lus.

LES CHIFFRES DE DÉPART, RELEVÉS SUR L'ANNÉE

1200	salariés, siège et agences
110 + 150	départs et mobilités par an
34 jours	en moyenne, de la date de départ au retrait
4	transcriptions de l'outil RH à l'application

CE QU'ILS ONT FAIT

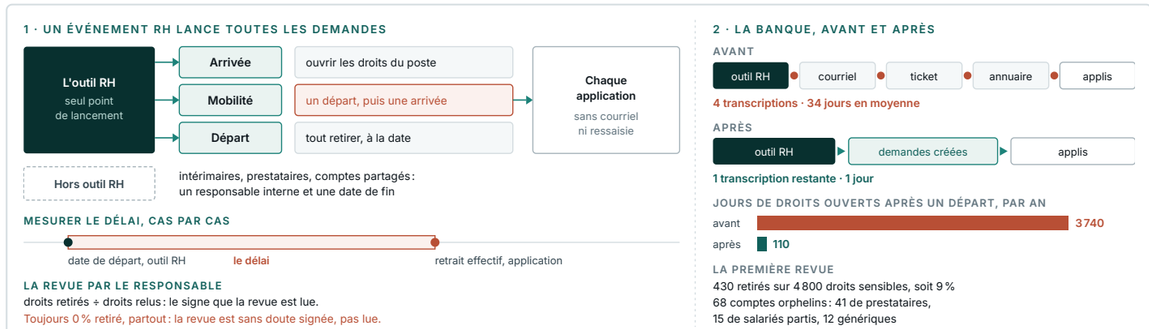
Six dossiers suivis de bout en bout, l'outil RH comme seul point de lancement, puis une première revue par les responsables.

LE DÉCLENCHEUR	LE GESTE	CE QU'ILS ONT VU	LA DÉCISION
Le constat d'audit sur le chargé de clientèle passé à l'épargne.	Trois départs et trois mobilités suivis de l'outil RH au retrait.	Quatre transcriptions par départ ou mobilité. Aucune mobilité ne lançait de retrait.	L'événement RH crée les retraits. Revue des droits sensibles chaque trimestre.

CE QUE ÇA A DONNÉ

34 → 1 jour	Le délai moyen entre la date de départ et le retrait effectif, mesuré sur les départs des trois mois suivants.
3 740 → 110	Les jours de droits ouverts après un départ, par an : 110 départs × 34 jours, puis 110 × 1 jour.
195 h	Le temps rendu par an : 4 → 1 transcription, soit 260 événements × 3 × 15 min (hypothèse), 10 725 € à 55 € l'heure.
0 → 9 %	Les droits retirés à la première revue : 430 sur 4 800 droits sensibles relus. Et 68 comptes orphelins, de prestataires pour la plupart.

Refaites-le avec vos départs : pour trois mois, la date dans l'outil RH et la date du retrait dans chaque application. L'écart moyen va au comité, chaque mois.



À gauche, le circuit : un seul point de lancement, la mobilité comme départ puis arrivée, le délai et la revue. À droite, le cas de la banque, avant et après.

L'exemple est un cas type, reconstruit à partir de situations courantes du tertiaire. Aucune situation client n'y est identifiable.