



## Les droits suivent l'organisation, pas l'inverse



### Le problème : les droits ne suivent plus l'organisation

Dans la plupart des organisations, les droits d'accès s'accumulent avec le temps : arrivées, mobilités, départs, prestataires, comptes techniques, rôles SAP, accès documentaires et applications métiers. Le risque apparaît lorsque l'organisation évolue plus vite que les droits d'accès.

#### Enjeux clés :

- **Savoir qui a accès à quoi**, à tout moment, sur l'ensemble du SI.
- **Automatiser les entrées, mobilités et sorties** pour éviter les droits obsolètes.
- **Réduire la surface d'attaque** liée aux comptes dormants, droits excessifs et accès orphelins.
- **Contrôler les SoD** et les conflits d'autorisations, notamment sur SAP.
- **Produire des preuves d'audit** fiables, sans campagnes manuelles lourdes.
- **Gouverner les accès applicatifs, documentaires et processus** depuis une même logique organisationnelle.

L'IGA ROK répond à une idée simple : **l'organigramme dit qui fait quoi, l'IGA dit qui a accès à quoi**. Quand l'organisation évolue, les droits suivent.



### La réponse ROK : l'organisation devient le socle des accès

- **Organigramme dynamique comme source de vérité** : les postes, sites et processus associés déterminent les droits d'accès. Ces droits ne sont plus gérés comme des objets techniques isolés, mais comme la conséquence de l'organisation réelle.
- **Cycle de vie des identités automatisé** : chaque mouvement IN / MOVE / OUT déclenche l'attribution, la modification ou le retrait des droits : onboarding, mobilité interne, offboarding, prestataires, sous-traitants.
- **Cartographie complète des accès** : vision par collaborateur, application, poste, droits ou périmètre. ROK permet de répondre rapidement à la question : "qui a accès à quoi, pourquoi, depuis quand ?"
- **Contrôle continu des risques** : SoD, accès à privilèges, comptes dormants, droits orphelins, accès temporaires et anomalies sont détectés et suivis dans le temps.
- **Gestion SAP native** : profils, rôles, autorisations, SoD et licences SAP sont pilotés depuis ROK, avec historique complet des attributions et optimisation possible des licences.
- **Compliant-by-design** : les droits, processus et contrôles restent cohérents dès la conception. La piste d'audit est disponible en continu, sans reconstituer les preuves au moment du contrôle.



## Les preuves : résultats observés chez nos clients



### Novares

(industrie, 23 pays multi-filiales)

- Organisation et IGA unifiés dans 23 pays.
- Référentiel unique à jour en continu.
- Validation RH passée de plusieurs semaines à 24 h après alignement de l'organisation.



### Elis

(ERP, déploiement international)

- Accès ERP/SAP standardisés et automatisés sur un périmètre international.
- Droits délivrés 5× plus vite.
- Coûts d'administration ÷10, avec une gouvernance plus fiable des droits d'accès.



### Transdev

(référentiel fournisseurs / P2P)

- Référentiel fournisseurs fiabilisé.
- Plus de 1 000 demandes par mois traitées via workflows, OCR/RPA et contrôles.
- Traçabilité et conformité renforcées.

**ROK a accompagné 7 000 agents HSBC sur l'alignement à un référentiel unique conforme aux exigences ACPR, avec une gouvernance structurée des postes, processus et droits d'accès.**

**Concrètement chez vous :** mêmes mécanismes activables pour gouverner les droits d'accès, fiabiliser les référentiels, automatiser les contrôles réguliers des accès IT et produire des preuves d'audit à tout moment.



## Modules clés ROK

### A. Cartographie des accès

- Vue par collaborateur : accès actifs, source, justification, historique.
- Vue par application : utilisateurs autorisés, niveau de droits, anomalies.
- Vue par poste : droits associés dans l'organigramme.
- Détection des accès orphelins, droits excessifs et comptes dormants.

### B. Cycle de vie des identités

- Gestion des arrivées, mobilités et départs depuis les événements RH.
- Attribution et retrait automatiques des droits selon le poste, le site et le type de profil (collaborateur, prestataire, intérimaire, compte technique).
- Gestion des collaborateurs, prestataires, sous-traitants, comptes techniques et accès temporaires.
- Suppression immédiate des accès lors d'un départ ou d'un changement de poste.

### C. Provisioning automatique

- Attribution des droits applicatifs, documentaires et processus selon l'organisation.
- Provisioning vers ERP, CRM, SIRH, applications métiers, GED, SharePoint, drives partagés et workflows ROK.
- Réduction des tickets IT, des erreurs manuelles et des délais d'attribution.

### D. SoD, risques et conformité

- Détection des conflits de séparation des tâches en temps réel.
- Revues d'accès périodiques avec validation managériale.

- Contrôles compensatoires documentés.
- Rapports de conformité disponibles à la demande : SOX, RGPD, ISO 27001, NIS2.

#### E. Gestion SAP, rôles et licences

- Gestion des profils, rôles, autorisations et SoD SAP depuis ROK.
- Détection des conflits avant attribution des droits.
- Historique complet des attributions prêt pour audit SAP.
- Identification des licences inutilisées ou sous-utilisées, libération lors d'un départ ou d'un changement de rôle.

#### F. Accès aux documents et processus

- Droits documentaires liés au poste et aux processus associés.
- Héritage automatique des droits lors des mobilités.
- Accès aux workflows ROK selon les rôles autorisés.
- Vision unifiée des droits applicatifs, documentaires et processus.

#### G. Sécurité organisationnelle by design

- Les accès découlent de la structure réelle de l'entreprise.
- La cohérence organisation, droits et processus est maintenue en continu.
- La sécurité devient une conséquence de l'architecture, et non un module ajouté après coup.



#### Bénéfices attendus

- **Sécurité** : réduction des droits excessifs, comptes dormants, accès orphelins et accès hors procédure.
- **Conformité** : preuves d'audit disponibles en continu, revues standardisées, SoD contrôlées.
- **Efficacité IT** : moins de tickets, moins de reprises, attribution et retrait des droits plus rapides.
- **Maîtrise SAP** : rôles, profils, SoD et licences mieux gouvernés, avec historique complet.
- **Pilotage** : tableaux de bord sur les accès actifs, accès à risque, revues en cours et anomalies.
- **Cohérence organisationnelle** : chaque droit est relié à un poste, une application ou un processus identifié.
- **Réduction du Shadow IT** : moins d'applications hors gouvernance, plus de visibilité sur les flux métier réels.



Et si nous organisions un échange de 15 minutes ?



**Qui fait quoi. Qui accède à quoi. Tout reste aligné.**  
ROK Solution

[rok-solution.com](http://rok-solution.com)