AYI NEDJIMI Consultants

Identity Governance IGA : automatiser le cycle de vie

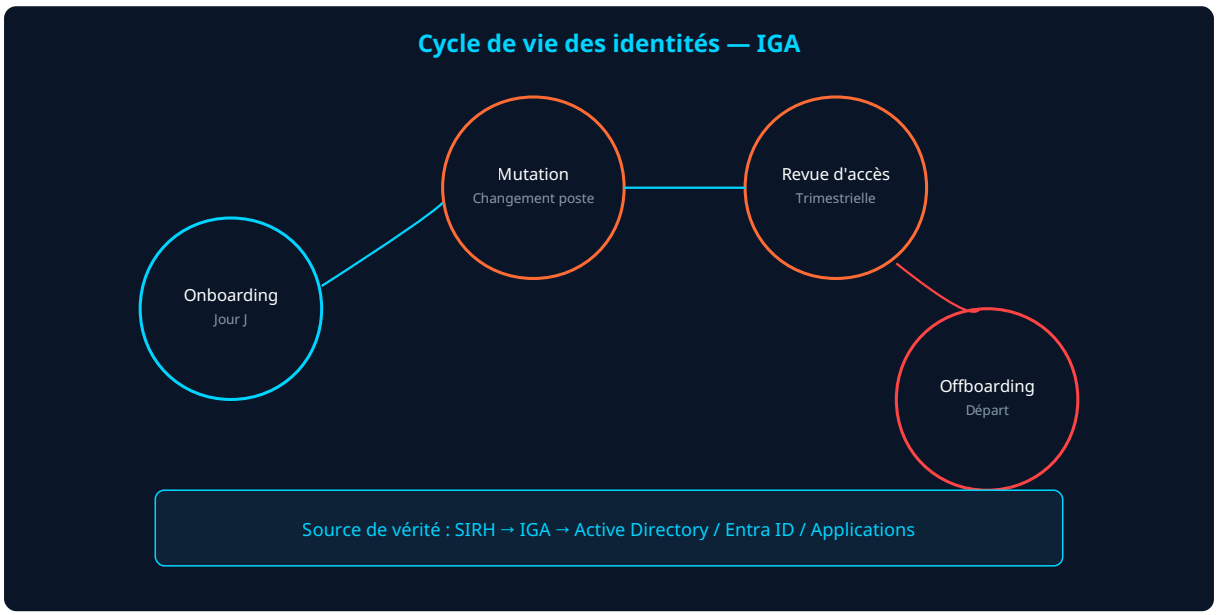
Catégorie : IAM et Gestion des Identités Lecture : 6 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Automatisez le cycle de vie des identités avec l'IGA : provisioning, revue d'accès, séparation des tâches et conformité réglementaire en entreprise.

Un collaborateur rejoint l'entreprise lundi matin et attend trois jours pour obtenir ses accès. Un prestataire parti depuis six mois conserve son compte Active Directory actif. Un manager cumule les droits de ses quatre précédents postes sans que personne ne s'en aperçoive. Ces scénarios, vous les connaissez. Ils illustrent le problème fondamental que l'Identity Governance and Administration (IGA) résout : la gestion automatisée du cycle de vie des identités et de leurs droits d'accès. L'IGA va au-delà du simple provisioning. Elle englobe la certification des accès, la séparation des tâches, la détection des droits orphelins et la conformité réglementaire. Ce guide vous présente les concepts clés, les architectures de référence et les stratégies de déploiement pour transformer votre gestion des identités d'un processus manuel et error-prone en un système automatisé, auditable et conforme. Nous nous appuyons sur des retours d'expérience concrets avec les solutions leaders du marché : SailPoint, Saviynt, Omada et les fonctionnalités natives d'Entra ID Governance.

Points clés à retenir

- L'**IGA** automatise quatre processus critiques : onboarding, mutation, offboarding et revue d'accès
- Le **provisioning automatique** réduit le délai d'attribution des accès de 3 jours à 15 minutes
- Les **revues d'accès** trimestrielles détectent en moyenne 12% de droits obsolètes par campagne
- La **séparation des tâches** (SoD) prévient les fraudes par cumul de droits incompatibles
- Le ROI d'un projet IGA se mesure en productivité RH/IT et en conformité réglementaire



Le cycle de vie des identités en quatre phases

Le cycle de vie d'une identité numérique commence avant même le premier jour du collaborateur. La phase d'**onboarding** démarre dès la validation de l'embauche dans le SIRH. Le système IGA détecte la création du dossier RH, calcule les droits d'accès en fonction du poste, du département et de la localisation, puis provisionne automatiquement les comptes AD, la boîte mail Exchange, les licences Microsoft 365, les groupes de sécurité et les accès applicatifs métier. Le collaborateur arrive lundi matin et tout est prêt.

La phase de **mutation** gère les changements de poste. Quand le SIRH enregistre un changement de fonction, l'IGA recalcule les droits : ajoute les nouveaux accès, retire ceux de l'ancien poste. C'est ici que la plupart des organisations échouent sans IGA — les droits s'accumulent sans jamais être retirés. L'accumulation de privilèges dans Active Directory est un vecteur d'attaque majeur que l'IGA adresse directement.

Provisioning automatique : architecture et connecteurs

L'architecture de provisioning repose sur trois couches. La *source autoritaire* (SIRH : Workday, SAP SuccessFactors, Lucca) fournit les données de référence sur les identités. Le *moteur IGA* applique les règles de calcul des droits (role mining, politiques de provisioning). Les *connecteurs* cibles propagent les modifications vers Active Directory, Entra ID, les applications SaaS (Salesforce, ServiceNow) et les systèmes on-premise.

Le connecteur SCIM 2.0 est le standard pour le provisioning vers les applications cloud. Pour Entra ID, le connecteur natif Microsoft gère le provisioning bidirectionnel. Pour Active Directory on-premise, des agents de provisioning locaux assurent la synchronisation. La latence cible : moins de 15 minutes entre le changement SIRH et la création effective des comptes. Les solutions comme **SailPoint IdentityNow** ou **Saviynt** atteignent cette cible grâce à des pipelines événementiels plutôt que des synchronisations batch.

Revues d'accès : certification et remédiation

Les **revues d'accès** (access certifications) sont le contrôle périodique qui vérifie que chaque utilisateur dispose uniquement des droits nécessaires à sa fonction actuelle. Une campagne de revue type cible un périmètre spécifique : les accès aux applications financières, les comptes à privilèges, les groupes de sécurité sensibles. Chaque manager reçoit la liste des droits de ses subordonnés et doit confirmer ou révoquer chaque accès.

Les chiffres parlent d'eux-mêmes : une première campagne de revue détecte généralement entre 10% et 15% de droits obsolètes. Les comptes orphelins (collaborateurs partis sans offboarding complet) représentent en moyenne 8% du total. Ces chemins d'accès non maîtrisés sont une aubaine pour les attaquants. La fonctionnalité Access Reviews d'**Entra ID Governance** automatise ce processus pour les ressources cloud, tandis que les solutions IGA spécialisées couvrent aussi le périmètre on-premise.

Séparation des tâches et détection de conflits

La *séparation des tâches* (Segregation of Duties, SoD) est un principe de contrôle interne qui interdit à une même personne de cumuler des droits incompatibles. Exemple classique : un utilisateur ne devrait pas pouvoir à la fois créer un fournisseur et valider un paiement dans l'ERP. Sans contrôle SoD automatisé, ces conflits s'accumulent silencieusement. Un audit financier les découvre — généralement au pire moment.

L'IGA implémente les contrôles SoD via des matrices de conflits configurées par l'équipe conformité. Chaque demande d'accès est vérifiée en temps réel contre ces matrices. Si un conflit est détecté, la demande est bloquée ou escaladée vers un approbateur habilité avec une justification obligatoire. Les solutions comme SailPoint et Saviynt offrent des moteurs SoD intégrés avec des bibliothèques de règles préconfigurées pour les ERP courants (SAP, Oracle). La conformité RGPD impose aussi des restrictions d'accès aux données personnelles que la SoD permet de faire respecter.

Processus IGA	Manuel	Automatisé	Gain
Onboarding complet	3-5 jours	15 minutes	-97% de délai
Offboarding	1-7 jours	Instantané	Risque éliminé
Revue d'accès (1000 users)	3 semaines	5 jours	-76% d'effort
Détection de conflits SoD	Audit annuel	Temps réel	Prévention vs détection
Rapport de conformité	2 jours	1 clic	Auditabilité permanente

Comparatif des solutions IGA du marché

SailPoint IdentityNow est le leader reconnu par Gartner, avec la couverture fonctionnelle la plus large et un écosystème de connecteurs impressionnant (200+). Son positionnement premium le destine aux grandes organisations (> 5000 identités). **Saviynt** se distingue par son

approche cloud-native et sa convergence IGA/PAM/CIEM, idéale pour les environnements multi-cloud. **Omada Identity** cible le marché européen avec une conformité RGPD native et un déploiement plus rapide que les leaders. Pour les organisations déjà fortement investies dans l'écosystème Microsoft, **Entra ID Governance** offre des fonctionnalités IGA intégrées (access reviews, entitlement management, lifecycle workflows) sans outil tiers.

Le choix dépend de trois critères : la taille de votre organisation, la complexité de votre paysage applicatif et votre budget. Un vCISO externalisé peut vous accompagner dans l'évaluation et le cadrage du projet IGA. Le Magic Quadrant Gartner IGA fournit une analyse comparative actualisée chaque année.

Déploiement IGA : méthodologie et pièges

Le déploiement d'une solution IGA suit une méthodologie en cinq phases. La phase de cadrage (4-6 semaines) définit le périmètre, les cas d'usage prioritaires et l'architecture cible. La phase de modélisation (6-8 semaines) cartographie les rôles métier, les droits applicatifs et les règles SoD. La phase de configuration (8-12 semaines) installe la solution, configure les connecteurs et implémente les workflows. La phase de pilote (4 semaines) teste sur un périmètre restreint. La phase de déploiement (4-8 semaines) généralise progressivement.

Les pièges classiques : vouloir tout automatiser dès le départ (commencez par 3-5 applications critiques), négliger la qualité des données SIRH (garbage in, garbage out), sous-estimer la conduite du changement auprès des managers (ils doivent approuver les revues d'accès). Un business case solide pour le COMEX est indispensable car un projet IGA mobilise des ressources sur 6 à 12 mois.

Questions fréquentes sur l'Identity Governance

Quelle différence entre IAM, IGA et PAM ?

L'IAM est le cadre global de gestion des identités et des accès. L'IGA est le sous-ensemble qui gère la gouvernance : cycle de vie, revues d'accès, séparation des tâches, conformité. Le PAM gère spécifiquement les comptes à privilèges élevés. Ces trois disciplines sont complémentaires : l'IGA provisionne les comptes, l'IAM gère l'authentification, le PAM sécurise les accès critiques. Un programme identité mature implémente les trois.

Comment gérer les identités non-humaines dans l'IGA ?

Les comptes de service, les API keys et les identités machine représentent souvent plus de 50% des identités d'une organisation. L'IGA doit les intégrer avec un cycle de vie dédié : propriétaire identifié, revue semestrielle, rotation automatique des credentials. Les solutions modernes comme Saviynt proposent des modules spécifiques pour les non-human identities avec découverte automatique et classification par risque.

Peut-on déployer l'IGA avec Entra ID Governance seul ?

Pour les organisations nativement cloud avec un paysage applicatif limité (< 50 applications), Entra ID Governance couvre les besoins essentiels : lifecycle workflows, access packages, access reviews et entitlement management. Pour les environnements hybrides complexes avec des applications on-premise et des exigences SoD avancées, une solution IGA dédiée comme SailPoint ou Saviynt reste nécessaire. L'approche hybride — Entra ID Governance pour le cloud, solution IGA pour le legacy — est fréquente.

Sources et références : ANSSI · MITRE ATT&CK

Synthèse et recommandations pratiques

L'IGA transforme la gestion des identités d'un fardeau administratif en un avantage compétitif. Commencez par le cas d'usage à plus fort impact : l'automatisation de l'offboarding (zéro compte orphelin). Enchaînez avec le provisioning automatique de l'onboarding (satisfaction des nouveaux arrivants). Puis lancez les revues d'accès trimestrielles pour nettoyer les droits accumulés. Chaque étape renforce votre posture de sécurité et simplifie la conformité réglementaire. La maturité IGA se construit par itérations successives, pas par big bang. Pour approfondir les aspects réglementaires, consultez les recommandations ANSSI sur la gestion des identités.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr