WAVESTONE

IDENTITY AND ACCESS GOVERNANCE

LA GESTION DES IDENTITÉS A-T-ELLE ENFIN DES YEUX ET DES OREILLES ?

À n'en pas douter, un projet de gestion des identités est un projet de transformation : processus opérationnels, organisations et moyens informatiques sont amenés à être analysés, évalués et enfin améliorés. Si ce domaine peut se prévaloir de très belles réussites, il est également entaché d'échecs, a minima partiels. L'IAG détient-elle une partie des clés du succès de ces projets ?

D'OÙ PROVIENNENT LES ÉCHECS EN MATIÈRE D'IAM ? ET POURQUOI PARLER D'IAG ?

L'analyse de ces échecs révèle deux causes majeures. La première : l'inadéquation entre les ambitions visées et les moyens alloués. Elle se traduit concrètement par l'absence de gouvernance et de sponsoring transverse, de vision stratégique moyen terme reflet des enjeux métier ou encore de dynamique de construction et d'amélioration dans la durée.

La seconde : l'absence de métrique et d'outillage simple permettant de démontrer et de communiquer sur la situation réelle des habilitations, les apports ou encore le bien-fondé des choix retenus. C'est à ce second écueil que doit répondre l'IAG (Identity and Access Governance). Par effet de rebond, elle doit également fournir les indicateurs opérationnels pour mieux mobiliser les bons relais dans le management et dans les métiers.

AUTEUR

PATRICK MARACHE
patrick.marache@wavestone.com

QU'EST-CE QUE L'IAG ? QUELLES FONCTIONNALITÉS EN ATTENDRE ?

De manière simplifiée, l'IAG (parfois également appelée Identity & Access Intelligence ou encore Identity Analytics & Intelligence voire Governance Risk & Compliance) vise à fournir les moyens nécessaires au pilotage des données et des usages de l'IAM.

Pour ce faire, elle se positionne comme une « tour de contrôle transverse », alimentée autant par les référentiels Qualité et les règles du contrôle interne que les données de l'IAM et des applications. Au-delà du contrôle, l'IAG doit également offrir des moyens d'analyse avancés, puis permettre de conduire les actions de remédiation.

> « Ce qui ne se mesure pas ne s'améliore pas »
>
> E. DEMING

Concrètement, une solution d'IAG va importer l'ensemble des comptes et habilitations pour les comparer avec les règles métiers ; et en les croisant avec les schémas d'organisation, elle proposera des bilans structurés des écarts et des risques.

Comme illustré sur le schéma ci-contre, elle doit ainsi permettre :

- prendre en compte l'ensemble des règles et contrôles métiers de l'entreprise (combinaisons toxiques de pouvoirs, accès limités à certaines populations, certaines plages horaires…) ;
- corréler et présenter les données opérationnelles de l'IAM, et de chaque application, à l'aune de ces règles ;
- organiser et suivre les actions de remédiation nécessaires à la correction des éventuels écarts.

C'est donc un service essentiel pour s'assurer du bon fonctionnement et du bon usage du système IAM, corriger les biais de données et, *in fine*, améliorer la qualité perçue du service rendu.

C'est également une clé pour réaliser rapidement un diagnostic de l'existant et ainsi déclencher une prise de conscience des efforts à réaliser.

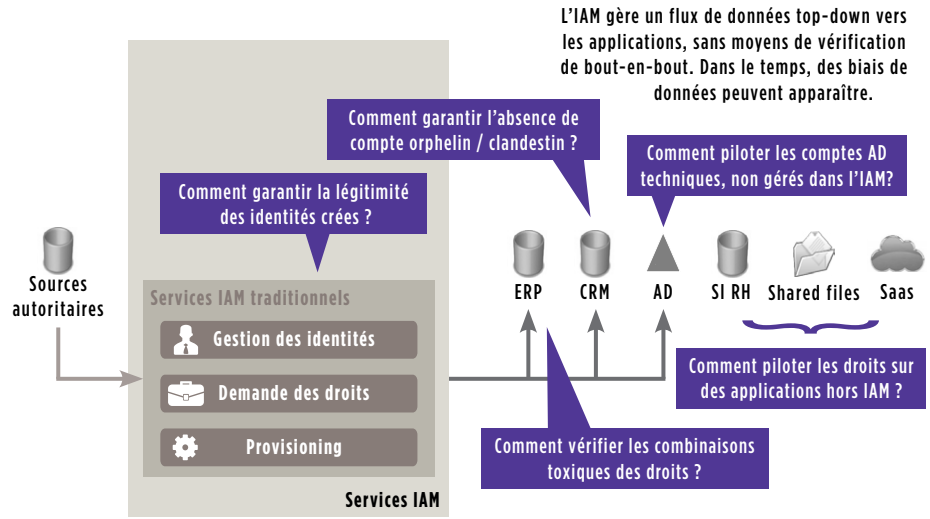
DANS QUELS CONTEXTES L'IAG EST-ELLE PERTINENTE ?

Une approche IAG se révèle intéressante autant pour les organisations n'ayant pas engagé de démarche IAM, que pour celles ayant déjà conduit certains chantiers.

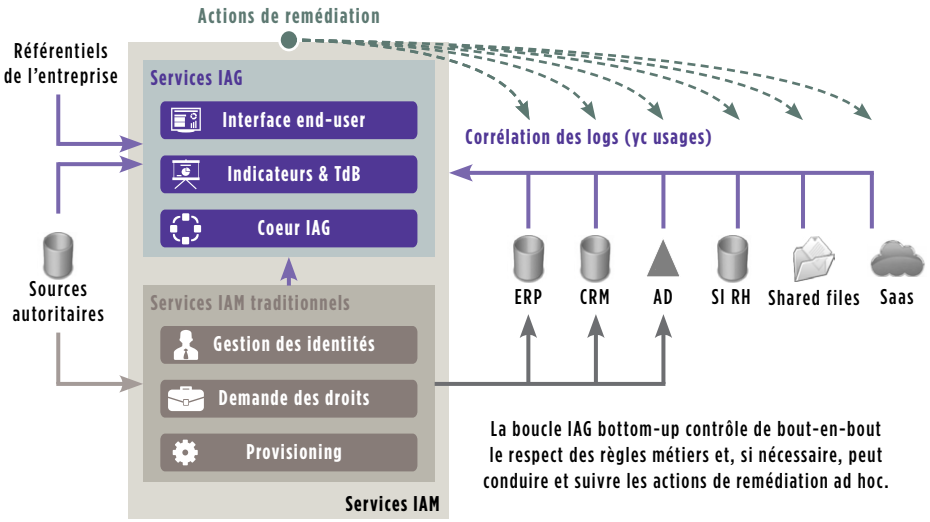
Pour les premières, le recours à l'IAG permet de conduire des démarches plus opérationnelles, en prise directe et immédiate avec l'existant en matière de comptes et de droits sur les applicatifs. Ainsi, cette approche *bottom-up* permet de réaliser un diagnostic concret, argumenté d'exemples parlants. La prise de conscience est donc simplifiée pour les Métiers. L'ensemble des ingrédients est alors réuni pour engager une démarche d'amélioration plus structurante.

Pour les secondes, nombre d'initiatives pâtissent d'un manque d'indicateurs de suivi d'usage et de qualité. Ce manque est nuisible à la « qualité perçue » du système IAM. Il se révèle également des plus handicapants en cas de suspicion de dysfonctionnement et lors des phases d'investigations associées. Ainsi, l'IAG se pose comme une réponse à ce manque de visibilité.

Services IAM « traditionnels » seuls



Positionnement des services IAG



COMMENT ADAPTER SA DÉMARCHE PROJET POUR EN TIRER LE MEILLEUR PARTI ?

Pour tirer le meilleur parti de l'IAG, il convient d'adapter l'approche projet au contexte.

Pour simplifier, nous pouvons définir 4 approches-types, selon l'objectif visé (maîtrise des risques ou efficacité opérationnelle) et l'angle d'analyse retenu (règles prédéfinies ou analyse de données).

Bien évidemment, les projets d'IAG mélangent souvent plusieurs de ces approches-types. Encore faut-il ne pas perdre de vue les objectifs initiaux. Réalisons un tour d'horizon de ces différentes approches.

L'approche « mise sous contrôle de l'existant »

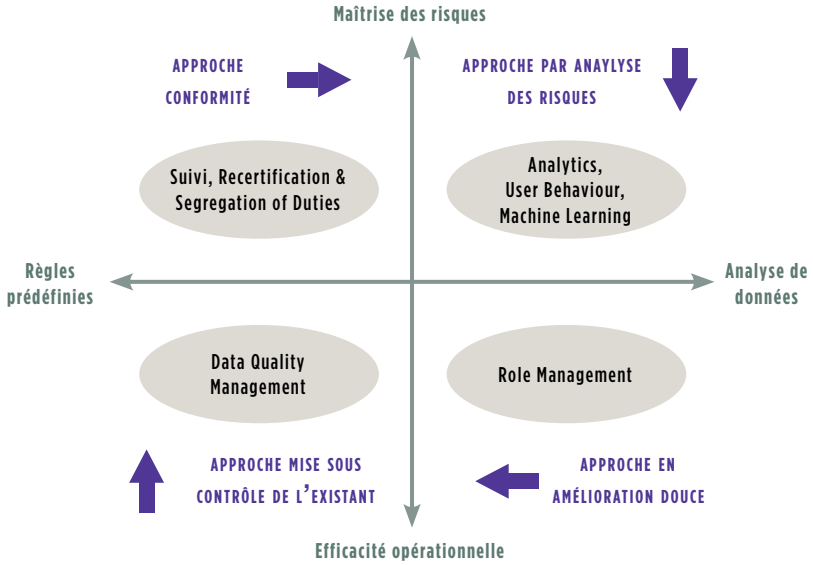
Cette approche vise à vérifier l'efficacité opérationnelle de l'IAM par rapport aux règles prédéfinies (format des identifiants, nomenclatures des comptes, droits réels…).

C'est une démarche de mise en qualité des données. Elle consiste à comparer les données réelles d'une part (comptes dans les applications…) et les référentiels qui régissent l'IAM (liste des demandes d'habilitations…).

Pour les organisations ne disposant pas de service IAM, cette approche permet de s'assurer de la bonne réalisation des opérations manuelles. Elle permet de détecter et de corriger les éventuels biais survenus au cours du temps : erreur de saisie dans le nom d'un utilisateur, erreur dans l'attribution d'un droit, non-suppression d'un compte en cas de départ…

Pour les organisations possédant des outils IAM, elle permet de s'assurer du bon fonctionnement de ce dernier. Elle sera notamment d'une aide précieuse lors des investigations en cas de dysfonctionnement ou de plainte d'un utilisateur. En effet, l'IAG conserve l'historique des identités et des droits. Elle permet donc d'identifier immédiatement si une identité a été modifiée, pour quelles raisons et quelles en sont les conséquences.

Quelles plus-values attendre de ces nouvelles fonctionnalités ?



Enfin, cette approche de l'IAG permettra de s'assurer de la bonne prise en compte des événements non-standards (rachat de société et fusion des bases d'identités…) traités dans l'IAM via batch technique et souvent dépourvus de contrôles.

L'approche conformité

Cette approche vise à donner de la visibilité sur les droits sensibles et à s'assurer du respect des règles internes et du cadre réglementaires liés aux habilitations.

C'est une approche qui peut être conduite que l'on dispose ou non d'une solution d'IAM conventionnelle. Elle consiste à consolider les droits réels des applications sensibles pour pouvoir les comparer aux règles de l'entreprise.

Plusieurs actions sont ensuite envisageables : suppression des droits suspects, demande de dérogation temporaire, re-certification des droits à risques. Ou encore, si la règle s'avère inapplicable, adaptation de celle-ci et des moyens de mitigation associés.

Un point remarquable est que l'IAG s'inscrit dans une démarche d'audit, *a posteriori* de la demande d'habilitation. Cela permet de simplifier grandement les processus d'approbation et de certification ainsi que les workflows de gestion des demandes ; les cas d'exception pourront alors être détectés et instruits dans une démarche d'audit et de révision de droits.

Enfin, selon son contexte, une organisation devra choisir où porter son effort. Sur le stock, c'est à dire sur la mise en conformité des droits déjà attribués ; ou sur le flux, c'est à dire sur les nouvelles attributions de droits sensibles. En effet, l'IAG conservant les historiques des droits, elle pourra identifier quotidiennement les nouvelles attributions de droits et déclencher les processus *ad hoc*.

Une approche par le flux, si elle ne permet pas de traiter l'existant déjà attribué, s'avère beaucoup plus simple à conduire : les demandes sont récentes, les approbateurs présents… Il est donc aisé de comprendre le contexte et les raisons ayant conduit à la demande. Elle pourra également constituer un premier palier *quick-win* du projet IAG.

L'approche par l'analyse des risques

Cette approche s'appuie sur des fonctionnalités d'analyse et de corrélation de données afin d'améliorer la maîtrise des risques, et en particulier détecter des fraudes. Elle vise donc à mettre en lumière des risques potentiels sans s'appuyer sur des règles ou des schémas de fraude préconfigurés.

Ainsi, les solutions les plus innovantes vont combiner des approches Big Data, Machine Learning, UBA (User Behaviour Analytics) afin de détecter des « comportements à risques » ou, du moins, en décalage par rapport aux comportements les plus courants. Une analyse spécifique de chaque alerte est ensuite nécessaire afin de séparer les cas réels de fraude des faux-positifs.

À titre d'illustration, ce type d'analyse pourra détecter un « balayage » de répertoires réseaux (indice potentiel de fuites de données) ou encore des risques de collusion (si, par exemple, les demandes d'achat d'un bénéficiaire sont systématiquement acceptées par la même personne au sein de la cellule de validation).

Ces fonctionnalités peuvent également être utilisées *a posteriori*, après qu'une fraude ait eu lieu. Dans ce cas, l'analyse des données historiées pourra permettre de comprendre le schéma de fraude. Elle pourra également identifier des indices et des comportements précurseurs à la fraude ; et ainsi lever des alertes ou implémenter des contrôles supplémentaires pour éviter de reproduire ce schéma de fraude.

L'approche en amélioration douce

L'approche en amélioration douce fait le choix de l'amélioration continue pour offrir une meilleure efficacité opérationnelle. Pour cela, elle analyse et compare les pratiques IAM constatées au quotidien dans l'entreprise. Elle vise ainsi à améliorer l'IAM en optimisant ses processus et la modélisation des habilitations.

À titre d'illustration, quelques exemples d'analyse de pratiques constatées : deux profils d'accès toujours possédés simultanément et qui pourraient constituer un profil métier, profils possédés par moins de 0,1% des personnes et qui pourraient être supprimés ou masqués, profils métiers redondants en termes de profils d'accès, profils possédés par plus de 80% des personnes d'une équipe et qui pourraient être recommandés en cas d'embauche…

Sur la base de ces constats réels, il sera plus simple d'obtenir l'adhésion des métiers et des propriétaires d'application et ainsi faire évoluer la solution vers plus de pragmatisme.

Cette approche peut paraître plus avancée, et donc requérir un niveau de maturité important. Dans la pratique, les solutions d'IAG sont suffisamment souples pour permettre des démarches empiriques, en échange constant avec les Métiers.

Combien de temps pour une démarche IAG ?

- Quelques semaines suffisent pour mettre en lumière les menaces et les incohérences majeures portées par les habilitations ;
- Quelques mois permettent de corriger ces écarts ;
- Mais c'est dans la durée que doit se conduire une stratégie IAG, pour inscrire sa gestion des identités dans une démarche vertueuse d'amélioration durable.

Et le premier objectif n'est pas de tout analyser et comparer. Mais bien de se concentrer sur les cas les plus courants, les plus visibles, les plus significatifs pour les utilisateurs au quotidien.

ALORS, L'IAG, « POTION MAGIQUE » POUR RÉUSSIR SON PROJET DE GESTION DES IDENTITÉS ?

En informatique, rien n'est magique ! Toutefois, avec ses fonctionnalités avancées d'analyse et de restitution, l'IAG offre enfin les moyens de mesurer l'efficacité de sa gestion des identités. Et, au prix d'une démarche adaptée, elle permet une prise de conscience parlante par les Métiers et le management.

Les Directions en charge des processus internes, de la qualité ou encore le contrôle interne ont alors un rôle clé de sponsoring à jouer. Elles doivent supporter les initiatives IAG et garantir leur pérennité dans le temps.

En effet, quelques semaines suffisent pour mettre en lumière les menaces et les incohérences majeures portées par les habilitations. Et quelques mois permettent de corriger ces écarts. Mais c'est dans la durée que doit se conduire une stratégie IAG, pour inscrire sa gestion des identités dans une démarche vertueuse d'amélioration durable.

WAVESTONE

www.wavestone.com

Wavestone est un cabinet de conseil, issu du rapprochement de Solucom et des activités européennes de Kurt Salmon (hors consulting dans les secteurs retail & consumer goods). Il figure parmi les leaders indépendants du conseil en Europe.

La mission de Wavestone est d'éclairer et guider ses clients dans leurs décisions les plus stratégiques en s'appuyant sur une triple expertise fonctionnelle, sectorielle et technologique.