Guide des dirigeants IAM sur la gouvernance et l'administration des identités

16 août 2023 - G00740533 - 16 minutes de lecture

Par et 1 de plus Brian Guthrie , David Collinson ,

IGA est un marché mature et complexe de gestion des identités et des accès, en pleine évolution. Les responsables de la sécurité et de la gestion des risques responsables de l'IAM devraient adopter les meilleures pratiques et adopter de nouvelles fonctionnalités telles que l'analyse des identités pour une gouvernance plus autonome et prédictive.

Hypothèse de planification

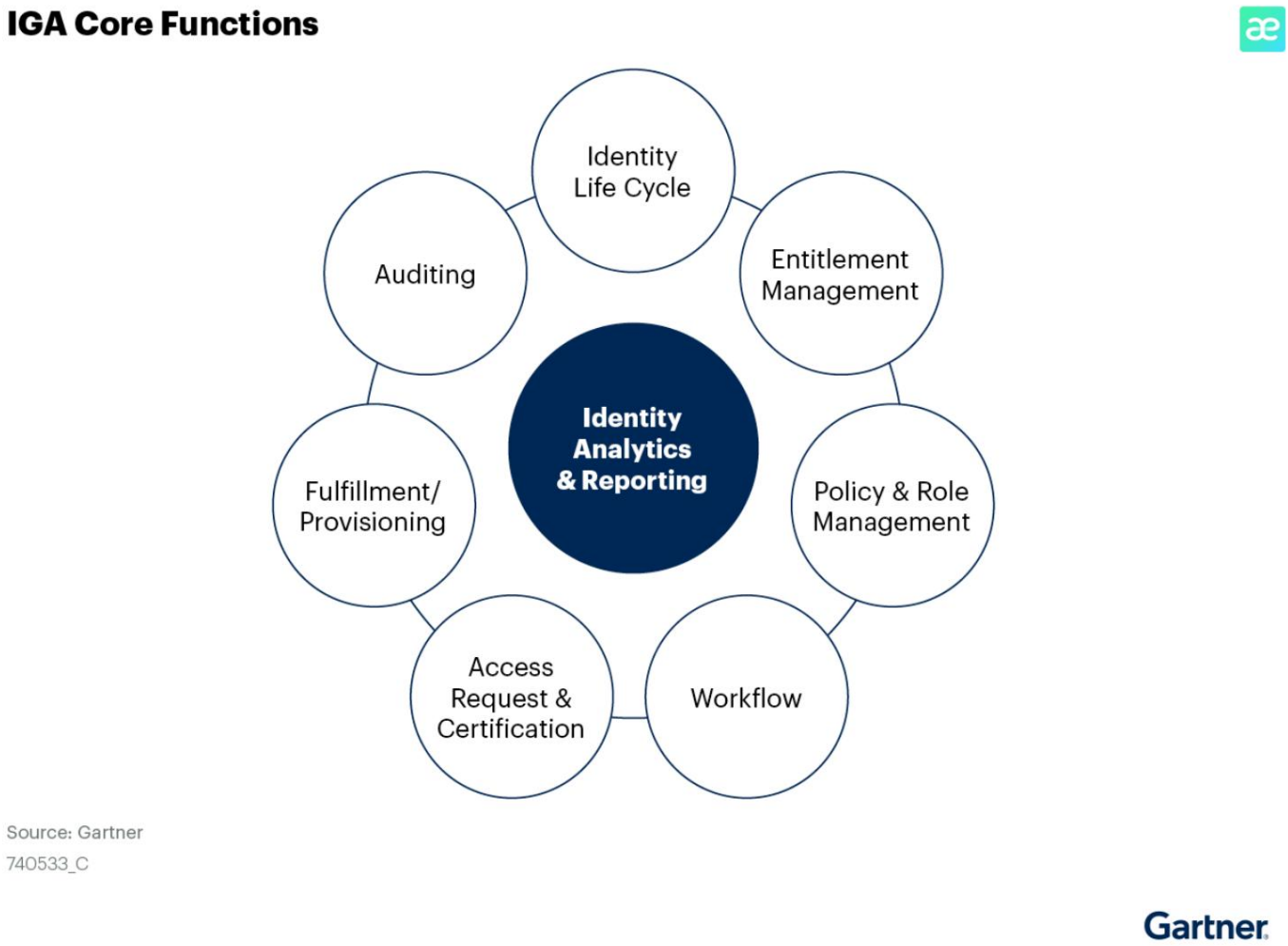
Analyser

La discipline IGA existe pour garantir que les bonnes personnes obtiennent le bon accès aux bonnes ressources (par exemple, les applications et les données) au bon moment et pour les bonnes raisons. Les IGA englobent les cycles d'identité et de droits au moment de l'administration, chacun incluant des analyses.

IGA est un élément fondamental de la stratégie de gestion des identités et des accès (IAM) d'une organisation. IGA améliore la maturité des processus d'identité, facilite la conformité et réduit le risque d'accès non autorisé, et fournit également des contrôles plus visibles et plus efficaces pour les processus d'administration du cycle de vie des identités. Utilisez le Guide du marché de Gartner pour la gouvernance et l'administration des identités pour comprendre les capacités IGA, ainsi que les tendances futures, afin de prendre les meilleures décisions en matière d'outils pour leurs organisations.

Gartner recommande toujours d'envisager les outils IGA classiques et complets au cours des prochaines années, et ils devraient être l'approche privilégiée lors de la première mise en œuvre d'IGA , ou si toutes les fonctionnalités fournies par IGA sont nécessaires (voir Figure 1).

Figure 1 : Fonctions de base de l'IGA



Cependant, recherchez des produits et services qui incluent des innovations telles qu'une gouvernance autonome et prédictive, alimentée par l'analyse des identités. L'analyse de l'identité devrait être au centre de chaque initiative IGA. La plupart des nouvelles ventes sur le segment de marché IGA ont tendance à être des remplacements de produits compétitifs, mais en mettant l'accent sur le coût et le cloud.

Les capacités incontournables d'IGA :

- Gestion du cycle de vie des identités
- Processus de demande d'accès
- Analyses et rapports de base

Capacités standards d'IGA :

- Certification d'accès (également appelée attestation ou examen)
- Audit
- Gestion des politiques et des rôles
- Provisionnement via des connecteurs automatisés

- Contrôles de séparation des tâches (SOD)
- Orchestration du flux de travail
- Fonctionnalités de gestion des droits (découverte, gestion du catalogue des droits, enrichissement des données sur les droits, y compris les descriptions, les propriétaires et les évaluations des risques)

Capacités optionnelles d'IGA :

- Analyses avancées, pour permettre des améliorations rapides (modélisation/recommandations de règles de provisionnement de rôles, détection des violations SOD, recommandations d'approbation/certification d'accès, etc.)
- Enregistrement des identités et gestion des profils pour les identités/attributs non gérés par les systèmes sources RH
- Gestion des droits d'infrastructure cloud (CIEM)
- Possibilité d'intégration avec des outils d'autorisation pour permettre des décisions contextuelles en partageant la politique

IGA fournit également plusieurs fonctions auxiliaires, notamment la gestion des mots de passe, des capacités en libre-service pour la gestion des profils et la gestion des cas pour l'audit et la résolution des violations de politique, telles que SOD.

N'essayez pas de déployer les outils IGA par vous-même ou avec une équipe limitée ; attendez-vous à une quantité importante de services professionnels . Les services professionnels doivent être planifiés et attendus, car IGA est généralement l'initiative IAM la plus complexe et la plus coûteuse, avec de nombreux pièges potentiels, principalement dus à ses possibilités d'intégration et de personnalisation. Attendez-vous à de longs délais de mise en œuvre, augmentés par des changements de processus nécessaires qui nécessitent le parrainage de la direction. (Rapportez-vous à l'outil Gartner : liste des services professionnels IAM pour sélectionner un fournisseur.)

Face à l'augmentation du paysage des menaces, les adoptions IGA les plus réussies ont choisi de se concentrer davantage sur la sécurité et la gestion des risques, plutôt que sur l'automatisation des processus. Les IGA déployés qui donnent la priorité aux initiatives de sécurité et de gestion des risques sont souvent plus efficaces que ceux qui ne le font pas, et ils exploitent généralement l'analyse des identités pour montrer une meilleure valeur plus tôt dans le processus d'adoption. .

IGA est une solution complexe à un défi complexe. Équilibrer les risques liés à l'identité et améliorer l'efficacité des processus d'identité est un objectif difficile, mais réalisable.

Faits saillants de la recherche

Les défis liés à l'adoption d'IGA

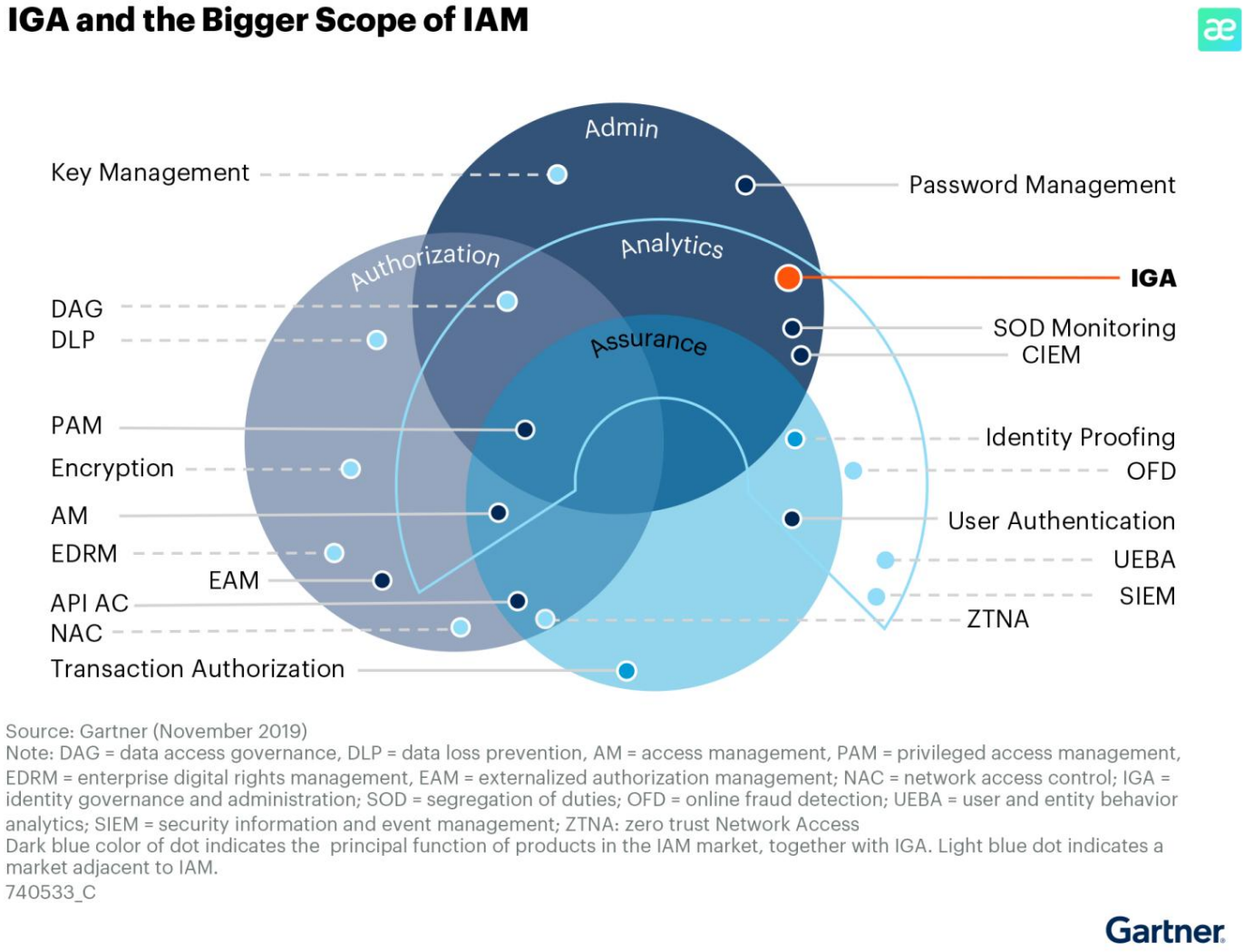
Les dirigeants de l'IAM doivent utiliser ce guide comme référence aux recherches, aux meilleures pratiques et aux recommandations de Gartner pour adopter l'IGA et relever les défis les plus courants, comme décrit par les sujets suivants :

- Comment les capacités IGA s'intègrent dans un programme IAM plus vaste
- Comment déployer IGA
- Comment utiliser l'analyse d'identité pour une IGA prédictive et autonome
- Comment définir un cadre efficace pour la politique d'entreprise et la gestion des rôles
- Comment choisir la meilleure stratégie d'exécution et d'approvisionnement
- définir des métriques IGA basées sur les KPI
- Comment choisir un outil IGA

Comment les capacités IGA s'intègrent dans un programme IAM plus vaste

L'image plus large de la portée d'un programme IAM comprend quatre domaines principaux : l'administration, l'autorisation, l'assurance et l'analyse (voir Figure 2). La discipline IGA fait partie du domaine d'administration d'IAM, qui récupère l'analyse et est responsable de l'établissement et de l'orchestration du processus de cycle de vie de l'identité et des fonctions principales IGA restantes décrites précédemment.

Figure 2 : IGA et la portée plus large de l'IAM



Un programme IAM bien organisé doit prendre en compte la manière dont l'IGA s'intègre aux initiatives adjacentes et doit :

- Fournir la structure de tous les services IAM.
- Coordonner les projets technologiques qui nécessitent des services liés à l'identité.
- Assurer l'alignement avec les besoins de l'entreprise.
- Assurer, par le biais de la gouvernance et de la gestion, la supervision du développement continu et des activités opérationnelles.

L'initiative IGA est l'un des nombreux programmes exécutés par le Bureau de gestion lieu programme du . Le choix d'un outil IGA et le déploiement d'un processus IGA doivent avoir IAM après la définition de la vision, de la feuille de route, de l'architecture et des analyses de rentabilisation IAM.

Découvrez plus de détails sur la façon de définir un programme IAM dans la recherche suivante :

Guide des dirigeants IAM sur la gouvernance et l'administration des identités

Comment déployer IGA

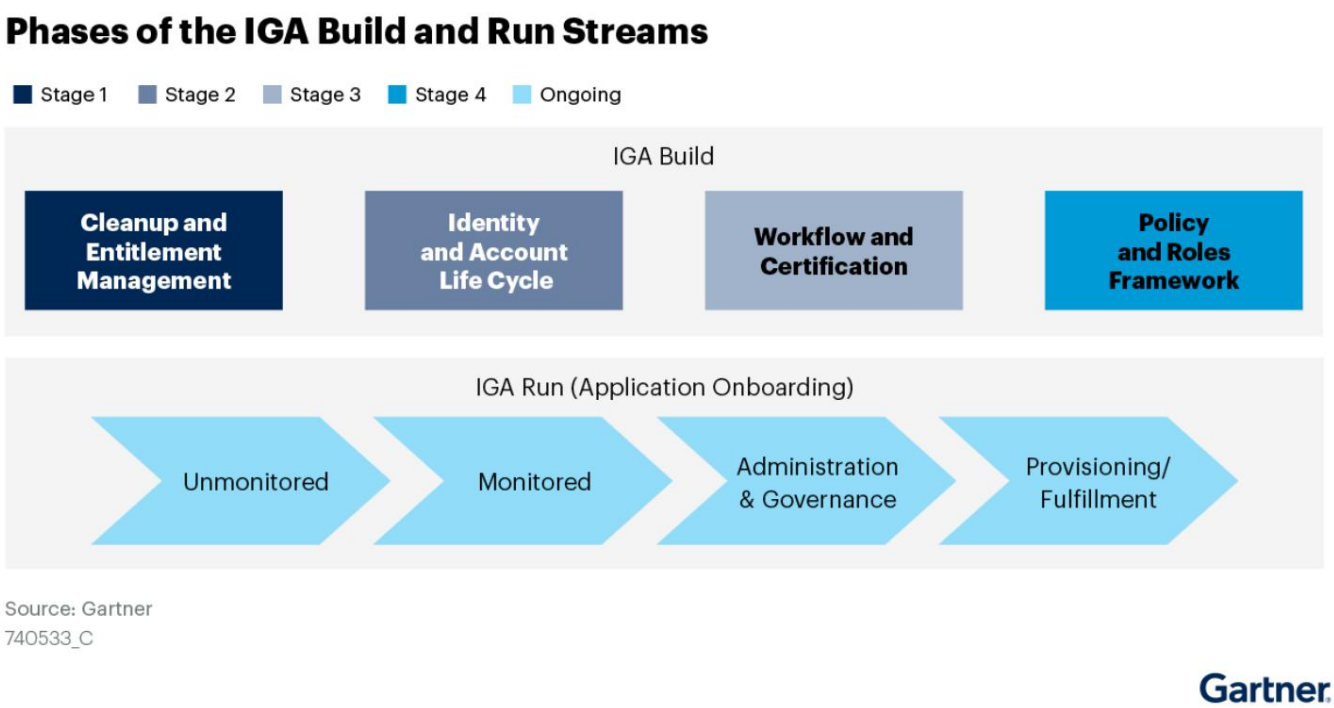
IGA doit être déployé en utilisant une approche « large et superficielle », plutôt que « étroite et approfondie », en déployant des capacités « minimales viables » sur plusieurs systèmes cibles pour tous les utilisateurs, puis en augmentant progressivement la profondeur des capacités. Il est préférable d'avoir une portée plus superficielle et plus large en termes de populations d'utilisateurs et de cibles intégrées, plutôt que d'aller trop loin dans les contrôles pour une très petite population d'utilisateurs ou seulement très peu d'applications. . Il est également recommandé de commencer par des capacités de gouvernance à plus forte valeur ajoutée, telles que des analyses permettant de signaler les comptes dormants et inutilisés, et de cibler l'automatisation plus tard dans le programme, une fois les problèmes de qualité des données. et les risques plus importants de privilèges inutiles atténués.

Le modèle de planification du déploiement de la gouvernance et de l'administration des identités de Gartner maximise la valeur et minimise les risques

Les responsables de la sécurité et de la gestion des risques sont impatients face aux déploiements IGA qui apportent trop peu d'avantages commerciaux et qui sont trop lents. Les responsables de l'IAM doivent suivre une approche méthodique, mais agile et basée sur les risques pour offrir des avantages supplémentaires au cours d'un programme de déploiement IGA.

Divisez le déploiement IGA en deux pistes distinctes : créer et exécuter (voir Figure 3).

Figure 3 : Phases des flux de création et d'exécution de l'IGA



Les quatre étapes recommandées pour la construction réduisent le risque d'adoption, en donnant la priorité aux activités qui serviraient d'étape fondamentale pour la suivante.

La piste d'exécution est l'endroit où ont lieu l'intégration des applications et des activités associées, telles que la gestion des droits et le provisionnement.

Au lieu d'une approche « tout ou rien », adoptez une approche itérative à plusieurs niveaux pour l'intégration des applications. Il est courant de voir les responsables IAM prioriser une sélection d'applications à intégrer, puis leur appliquer toutes les couches d'intégration (administration, gouvernance et automatisation du provisionnement) avant de passer à d'autres candidats. Un moyen plus efficace consiste à utiliser une analyse coûts-avantages et à définir quelles applications méritent d'être avancées jusqu'à l'automatisation du provisionnement, en fonction du volume des demandes.

La planification des déploiements IGA peut s'avérer difficile lorsque vous souhaitez maximiser la valeur et réduire les risques dès le début du processus. Les responsables de la sécurité et de la gestion des risques responsables de l'IAM doivent utiliser cette boîte à outils pour hiérarchiser l'ordre de leurs déploiements.

Adoptez une approche agile du déploiement IAM

La transformation et l'optimisation numérique des entreprises nécessitent une fourniture de services IAM rapide et incrémentielle. Les responsables de la sécurité et de la gestion des risques responsables de l'IAM doivent répondre à ces attentes ; DevOps et les méthodologies agiles fournissent des approches qui contribuent au développement de solutions réactives.

Comment utiliser l'analyse d'identité pour une IGA prédictive et autonome

La meilleure façon d'obtenir un retour sur investissement plus rapide sur un déploiement IGA est de se concentrer sur les stratégies d'absorption des risques plus tôt dans le processus, en donnant la priorité à l'analyse des identités.

Réponse rapide : Comment utiliser différents types d'analyse d'identité pour un IGA plus efficace

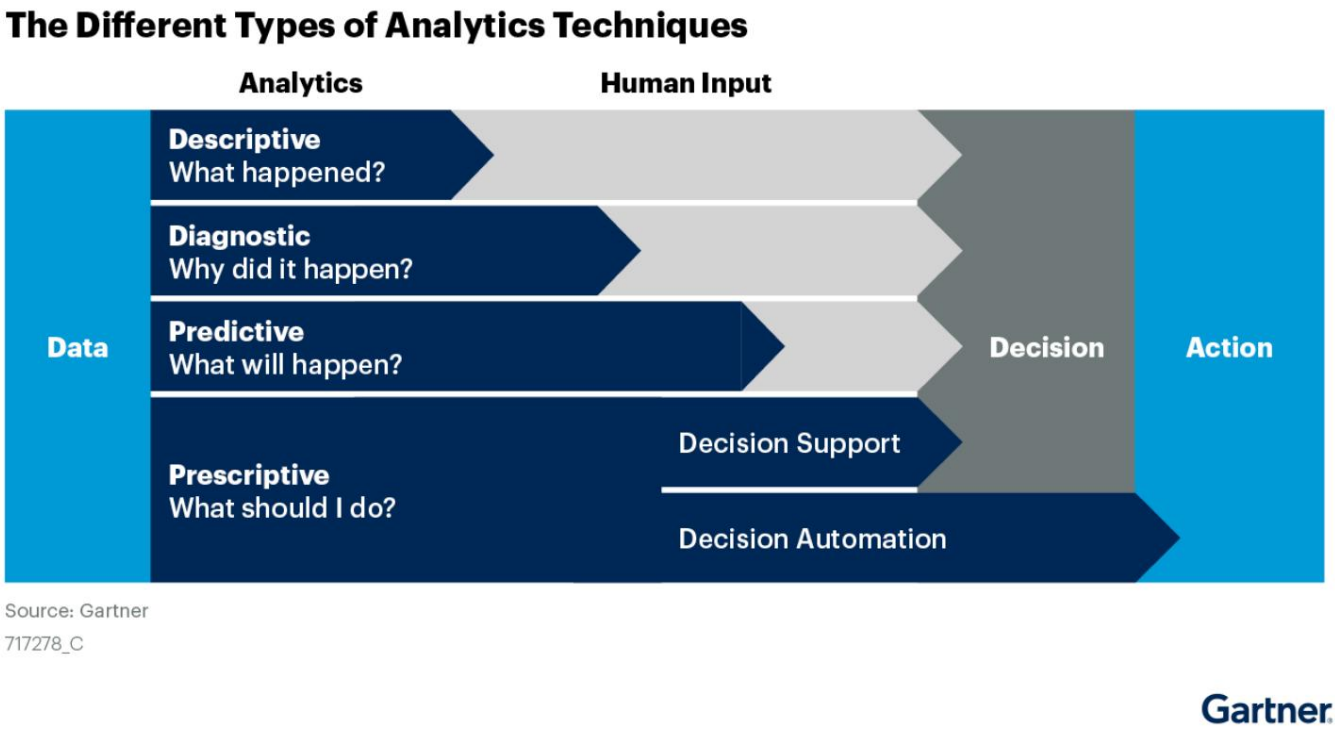
IGA est une initiative IAM complexe qui manque souvent ses objectifs en matière de fonctionnalité, de budget ou de calendrier. Les responsables de la sécurité et de la gestion des risques responsables de l'IAM doivent utiliser l'analyse des identités pour atténuer les risques liés à l'identité et obtenir des informations sur le déploiement des cas d'utilisation d'IGA.

Utiliser des mesures orientées sur les résultats pour générer de la valeur pour la gestion des identités et des accès

Tous les défis en matière de gouvernance et d'administration des identités ne seront pas résolus par les approches IGA traditionnelles. Les responsables de la sécurité et de la gestion des risques en charge de l'IAM devraient évaluer les marchés adjacents et naissants pour étendre l'IGA avec des analyses avancées afin de simplifier le poids de la gouvernance des identités.

L'analyse d'identité a gagné en popularité dans IGA au cours des cinq dernières années pour fournir des rapports soutenant la prise de décision humaine, traditionnellement utilisés pour l'exploration de rôles, par exemple, ou pour calculer un score de risque qui pourrait être utilisé pour expliquer ce qui s'est passé et pourquoi. La plupart des outils IGA n'ont fourni que des types d'analyses descriptives et diagnostiques (voir Figure 4).

Figure 4 : Les différents types de techniques d'analyse



Un tel outil IGA traditionnel ne peut rendre compte que de données historiques (et généralement statiques) pour calculer un score de risque.

Très peu de fournisseurs IGA ont commencé à proposer des fonctionnalités prédictives (telles que des recommandations qui anticipent les besoins des utilisateurs pour un droit particulier, compte tenu des similitudes entre de paires, par exemple).

L'analyse prescriptive existe dans certains outils d'analyse spécialisés et commence désormais à être utilisée sur des marchés naissants adjacents tels que la gestion des droits d'accès à l'infrastructure cloud (CIEM). CIEM étend IGA en simplifiant les tâches manuelles de gouvernance des accès aux droits très fins dans les scénarios IaaS multicloud.

Comment définir un cadre efficace pour la politique d'entreprise et la gestion des rôles

Un programme IGA réussi nécessitera un cadre formel pour la mise en œuvre et la gouvernance des politiques d'identité et des rôles dans l'entreprise. Les politiques d'identité et les rôles d'entreprise sont des éléments importants pour atteindre les demandes d'accès, les SOD et les objectifs d'exécution.

Bien qu'elles soient importantes pour des raisons de conformité et d'audit, et qu'elles fournissent des moyens d'atténuer les risques SOD, les approches traditionnelles de politique d'entreprise et de gestion des rôles (telles que le contrôle d' accès basé sur les rôles [RBAC]) se sont révélées moins efficaces dans des environnements dynamiques comportant des milliers de tâches à granularité fine. et des droits éphémères par utilisateur, tels que les environnements d'infrastructure cloud (IaaS). Dans ces situations, les outils d'analyse prescriptive fonctionnent sur les

Les anomalies, telles que le CIEM, constituent un bon complément à une approche traditionnelle de gestion des rôles en entreprise.

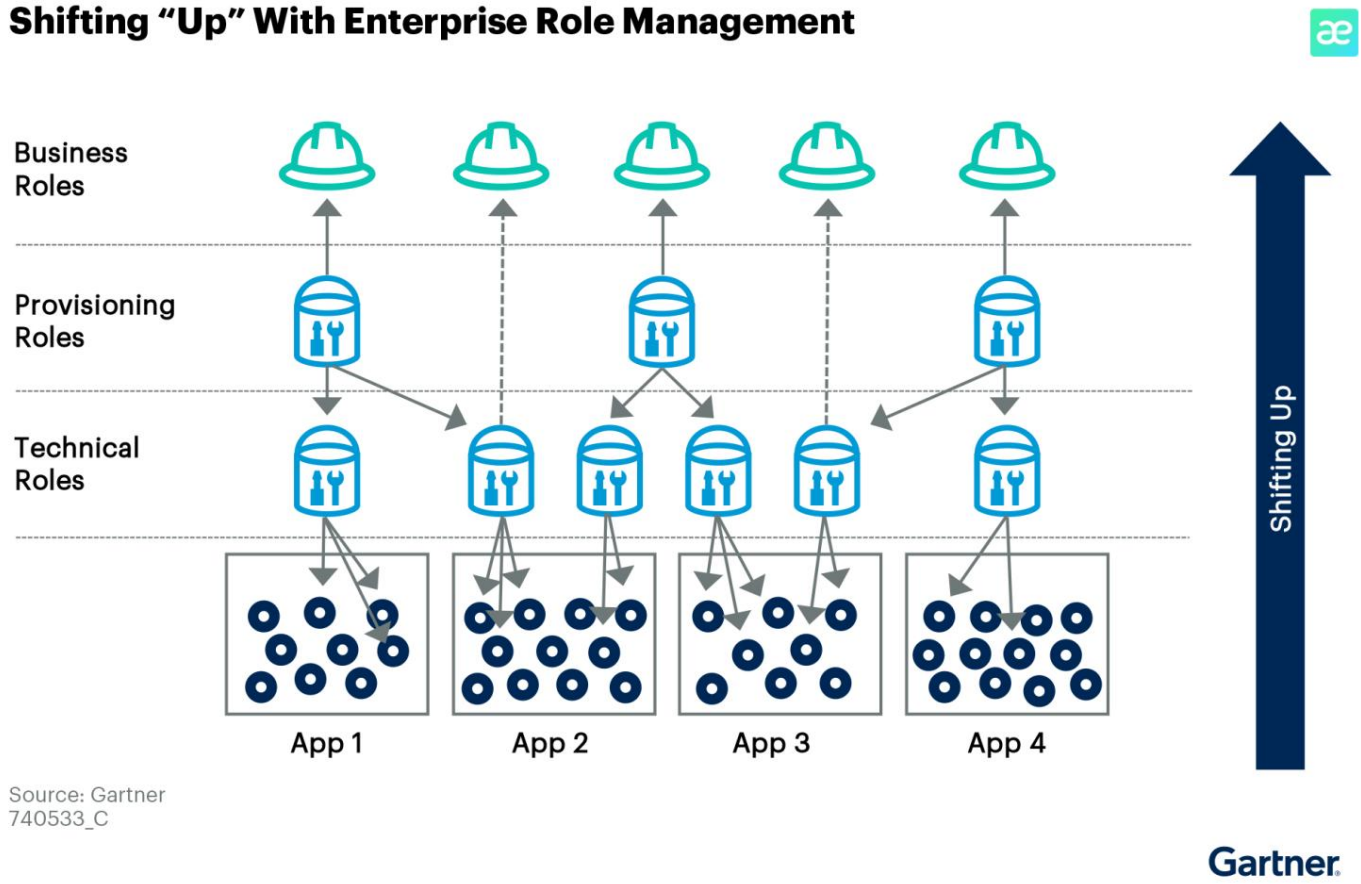
Meilleures pratiques de gestion des rôles

Les approches intuitives de l'ingénierie des politiques et des rôles avec les outils IGA n'ont pas réussi à produire les résultats souhaités par la plupart des organisations. Les responsables de la sécurité et de la gestion des risques doivent adopter la politique d'entreprise tridimensionnelle et le cadre de gestion des rôles de Gartner pour administrer efficacement les accès, en utilisant les rôles à l'échelle de l'entreprise.

La plupart des déploiements actuels d'outils IGA présentent des lacunes en matière de contrôle en raison du recours à des modèles de processus manuels pour la mise en œuvre. Les responsables de la sécurité et de la gestion des risques responsables de l'IAM doivent se concentrer sur trois niveaux de contrôle afin d'établir un modèle vérifiable pour leurs déploiements IGA.

À titre de recommandation, utilisez l'approche des chapeaux et des eaux, telle que décrite dans la recherche sur les meilleures pratiques répertoriées ci-dessus, pour une politique d'entreprise standardisée et une stratégie de contrôle d'accès basée sur les rôles (voir Figure 5). Concentrez-vous sur la gestion des droits sur une large population de systèmes et d'applications dès les premières phases des projets de déploiement IGA afin de fournir une image claire de « qui a accès à quoi ». Améliorez l'efficacité de l'archéologie pour les analystes de sécurité impliqués dans les processus indirects de traitement des comptes en tant qu'étape intermédiaire sur la voie de la création d'autres parties d'un cadre de gouvernance des accès.

Figure 5 : Passer « vers le haut » avec la gestion des rôles d'entreprise



Une stratégie réussie de gestion des rôles en entreprise comprendra un cadre de gestion des politiques. Parmi les politiques les plus importantes pour établir le contrôle des périmètres d'identité figurent celles liées aux cycles de vie de l'identité.

Le premier principe du contrôle du périmètre d'identité est qu'un cycle de vie doit être une boucle fermée - un processus avec un début et une fin, comme de l'embauche à la cessation d'emploi dans la relation de travail, mais aussi pour toutes les relations d'identités qui effectuent des interactions avec l'organisation. (qu'il s'agisse d'employés, de sous-traitants, de partenaires commerciaux ou de clients). Le deuxième principe du contrôle du périmètre d'identité est qu'une personne ne doit être représentée que par une seule identité au sein du référentiel d'identités d'un outil IGA. Le troisième principe est que l'intégrité de tous les cycles de vie de l'identité doit être surveillée.

De nombreuses organisations utilisant les outils IGA présentent des lacunes dans leurs contrôles clés en raison de processus de cycle de vie des identités mal conçues. Les responsables IAM doivent adopter ces bonnes pratiques en matière de cycle de vie des identités, qui incluent des indicateurs clés, pour que leurs déploiements IGA établissent correctement un périmètre d'identité.

Comment choisir la meilleure stratégie d'exécution et d'approvisionnement

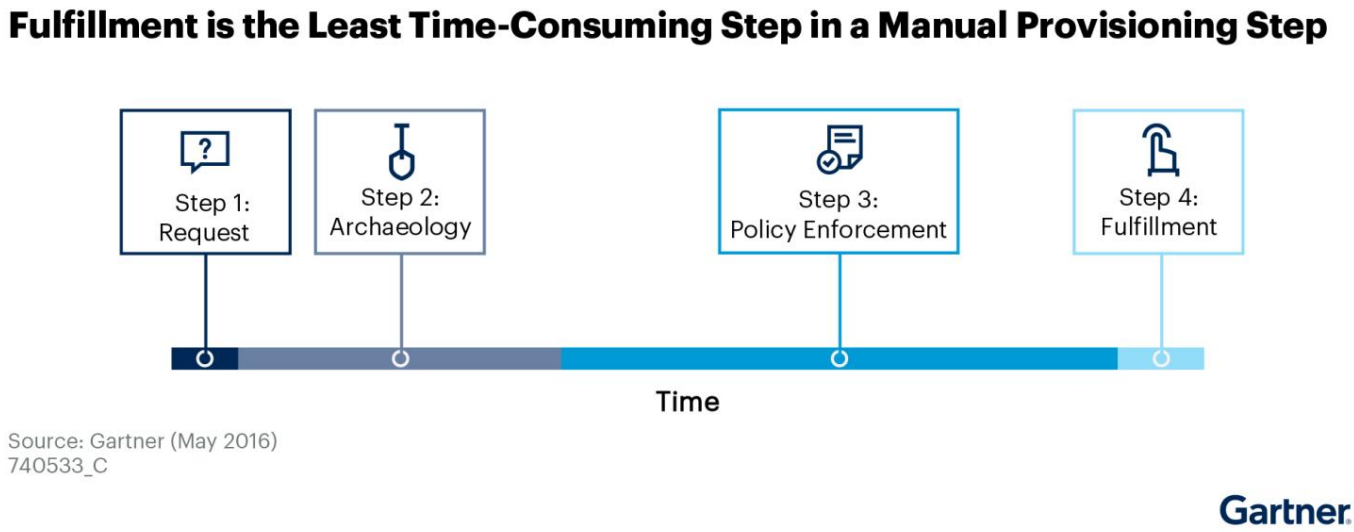
L'automatisation de bout en bout est coûteuse et semée d'embûches en matière d'intégration. Les responsables IAM qui mettent trop l’accent sur le provisionnement automatisé au début des déploiements IGA courent le risque de concentrer en début de période la majorité des risques du projet.

Il existe une idée fausse répandue parmi les dirigeants IAM selon laquelle, pour contrôler les référentiels de comptes, les plates-formes IGA doivent fournir une automatisation de bout en bout pilotée par des connecteurs. La conviction est que les besoins de contrôle ne sont satisfaits que lorsque l'accès est attribué via le système IGA et que l'exécution est gérée automatiquement sans intervention humaine. Cela conduit de nombreuses organisations à se concentrer sur le provisionnement automatisé dès le début du déploiement des produits IGA.

L'exécution automatisée semble simple au premier abord, mais, en réalité, il s'agit de l'élément le plus imprévisible et le plus coûteux des projets de déploiement IGA. Ce problème est plus aigu dans les premières phases d'un projet de déploiement d'IGA, avant que les processus n'aient été harmonisés ou rationalisés.

Le flux de processus classique de demande d'accès est décomposé dans la figure 6, montrant la durée de vie d'une demande d'accès depuis le moment où elle est générée jusqu'à son exécution.

Figure 6 : L'exécution est l'étape qui prend le moins de temps dans un manuel
Étape de provisionnement



L'essentiel à comprendre à propos de ce flux est qu'il n'est pas nécessaire d'automatiser tous les éléments en même temps. Chacune des étapes ajoute de la valeur au processus, tout en prenant du temps et en exigeant divers degrés d'intelligence (à la fois tacite et documentée) de la part des participants :

1. Les demandes soumises manuellement par les utilisateurs ou les gestionnaires sont souvent vagues.

2. La deuxième étape implique qu'un analyste de sécurité prenne la demande et la rende exploitable. Ce implique généralement des recherches « archéologiques », pour vérifier quels droits sont réellement nécessaires pour la demande. Lors de l'étape d'archéologie, il faut également savoir qui sont les approbateurs.

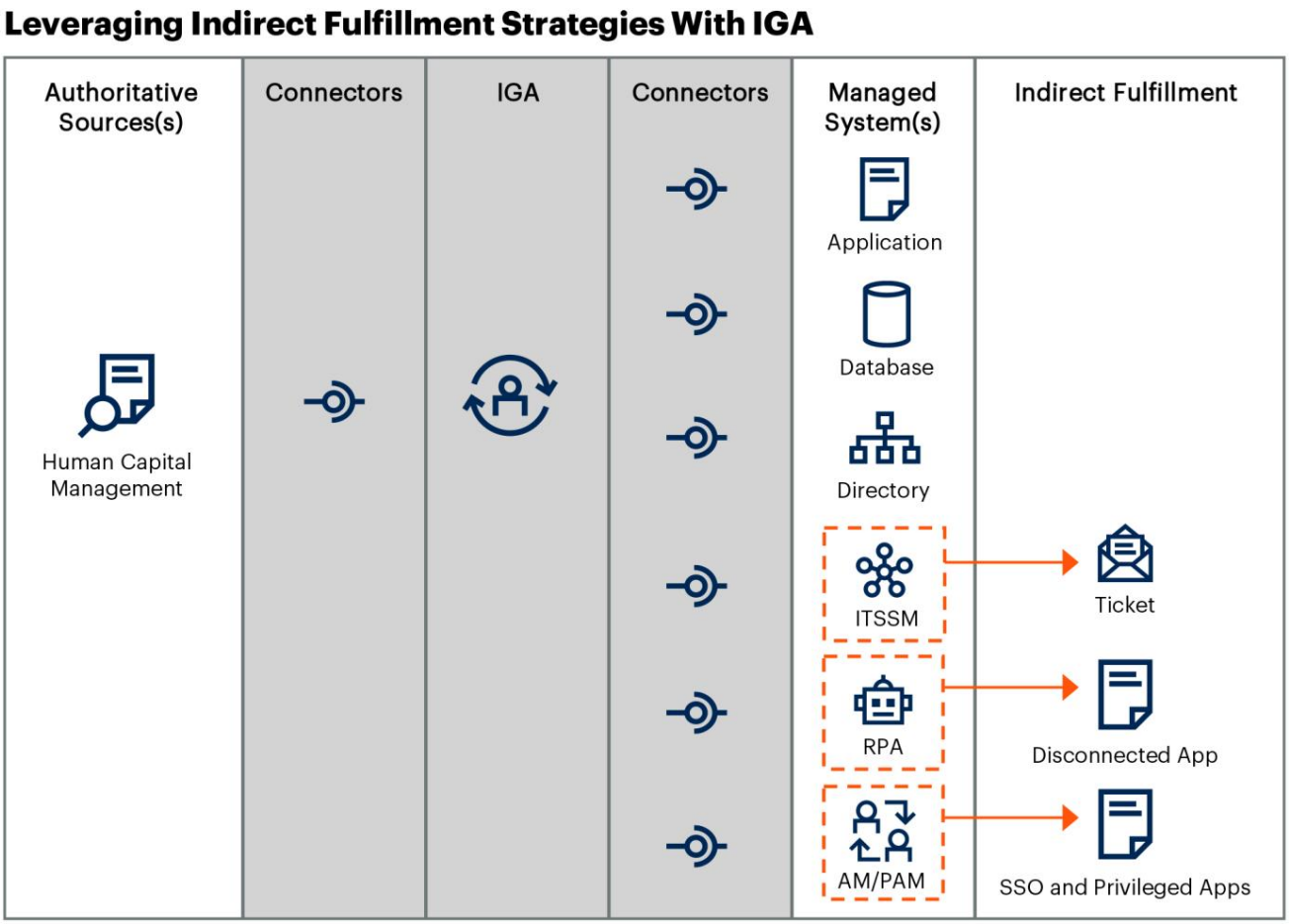
3. Une fois qu'une demande exploitable existe, les analystes de sécurité doivent déterminer si la demande se conforme aux politiques, et obtient et enregistre également les approbations. Cependant, une documentation médiocre et un volume élevé de demandes rendent ce travail très sujet aux erreurs.

4. La dernière étape est la plus simple du point de vue de l'implication humaine. L'accomplissement ne nécessitent autant d'expérience ou de puissance cérébrale que les étapes 2 et 3, il est donc possible d'accomplir cette tâche

effectué avec des procédures documentées par des ressources à moindre coût, telles que des techniciens du centre de service.

Pour éviter que ce type de problèmes ne fasse dérailler un projet IGA dans ses premières phases, il est nécessaire de prendre du recul par rapport au perfectionnisme du tout ou rien de l'automatisation de bout en bout et de reconnaître plutôt que l'intégration du dernier kilomètre est souvent la moindre des choses. élément important pour améliorer l'efficacité administrative et contrôler l'efficacité de la gestion des comptes avec IGA. L'approche de l'intégration du dernier kilomètre est grandement améliorée lorsque vous disposez d'une stratégie solide d'exécution indirecte. La gestion des services informatiques (ITSM) est le moyen le plus simple de traiter l'exécution indirecte des demandes d'accès, mais les solutions de gestion des accès et d'automatisation des processus robotiques (RPA) sont également des options à considérer (voir Figure 7).

Figure 7 : Tirer parti des stratégies de traitement indirect avec IGA



Lorsqu'un outil ITSM n'est pas disponible ou que l'intégration ITSM n'est pas réalisable, il est possible d'utiliser le produit IGA pour simuler le flux de processus ITSM avec workflow.

En moyenne, les organisations peuvent raisonnablement s'attendre à automatiser le provisionnement direct via des connecteurs pour 15 à 25 % des systèmes gérés cibles. Et 75 à 85 % des systèmes finiront par être indirectement réalisés. En donnant la priorité aux systèmes à volume élevé à automatiser, les organisations doivent

viser un traitement automatisé pour bien plus de 50 % des transactions d'exécution générées par l'outil IGA.

L'IGA est généralement l'initiative la plus risquée qu'un programme IAM poursuivra. Les responsables de la sécurité et de la gestion des risques responsables de l'IAM doivent adopter une approche de déploiement basée sur la gouvernance pour générer rapidement de la valeur commerciale tout en minimisant le risque global du projet.

À titre de recommandation, s'appuyer sur l'exécution indirecte orchestrée par l'outil IGA — en générant des tickets de service sur un outil ITSM, par exemple — pour l'exécution sur la plupart des systèmes cibles, en particulier pendant les premières phases de déploiement de ces systèmes cibles, où un manque de disponibilité est nécessaire. L'adaptateur "-the-box" n'est pas disponible.

Définir des métriques IGA basées sur les KPI

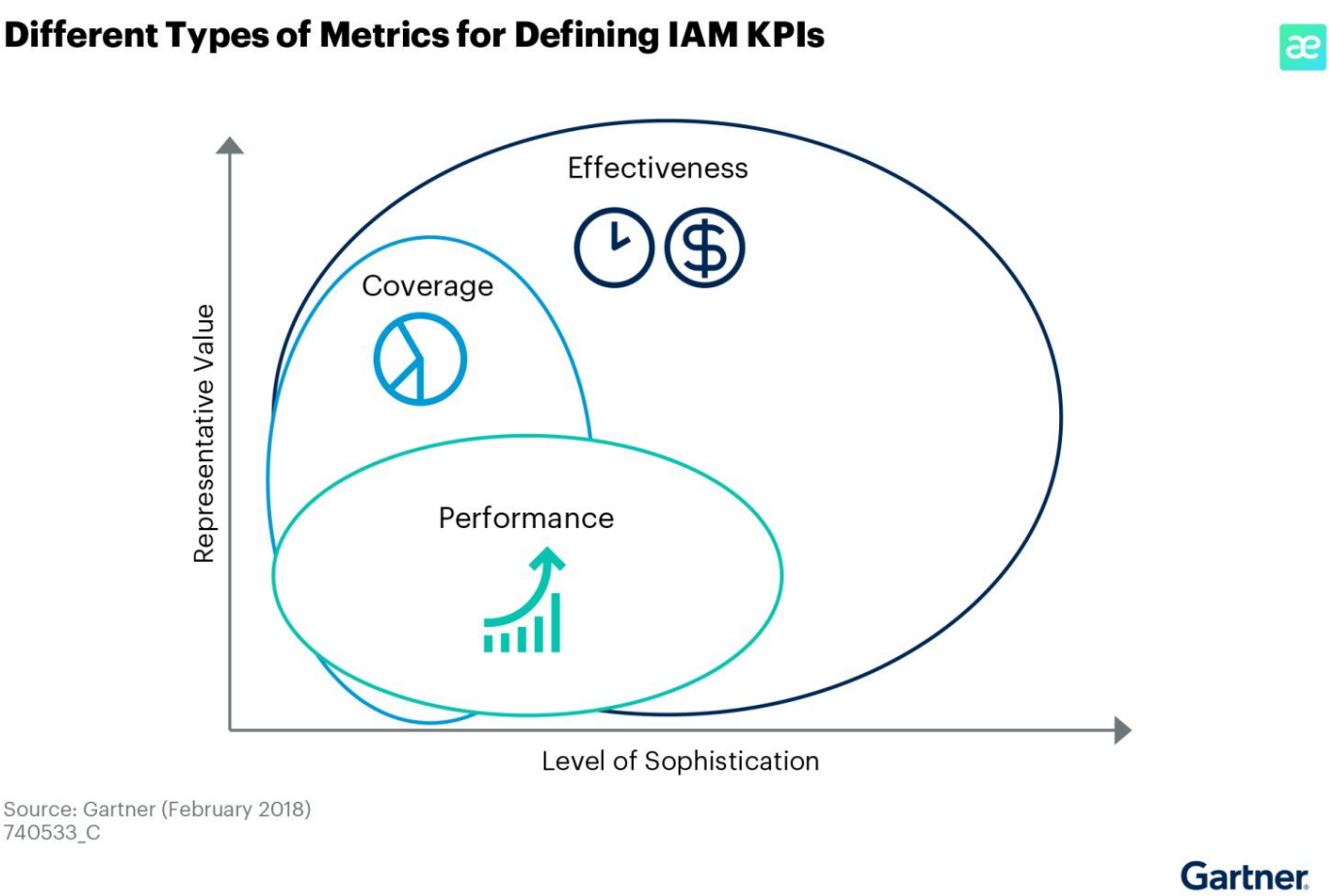
Les initiatives AGR nécessitent souvent une méthodologie de livraison plus rapide et plus flexible pour répondre à l'évolution des conditions commerciales. Les approches DevOps et agiles doivent être privilégiées pour que les services IGA soutiennent les initiatives numériques.

Lors de la planification du déploiement d'un produit IGA, les responsables IAM doivent travailler en étroite collaboration avec les parties prenantes commerciales et techniques, y compris les experts produits, pour évaluer les capacités discrètes et les intégrations potentielles qui pourraient être déployées à l'aide d'un cadre agile.

Les principales parties prenantes d'IGA devraient inclure la gestion du capital humain (HCM), la sécurité et la technologie, l'infrastructure, les propriétaires d'applications et même les équipes commerciales ou marketing. Il est fondamental que les parties prenantes soient alignées sur une vision unique et que des KPI appropriés soient définis pour mesurer l'efficacité de l'adoption du processus AGR.

Les mesures de performance et de couverture sont généralement plus faciles à produire, mais ajouteront moins de valeur aux parties prenantes de l'IGA (autres que les dirigeants de l'IAM). Les mesures d'efficacité sont souvent les plus difficiles à produire, mais elles peuvent également figurer parmi les mesures les plus importantes pour des parties prenantes spécifiques. Ces mesures sont généralement dérivées en illustrant des comparaisons ou des ratios de différentes valeurs de composants (voir Figure 8).

Figure 8 : Différents types de métriques pour définir les KPI IAM



Voici des exemples de mesures d'efficacité utiles pour l'IGA :

- Taux de révocation des certifications d'accès (pourcentage, tendance et évolution)
- Nombre de comptes orphelins supprimés du décompte des licences
- Nombre d'approbations automatisées basées sur des scores d'analyse à faible risque

Démontrer le contrôle de l'accès des utilisateurs grâce aux mesures d'efficacité IAM

Les métriques communiquent la valeur du programme IAM aux parties prenantes et permettent une évaluation et une gestion efficaces des services IAM. Les responsables de la sécurité et de la gestion des risques responsables de l'IAM doivent articuler et maintenir des mesures qui montrent la couverture, les performances et l'efficacité des services de leurs programmes IAM.

Comment choisir un outil IGA

Lors de la rédaction d'un appel d'offres IGA, limitez le nombre d'exigences en évoquant uniquement votre cas d'utilisation IGA le plus important et les fonctionnalités IGA obligatoires qui sont alignées sur les motivations des parties prenantes. Utilisez l'analyse d'identité comme condition de différenciation (voir Figure 9).

Figure 9 : Capacités IGA mappées aux cas d'utilisation

IGA Capabilities Mapped to Use Cases

H Highest Score, Mandatory Capabilities Based on Use Case
M Medium Score, Desired Capabilities Based on Use Case
L Lower Score, Optional Capabilities
Differentiator Capability

	Use Cases			
	Midsize	Automation	Governance	Global
Access Certification			H	
Access Requests	L	L		
Auditing			H	M
Ease of Deployment	H			
Entitlement Management			M	
Fulfillment		H		M
Identity Analytics and Reporting	M		H	H
Identity Life Cycle	L	M		M
Policy and Role Management		L	M	H
Scalability and Performance				H
Workflow				H

Source: Gartner
740533_C

Gartner

Guide de l'acheteur pour IGA : les 4 principaux éléments d'un appel d'offres réussi

IGA est l'un des composants IAM les plus coûteux qu'une organisation puisse jamais acquérir. Les responsables de la sécurité et de la gestion des risques responsables de l'IAM doivent appliquer les quatre éléments de réussite décrits dans ce guide de l'acheteur pour élaborer des appels d'offres IGA réussis qui génèrent des réponses de haute qualité et sont plus faciles à évaluer.

Sélectionnez des solutions évolutives en donnant la préférence aux fournisseurs IGA offrant une couverture géographique appropriée des services professionnels, des architectures modernes et des modèles de prestation SaaS. Cela signifie parfois disqualifier un fournisseur de l'appel d'offres si la présence géographique pour l'intégration des services n'est pas satisfaisante.

Guide du marché pour la gouvernance et l'administration des identités

Les responsables de la sécurité et de la gestion des risques devraient utiliser ce guide du marché pour les aider à prendre des décisions concernant les produits de gouvernance et d'administration des identités.

Leçons apprises par les pairs pour la mise en œuvre de solutions de gouvernance et d'administration des identités et
Gartner Peer Insights « Voix du client » : gouvernance et administration des identités

Les avis Gartner Peer Insights constituent les opinions subjectives d'utilisateurs finaux individuels, basées sur leurs propres expériences, et ne représentent pas les opinions de Gartner ou de ses filiales.

Comprendre la variété des technologies IGA est nécessaire, mais pas suffisant pour répondre aux besoins stratégiques ou tactiques. Les responsables IAM doivent également être efficaces dans leur choix parmi les technologies et les fournisseurs IGA.

Les différentes technologies IGA ont tendance à bien s'aligner sur des cas d'utilisation, des secteurs et des moteurs spécifiques, mais peuvent devoir être complétées dans d'autres cas.
Ainsi, les responsables IAM doivent déterminer l'éventail des cas d'utilisation et être capables d'adapter le choix des modèles de prestation IGA aux exigences et aux contraintes des organisations spécifiques.

L'adoption continue du cloud computing a perturbé les déploiements de logiciels IAM traditionnels, souvent en faveur de l'IAM fourni en mode SaaS. Les responsables de la sécurité et de la gestion des risques axés sur l'IAM doivent analyser les facteurs commerciaux et technologiques, ainsi que le coût total de possession (TCO), pour faire le choix approprié.