Saviynt

Gouvernance des accès aux applications : atteindre la maturité en 3 étapes

Assainir, maintenir et optimiser

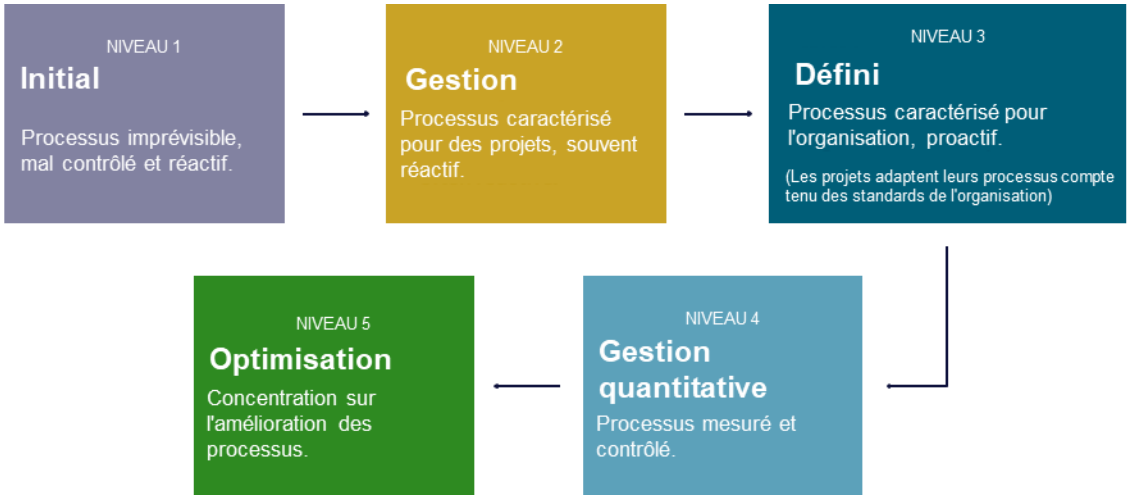
Sommaire

L'adoption rapide du cloud a soulevé de nouveaux défis pour les équipes IT et de sécurité qui ont pour mission de mettre en œuvre, sur l'ensemble de leurs applications cloud et sur site, des processus homogènes et efficaces autour de la gouvernance, du risque et de la conformité (GRC). Alors que le paysage des menaces évolue, il devient plus impératif que jamais de renforcer la sécurité. La fréquence des cyberattaques et des violations de données ne cesse d'augmenter, et ces incidents peuvent avoir des conséquences désastreuses pour votre organisation. Les lois Sarbanes-Oxley (SOX) et GLBA (Gramm-Leach-Bliley Act) ont été ratifiées afin d'imposer un cadre réglementaire contre les irrégularités financières. Elles exigent des entreprises, et tout particulièrement des institutions financières, qu'elles adoptent des pratiques d'excellence et utilisent la technologie de manière appropriée. Toute infraction à l'une de ces réglementations représente un coût non négligeable, et leur mise en application fait l'objet d'un suivi rigoureux. Depuis 2008, par exemple, les établissements bancaires se sont vus infliger 243 milliards de dollars d'amende pour non-respect de la réglementation.

Mais la mise en œuvre de leurs principes est bien moins simple qu'il n'y paraît. En moyenne, les entreprises utilisent 34 applications SaaS dans l'ensemble de leur environnement. Et alors qu'elles poursuivent leur migration vers le cloud, il devient plus important encore d'assurer une sécurité et une gouvernance, tant au niveau des applications individuelles qu'à l'échelle de toutes les applications. Pour mettre en conformité la totalité de leur environnement, les entreprises ont tendance à commencer par leur système financier stratégique, puis à étendre leur démarche à des systèmes pertinents et interactifs qui entrent dans le périmètre de la loi SOX, de l'HIPAA (Health Insurance Portability and Accountability Act), etc., et à poursuivre ainsi, jusqu'à englober l'intégralité de leur environnement. Quel que soit le niveau de maturité des applications, le respect de ces étapes aide à faire progresser la gouvernance d'une application dans son cycle de maturité, en assurant une conformité continue et une surveillance standardisée.

Et c'est précisément à ce niveau qu'entrent en scène les bonnes pratiques de gouvernance. Car l'objectif de tout programme de gouvernance est d’assainir votre environnement, de le maintenir à cet état de manière pérenne et d'optimiser les pratiques de gouvernance et de gestion des risques. Pour y parvenir, les entreprises ont la possibilité de se référer au Capability Maturity Model (CMM) pour mettre en place des processus standardisés, mesurés, contrôlés et reproductibles qui favorisent une amélioration et une optimisation continues des processus. Pour aider votre organisation dans l'élaboration d'un programme de gestion des risques véritablement efficace, nous avons mis au point un processus simple en trois étapes : « Assainir, maintenir et optimiser »

Caractéristiques des niveaux de maturité



Assainir

Établir une ligne de base pour l'environnement de risque

Pour créer un processus standardisé et mesuré tout en instaurant efficacement votre approche de la gestion des risques, vous devez avant tout établir une ligne de base pour l'environnement de risque, qui prévoit, notamment, une séparation des tâches (SoD, Segration of Duties) pour les applications individuelles et l'ensemble des applications.

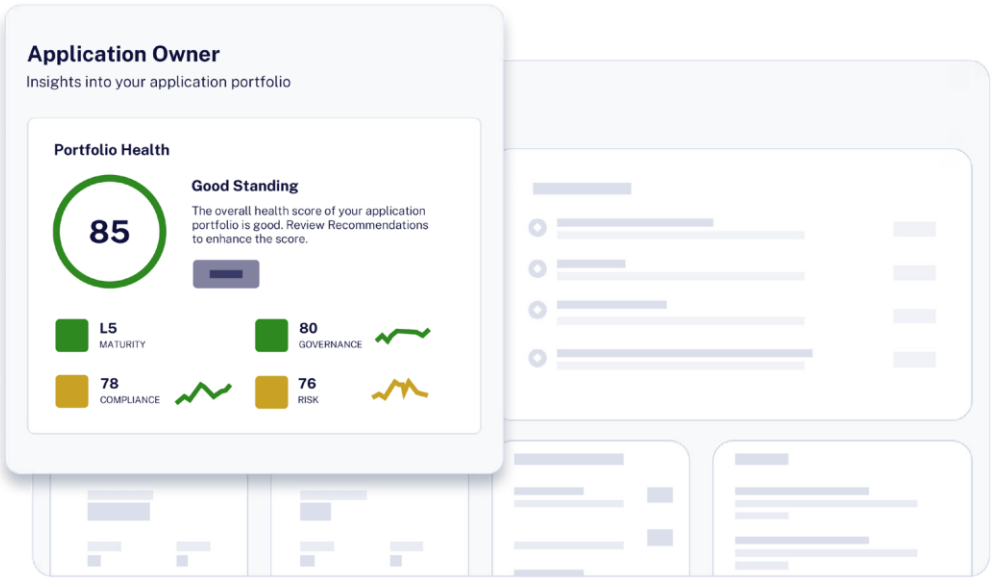
Quelques conseils pour y parvenir :

- ### Définir des ensembles de règles en matière de risques

  En mettant en place des ensembles de règles qui imposent une fine séparation des tâches et une habilitation rigoureuse des accès sensibles, tant pour les applications individuelles que pour les contrôles entre les différentes applications, les entreprises disposent d'une ligne de base adaptée à leur propre appétence au risque. La possibilité de personnaliser les niveaux de risque sur une échelle de « Faible » à « Critique » permet, par ailleurs, de prendre en compte les nuances propres au secteur d'activité et à l'entreprise elle-même. Les ensembles de règles établis en matière de risques serviront de ligne de base, autrement dit de référentiel, pour orienter l'évolution future du programme de gestion et de gouvernance des risques.

- Exécuter des évaluations de risques fondées sur les principes de la SoD

  Une fois les ensembles de règles mis en œuvre, l'entreprise doit instaurer une ligne de base pour l'environnement de risque actuel. La production d'un rapport de détection des risques permet de dresser un état des lieux de l'environnement actuel et d'orienter les objectifs d'évolution future. Les résultats des évaluations des risques peuvent être regroupés par degré de criticité, par domaine de processus, ou bien en différentes métriques composites afin de déterminer le niveau d'assainissement requis.



En matière de cybersécurité, il est important de comprendre l'état de santé de votre portefeuille d'applications actuel

- Documenter les mesures d'atténuation

  Il existe trois manières de traiter (« assainir ») un risque : corriger (éliminer) la menace auprès d'un utilisateur, atténuer le risque pour un utilisateur ou ignorer le risque. L'option retenue par chaque entreprise est fonction de son appétence au risque et de ses exigences en matière d'audit. Un exemple classique serait de signaler les risques de niveau Faible sans engager de quelconques mesures. À l'inverse, les risques de niveaux Moyen et Élevé imposeraient une atténuation ou une correction, et les risques de niveau Critique exigeraient une correction et il ne serait pas envisageable que les utilisateurs restent exposés à de tels risques. Les mesures d'atténuation sont des processus établis ou des rapports liés à un risque utilisateur qui sont déclenchés lorsqu'il est impossible de corriger la menace. Les mesures d'atténuation doivent documenter les procédures, contrôler la propriété et contrôler les risques approuvés.

- Traiter les risques dans les rapports SoD

  Après avoir établi la ligne de base de l'environnement de risque, et après avoir documenté les mesures d'atténuation et les avoir reliées à des risques approuvés, l'étape suivante consiste à assainir l'environnement. En fonction de l'appétence au risque définie, chaque risque pour l'utilisateur doit être signalé, corrigé en supprimant l'accès qui en est à l'origine, ou atténué par l'application d'un moyen de contrôle approuvé. La réussite de cette étape permet à l'entreprise de passer à un environnement « propre » à un certain point dans le temps.

Maintenir

Instaurer des processus reproductibles et automatisés avec des moyens de contrôle préventifs

À présent que l'environnement de risque initial a fait l'objet de contrôles de détection et de mesures d'atténuation/correction, l'étape suivante du parcours d'adoption d'un processus de gestion et de gouvernance des risques efficace consiste à instaurer des processus reproductibles et automatisés avec des moyens de contrôle préventifs conçus pour maintenir votre environnement. Voici les actions recommandées au cours de cette phase :

- Mettre en place des workflows de demande d'accès

  Les workflows de demande d'accès permettent de traiter tous les événements liés aux identités (arrivées, mutations et départs) en imposant des autorisations d'accès appropriées et des contrôles préventifs d'analyse des risques, avant de procéder à des changements d'accès dans le système.

- Instaurer des certifications d'accès

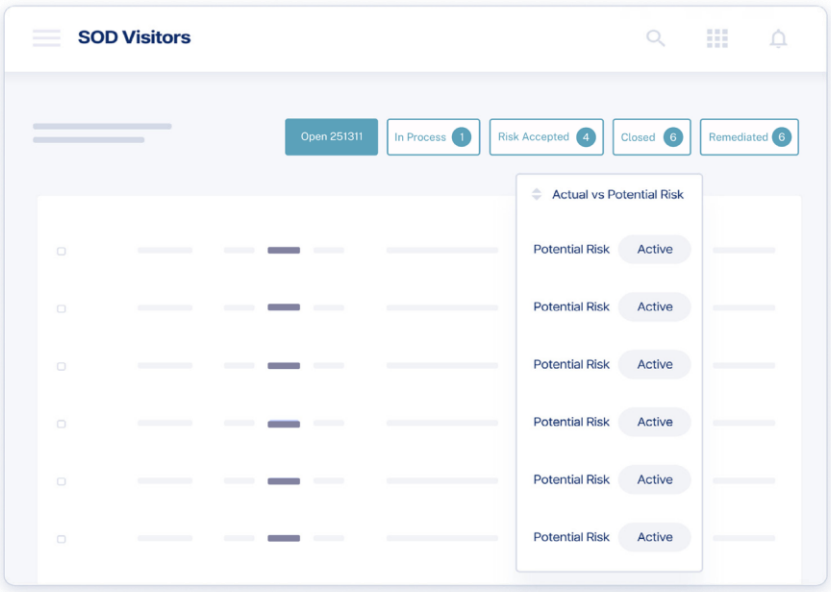
  Les certifications d'accès programmées permettent de maintenir l'environnement propre en veillant à ce que les utilisateurs ne conservent pas leurs anciens droits d'accès lorsque leurs responsabilités professionnelles évoluent. Pour chaque application, les accès doivent être revalidés selon une fréquence approuvée dans le cadre d'un audit.

- Établir des accès d'urgence

  La mise en place d'une norme consistant à interdire les accès permanents avec élévation de privilèges contribue à sécuriser l'environnement, en limitant les accès aux systèmes critiques et en exigeant des approbations et une surveillance pour tout accès d'urgence temporaire approuvé et effectif.

- Corriger les risques par une surveillance permanente de l'utilisation

  Alors que les utilisateurs exploitent en permanence différentes fonctionnalités applicatives et demandent constamment des changements d'accès et des renouvellements de leurs certifications d'accès, il est important d'évaluer la manière dont ils utilisent réellement les différentes fonctions afin de supprimer tout accès superflu (ou devenu inutile). Une surveillance constante de l'utilisation permet de répondre aux besoins d'accès des utilisateurs, tout en respectant les principes du moindre privilège d'accès.



Une visibilité globale permet d'identifier les risques réels et potentiels

Optimiser

Utiliser des moyens de contrôle intégrés, des simulations de risques intégrées et des outils de gestion d'habilitation/ingénierie des rôles

Pour la dernière phase du Capability Maturity Model, il peut être judicieux d'utiliser des moyens de contrôle intégrés, des simulations de risques intégrées et des outils de gestion d'habilitation/ingénierie des rôles. Cette approche permet de concentrer vos efforts sur l'amélioration continue de votre environnement après avoir établi un processus de gestion des risques documenté, reproductible et automatisé. Elle contribue à créer et maintenir, grâce à une solide visibilité, un environnement sécurisé et gouverné.

À ce stade, vous avez traité les risques existants qui ont été détectés, et mis en place des moyens de détection préventive des risques, de provisionnement automatisé des accès, de certification et de demandes d'accès d'urgence. Le moment est venu d'optimiser votre environnement grâce à la gestion et à la surveillance régulières des moyens de contrôle environnementaux, et via l'instauration d'un cycle de vie client complet, de bout en bout, en évitant les écarts susceptibles de poser problème sur le plan des audits et de la conformité. Voici les étapes à suivre :

- Utiliser des analyses d'accès

  Pour faire en sorte que votre environnement conserve une population de risques utilisateur « propre » (où les utilisateurs ne sont exposés à aucun risque, qui n'aurait pas fait l'objet de mesures d'atténuation) et pour atteindre l'objectif ultime d'un environnement soigneusement géré et surveillé, vous devez établir une surveillance automatisée des moyens de contrôle permanents, mettre en place une documentation et une formation standardisées aux processus de gouvernance, et maintenir des ensembles de règles régissant les changements d'utilisation des fonctionnalités. Il existe des moyens de contrôle prêts à l'emploi, inspirés de réglementations essentielles, telles que la loi SOX, le RGPD (Le règlement général sur la protection des données), l'HIPAA, etc., qui peuvent être personnalisés afin d'établir des KPI mesurables.

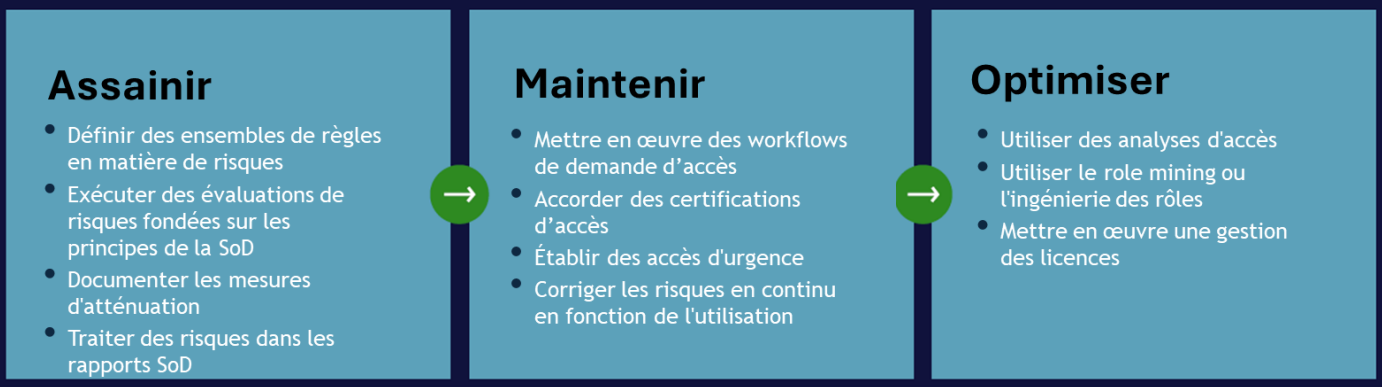
- Utiliser le role mining ou l'ingénierie des rôles

  L'habilitation des rôles doit être mise à jour chaque fois que l'utilisation des accès évolue. L'optimisation d'un système consiste, en partie, à surveiller constamment les changements d'utilisation et de fonctionnalité pour limiter les accès superflus et de respecter les principes du moindre privilège d'accès. Lorsqu'un processus de gouvernance est reconnu « propre », les responsables de la sécurité peuvent reporter leur attention et concentrer le temps dont ils disposent sur l'analyse des modèles de conception et de l'utilisation des accès afin d'identifier des moyens de mieux aligner les habilitations sur les besoins des utilisateurs.

- Gérer les licences

  La mise en place d'examens de gestion des licences en continu permet de reclasser les licences au fil de l'évolution des fonctionnalités utilisateur. Cette reclassification contribue à maintenir une structure de licence qui reflète l'utilisation actuelle de l'entreprise et évite les surcoûts dus à des erreurs d'attribution de licences.

Les étapes du cycle de vie pour la mise en œuvre d'une gestion des risques liés aux accès aux applications



1

L'application du Capability Maturity Model à votre programme de gouvernance et de sécurité vous permet d'établir des processus standardisés, mesurés, contrôlés et reproductibles, propices à une amélioration et à une optimisation continues des processus. Après avoir assaini, maintenu et optimisé votre environnement, vous pouvez contrôler qui accède aux systèmes et de quelle manière, sécuriser l'octroi d'accès et conserver continuellement une visibilité complète sur vos initiatives de conformité et de gestion des risques liés aux accès.

Pour en savoir plus ou pour obtenir une démo, rendez-vous sur saviynt.com/fr.

À PROPOS DE SAVIYNT

Saviynt est la principale plateforme de gouvernance d'identités conçue pour le cloud. Nous aidons les entreprises à accélérer les initiatives de cloud moderne et à relever, en un temps record, les défis les plus complexes en matière de sécurité et de conformité. Saviynt Identity Cloud regroupe des fonctions de gouvernance et d'administration d'identités (IGA), d'accès granulaire aux applications, de sécurité cloud et d'accès à privilèges dans la seule plateforme SaaS d'entreprise disponible sur le marché.
Pour en savoir plus, rendez-vous sur saviynt.com/fr.

Saviynt

Siège social, 1301 E
El Segundo Bl, Suit e D, El Segundo,
CA 90245, États-Unis

310. 641. 1664 | info@saviynt.com
www.saviynt.com/fr