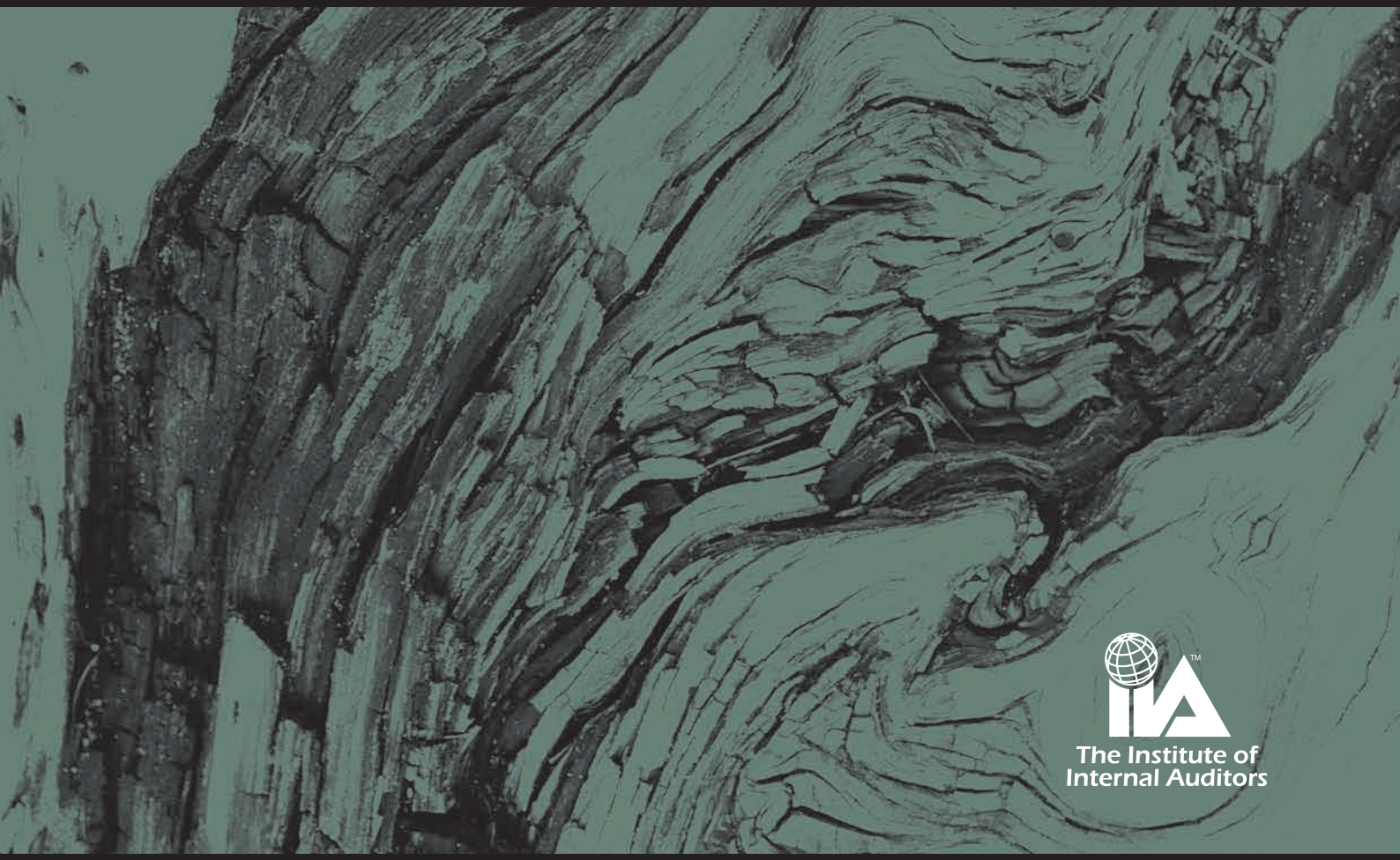
GTAG®

GUIDE PRATIQUE D'AUDIT DES TECHNOLOGIES DE L'INFORMATION

Gestion des identités et des accès



The Institute of Internal Auditors

À propos des guides pratiques d'audit des technologies de l'information

Élaboré par l'Institute of Internal Auditors (IIA), chaque guide est rédigé dans des termes simples et traite d'un thème d'actualité qui a trait à la gestion, le contrôle et la sécurité des TI. Cette série de guides constitue un précieux outil pour les responsables de l'audit interne, qui peuvent ainsi s'informer sur les différents risques induits par la technologie et sur les pratiques recommandées.

Guide 1 : *Les contrôles des systèmes de l'information*

Guide 2 : *Contrôles de la gestion du changement et des patchs : un facteur clé de la réussite pour toute organisation*

Guide 3 : *Audit continu : répercussions sur l'assurance, le pilotage et l'évaluation des risques*

Guide 4 : *Management de l'audit des systèmes d'information*

Guide 5 : *Le management et l'audit des risques d'atteinte à la vie privée*

Guide 6 : *Gérer et auditer les vulnérabilités des technologies de l'information*

Guide 7 : *L'infogérance*

Guide 8 : *Audit des contrôles applicatifs*

La série complète peut être téléchargée sur le site Web de l'IIA : www.theiia.org/technology.

Gestion des identités et des accès

Chef de projet

Sajay Rai, Ernst & Young LLP

Auteurs

Frank Bresz, Ernst & Young LLP

Tim Renshaw, Ernst & Young LLP

Jeffrey Rozek, Ernst & Young LLP

Torpey White, Goldenberg Rosenthal LLP

Novembre 2007

Sommaire

1. RÉSUMÉ **1**

2. INTRODUCTION **2**

2.1 Facteurs opérationnels déterminants 2

2.2 Concepts relatifs à la gestion des identités et des accès 4

2.3 Risques liés à la gestion des identités et accès 4

3. DÉFINITION DES PRINCIPAUX CONCEPTS **6**

3.1 Gestion des identités et gestion des habilitations 7

3.2 Éléments de la gestion des identités et des accès 7

3.3 Droits d'accès et habilitations 7

3.4 Provisionnement 8

3.5 Administration des identités et des droits d'accès 10

3.6 Mise en place des processus 11

3.7 Recours aux technologies pour la gestion des identités et des accès 12

4. LE RÔLE DES AUDITEURS INTERNES **14**

4.1 Processus de gestion des identités et des accès actuels 14

4.2 Audit du programme de gestion des identités et des accès 16

ANNEXE A : LISTE DE CONTRÔLE PORTANT SUR LES REVUES DE LA GESTION DES IDENTITÉS ET DES ACCÈS **19**

ANNEXE B : INFORMATIONS SUPPLÉMENTAIRES **24**

GLOSSAIRE **25**

À PROPOS DES AUTEURS **26**

1. Résumé

La gestion des identités et des accès (IAM, *Identity and Access Management*) consiste à déterminer qui a accès à quelle information sur une période donnée. Il s'agit d'une activité transversale qui suppose la création d'identités, différentes pour les individus et les systèmes, associées à des comptes dans les systèmes et les applications.

Les processus de gestion des identités et des accès permettent d'initialiser, d'identifier, d'enregistrer et de gérer les identités des utilisateurs et les droits d'accès aux informations exclusives de l'organisation qui leur sont associées. Les utilisateurs ne se limitent pas forcément aux employés de la société mais peuvent inclure, entre autres, les fournisseurs, les clients, les machines fixes, les comptes administrateur génériques et les badges électroniques d'accès physique. La gestion des identités et des accès se base sur les moyens utilisés par l'organisation pour faciliter l'administration des comptes utilisateur et mettre en œuvre des contrôles efficaces pour assurer la sécurité des données.

Même si de nombreux dirigeants estiment que la gestion des identités et des accès relève de la direction des systèmes d'informations (DSI), elle concerne en fait toutes les directions métiers de l'entreprise. La direction générale doit avoir l'assurance qu'il existe une procédure de gestion des accès aux ressources de l'entreprise et que les risques associés ont été pris en compte. Les directions métiers ont besoin de savoir ce qu'est la gestion des identités et des accès et comment la gérer efficacement. Et, la DSI doit comprendre en quoi la gestion des identités et des accès peut étayer des processus de l'entreprise. Ainsi, elle pourra fournir des solutions solides afin d'atteindre les objectifs de l'entreprise sans l'exposer à des risques inutiles.

Pour satisfaire ces différentes exigences, il faut bien comprendre les concepts fondamentaux de la gestion des identités et des accès.

Il faut également obtenir des informations des responsables métiers et informatiques pour se faire une idée de l'état actuel des processus de gestion des identités et des accès en place dans l'entreprise. Ensuite, il sera possible d'élaborer une stratégie en fonction du niveau d'adéquation entre les processus existants et les objectifs d'affaires de l'organisation, sa tolérance au risque et ses besoins.

Cette stratégie de gestion des identités et des accès est élaborée en fonction des thèmes suivants :

- les risques associés à la gestion des identités et des accès et la manière dont ils sont gérés ;
- les besoins de l'organisation ;
- les modalités d'approche de la gestion des identités et des accès au sein de l'organisation et les caractéristiques d'un processus de gestion des identités et des accès efficace ;
- les processus d'identification des utilisateurs et le nombre d'utilisateurs au sein de l'organisation ;
- les processus d'authentification des utilisateurs ;
- les droits d'accès accordés aux utilisateurs ;
- l'identification des accès non autorisés aux ressources informatiques ;
- le processus de suivi et d'enregistrement de l'activité des utilisateurs.

À mesure que l'entreprise évolue, elle doit adapter son système de gestion des identités et des accès. La direction générale doit veiller à ce que les changements ne rendent pas le processus de gestion des identités et des accès trop rigide ou ingérable et qu'il n'expose pas l'organisation à des risques inutiles liés à une mauvaise utilisation des ressources informatiques.

Rôle des auditeurs internes

Comme la gestion des identités et des accès concerne tous les niveaux de l'organisation, depuis l'accès à la porte principale d'un bâtiment jusqu'à la récupération des données bancaires et financières de l'organisation, les responsables de l'audit interne sont amenés à identifier les moyens mis à la disposition de l'organisation pour rendre plus efficace le contrôle des accès, afin de mieux appréhender le rôle actuel de la gestion des identités et des accès. Dans un premier temps, pour contrôler efficacement les accès, le management doit identifier les points d'entrée physiques et logiques. Des processus de gestion des identités et des accès insuffisants ou peu contrôlés peuvent entraîner des violations de la réglementation et empêcher l'entreprise de détecter les cas de détournement de ses données.

Il est donc important que le responsable de l'audit interne soit impliqué dans l'élaboration de la stratégie de gestion des identités et des accès de l'organisation. Il apporte un point de vue original sur la façon dont les processus de gestion des identités et des accès peuvent renforcer l'efficacité des contrôles d'accès tout en aidant les auditeurs à mieux appréhender le fonctionnement de ces contrôles.

L'objectif de ce GTAG est d'aider à comprendre le rôle de la gestion des identités et des accès pour l'organisation et de suggérer les points à approfondir lors d'un audit interne. Outre une participation au développement de la stratégie de gestion des identités et des accès, il incombe au responsable de l'audit interne de se renseigner auprès des responsables métiers et informatiques que les processus de gestion des identités et des accès déjà en place sont gérés. Ce document ne prétend pas être la référence absolue en la matière, mais il peut aider le responsable de l'audit interne et les auditeurs internes à comprendre, analyser et surveiller les processus de gestion des identités et des accès de leur organisation.

2. Introduction

Depuis des années, les organisations sont confrontées à la difficulté de gérer les identités et les authentifiants qui permettent d'accéder aux ressources technologiques. Cette question, auparavant simple et limitée au centre de données, s'est transformée pour les organisations de toute taille en une problématique de plus en plus vaste et complexe.

Ainsi, de nombreuses grandes organisations sont incapables de gérer efficacement les identités et les droits d'accès accordés aux utilisateurs, en particulier dans les environnements informatiques distribués. Depuis quelques années, la DSI crée des groupes d'administration système pour gérer la multitude de serveurs, de bases de données et d'ordinateurs de bureau utilisés par leur organisation. Malgré cela, la gestion des accès aux ressources reste délicate.

En dépit de ces évolutions, les ressources humaines et les processus manuels sont parfois dans l'incapacité de gérer la complexité des tâches et les coûts administratifs liés à la gestion des identités des utilisateurs dans l'organisation. De plus, ces dernières années, les obligations réglementaires et les processus de gestion des accès sont de plus en plus surveillés par des instances extérieures.

Ces obligations réglementaires et les pratiques de gestion prudentes ont conduit les organisations à accroître au maximum le degré de granularité des droits d'accès. Le management doit déterminer avec précision les droits nécessaires aux utilisateurs au lieu de leur accorder des ressources dont ils n'ont pas vraiment besoin.

Si le terme de gestion des identités et des accès (*Identity and Access Management* – IAM) est maintenant généralement adopté par les professionnels, les définitions varient en fonction du secteur, du fournisseur ou du consultant. Toutefois, les principes de base restent les mêmes. Ce guide ne prétend pas donner LA définition de référence, mais englobe différentes définitions utilisées dans le secteur informatique.

2.1 Facteurs opérationnels déterminants

D'après un rapport prévisionnel récent[1] du groupe de presse International Data Group (IDG), les dépenses consacrées à la gestion des identités et des accès et aux systèmes connexes devraient augmenter rapidement. Aux États-Unis, cette tendance est due essentiellement à la loi Sarbanes-Oxley de 2002, au *Health Insurance Portability and Accountability Act* (HIPAA) de 1996, au *Gramm-Leach-Bliley Act* (GLBA) de 1999, au Nouvel accord de Bâle (dit Bâle II) et à d'autres réglementations sectorielles. Les services financiers, par exemple, doivent respecter une directive qui impose l'utilisation de plusieurs ensembles d'authentifiants (authentification multifacteur). Dans ce rapport, le marché mondial de la gestion des identités et des accès devrait augmenter d'au moins 10 % par an, pour atteindre 5 milliards de dollars en 2010. La gestion des identités et des accès devrait donc bientôt figurer au premier rang des projets informatiques de nombreuses organisations.

Face à cette envolée, il est important d'examiner dans quels buts les organisations s'engagent dans des projets de gestion des identités et des accès :

- Amélioration de la conformité réglementaire ;
- Réduction des risques liés à la sécurité des informations ;
- Réduction des coûts de fonctionnement et de développement des systèmes d'information (SI) ;
- Renforcement de l'efficacité et de la transparence des opérations ;
- Satisfaction accrue des utilisateurs ;
- Amélioration de l'efficacité des opérations clés.

2.1.1 Amélioration de la conformité réglementaire

Sans exagérer les conséquences des réglementations évoquées précédemment, il est important de noter que les lois Sarbanes-Oxley, HIPAA, GLBA, Bâle II, etc. ont eu des répercussions sur les organisations du monde entier. Toutefois, si les projets de gestion des identités et des accès ont contribué à combler les lacunes dans les contrôles d'accès aux systèmes, ils n'ont pas forcément été suffisants. De nombreux projets de gestion des identités et des accès ne sont que des solutions temporelles pour se mettre en conformité avec la réglementation. Si cette façon d'aborder la gestion des identités et des accès permet de se conformer à des tests d'audit, elle risque à terme de se révéler néfaste pour l'organisation si le programme de gestion des identités et des accès devient excessivement complexe, inopérant et coûteux. Il faut également savoir que les programmes de gestion des identités et des accès collectent souvent des données personnelles sur les utilisateurs du système. Ils doivent donc être en conformité avec la législation sur la confidentialité et la protection des données, notamment la Directive européenne de 1995 relative à la protection des données personnelles[2].

2.1.2 Réduction des risques liés à la sécurité des informations

L'un des principaux facteurs de réussite des stratégies de gestion des identités et des accès tient à une meilleure protection face aux risques. Celle-ci est obtenue grâce à la

[1] Rapport IDG n° 204639 : *Worldwide Identity and Access Management 2006-2010 Forecast Update With Submarket Segments,* décembre 2006.

[2] Directive 95 / 46 / CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

mise en œuvre de systèmes renforcés de contrôle des accès et des identités. Parce qu'il permet de savoir qui a accès à quelles ressources et en quoi tel ou tel accès est directement utile pour une tâche ou une fonction données, le système de gestion des identités et des accès renforce l'ensemble de l'environnement de contrôle de l'organisation.

Dans de nombreuses organisations, la suppression des droits d'accès utilisateur ou des droits d'accès associés à une identité numérique, peut prendre jusqu'à trois ou quatre mois. Cela peut représenter un risque inacceptable, surtout si l'utilisateur peut encore accéder aux systèmes et ressources de l'organisation alors que ce dernier a été révoqué. Par exemple, il est arrivé que certains utilisateurs, notamment des sous-traitants, conservent leurs droits d'accès pendant des années. Ils continuent donc de bénéficier d'un accès non autorisé aux systèmes, ce qui expose l'infrastructure de l'organisation à des tentatives de piratage.

2.1.3 Réduction des coûts de fonctionnement et de développement des systèmes d'information

Paradoxalement, la multiplication des systèmes automatiques peut nuire à l'efficacité des employés à cause des différents dispositifs d'ouverture de session utilisés. Les employés doivent mémoriser ou garder sur eux toute une série d'authentifiants fréquemment renouvelés. Ainsi, un employé lambda peut avoir un nom d'utilisateur et un mot de passe pour son ordinateur de bureau, un nom d'utilisateur et un mot de passe différents pour accéder à d'autres systèmes, plusieurs autres noms d'utilisateur et mots de passe pour diverses applications bureautiques ou navigateurs, plus un numéro d'identification personnel (PIN) assorti d'un mot de passe à usage unique pour les accès à distance.

Cette grande quantité d'authentifiant, multipliée par la fréquence de renouvellement des mots de passe, peut en rendre la gestion excessivement complexe et délicate pour les utilisateurs. Ce qui provoque souvent leur mécontentement vis-à-vis du processus, sans compter les oublis de mots de passe. Cette situation se traduit par une baisse d'efficience des employés et se répercute de façon notable sur les fonctions d'assistance, notamment le centre d'assistance qui administre les authentifiants et doit traiter les demandes de rappel des mots de passe oubliés.

La multiplication des systèmes automatiques peut également accroître considérablement les frais d'exploitation par une accumulation des répertoires et des bases de données d'identités utilisateur, se traduisant alors par des performances médiocres et une augmentation des coûts, cachés pour la plupart. De nombreuses organisations sont ainsi confrontées aux problèmes suivants :

- Absence de processus d'approbation définis et automatiques : les agents administratifs supposent les identités, et improvisent donc lorsqu'ils initient un processus de provisionnement et traitent les demandes d'accès.
- Nombre croissant d'appels au centre d'assistance : les appels concernant les identités et les accès (notamment les demandes de réinitialisation des mots de passe) sont plus nombreux.
- Délai d'attente : les nouveaux employés obtiennent un accès de base aux systèmes informatiques, notamment à la messagerie et aux ressources réseau une semaine après leur arrivée.
- Absence de documentation des accès nécessaires en fonction des rôles : les utilisateurs effectuent plusieurs relances avant d'obtenir les accès dont ils ont réellement besoin.

2.1.4 Renforcement de l'efficacité et de la transparence des opérations

L'existence d'un processus de gestion de l'accès aux informations bien défini peut être un facteur important de l'efficacité des opérations d'une entreprise. Très souvent, les organisations ont du mal à donner aux utilisateurs les droits d'accès dont ils ont besoin pour assurer leurs fonctions. Dans certains cas, les demandes sont transmises à plusieurs membres des services informatique ou administratif, et eux-mêmes ne savent pas toujours quels accès ou quelle information donner en fonction des besoins de l'utilisateur dans le cadre de son travail. De plus, faute d'une procédure précise, les demandes peuvent être incorrectement traitées ou ne pas être traitées du tout, générant du travail supplémentaire pour les membres des services informatique ou administratif.

Par conséquent, la mise en œuvre d'un processus de gestion des identités et des accès bien défini peut donc rendre le système beaucoup plus efficace. Dans les grandes organisations, l'utilisation appropriée de technologies de gestion des identités et des accès permet de garantir que les demandes sont transmises à la bonne personne pour approbation, au système de configuration approprié ou au système de provisionnement automatique qui convient. De plus, elle permet de réduire les délais de traitement des demandes d'accès de plusieurs semaines à quelques jours et améliore l'élaboration de rapports de conformité grâce à l'utilisation de processus d'approbation dans le cadre de la gestion des identités et des accès en place.

2.1.5 Satisfaction accrue des utilisateurs

Outre l'efficience opérationnelle déjà mentionnée, la mise en œuvre d'un processus de gestion des identités et des accès efficace peut aider les utilisateurs à identifier les accès dont ils ont besoin, à soumettre la demande à l'approbateur concerné et à obtenir rapidement l'accès aux informations de travail. Il en résulte moins de mécontentement, un point particulièrement important lors de l'embauche de nouveaux

employés (par exemple, la productivité des nouveaux membres d'une équipe s'accroît lorsqu'ils obtiennent au plus tôt les accès nécessaires pour remplir leur mission).

2.1.6 Efficacité accrue des grands changements au niveau de l'entreprise

Certains changements au niveau de l'organisation nécessitent souvent une modification des droits d'accès. C'est le cas notamment des coentreprises, des contrats de sous-traitance, des désinvestissements, des fusions et des acquisitions. Pour les organisations concernées, la capacité à donner rapidement l'accès à l'information de niveau approprié conditionne le degré de réussite de l'opération. À l'inverse, en l'absence de processus défini, il peut être difficile de déterminer si le niveau correct d'accès a été accordé ou supprimé. Ainsi, pour une coentreprise ou une fusion, il est vital de pouvoir accorder rapidement l'accès aux informations pertinentes et résilier tout aussi rapidement les autorisations d'accès à certaines ressources de la société.

2.2 Concepts relatifs à la gestion des identités et des accès

La gestion des identités et des accès est un processus complexe qui intègre différentes règles, procédures, opérations et technologies nécessitant la coordination de nombreuses entités dans l'ensemble de l'organisation, notamment les ressources humaines et l'équipe informatique. Ce guide doit aider les responsables de l'audit interne à bien connaître les différentes composantes de la gestion des identités et des accès pour mieux appréhender le sujet. Pour une définition plus complète de ces différentes composantes, reportez-vous au glossaire fourni à la fin de cet ouvrage.

Fondamentalement, la gestion des identités et des accès tente de répondre à trois grandes questions :

1. **Qui a accès à quelles informations ?** Un système solide de gestion des identités et des accès aide la société non seulement à gérer les identités numériques, mais également à gérer l'accès aux ressources, aux applications et aux informations dont ces identités ont besoin.
2. **L'accès est-il adapté au travail à accomplir ?** Cette question comporte deux volets. D'abord, l'accès est-il adapté et défini de façon à permettre la réalisation d'une mission donnée ? Ensuite, l'accès à une ressource donnée entre-t-il en conflit avec d'autres droits d'accès et peut-il entraîner un problème de séparation des tâches ?
3. **L'accès et les opérations réalisées sont-ils correctement surveillés, consignés et enregistrés ?** Outre les gains d'efficacité dont bénéficie l'utilisateur, les procédures de gestion des identités et des accès devraient être conçues afin de faciliter la conformité réglementaire. L'une des principales conséquences concrètes de la loi Sarbanes-Oxley, entre autres, est l'obligation de définir, documenter, surveiller, consigner et enregistrer correctement les droits d'accès.

2.3 Risques liés à la gestion des identités et accès

La création d'une procédure de gestion des identités et des accès permet des changements dans les activités de l'entreprise et du personnel, mais nécessite aussi des investissements en capitaux. L'instauration, dans une organisation, de procédures de gestion des identités et des accès peut réduire certains risques existants et en créer d'autres. Lors de la mise en œuvre de nouvelles procédures ou leur modification, il convient d'analyser et de bien comprendre ces risques. Il faut notamment tenir compte des points suivants :

- **Passivité.** De nombreuses organisations se contentent de maintenir certains processus sans rien modifier, même si, en l'état, ils ne permettent pas un contrôle efficace et adapté.
- **Participation.** Pour réussir, tout projet d'envergure nécessite du temps et l'implication de différentes ressources. Si l'organisation ne leur consacre pas suffisamment de temps, les opérations qui le constituent risquent de ne pas être correctement réalisées.
- **Planification.** Pour réussir un projet, il faut des plans bien construits, des jalons de livraison et des processus permettant la conduite du changement pour atteindre les objectifs au regard des contraintes de ressources et de délais.
- **Communication.** Les objectifs du projet de gestion des identités et des accès, les opérations prévues et les besoins en ressources doivent être communiqués aux partenaires concernés, sans quoi les personnes censées participer au projet ne seront pas en mesure d'apporter leur contribution.
- **Intégration de l'ensemble des systèmes au processus.** Les projets de gestion des identités et des accès sont complexes et demandent généralement beaucoup de temps. Très lourde, l'intégration en une seule fois de plusieurs systèmes informatiques dans la structure de gestion des identités et des accès peut être vouée à l'échec. Il est préférable, dans un premier temps, de hiérarchiser les principales zones de risque de l'entreprise et les ressources système concernées.
- **Complexité du processus.** Parallèlement au risque de passivité, réviser un processus complexe peut en compromettre la réussite. Les utilisateurs risquent alors, par exemple, de tenter de contourner le processus ou de créer leur propre processus.

- **Manque de précision du processus.** Si le processus de gestion des identités et des accès n'est pas précisément défini, s'il est flou ou s'il peut prêter à différentes interprétations, il encouragera des pratiques déviantes ne correspondant pas à une utilisation efficace du processus de gestion des identités et des accès.
- **Absence de contrainte dans l'utilisation.** Des contraintes adaptées doivent accompagner la mise en œuvre, le pilotage et l'utilisation du processus de gestion des identités et des accès, pour qu'il fonctionne comme prévu. Si les utilisateurs sont autorisés à employer des processus différents ou à contourner les processus établis, la réussite globale du projet peut être compromise.

Même si certains de ces risques peuvent être atténués ou éliminés, ils doivent être identifiés, compris et classés par ordre de priorité avant, pendant et après la conception du processus de gestion des identités et des accès.

3. Définition des principaux concepts

Les concepts ci-après seront traités dans les sections qui suivent :

- **Identité :** élément ou ensemble d'éléments permettant d'identifier une personne ou une machine de façon univoque. Il peut s'agir d'un élément à connaître, par exemple un mot de passe ou un numéro d'identification (ID) personnel ; d'un élément à avoir, par exemple une carte d'identification, un jeton de sécurité ou un jeton logiciel ; d'une caractéristique de la personne, par exemple une empreinte digitale ou rétinienne ; ou d'une combinaison de ces différents éléments.
- **Accès :** information correspondant aux droits accordés à une identité. Ces droits d'accès aux informations peuvent être affectés à des utilisateurs pour leur permettre de réaliser différents niveaux d'opérations, par exemple : la copie, le transfert, l'ajout, la modification, la suppression, la révision, l'approbation, la lecture seule et l'annulation.
- **Habilitations :** ensemble des droits d'accès nécessaires pour réaliser les opérations. Remarque : le terme habilitation est utilisé occasionnellement comme synonyme de droits d'accès.

Lorsque la notion d'identité est évoquée, la plupart des cadres pensent aux utilisateurs humains. Toutefois, il ne faut pas oublier qu'il existe aussi des comptes de service, des identités de machine et d'autres identités non humaines à gérer. L'absence de contrôle de l'une ou l'autre de ces identités et de leur accès peut être préjudiciable à la structure globale de contrôle de l'organisation.

Pour que les identités deviennent véritablement une partie intégrante de l'ADN des organisations et de son système de gestion des accès, elles doivent passer par :

- **Provisionnement.** Le provisionnement renvoie à la création, la modification, la résiliation, la validation, l'approbation, la diffusion et la communication d'une identité. L'étendue de cette opération et le temps nécessaire varient en fonction des besoins précis de l'organisation. De plus, le provisionnement doit être géré par des principes propres à l'organisation et universellement appliqué. Ces principes sont rédigés et mis à jour par la DSI avec la contribution des autres directions métiers.
- **Gestion des identités.** La gestion des identités doit faire partie des opérations courantes de l'organisation. Elle comprend l'élaboration d'une stratégie de gestion des identités et des accès, l'administration des évolutions sur la politique de gestion des identités et des accès, l'élaboration de paramètres applicables aux identités et aux mots de passe, l'administration des systèmes et processus manuels ou automatiques de gestion des identités et des accès et enfin, la surveillance, l'audit, le rapprochement périodiques des systèmes de gestion des identités et des accès et l'élaboration de rapports réguliers.
- **Utilisation.** L'utilisation passe par l'authentification, l'autorisation et l'enregistrement des identités utilisées dans les systèmes informatiques de l'organisation. Les droits d'accès sont essentiellement appliqués par le biais de processus ou de dispositifs automatiques.

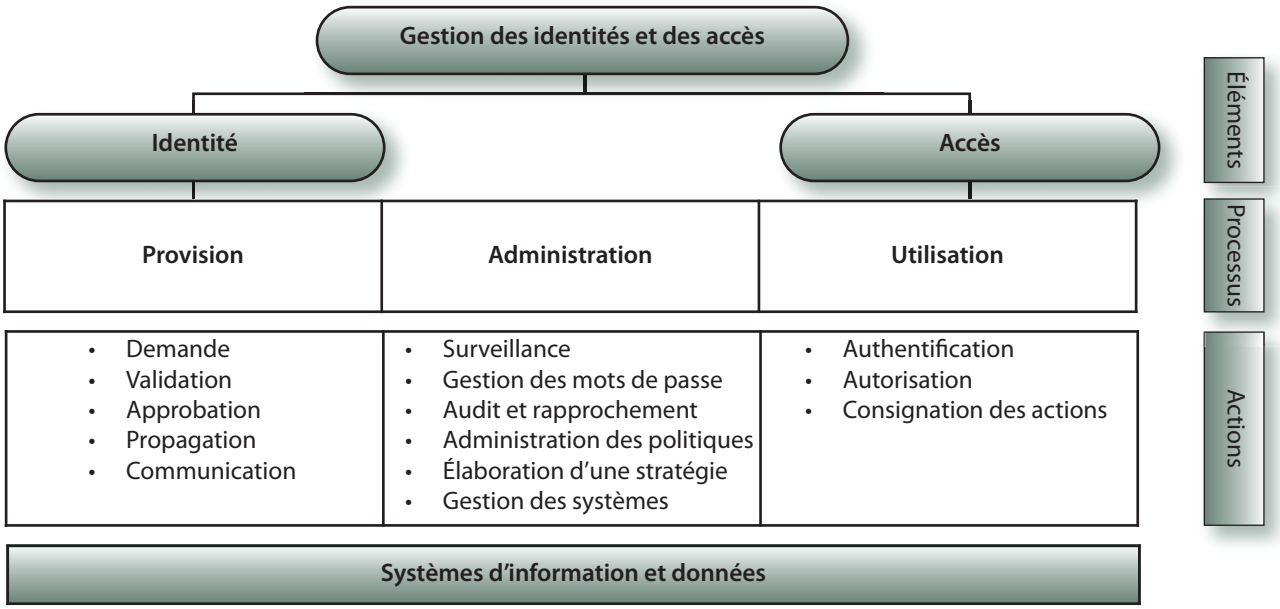


Figure 1. Relations entre éléments de la gestion des identités et des accès et concepts clés

3.1 Gestion des identités et gestions des habilitations

3.1.1 Processus de gestion des identités et des accès

L'objectif d'un processus de gestion des identités et des accès est d'initier, de modifier, de suivre, d'enregistrer et de résilier les identifiants spécifiquement associés à chaque compte, humain ou non, à l'aide des ressources informatiques de l'organisation. Cette dernière doit donc utiliser le processus de gestion des identités et des accès pour gérer ces identifiants et leur association avec des comptes utilisateur. Il faut pour cela que le processus de gestion des identités et des accès soit conçu de manière à intégrer les applications auxquelles le compte utilisateur doit pouvoir accéder et à déterminer de quelle façon les identifiants (s'ils sont différents d'une application à l'autre) sont associés à l'utilisateur. La figure 1 montre comment les différentes composantes de la gestion des identités et des accès s'articulent entre elles.

3.1.2 Gestion des habilitations

Dans le cadre du processus de gestion des identités et des accès, la gestion des habilitations doit être conçue pour créer, modifier, suivre, enregistrer et résilier des habilitations ou des permissions d'accès attribués aux comptes utilisateur. Quelle que soit la méthode utilisée par l'organisation pour regrouper les comptes utilisateurs sous des fonctions similaires (groupes de travail, rôles ou profils), les habilitations de chaque utilisateur doivent être correctement gérées. Elle doit donc procéder régulièrement à un inventaire des droits d'accès pour identifier les utilisateurs qui accumulent les habilitations à mesure qu'ils changent de poste au sein de l'organisation et ceux qui se voient attribuer des habilitations incorrectes. Pour réaliser cette revue des droits d'accès, les directions métiers doivent demander un relevé des droits et communiquer les changements nécessaires à la DSI via les dispositifs de gestion des identités et des accès adéquats.

Un processus de gestion des habilitations bien conçu doit intégrer une analyse de la séparation des fonctions. Celle-ci peut empêcher l'attribution d'un ensemble d'habilitations, qui donnerait à une personne un accès inapproprié à un processus, ou permettre de détecter les conflits existants.

3.2 Éléments de la gestion des identités et des accès

3.2.1 Types d'identités

Dans une organisation, les identités revêtent des formes multiples et doivent toutes êtres prises en compte dans un processus de gestion des identités.

Voici quelques-uns des types d'identités susceptibles d'être présents :

- employés utilisant les ressources informatiques ;
- fournisseurs (par exemple, sous-traitants) ;
- dispositifs informatiques (par exemple, matériels assurant des fonctions similaires à celles d'un utilisateur, notamment les applications fixes et mobiles) ;
- comptes de services applicatifs (par exemple, comptes prédéfinis fournis par le fournisseur du logiciel) ;
- comptes machine (par exemple, matériels réalisant des fonctions à l'intérieur ou entre des environnements ou des applications informatiques tels que les serveurs) ;
- comptes fonctionnels ou comptes systèmes (par exemple, comptes utilisés pour réaliser des traitements par lots, comme la génération nocturne de rapports).

Lors de l'audit des identités présentes dans l'organisation, les auditeurs doivent déterminer si un identifiant spécifique est systématiquement associé à chaque type d'identité. Cela permet d'appliquer des règles différentes aux procédures de gestion et d'analyse correspondant aux divers types de comptes. Ainsi, un compte système peut être soumis à des règles et nécessiter un type d'analyse différent de ceux d'un compte utilisateur.

3.2.2 Gestion des arrivées (Onboarding)

Lorsqu'une identité est nécessaire, il faut la créer dans l'environnement informatique. Le processus manuel ou automatique qui permet de créer l'identité est appelé « Gestion des arrivées » ou « *Onboarding* » et comprend la création du profil de l'identité et des informations nécessaires pour décrire cette identité.

3.2.3 Gestion des départs (Offboarding)

La gestion des départs ou « *offboarding* » est l'inverse de la gestion des arrivées. Au cours de ce processus, les identités qui n'ont plus besoin de droits d'accès à l'environnement informatique sont identifiées et désactivées. On vérifie qu'elles sont inactives et on les supprime de l'environnement informatique au terme d'un délai prédéfini.

3.3 Droits d'accès et habilitations

3.3.1 Modification des droits d'accès des identités ou des habilitations

Provisionnement et modification des droits d'accès

Lorsqu'à la suite d'un processus de provisionnement, un utilisateur se voit attribuer une identité, l'approbation par le

propriétaire du système et l'analyse de la demande d'accès par la DSI doivent inclure une évaluation des droits d'accès accordés ou modifiés. La DSI ne doit pas être responsable de l'approbation des identités des utilisateurs, mais doit participer à l'opération car c'est elle qui sait le mieux comment s'articulent les droits d'accès accordés sur les différents systèmes informatiques.

Droits d'accès des comptes non humains

De nombreuses applications, bases de données et outils nécessitent l'utilisation de comptes fonctionnels. Ces comptes ne servent généralement pas à l'authentification d'un utilisateur particulier mais à la communication entre deux composants du système. Ainsi, pour fonctionner, la plupart des systèmes de gestion de bases de données (SGDB) exigent la création et l'activation de comptes spécifiques pour le système qui les héberge. L'organisation doit donc mettre en place une procédure adaptée pour la création de ces comptes, limiter leur accès aux habilitations concernées, surveiller qui a accès aux authentifiants du compte et révoquer les comptes quand ils ne sont plus utiles.

3.3.2 Accorder des droits d'accès à des comptes privilégiés

Accorder un accès de compte privilégié à une identité

Les comptes privilégiés sont généralement attribués à la personne, au sein de la DSI, chargée de l'administration des systèmes informatiques, notamment des périphériques et des applications réseau et de l'infrastructure informatique générale. En général, l'organisation accorde à ces utilisateurs un niveau d'accès qui leur permet d'apporter des modifications globales, parfois non documentées, à l'environnement informatique. Pour empêcher tout accès non justifié ou inopportun à ces comptes, l'organisation doit inclure, dans sa politique de gestion des identités et des accès, une section concernant leurs règles de provisionnement, d'administration et d'utilisation.

Surveillance des comptes privilégiés

Il existe des comptes privilégiés dans toutes les organisations. En raison des risques qu'ils représentent, ils sont généralement confiés à des personnes fiables. Malgré toute la confiance accordée à ces personnes, la DSI doit régulièrement effectuer certaines des opérations suivantes :

- vérifier la liste des utilisateurs bénéficiant d'un accès privilégié ;
- vérifier, dans la mesure du possible, les activités des comptes privilégiés ;
- vérifier les opérations en ligne de ces comptes privilégiés pour détecter toute transmission non justifiée de données sensibles ou l'introduction inappropriée d'applications non approuvées.

3.3.3 Séparation des fonctions

Conflits

Au cours du processus de provisionnement, les personnes chargées d'approuver les demandes d'accès doivent déterminer si la demande risque de provoquer un conflit de séparation des tâches. La DSI peut constater ce type de conflit en créant ou en modifiant l'identité d'un utilisateur. Dans ce cas, il doit signaler le problème au propriétaire du système ou à l'approbateur. L'analyse de la séparation des tâches peut être automatisée et servir de contrôle préventif avant tout octroi de nouveaux droits d'accès.

Surveillance périodique des droits d'accès

Dans le cadre du processus de surveillance de la gestion des identités et des accès, l'organisation doit mettre en place une méthodologie de vérification périodique des droits d'accès accordés à toutes les identités présentes dans l'environnement informatique. Cette vérification, bien que facilité par la DSI, devrait être essentiellement menée par l'entité concernée avec l'approbation de chaque propriétaire de système responsable. Par ailleurs, les identités des comptes privilégiés et des comptes informatiques doivent être vérifiées par le responsable ou le propriétaire de système concerné.

3.4 Provisionnement

La figure 2 présente la progression logique des opérations du processus de provisionnement.

3.4.1 Demande d'accès

Le processus de demande de création, suppression ou modification d'une identité doit être détaillé dans une procédure :

- Comment sont effectuées les demandes pour les différents types d'identités (par exemple, demandes manuelles ou électroniques, appels au centre d'assistance) ?
- Où doivent être transférées les demandes ?
- Quels sont les délais à respecter pour déposer une demande ?
- Quel est le résultat attendu ?

3.4.2 Approbation

Toute demande d'identité doit faire l'objet d'un processus d'approbation en plusieurs étapes. La requête initiale doit être approuvée par le responsable hiérarchique direct du demandeur, avant que la demande ne soit transmise à la DSI. Lorsque le premier niveau d'approbation est franchi, un second niveau peut être requis et sera alors accordé par le propriétaire de l'application. Une fois les approbations

nécessaires obtenues, la demande doit être transmise à la DSI ou au système concerné pour être traitée.

3.4.3 Propagation et création d'identités

Lorsque la création de l'identité a été approuvée conformément aux règles de l'organisation, l'identité est créée par un membre de la DSI ou par une application automatique gérée par celle-ci. Les éléments suivants doivent être pris en compte lors de la création d'une identité :

- fonction du demandeur au sein de l'organisation ;
- utilisation prévue de l'identité ;
- accès accordé au titulaire de l'identité, basé sur des rôles, des règles ou des besoins spécifiques de l'utilisateur ;
- L'identité peut-elle être dupliquée à partir d'un rôle existant ou faudra-t-il créer un nouveau rôle correspondant aux besoins de l'utilisateur ?

Pour créer une identité, il faut savoir comment elle sera employée, quelles applications elle utilisera et le temps de restrictions qui lui seront appliquées ou pas. La création de l'identité et d'un mot de passe associé doit également tenir compte des restrictions associées à chaque application, conformément à la politique de l'organisation.

Lorsque la DSI attribue une identité à une personne, elle lui affecte le plus souvent un mot de passe temporaire à modifier dès la première tentative de connexion.

Pendant cette étape du processus de gestion des identités et des accès, les habilitations ou droits d'accès affectés à l'identité doivent être évalués en tenant compte de la fonction de l'identité dans l'organisation, afin de déterminer s'il y a des conflits d'intérêt au niveau de la séparation des tâches.

3.4.4 Communication

Dans sa politique, l'organisation doit définir ses procédures d'information lors de la création, de la suppression ou de la modification des identités utilisateur. Elle doit également désigner un lieu ou un service centralisé, différent de la DSI, depuis lesquels les communications sur les identités seront adressées.

Par ailleurs, la DSI doit utiliser un dispositif dédié à la réception et à l'envoi des communications concernant la création, la suppression ou la modification des identités. Ce moyen de communication peut prendre la forme d'un message automatique, d'un message verbal ou d'un document papier.

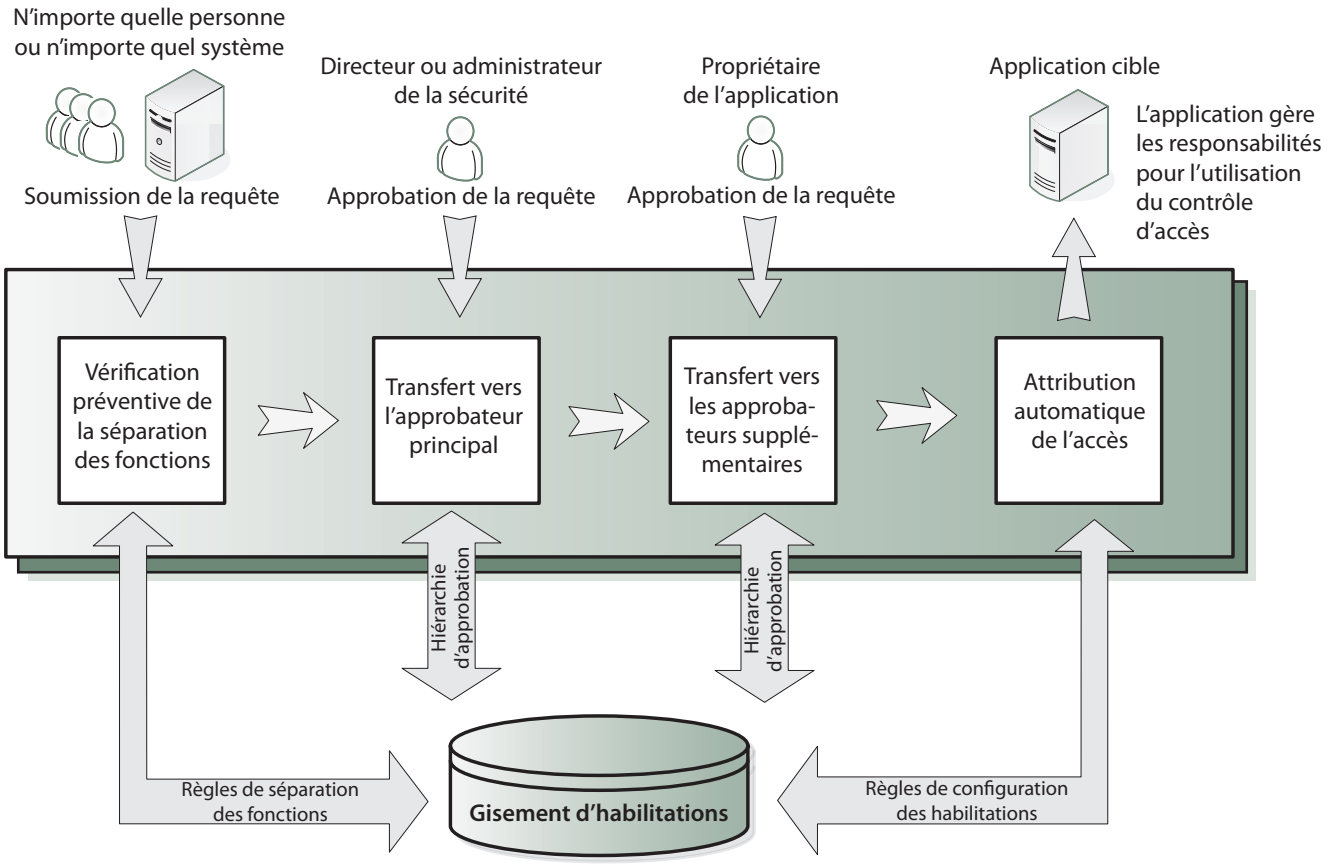


Figure 2. Schéma d'un flux logique de provisionnement automatique.

Toute communication relative aux identités doit respecter la politique de classification des données de l'organisation. Si la création ou la modification d'une identité sont notifiées par voie électronique ou sur papier, le personnel doit connaître les restrictions, en fonction de la classification de ces données, et les exigences applicables aux informations de configuration de l'identité. Par exemple, les communications contenant un mot de passe devraient être envoyées sous enveloppe cachetée, dans des messages électroniques codés ou par d'autres moyens sécurisés. L'organisation doit également demander aux utilisateurs de changer leur mot de passe après la première utilisation pour éviter toute usurpation d'identité et pour réduire les risques liés à l'interception du mot de passe par un tiers non autorisé.

3.4.5 Consignation

Un gisement d'habilitations est un système qui réalise le suivi des privilèges accordés au fil du temps aux utilisateurs et qui enregistre les demandes d'accès, les approbations, les dates de début et de fin et les informations détaillées relatives à l'accès accordé. Ces données peuvent servir lors de l'audit des accès, de la revue des habilitations des utilisateurs et de la vérification de l'approbation des opérations d'accès.

Les données consignées doivent être conservées pendant une période définie, puis détruites. La durée de conservation doit dépendre de la nature de l'accès consigné, des exigences réglementaires et des obligations d'audit, des politiques de l'entreprise et des contraintes de stockage des données.

3.5 Administration des identités et des droits d'accès

3.5.1 Audit et rapprochement périodiques des identités et des habilitations

Audits périodiques

Pour évaluer la conception et l'efficacité du système de gestion des identités et des accès d'une organisation, des audits périodiques du processus s'imposent. La fréquence des audits doit être définie lors de l'élaboration des plans annuels d'audit, qui découle de l'évaluation annuelle des risques réalisée par l'audit interne. Les audits eux-mêmes doivent comporter les éléments suivants :

- une identification de la concentration des risques liés aux identités, de la plus élevée à la plus faible ;
- un réexamen du processus de gestion des identités et des accès tel qu'il a été conçu ;
- un examen de l'efficacité fonctionnelle du processus de gestion des identités et des accès ;
- une analyse du processus de provisionnement, qui doit inclure une évaluation d'un échantillon représentatif des identités actives au cours d'un intervalle quelconque de la période contrôlée ;
- un examen de l'efficacité des opérations d'exécution de la gestion des identités et des accès ;
- un examen de l'efficacité des opérations administratives de gestion des identités et des accès.

Séparation des fonctions

Les processus et méthodologies de gestion des identités et des accès ne doivent pas être les seuls dispositifs de contrôle utilisés pour empêcher les identités utilisateur d'accéder à des données qui ne les concernent pas. L'organisation doit donc mettre en place des méthodes de vérification ou de rapprochement des identités des utilisateurs et de leurs droits d'accès avec ceux initialement approuvés. Ce rapprochement peut faire apparaître les situations suivantes :

- Les identités possèdent les droits d'accès correspondant à ceux approuvés.
- Les identités n'ont pas été les droits d'accès vérifiés et approuvés à la fréquence prévue.
- Les identités possèdent des droits d'accès qui ne correspondent pas aux droits approuvés.
- Il existe encore, dans l'environnement informatique, des identités associées à des utilisateurs qui ont été révoqués ou désactivés.
- Certains utilisateurs qui possèdent une identité et des droits d'accès n'ont fait l'objet d'aucune demande d'accès ou d'approbation.

Si le processus de vérification et de rapprochement révèle un décalage entre les identités et les droits d'accès, l'organisation doit disposer d'un moyen pour signaler ces problèmes, déterminer les mesures à prendre et obtenir les approbations nécessaires pour corriger ces défaillances.

Examen des habilitations

L'existence de processus de gestion des identités et des accès matures peut faciliter l'examen des accès par les managers et les propriétaires d'applications. Les managers peuvent vérifier les accès accordés à leurs employés directs, tandis que les propriétaires d'applications vérifieront les accès octroyés à toutes les personnes utilisant l'application, afin d'identifier et de révoquer les droits d'accès injustifiés. Cette vérification doit être réalisée au moins une fois par an, voire plus souvent pour les applications stratégiques ou les personnes à haut risque.

3.5.2 Gestion de la politique

L'organisation doit disposer d'un moyen de vérifier et réviser périodiquement sa politique de gestion des identités et des accès afin qu'il tienne compte des processus et des activités actuels pertinents.

3.5.3 Stratégie de gestion des identités et des accès

Un plan complet de création, de modification et de maintien des politiques, composantes, processus et activités de gestion des identités et des accès doit être élaboré soit par la DSI, soit par un groupe stratégique au sein de l'organisation. Ce plan doit indiquer comment l'organisation doit traiter le processus de gestion des identités et des accès ainsi que les risques y afférents, présents et à venir ; il doit préciser si les processus de gestion des identités et des accès et les activités associées seront effectués par des moyens manuels ou électroniques ; il doit enfin signaler si le processus de gestion des identités et des accès couvrira ou non tous les secteurs de l'organisation.

3.5.4 Administration des systèmes de gestion des identités et des accès

Lorsque les processus de gestion des identités et des accès sont en place dans l'organisation, ils doivent être administrés soit manuellement, soit par des moyens électroniques, soit par une combinaison des deux. L'administration du processus de gestion des identités et des accès passe d'abord par l'administration de l'infrastructure. Il s'agit notamment de déterminer :

- l'endroit où sont centralisés les processus de gestion des identités et des accès ;
- si l'administration des processus de gestion des identités et des accès doit faire appel à des technologies et, si c'est le cas, l'endroit où elles seront hébergées ;
- qui sont les propriétaires du processus de gestion des identités et des accès, à la DSI et dans les différentes directions ;
- quelles méthodes de documentation et de consignation des changements sont utilisées.

3.5.5 Administration des mots de passe des utilisateurs finaux

Lorsqu'une identité est créée, un mot de passe initial lui est généralement attribué. Ce mot de passe initial, généré manuellement ou automatiquement, est communiqué à l'utilisateur par la DSI. Si la gestion des identités et des accès renvoie avant tout aux identités et aux droits d'accès des utilisateurs, l'émission et la gestion des mots de passe des utilisateurs sont également à prendre en compte. Les paramètres, la structure et les règles d'utilisation des mots de passe doivent être détaillés dans la politique de sécurité de l'organisation.

La gestion des mots de passe utilisateur est un facteur essentiel de l'efficacité du processus de gestion des identités et des accès. La gestion des mots de passe comprend les tâches suivantes :

- émission des mots de passe initiaux ;
- communication des mots de passe aux utilisateurs ;
- réinitialisation des mots de passe pour les utilisateurs bloqués ;
- vérification des opérations sur les mots de passe selon les règles définies dans la politique de l'organisation ;
- recherche des mots de passe faciles à deviner, qui peuvent entraîner un détournement des ressources informatiques de l'organisation.

3.5.6 Remarques sur la conservation et le traitement

Le processus de gestion des identités et des accès doit également préciser les moyens mis en œuvre par l'organisation pour la conservation, l'élaboration de rapports, la protection et la gestion des identités et des droits d'accès. Quand l'organisation conserve des identités et des droits d'accès, elle doit savoir où se trouvent ces informations, savoir comment elles apparaîtront à l'affichage ou dans les rapports (autrement dit, s'ils seront masqués ou en texte clair), connaître la durée de conservation et savoir comment les identités désactivées, mises hors service et supprimées seront conservées.

3.5.7 Élaboration de rapports

Le processus de provisionnement nécessite la création et l'utilisation de différents types de rapports. La plupart des rapports généralement créés sont utilisés pour des opérations telles que les mesures de performance du système, la gestion des tâches et des files d'attente et les événements dans le cadre des rapprochements. Les rapports d'audit décrivent notamment :

- les listes des identités et des accès associés ;
- la personne chargée d'approuver l'accès à des informations données ;
- la gestion des comptes de groupe et des comptes de supervision ;
- le nombre d'utilisateurs qui accèdent à une application ou à une ressource informative donnée.

De plus, les processus et les systèmes auxiliaires doivent être documentés grâce à des rapports détaillant les approbations et les vérifications d'accès. Il s'agit souvent des points faibles identifiés au moment de l'audit du processus de gestion des identités et des accès.

3.6 Mise en place des processus

3.6.1 Authentification et autorisation

La mise en place des identités et droits d'accès correspondants est effective lorsque l'utilisateur ouvre une session sur l'application (cf. figure 3). A l'ouverture de la session, l'application vérifie l'identité de l'utilisateur avant de la valider. Cette opération, appelée authentification, peut revêtir des formes diverses.

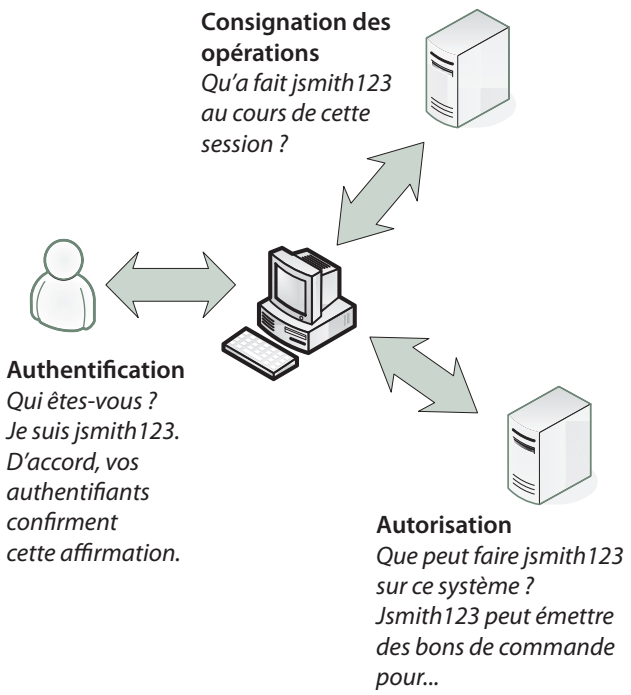


Figure 3. Mise en place des droits d'accès des utilisateurs.

Ainsi, sur certains systèmes, l'authentification peut exiger l'emploi d'une caractéristique de l'utilisateur (par exemple, identification par empreinte digitale ou par reconnaissance vocale), d'un objet de l'utilisateur (une carte à puce, un badge, un porte-clé, etc.) ou d'une information connue de lui seul (par exemple, un mot ou une phrase de passe).

Une fois l'identité reconnue et validée, l'utilisateur peut utiliser les fonctions de l'application selon ses droits d'accès. Une autorisation de l'identité utilisateur doit s'appuyer sur les droits d'accès accordés lors du processus de provisionnement. Souvent, l'autorisation d'une identité utilisateur peut ne pas correspondre aux droits d'accès prévus lors du provisionnement. La surveillance et la vérification des droits d'accès sont donc des composantes importantes du processus de gestion des identités et des accès.

3.6.2 Enregistrement

L'enregistrement des identités utilisateur, de leurs droits d'accès et de leurs fonctions dans l'application permet à l'organisation de vérifier différents points :

- Les droits d'accès correspondent-ils aux droits d'accès approuvés pour l'identité utilisateur en question ?
- Les identités utilisateur et les droits d'accès associés sont-ils en décalage par rapport aux droits d'accès requis par l'identité utilisateur pour remplir sa mission ?
- Les identités utilisateur exploitent-elles toutes les fonctions qui leur ont été accordées lors du processus de provisionnement ?
- Les identités utilisateur demandent-elles fréquemment une modification du mot de passe ?
- Les identités utilisateur accèdent-elles ou tentent-elles d'accéder aux applications en dehors des heures habituelles de travail ?
- Des utilisateurs, enregistrés ou non, tentent-ils d'exécuter certaines fonctions sans y être autorisés ?

3.7 Recours aux technologies pour la gestion des identités et des accès

3.7.1 Quels sont les types de technologies disponibles ?

Pour l'administration des activités de gestion des identités et des accès, il est possible d'automatiser la plupart des processus de provisionnement et de mise en place grâce à des logiciels de gestion des identités et des accès. Ces applications peuvent être faciles à installer et utilisables par les organisations disposant d'une DSI restreinte (par exemple, de moins de 10 personnes) ou nécessiter une personnalisation, et seront alors utilisées par des organisations possédant une DSI importante ou centrale.

3.7.2 Avantages et inconvénients du recours à la technologie

Si le recours à la technologie facilite indéniablement la gestion des identités et des accès, il présente des avantages et des inconvénients. Parmi les avantages :

- temps de réponse plus courts ;
- indices d'activité facilement accessible;
- automatisation des processus d'approbation et de communication ;
- amélioration de la gestion des gros volumes de données ;
- centralisation de l'administration et la surveillance des systèmes.

Parmi les inconvénients :

- propriété mal définie;
- mauvaise connaissance de l'usage des outils ;
- outils parfois inadaptés à la taille ou à la complexité de l'organisation.

3.7.3 Comment la technologie est-elle utilisée ?

Le recours à la technologie dans le processus de gestion des identités et des accès permet de remplacer certaines activités manuelles ou de compenser l'absence de certaines activités de gestion des identités et des accès. Les directions métiers doivent bien connaître les technologies mises en œuvre et comprendre les raisons de cette utilisation. La DSI, quant à elle, doit se charger d'installer les outils nécessaires et de les gérer pour répondre aux besoins de l'organisation.

Les outils peuvent être utilisés pour les opérations suivantes :

- générer des formulaires de demande d'accès ;
- transférer des formulaires de demande d'accès vers les approbateurs ;
- analyser en amont les conflits de séparation des tâches ;
- notifier la création, la modification et la résiliation des identités ;
- authentifier et autoriser des identités pouvant accéder aux applications ;
- générer des fichiers-journaux où figurent les identités et leur utilisation ;
- générer des mots de passe.

3.7.4 Autres concepts

Authentification unique (*Single sign-on* ou SSO)

Il existe de nombreuses façons d'authentifier une identité dans un système de gestion des identités et des accès. L'authentification unique est une méthode automatique d'authentification d'une identité applicable à toutes les ressources informatiques sur lesquelles cette identité dispose de droits d'accès, sans qu'elle ait à fournir plusieurs fois ses données d'authentification (identification et mot de passe de l'utilisateur).

Authentification à distance

Dans de nombreuses organisations, les identités, et plus particulièrement les identités humaines, se voient accorder des droits d'accès pour s'authentifier sur les ressources informatiques lorsque l'utilisateur se trouve à l'extérieur de l'organisation. Ce type d'accès et d'authentification à distance peut se faire selon différentes méthodes plus ou moins sécurisées. En voici quelques exemples :

- Réseaux privés virtuels : connexions grâce à des périphériques réseau entre les bureaux de l'organisation et le site distant où se trouve l'identité.
- Portails Web : connexions avec les bureaux de l'organisation via une interface Internet.
- Modems à numérotation automatique : connexions entre le site de l'identité et celui de l'organisation par le biais des lignes téléphoniques, comme pour les appels vocaux.

Ces types de connexion à distance ont chacun des avantages et des inconvénients. Ainsi, l'accès par un portail Web est le plus universel, puisqu'il permet aux utilisateurs d'accéder aux ressources depuis pratiquement n'importe quel système connecté à Internet. Cependant, les informations privées et confidentielles sont exposées au risque d'être compromises étant donné que le système sur lequel se trouve le navigateur Web n'est pas contrôlé. Les modems à numérotation automatique offrent une connexion directe avec le réseau interne relativement sûre, mais beaucoup moins rapide que les solutions utilisant une connexion Internet haut débit. Ce ne sont là que deux exemples des nombreux facteurs à prendre en compte lorsque l'on détermine quels utilisateurs doivent être autorisés à se connecter à distance à l'environnement informatique et selon quelles méthodes.

4. Le rôle des auditeurs internes

Les auditeurs internes ont un rôle important à jouer dans l'élaboration de processus efficaces pour la gestion des identités et des accès et dans la surveillance de leur mise en œuvre dans l'organisation. Avant de procéder à un audit de la gestion des identités et des accès, les auditeurs doivent bien cerner la structure existante de la gestion des identités et des accès, notamment l'architecture de l'organisation et ses règles de gestion des identités et des accès, ainsi que les obligations légales, réglementaires et autres à respecter. Lors de l'audit, ils doivent répertorier les processus de l'organisation qui concernent les identités et les habilitations, comme par exemple les annuaires de données et les étapes du cycle de vie de chacun de ces processus. Ils doivent aussi évaluer les contrôles existants pour les activités de gestion des identités et des accès.

4.1 Processus de gestion des identités et des accès actuels

La première étape du processus de gestion des identités et des accès consiste à déterminer si l'entreprise a établi un programme de gestion des identités et des accès. Pour cela, on peut s'aider des questions suivantes :

- Existe-t-il des politiques de gestion et d'administration des activités des identités et des accès ?
- Une stratégie a-t-elle été mise en place pour le traitement des risques liés au processus de gestion des identités et des accès ?
- Existe-t-il un modèle de référence utilisable par l'organisation au cours du processus d'administration ?

En répondant à ces questions, il est important de préciser s'il existe déjà une documentation traitant, dans une certaine mesure, de ces problèmes.

Par ailleurs, les auditeurs internes qui évaluent la position d'une organisation vis-à-vis de la gestion des identités et des accès doivent identifier certains éléments clés.

Comme le montre la figure ci-après, ces éléments ne sont pas tous de nature technologique mais incluent également :

- l'alignement métier et la gestion des entités ;
- la connaissance des lois et réglementations existantes ;
- l'élaboration de budgets ;
- le développement de plans de mise en œuvre réalisables ;
- l'identification des moyens technologiques favorisant un environnement de contrôle plus efficace.

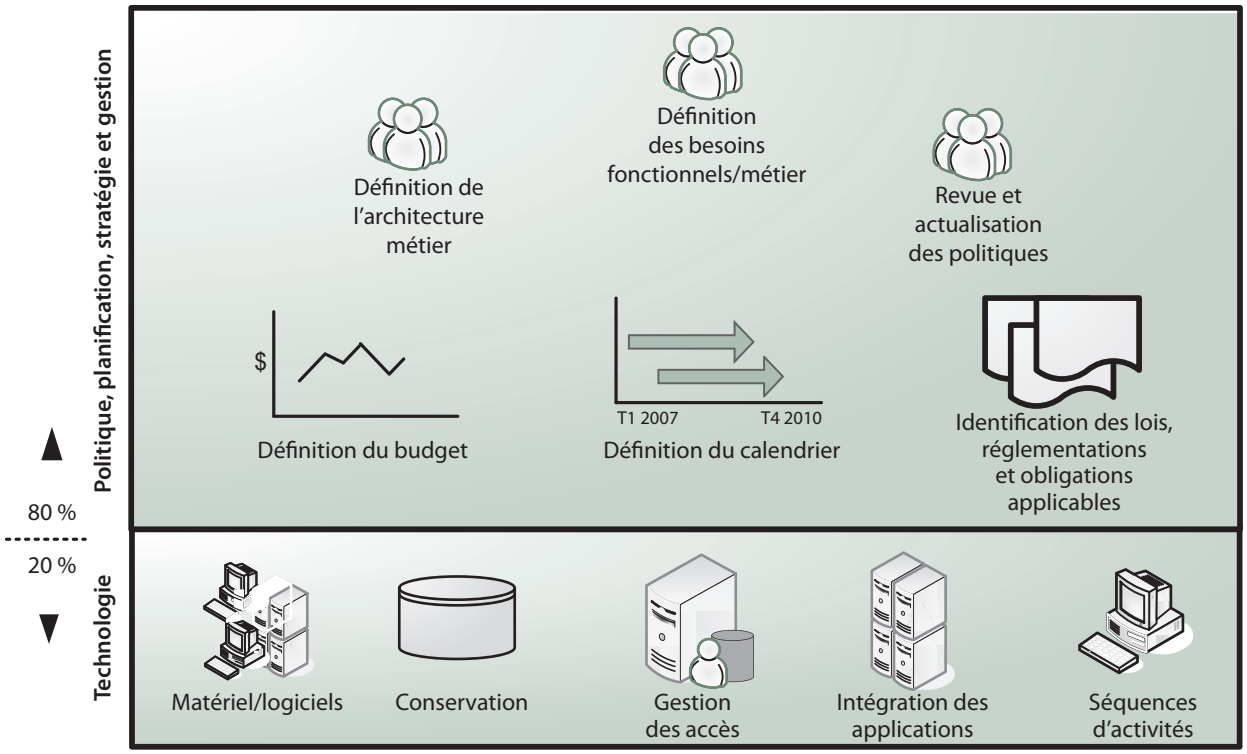


Figure 4. La gestion des identités et des accès, un système axé sur les processus.

4.1.1 Architecture d'entreprise

L'architecture de la gestion des identités et des accès des directions métiers fait référence aux procédures et à la logique des séquences d'activités mises en œuvre parallèlement à un logiciel de gestion des identités et des accès. La définition et la documentation de cette architecture constituent une étape essentielle pour la gestion des risques « métiers » actuels et futurs. Comme le montre la figure 4, la gestion des identités et des accès ne concerne pas exclusivement le recours à des outils technologiques permettant d'appliquer des règles. Il est plutôt axé sur les processus et varie beaucoup d'une organisation à l'autre. Par exemple, comme avec n'importe quel processus métiers, il est possible d'utiliser simultanément des contrôles automatiques et manuels. Il est donc important pour l'organisation de bien comprendre les contrôles qui participent à la gestion des identités et des accès.

En outre, il est vital pour l'organisation de bien comprendre les rôles et responsabilités des personnes chargées de l'environnement de contrôle et de la gestion des contrôles. Comme de nombreux contrôles sont automatisés ou accomplissent des fonctions informatiques, le management considère souvent qu'ils relèvent de la responsabilité de la DSI. Néanmoins, ce sont les directeurs des directions métiers et les propriétaires des données qui sont responsables du processus d'approbation.

L'engagement de la direction générale est tout autant capital. Elle doit notamment comprendre que les processus applicables à l'organisation doivent être correctement appuyés par les directeurs des directions métiers. Si, par exemple, elle ne s'intéresse pas suffisamment à la gestion des identités et des accès, alors ce processus aura une moindre importance dans l'organisation.

4.1.2 Politiques

Lorsque l'architecture métier a été documentée ou au moins comprise au sein de l'organisation, il reste à examiner ses politiques et ses procédures et celles qui régissent la gestion des accès. Si ces politiques sont souvent complexes et expriment la volonté de l'organisation de gérer l'information de façon sûre, il importe qu'elles soient toutes appuyées par des normes, des procédures, des règles et des principes. Cet ensemble de documents est souvent appelé « cadre de stratégie de l'entreprise ».

De plus, même si la forme et la nature des documents sont spécifiques à chaque organisation, le cadre de la politique doit donner à l'ensemble du personnel suffisamment d'informations sur la façon dont les identités utilisateur et les droits d'accès doivent être gérés, examinés et approuvés. Il explique aussi comment configurer les nouveaux processus, applications, systèmes et annuaires de données pour les adapter à ce cadre et veiller à ce que les nouvelles politiques n'exposent pas l'organisation à des risques excessifs.

4.1.3 Lois, réglementations et obligations

Il est important que l'organisation préserve l'efficacité de ses opérations et applique des processus qui lui permettront de respecter tout un ensemble de lois, réglementations et obligations nationales ou locales. Il ne suffit pas de comprendre ces lois et réglementations : les organisations doivent également en déterminer les impacts sur les processus de gestion des identités et des accès.

Très souvent, les types de données qui peuvent être recueillies et transférées vers ou depuis l'étranger sont strictement définis. Ainsi, les pays dont la législation doit respecter la Directive sur la protection des données personnelles peuvent limiter les informations sur le personnel qui peuvent être transmises à des systèmes et des administrateurs situés dans d'autres pays que celui de l'utilisateur. Toutefois, comme ces données personnelles peuvent être nécessaires à l'examen des habilitations et l'octroi à l'utilisateur d'un accès à des systèmes hébergés dans d'autres pays, il convient de mettre en place des procédures juridiques adaptées à cette situation ou à d'autres situations comparables. C'est pourquoi, lors de l'audit du cadre des politiques régissant le traitement des informations personnelles par l'organisation, il doit exister un processus permettant de déterminer si les lois en vigueur sont bien prises en compte.

4.1.4 Budget

Le budget des projets de gestion des identités et des accès tient compte de la mise en œuvre de nouvelles procédures et d'éventuelles technologies auxiliaires, ainsi que des opérations nécessitées par les nouveaux processus de gestion des identités et des accès. L'évolution de l'organisation en termes de gestion des identités et des accès et la mise en œuvre d'outils technologiques peuvent demander beaucoup de temps et d'argent. Ce financement peut être consacré à du matériel, des logiciels et des consultants ou sous-traitants chargés de mettre en œuvre cette technologie. Lorsque celle-ci a été déployée, des moyens financiers doivent encore être alloués pour les frais de licence et la rémunération du personnel d'assistance interne ou externe. Selon le cycle budgétaire de l'organisation, il peut être nécessaire de procéder à une analyse de rentabilité de la gestion des identités et des accès et de l'intégrer dans le processus budgétaire annuel.

4.1.5 Calendrier

Si un programme de gestion des identités et des accès est en place ou en préparation, il convient d'évaluer les délais de mise en œuvre et de s'adapter aux règles d'élaboration des rapports sur la gestion des programmes de l'organisation. S'il faut respecter des exigences particulières pour l'élaboration de rapports, il est important que les dates correspondantes soient communiquées et gérées conjointement par les bureaux de management du programme de

gestion des identités et des accès et d'autres programmes. En outre, comme pour tout programme complexe, des problèmes de délais peuvent se poser. La revue des programmes et de la capacité à gérer correctement les changements de calendrier permet à l'équipe d'audit de déterminer si le projet a des chances de respecter les délais et les échéances à venir.

4.1.6 Besoins métiers

Qu'il existe ou non un programme de gestion des identités et des accès formel, tous les systèmes doivent pouvoir respecter les exigences de performances. Si un programme est en place, il faut, avant qu'il soit déployé, appliquer un processus simple permettant de savoir si les exigences des partenaires ont été recueillies et examinées. Selon l'état d'avancement du programme, l'organisation doit pouvoir vérifier si les systèmes existants offrent les fonctionnalités nécessaires pour permettre au programme de gestion des identités et des accès de fonctionner efficacement. En l'absence de programme de gestion des identités et des accès formel, ce peut être plus difficile. Les besoins ne sont pas forcément bien documentés ou bien connus du personnel en charge de la gestion de l'environnement informatique.

Avec la loi Sarbanes-Oxley et d'autres réglementations comparables dans le monde entier, de nombreuses organisations ont instauré des contrôles plus stricts sur les processus d'administration des accès. C'est pourquoi, il est recommandé de proposer en interne des informations sur les conditions à remplir pour respecter telle ou telle obligation réglementaire. Il faut dans tous les cas pouvoir répondre *in fine* aux questions suivantes :

- Qui bénéficie d'un accès logique aux informations ?
- Le niveau d'accès est-il adapté ?
- Qui a approuvé l'accès ?

4.2 Audit du programme de gestion des identités et des accès

Qu'un programme défini soit en place ou non, les auditeurs internes doivent examiner les processus de gestion des identités et des accès présents dans le système.

4.2.1 Évaluation de la gestion des identités et des accès

Avant d'élaborer une méthodologie d'audit de la gestion des identités et des accès ou de participer à la création de processus de gestion des identités et des accès, il convient d'examiner les politiques et procédures de gestion des identités existantes. Après avoir identifié les processus en vigueur, les auditeurs internes peuvent aider le management à réaliser une évaluation des risques pour aider l'organisation à construire un processus efficace de gestion des identités.

Outre cette évaluation des risques, les auditeurs internes peuvent aider le management ou l'équipe dédié à la gestion des identités afin de localiser les services de l'organisation dans lesquels pourraient être recrutés de nouveaux membres ou des membres supplémentaires pour leur équipe. À cet égard, les auditeurs internes peuvent être d'une aide précieuse, car ils ont une bonne visibilité de tous les niveaux de l'organisation et connaissent où les secteurs la gestion des identités devrait se concentrer.

Inventaire des identités

Les auditeurs doivent notamment identifier clairement les différentes identités utilisateur présentes dans l'organisation (voir la liste des types d'identités en page 7). Dans chaque catégorie d'utilisateurs, en particulier dans les organisations complexes, certains groupes peuvent être divisés en sous-groupes. Les groupes Fournisseurs et Comptes systèmes sont les plus susceptibles de comporter plusieurs sous-groupes.

Définition des étapes du cycle de vie des identités

Les étapes du cycle de vie des identités sont le provisionnement, l'administration et l'exécution. Pour les définir, les auditeurs doivent déterminer le processus, les contrôles et la documentation correspondant au provisionnement. Par exemple, si les processus sont manuels, de quelle orientation / formation les administrateurs ont-ils bénéficié ? S'ils sont automatisés, le bon fonctionnement de chaque processus est-il confirmé par un retour d'information ?

Identification des contrôles dans le processus de cycle de vie des identités

Comme pour n'importe quel processus, il est vital d'identifier les contrôles y afférents. Dans le processus de cycle de vie des identités, il existe plusieurs points de contrôle clés à vérifier. Les contrôles peuvent porter sur les processus d'approbation pour la création d'identités, les processus de révocation des accès, les revues d'habilitation et l'enregistrement des accès.

Toute création d'identité doit être préalablement approuvée par un membre de l'organisation. Par exemple, toute embauche sera normalement approuvée par un directeur qui, en partenariat avec les Ressources Humaines, aidera à créer l'identité de la nouvelle recrue dans le système. Ce processus consiste notamment à collecter différentes informations personnelles, à vérifier si la personne a déjà travaillé pour l'organisation et, éventuellement, à créer des comptes informatiques pour la personne. Chaque étape de ce processus doit faire l'objet d'une vérification, pour s'assurer de la présence de contrôles suffisants tout au long du cycle de vie de l'identité. La création des identités doit, en effet, être contrôlée pour éviter l'intrusion d'utilisateurs inconnus dans l'environnement informatique.

De plus, l'organisation doit désactiver ou supprimer correctement les identités utilisateur dont elle n'a plus besoin.

C'est pourquoi, les politiques doivent indiquer clairement les procédures lorsque des employés quittent l'organisation. Des revues doivent également être effectuées pour confirmer que les mesures requises ont bien été appliquées.

Localisation des annuaires d'identités

Pour identifier les annuaires, les auditeurs internes doivent déterminer à quel emplacement sont conservées les informations concernant les identités. Il s'agit généralement des ressources humaines et des bases de données de sous-traitants, de fournisseurs de services d'infogérance et des bases de données relatives à la force de vente externe.

Pour les comptes n'ayant pas trait à des personnes, notamment les comptes système, il peut être plus difficile de collecter des données sur la méthode de création, les utilisateurs qui y ont accès ou les informations enregistrées et conservées. Néanmoins, il faut établir une méthodologie pour documenter les types de comptes utilisés.

Identification des contrôles sur les annuaires d'identités

Lorsque les annuaires d'identités ont été identifiés, il faut évaluer les contrôles permettant de protéger les données conservées dans ces annuaires. Cette tâche suppose la réalisation de plusieurs revues détaillées couvrant différents contrôles. Toutefois, ces revues peuvent être menées de la même façon que les revues classiques des systèmes, des bases de données et des applications. Par exemple :

- Les machines, où sont conservées les informations, sont-elles sécurisées ?
- Quelles sont les normes de sécurité appliquées?
- L'organisation applique-t-elle des normes de gestion et d'utilisation de ces systèmes ?
- Les systèmes relèvent-ils des mêmes normes que pour les applications financières en général ?
- L'accès aux systèmes, aux outils et aux annuaires de données relatives à la gestion des identités et des accès est-il géré via le système de gestion des identités et des accès ou par d'autres moyens ?

4.2.2 Évaluation de la gestion des habilitations

Identification des habilitations

Pour être efficaces, les processus de gestion des habilitations nécessitent la collecte de données sur les habilitations accordées, entre autres, aux utilisateurs des plateformes, des applications et de leurs rôles dans les applications. C'est aux auditeurs internes qu'il incombe de déterminer comment les habilitations sont regroupées et quelles sont les permissions dont disposent les utilisateurs pour les périphériques informatiques, les comptes de services, les comptes de machines et les comptes de lots.

Identification du cycle de vie des habilitations

Les auditeurs doivent identifier et documenter toutes les différences entre le cycle de vie des habilitations et celui des identités. En général, il faut identifier, d'une manière ou d'une autre, les grandes étapes suivantes : création, affectation et suppression de l'habilitation.

Par ailleurs, les auditeurs ne doivent pas oublier que les grands programmes de gestion des identités et des accès peuvent comporter des processus destinés à créer de nouvelles habilitations, à les regrouper et à les affecter, soit à des personnes soit à des rôles dans l'organisation. Les organisations de petite taille, elles, peuvent utiliser des formulaires papier ou des feuilles de calcul pour demander et suivre les accès. Quelle que soit la méthode utilisée, il faut qu'une personne de l'organisation approuve l'accès et vérifie qu'il est bien accordé sur le système ou sur l'application.

Identification des contrôles portant sur le cycle de vie des habilitations

L'approbation des accès est l'un des contrôles essentiels du cycle de gestion des habilitations. Ce processus doit être soigneusement étudié en fonction de la nature de l'organisation. Ainsi, dans les petites entreprises, la décision d'accorder des droits d'accès est généralement simple à prendre. Dans des organisations plus grandes, en revanche, il peut être difficile de déterminer de quel accès une personne a vraiment besoin dans le cadre de son travail. De plus, en raison de la complexité de la structure hiérarchique et administrative de nombreuses organisations, l'approbateur désigné peut avoir du mal à savoir quel type d'accès est nécessaire pour la réalisation d'une mission particulière. Enfin, il doit exister des contrôles ne permettant la configuration des systèmes qu'après obtention de l'approbation correspondante.

Identification des annuaires d'habilitations

Les gisements d'habilitations comportent divers mécanismes d'exécution qui doivent être correctement configurés. Pour ce faire, de nombreuses applications sont capables de gérer indépendamment les habilitations. Cette opération passe souvent par des fonctions d'authentification et d'autorisation. Les applications peuvent, par exemple, recourir à un mécanisme d'authentification central, tel qu'un répertoire, ou à un mécanisme d'autorisation central, par exemple un portail ou un système de gestion des accès sur le Web.

De nombreux processus d'entreprise s'appuient sur plusieurs applications et utilisent différents mécanismes d'exécution des authentifications et des autorisations. Quel que soit le mécanisme d'habilitation, les auditeurs internes

doivent déterminer le lieu de conservation des informations d'habilitation et la manière dont elles sont gérées.

Identification des contrôles portant sur les annuaires d'habilitations

Le plus important, lors de l'identification des contrôles sur les annuaires d'habilitations, est de vérifier si le système audité contient les habilitations nécessaires. Les auditeurs doivent notamment déterminer si l'annuaire d'habilitations rend compte avec exactitude des habilitations déjà en vigueur. Il existe souvent des différences entre habilitations théoriques et réelles et il peut être difficile de déterminer l'origine de ces problèmes.

Comme pour les annuaires d'identités, il convient de vérifier tous les systèmes standard, bases de données et normes de sécurité des applications. La revue de la configuration des machines doit être conduite comme toute autre revue de configuration, exactement comme pour l'examen des contrôles portant sur les annuaires d'identités.

Identification du mode d'exécution des rapprochements et de la supervision

Le rapprochement sert avant tout à vérifier que les accès effectifs correspondent bien aux accès approuvés, comme nous l'avons vu précédemment. De nombreuses organisations ont mis en œuvre des processus spécifiques pour la vérification et le rapprochement des accès. Les trois questions suivantes ont trait aux points essentiels du processus, à vérifier :

1) Un rapprochement reproductible et fiable est-il effectué ?

Les auditeurs internes doivent vérifier si les rapprochements réalisés sont pérennes et reproductibles. Ils doivent également en contrôler la fiabilité. En d'autres termes, le rapprochement entraîne-t-il une amélioration mesurable de l'état du contrôle d'accès logique ? Il ne suffit pas d'examiner l'accès logique et de déclarer qu'il convient. Beaucoup de grandes organisations connaissent bien ces revues par lesquelles le responsable donne automatiquement son aval à la demande d'habilitation, car il doit gérer et examiner un grand nombre de demandes.

Comme la revue peut être considérée comme une forme de validation de l'identification, le responsable doit pouvoir connaître un tant soit peu les individus dont il est garant (c'est-à-dire pouvoir déclarer que l'accès à telle application leur est nécessaire). Si le processus est conçu de telle sorte qu'il est impossible pour les personnes chargées de valider les accès de connaître tous les utilisateurs, il faut en renforcer l'efficacité. Une solution consiste à demander aux cadres intermédiaires d'effectuer eux-mêmes la revue des personnes placées directement sous leur responsabilité, plutôt que de confier cette tâche à un cadre supérieur rarement en contact avec elles.

2) Quelle est la fréquence des rapprochements ?

De nombreuses organisations effectuent des rapprochements deux fois par an. Cependant, si le processus est automatisé, il peut être effectué pratiquement tous les jours, les exceptions étant alors automatiquement corrigées ou signalées aux responsables de la gestion des accès.

3) Comment sont gérés les rapprochements ?

Pour le savoir, les auditeurs internes peuvent poser les questions suivantes :

- Que se passe-t-il en cas de problème lors du rapprochement (c'est-à-dire si celui-ci ne fait pas ce qu'il devrait) ?
- Le problème est-il simplement consigné pour être examiné ultérieurement ?
- Les systèmes se reconfigurent-ils automatiquement en fonction de ce qui est prévu ?
- Quelles sont les mesures prises pour identifier la cause fondamentale du problème ?
- L'événement est-il simplement dû à un problème technique ou a-t-on apporté des modifications non autorisées à un système ?

Annexe A : Liste de contrôle portant sur les revues de la gestion des identités et des accès

Lors d'un audit de la gestion des identités et des accès, la répartition des informations sous trois grands thèmes (administration, provisionnement et exécution) permet d'effectuer une analyse complète de l'environnement et de répondre à quelques questions essentielles. La liste de contrôle suivante est très générale et ne prétend pas être un programme d'audit complet ni traiter les risques liés à la gestion des identités et des accès.

Domaines :

- **Administration :** Quelles sont les mesures en place pour élaborer et maintenir la stratégie, les politiques, les procédures et les opérations de gestion des identités et des accès ?
- **Provisionnement :** Comment l'accès est-il accordé, surveillé et supprimé dans l'environnement ?
- **Exécution :** Des mesures adaptées sont-elles mises en place pour dissuader, empêcher et détecter les tentatives de violation des processus de gestion des identités et des accès ?

Question / Thème d'audit	Statut
1.1 **Une stratégie de gestion des identités et des accès a-t-elle été mise en place ?** L'un des éléments essentiels d'un processus de gestion des identités et des accès efficace est l'existence d'une méthodologie cohérente de gestion de l'infrastructure informatique sous-jacente. Si une stratégie cohérente s'applique à l'ensemble de l'organisation, tous les services peuvent utiliser les mêmes processus pour gérer les membres du personnel, leurs identités et les accès nécessaires, même s'ils n'utilisent pas forcément les mêmes technologies. • Se renseigner sur les stratégies de gestion des identités et des accès en cours dans l'organisation. • Si des stratégies sont en place, déterminer comment et par qui elles sont gérées.	
1.2 **Les risques liés au processus de gestion des identités et des accès sont-ils bien compris par la direction générale et les autres personnes concernées ? La stratégie prend-elle ces risques en compte ?** Même si une stratégie est en place, elle ne couvre pas forcément tous les risques inhérents à la gestion des identités et des accès. Il est important que la stratégie comprenne des éléments permettant d'identifier tous les risques potentiels. • Déterminer si une évaluation des risques des processus de gestion des identités et des accès établis a été menée. • Déterminer comment les risques sont identifiés et traités.	
1.3 **Si l'organisation crée ou modifie un processus de gestion des identités et des accès, est-ce uniquement pour des questions de réglementation ?** Les processus de gestion des identités et des accès doivent absolument s'intégrer à des projets et des stratégies d'entreprise plus vastes. L'existence d'un environnement de gestion des identités et des accès solide présente de nombreux avantages, parmi lesquels la présence d'un meilleur système de contrôle interne. • Déterminer les besoins de l'organisation en termes de gestion des identités et des accès. • Déterminer si les processus de gestion des identités et des accès répondent aux exigences de l'organisation ou seulement aux exigences externes.	
1.4 **Les réglementations applicables à l'organisation sont-elles bien comprises ?** De nouvelles réglementations sont créées et, pour les grandes multinationales, il peut être difficile d'identifier toutes les obligations réglementaires à respecter. • Comment l'organisation détermine-t-elle les obligations réglementaires qui la concernent ? • Comment l'organisation se tient-elle au courant de ces réglementations ? • Comment fait l'organisation pour capturer, stocker et récupérer ces informations ?	

Question / Thème d'audit	Statut
1.5 **Existe-t-il des méthodes précises pour rendre compte des problèmes liés à la séparation des fonctions ?** Bien que plusieurs domaines de l'organisation aient définis des règles précises pour gérer les problèmes par séparation des tâches, celles-ci ne sont pas toujours bien documentées et bien comprises. La principale question à poser concerne la capacité des managers et autres personnes chargées de l'approbation des accès à reconnaître les failles dans la séparation des fonctions. • Les conflits de séparation des fonctions sont-ils identifiés dans le cadre des processus de gestion des identités et des accès ? • Comment ces conflits sont-ils traités ? À qui incombe cette tâche ? • Des mécanismes ont-ils été instaurés pour isoler ou identifier ces conflits avant d'accorder un accès ?	
1.6 **L'environnement de gestion des identités et des accès est-il centralisé ou distribué selon la même structure que l'organisation ?** Sur le plan technique, l'idéal serait d'avoir un seul logiciel avec des processus cohérents, clairement documentés et gérés via un même outil de mise en œuvre. Toutefois, en raison des difficultés d'intégration des systèmes hérités et de la modification des processus permettant d'accorder les approbations, ces technologies sont moins performantes que prévu. • S'il existe plusieurs solutions de gestion des identités et des accès, comment sont-elles gérées pour identifier, éviter ou détecter les permissions non autorisées ou non justifiées accordées aux utilisateurs ?	
1.7 **Comment sont élaborées les règles des mots de passe et sont-elles suffisantes ?** Les règles des processus de gestion des identités et des accès constituent un important facteur de l'efficacité de toute solution. Il est donc important de comprendre la méthode dont ces règles sont élaborées et communiquées, ainsi que les éléments technologiques de l'environnement qui contribuent à en assurer le respect. • Quels paramètres des mots de passe sont élaborés pour les applications utilisées dans toute l'organisation ? • Sont-ils systématiquement appliqués ? • Comment les modifications apportées à ces paramètres sont-elles contrôlées ?	

Question / Thème d'audit	Statut
2.1 **L'organisation dispose-t-elle de processus cohérents pour la gestion des accès au système ?** Plusieurs aspects du provisionnement suscitent des questions. Ces questions doivent être posées et obtenir tôt ou tard une réponse. Elles concernent les connaissances des individus sur les processus, les documents produits et le respect des processus définis. • Déterminer s'il existe dans l'organisation des politiques et des procédures de gestion des identités et des accès. • Déterminer si ces politiques et procédures ont été communiquées aux individus concernés dans l'organisation.	
2.2 **Les auditeurs internes peuvent-ils identifier individuellement les personnes qui ont accès aux systèmes de l'organisation, en fonction des authentifiants de connexion qui leur sont attribués ?** L'un des éléments essentiels du processus de provisionnement est la capacité d'identifier correctement les personnes dont on gère les accès. • Les utilisateurs de ressources informatiques ont-ils des identifiants uniques ? • Comment ces identifiants sont-ils suivis et enregistrés ?	
2.3 **La productivité du personnel pâtit-elle de la difficulté à obtenir et à conserver l'accès aux systèmes ?** Comme nous l'avons vu, le principal motif d'adoption d'un système de gestion des identités et des accès tient aux obligations règlementaires, qui exigent des contrôles plus efficaces. La mise en œuvre de tels systèmes présente des avantages évidents. Toutefois, les processus manuels généralement employés pour gérer les accès sont incapables de donner immédiatement accès à ces systèmes. • Comment le processus de gestion des identités et des accès est-il géré dans l'organisation ? • Y a-t-il des avantages à rendre les utilisateurs plus autonomes par rapport à certains aspects du processus de gestion des identités et des accès (par exemple, la réinitialisation des mots de passe, le recours à une application d'assistance plutôt qu'à un numéro d'appel) ?	
2.4 **Qui doit approuver l'accès d'un utilisateur dans l'environnement ?** C'est une question importante, qui appelle une réponse. Autre question essentielle : plusieurs personnes doivent-elles participer au processus d'approbation ? • Déterminer les méthodes utilisées pour approuver les demandes d'accès des utilisateurs. • Déterminer si l'approbation relève de la direction métiers ou de la DSI. • Déterminer comment s'opère l'approbation en cas de conflit de séparation des fonctions.	
2.5 **L'organisation peut-elle prouver que seules les personnes habilitées ont accès aux informations ?** C'est une question cruciale à laquelle l'auditeur interne doit impérativement répondre. Toutefois, il peut être difficile de démontrer que l'organisation maîtrise les accès des utilisateurs. • À quelle fréquence l'organisation vérifie-t-elle les accès accordés à ses utilisateurs ? • En cas de revue, comment les accès non justifiés sont-ils identifiés, consignés et traités ?	

Question / Thème d'audit	Statut
2.6 **Existe-t-il des contrôles permettant d'empêcher quiconque d'ajouter des accès aux systèmes et aux applications sans suivre la procédure approuvée ?** L'existence d'un processus de gestion des identités et des accès aux systèmes et aux applications semble être la situation idéale. Toutefois, quels sont les moyens pour l'organisation de s'assurer que nul ne contourne le processus et n'ajoute des comptes (pour soi ou pour d'autres) sans les autorisations adéquates et sans respecter les procédures définies ? • Déterminer qui, dans l'organisation, peut ajouter, modifier ou supprimer des utilisateurs pour les applications utilisées dans l'environnement. • Déterminer si l'organisation réalise un inventaire périodique des utilisateurs, permettant de contrôler les permissions d'accès aux formulaires de demande d'accès.	
2.7 **Lorsqu'une personne quitte l'organisation, ses accès aux systèmes sont-ils vérifiés et révoqués rapidement ?** Les audits de la gestion des identités et des accès permettent de constater fréquemment que des comptes ont conservé leurs accès longtemps après que leurs titulaires aient quitté l'organisation. La difficulté consiste à identifier tous les accès associés à un utilisateur donné. • L'organisation a-t-elle mis en place un processus permettant de désactiver ou de supprimer les permissions d'accès des utilisateurs lorsqu'elles ne sont plus nécessaires ? • Comment l'organisation s'assure-t-elle que tous les noms de compte associés à une personne donnée ont été désactivés ou supprimés ?	
2.8 **Comment l'organisation traite-t-elle les comptes n'ayant pas trait à des personnes ?** Ces comptes posent plusieurs difficultés, notamment en ce qui concerne la détermination des contrôles y afférents. • Quelles sont les fonctions de ce compte ? • L'existence et l'activation de ce compte sont-elles nécessaires ? • Qui a accès à ce compte ? • Existe-t-il un mot de passe partagé pour ce compte ? • Combien de personnes connaissent le mot de passe ? • Comment la responsabilité des opérations effectuées par le compte est-elle établie ?	
2.9 **Comment l'organisation traite-t-elle les comptes privilégiés ?** Les comptes privilégiés posent des difficultés particulières. Ils sont nécessaires pour la gestion de l'environnement et l'apport d'une assistance homogène, rapide et efficace. Toutefois, les comptes privilégiés ont la possibilité de contourner la plupart des contrôles mis en place pour gérer les accès des comptes ordinaires. • Quelles sont les personnes qui, dans l'organisation, bénéficient de permissions d'accès privilégiées aux applications ? • Comment ces permissions d'accès privilégiées sont-elles demandées, approuvées et accordées à ces personnes ? • À quelle fréquence les permissions d'accès accordées sont-elles revues ?	

Question / Thème d'audit	Statut
3.1 **Quelle est l'efficacité des contrôles mis en place pour éviter que certaines personnes ne contournent les contrôles d'authentification ou d'autorisation ?** L'une des principales difficultés concernant les applications est l'exécution des accès et la façon dont chaque application gère les authentifications et les autorisations. • Déterminer les moyens d'authentification utilisés pour les applications existantes. • Déterminer si les moyens d'authentification offrent aux utilisateurs la possibilité de contourner le processus d'authentification (par exemple, mot de passe peu résistant ou sauvegardé).	
3.2 **L'exécution des accès par les applications suit-elle toujours la même méthodologie ?** Les responsables informatiques doivent définir la façon dont ce problème sera géré et les systèmes qui exécuteront les décisions prises. • Les mots de passe sont-ils synchronisés entre les applications utilisées dans l'organisation ? • Le cas échéant, comment les mécanismes de synchronisation sont-ils gérés ? • En l'absence de synchronisation, quels sont les mécanismes en place pour empêcher les utilisateurs d'accéder aux applications auxquelles ils ne sont pas censés avoir accès ?	
3.3 **Comment les informations sont-elles consignées, collectées et analysées ?** Il est important de comprendre les types d'événements consignés, leur localisation et la fréquence de l'analyse. • Déterminer si, pour la gestion des identités et des accès, l'organisation a recours à la journalisation des événements. • Si des journaux d'événements sont utilisés, déterminer quand et comment ils sont analysés. • Si les journaux sont analysés et que des écarts sont détectés, comment le problème est-il résolu ?	

Annexe B : Informations supplémentaires

Pour de plus amples informations, vous pouvez consulter les ressources externes suivantes :

- Canaudit, www.canaudit.com.
- Revue *Chief Information Officer* (CIO), www.cio.com.
- Revue *Chief Security Officer* (CSO), www.csoonline.com.
- Control Objectives for Information and related Technology (CobiT), www.isaca.org/cobit.
- Federal Financial Institutions Examination Council (FFIEC), www.ffiec.gov.
- IBM Corp., www.ibm.com/software/tivoli.
- ISACA, www.isaca.org.
- The Institute of Internal Auditors, www.theiia.org.
- Microsoft Corp., www.microsoft.com/technet/security/guidance/identitymanagement.
- Oracle, www.oracle.com/products/middleware/identity-management/identity-management.html.
- Public Company Accounting Oversight Board (PCAOB), www.pcaobus.org.
- Institut SysAdmin, Audit, Network, Security (SANS), www.sans.org.

Glossaire

Accès : Droit ou permission accordés à une identité. Ces droits d'accès à l'information qui sont octroyés aux utilisateurs leur permettent d'exécuter différents niveaux de fonctions transactionnelles.

Annuaire de gestion des identités et des accès : Système de stockage des données contenant toutes les données actuelles et historiques relatives au système de gestion des identités et des accès.

Authentification : Processus visant à vérifier une identité en la comparant aux valeurs enregistrées dans un annuaire d'identités. L'authentification permet de s'assurer que les utilisateurs sont bien qui ils prétendent être.

Autorisation : Processus permettant de déterminer les types d'activités autorisées. En général, lorsqu'un utilisateur a été authentifié, il peut être autorisé à réaliser différents types d'opérations ou obtenir certains droits d'accès.

Événement du cycle de vie : Événement survenant au cours du cycle de vie d'un utilisateur et susceptible de déclencher une action du système de gestion des identités et des accès (par exemple, une résiliation ou un transfert).

Habilitation sensible : Ressource ou accès signalé(e) comme pouvant présenter un certain risque pour la sécurité de l'organisation en cas ou au moment du provisionnement. Il peut s'agir de pouvoirs spéciaux, de groupes d'administrateurs de domaine et de l'accès au compte racine.

Habilitation : Accès à des fonctionnalités spécifiques d'un système ou d'une application, accordé à un utilisateur particulier. La plupart des membres d'une organisation bénéficient de plusieurs habilitations permettant d'accéder à différents systèmes.

Identification d'utilisateur : Identifiant ou ID de connexion sur une ressource spécifique, permettant de gérer l'accès à la ressource en question.

Identité : Séquence ou ensemble unique de caractéristiques permettant d'identifier un individu de façon univoque.

Modèle de sécurité : Règle de sécurité au sein d'une application reliant le niveau de sécurité le plus étroit (paramètres de sécurité) au niveau de sécurité le plus large (groupes de sécurité). Les groupes de sécurité sont affectés aux utilisateurs.

***Offboarding* (gestion des départs) :** Processus qui impose à un employé ou à un sous-traitant quittant une organisation à rendre les ressources physiques qui lui ont été attribuées, qui révoque ses droits d'accès physique et qui résilie ses droits d'accès logique (aux applications et aux systèmes).

***Onboarding* (gestion des arrivées) :** Processus d'identification des personnes à intégrer à l'entreprise en tant qu'employé ou sous-traitant ; octroi à ces personnes des outils nécessaires à la réalisation de leur mission ; et création d'une identité, de comptes et de droits d'accès adaptés à leurs fonctions.

Provisionnement : Processus permettant de créer une identité, de l'associer à un accès et de configurer le système en conséquence.

Ressource : Élément du système de gestion des identités et des accès qui peut être demandé par un utilisateur. Il peut s'agir d'une application, d'un composant de l'infrastructure technologique (par exemple, un système), d'un accès ou d'une habilitation spécifique (par exemple, un groupe ou un profil).

Séparation des fonctions : Mécanisme de contrôle qui divise un processus en différents éléments constitutifs et répartit entre plusieurs individus la responsabilité de l'exécution de chacun de ces éléments. La séparation des fonctions segmente le processus de telle sorte qu'aucun individu ne dispose d'une capacité excessive à effectuer des transactions ou à couvrir unilatéralement des fraudes sans que cela soit détecté.

Système de gestion des identités et des accès : Système composé d'un ou plusieurs sous-systèmes et composants destiné à faciliter l'élaboration, la gestion et la révocation des identités et des accès aux ressources.

Transfert : Événement dans le cycle de vie, par lequel un utilisateur change de responsabilité ou de fonction.

À propos des auteurs

Frank Bresz, CISSP

Frank Bresz est directeur général de la division des services financiers chez Ernst & Young. Il est responsable de la stratégie de sécurité des systèmes d'information et de l'exploitation des programmes stratégiques. Il a travaillé avec différents clients sur le développement de leurs programmes de sécurité informatique. Dans ce cadre, il s'est attaché à harmoniser la conception du programme de sécurité avec les réglementations en vigueur ou à l'étude.

Frank Bresz a plus de 22 ans d'expérience dans le domaine de la sécurité de l'information et l'exploitation de centres de données. Il connaît parfaitement le développement de grands programmes de gestion des identités et des accès intégrés à des projets plus vastes de sécurité de l'information. Avant de rejoindre Ernst & Young, il a été responsable pendant dix ans de la gestion des systèmes d'information (SI) et a beaucoup travaillé avec Sybase au développement d'applications Web.

Frank Bresz est titulaire d'une licence en informatique délivrée par l'Université de Pittsburgh. Il a obtenu la certification CISSP (Expert en sécurité des systèmes d'information).

Sajay Rai, CISSP, CISM

Sajay Rai est l'un des associés du cabinet de services de conseil en gestion du risque d'Ernst & Young. Il a plus de 30 ans d'expérience dans le domaine des SI, notamment de la sécurité de l'information, la continuité d'activité et la gestion du risque. Sajay Rai a travaillé chez IBM comme directeur général du cabinet de conseil en continuité d'activité et gestion des urgences. Il a participé à la création du cabinet de conseil en sécurité de l'information d'Ernst & Young et à l'administration du cabinet de conseil en SI de cette société en Amérique latine.

Sajay Rai a co-signé un ouvrage récent intitulé *Defending the Digital Frontier: A Security Agenda*, qui montre aux cadres dirigeants et aux responsables informatiques comment développer un programme de sécurité de l'information opérationnel et efficace. Il figure dans le *Who's Who in Technology*, l'annuaire des experts en technologies de la revue *Crain's Cleveland Business*.

Sajay Rai est titulaire d'un mastère en gestion de l'information de l'Université de Washington et d'une licence en informatique du Fontbonne College. Il a obtenu les certifications CISSP (Expert en sécurité des systèmes d'information) et CISM (Management de la sécurité de l'information).

Tim Renshaw, CISSP

Tim Renshaw est conseiller principal à la division des services financiers d'Ernst & Young. Il a une grande expérience de la gestion des programmes et des SI dans le secteur des services financiers et l'industrie pharmaceutique. Tim Renshaw a élaboré des stratégies de mise en œuvre de la gestion des identités et des accès pour plusieurs institutions financières mondiales et a développé pour le secteur des services financiers des programmes d'autoévaluation des risques et des plans stratégiques de sécurité de l'information. Par ailleurs, il a créé et dirigé des bureaux de gestion des programmes de SI, réalisé des analyses indépendantes des projets de mise en œuvre technologique à l'échelle des entreprises, et collaboré à des projets de reconfiguration des processus d'entreprise.

Tim Renshaw est titulaire d'une licence en systèmes d'information et en économie de l'université Carnegie Mellon University. Il a obtenu la certification CISSP.

Jeffrey Rozek, CISSP

Jeffrey Rozek est directeur principal dans le cabinet de conseil en risque mondial d'Ernst & Young, où il s'intéresse plus particulièrement à la sécurité de l'information. Il a près de 15 ans d'expérience dans le domaine des systèmes d'information et la sécurité pour divers secteurs (services financiers, télécommunications, industrie et services d'utilité publique). Jeffrey Rozek a supervisé de nombreux projets sur la sécurité, notamment pour des mises en œuvre d'envergure, à l'échelle internationale et dans plusieurs langues. Il s'est attaché avant tout à fournir des solutions de contrôle d'accès, d'authentification et d'autorisation. Il a collaboré avec plusieurs sociétés de la liste Fortune 100 à l'évaluation et au développement de leurs modèles de maturité et de leur cadre général de sécurité et de gestion du risque, et a également aidé plusieurs clients à structurer, concevoir et déployer des architectures de sécurité technique.

Jeffrey Rozek est titulaire d'une licence de comptabilité de l'université John Carroll University et de la certification CISSP.

Torpey White, CPA, CISA

Torpey White est directeur du cabinet de conseil en gestion de Goldenberg Rosenthal, où il propose des services de conseil et d'attestation à des sociétés Fortune 1000, des moyennes entreprises et des organisations à but non lucratif. Il a une grande expérience de l'évaluation des contrôles internes, des revues opérationnelles, des audits SAS 70, de l'administration de projets soumis à la loi américaine Sarbanes-Oxley de 2002, Section 404, des audits internes, de l'assistance comptable, de l'information et de l'analyse financières, de l'analyse des processus d'entreprise, ainsi que de la documentation et de la reconfiguration des processus.

En 20 ans, Torpey White a travaillé pour des organisations opérant dans divers secteurs, notamment le développement logiciel, les services d'utilité publique, la concession automobile, les adjudications, les courses hippiques, la santé, les organisations à but non lucratif et l'industrie légère. Il s'occupe également du développement et de la gestion de plans d'audit interne, de la mise en œuvre de systèmes financiers, des budgets et des prévisions, de la prise en charge des systèmes patrimoniaux, de l'accompagnement des acquisitions et de la réalisation de projets spéciaux.

Torpey White possède une licence en comptabilité et en finance de l'université LaSalle University. Il est expert-comptable, titulaire des certifications CPA et CISA.

Réviseurs

L'IIA tient à remercier les personnes et organisations suivantes pour leurs précieux commentaires et leurs apports à cet ouvrage :

- Ken Askelson, JCPenney, États-Unis.
- Lily Bi, The IIA.
- Lawrence P. Brown, The Options Clearing Corp., États-Unis.
- Tim Carless, Chrysler Financial, États-Unis.
- Christopher Fox, ASA, eDelta, New York, États-Unis.
- Nelson Gibbs, Deloitte & Touché LLP, États-Unis.
- Steve Hunt, Enterprise Controls Consulting LP, États-Unis.
- Stuart McCubbrey, General Motors Corp., États-Unis.
- Heriot Prentice, The IIA.
- James M. Reinhard, Simon Property Group Inc., États-Unis.
- Paula Stockwell, IBM Corp., États-Unis.
- Jay R. Taylor, General Motors Corp., États-Unis.
- Hajime Yoshitake, Nihon Unisys Ltd., Japon.

AICPA : American Institute of Certified Public Accountants www.aicpa.org

CIS : Center for Internet Security www.cisecurity.org

CMU / SEI : Carnegie Mellon University Software Engineering Institute www.cmu.edu

ITPI : IT Process Institute www.itpi.org

NACD : National Association of Corporate Directors www.nacd.org

Institut SANS : www.sans.org

Gestion des identités et des accès

La gestion des identités et des accès est une activité transversale qui consiste à déterminer qui a accès à quelle information sur une période donnée. Elle permet d'initier, de capturer, d'enregistrer et de gérer les identités des utilisateurs et les droits correspondants d'accès aux informations exclusives de l'organisation. Des processus de gestion des identités et des accès médiocres ou mal contrôlés peuvent entraîner des violations de la réglementation par l'organisation et empêcher d'identifier les cas de détournement des données de l'entreprise.

Les responsables de l'audit interne doivent participer au développement de la stratégie de gestion des identités et des accès de l'organisation et évaluer la mise en œuvre de cette stratégie, ainsi que l'efficacité des contrôles d'accès qui s'appliquent dans l'ensemble de la société. L'objectif de ce GTAG est d'aider à mieux comprendre le rôle de la gestion des identités et des accès pour l'organisation, et de suggérer des points de l'audit interne qui méritent un examen plus approfondi. Il peut aider les auditeurs internes, notamment les responsables de l'audit interne, à comprendre, analyser et surveiller les processus de gestion des identités et des accès de leur organisation.

Pour attribuer une note à ce guide ou formuler des commentaires, veuillez vous rendre sur www.theiia.org/guidance/technology/.

GTAG®

The Institute of Internal Auditors