



**GESTION DES RÔLES :  
RÉDUIRE LE COÛT  
DE LA GOUVERNANCE,  
DE LA GESTION DES RISQUES  
ET DE LA CONFORMITÉ**

Livre blanc  
Septembre 2008

# Table des matières

Synthèse .....	1
Les enjeux clés de la gestion des rôles .....	3
Gouvernance, gestion des Risques et Conformité (GRC) .....	3
Le coût de la GRC .....	4
L'automatisation des processus de la GRC : une nécessité .....	6
La solution intégrée de gestion des rôles de Sun en partenariat avec Accenture . . . .	7
Exemples d'utilisation de la solution : la gestion des rôles en conditions réelles . . . .	9
Scénario 1 :	
Garantir la ségrégation des tâches dans une grande entreprise industrielle . . . . .	9
Scénario 2 :	
Automatiser la vérification des accès dans une grande compagnie d'assurance . . . .	10
Scénario 3 :	
Protéger la confidentialité des données personnelles des collaborateurs dans une entreprise technologique d'envergure mondiale .....	10
Conclusion .....	11

## Chapitre 1 Synthèse

La gestion des identités et des accès (IAM) continue d'influencer l'ensemble des initiatives informatiques des entreprises. Aujourd'hui, les solutions d'IAM sont le point central entre les métiers et le Système d'Information (SI).

En effet, dans le contexte actuel, les entreprises doivent assurer une Gouvernance SI et métier, une gestion des Risques et une mise en Conformité appropriées.

En parallèle, les entreprises doivent aussi rechercher les gains d'efficacité,

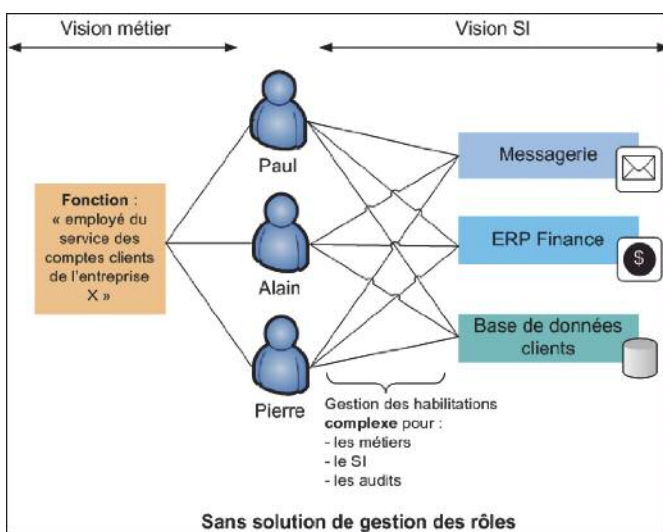
de productivité et de réduction des coûts.

Dans un tel environnement, les solutions d'IAM sont un choix stratégique afin de pouvoir répondre à l'expansion et à l'évolution des besoins de l'entreprise.

Les facteurs justifiant le déploiement d'une solution d'IAM demeurent inchangés : réduction des coûts, gain de productivité, Gouvernance, gestion des Risques, Conformité réglementaire, capacités d'audit et accès utilisateur approprié aux données, aux systèmes et aux applications critiques de l'entreprise.

La maturation des solutions d'IAM a toutefois fait émerger un nouveau facteur :

**la gestion des rôles.**

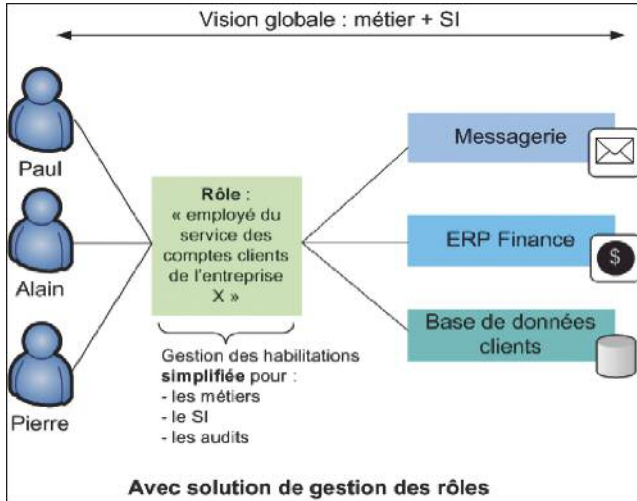


L'entreprise peut ainsi avoir le moyen de mieux gérer les droits et habilitations associées à ces rôles. La gestion des rôles s'affirme de plus en plus comme un composant « critique » d'une solution d'IAM complète afin de permettre à l'entreprise de répondre au mieux à ses évolutions.

Quelle est la définition exacte de la gestion des rôles, et comment répond-elle à ces différents besoins ? La gestion des rôles régit les accès en s'appuyant sur la fonction des utilisateurs. Par exemple, si Paul est un collaborateur nouvellement affecté au service des comptes clients de l'entreprise X, il lui faudra accéder aux ressources suivantes pour travailler : messagerie, ERP « finance » et base de données comptes clients. En l'absence d'une solution de gestion des rôles, il faudrait lui attribuer les habilitations informatiques brutes associées à chacune de ces ressources (Microsoft Exchange Server 2007, SAP FI/CO, IBM DB2, etc.).

Au lieu de valider une liste brute d'habilitations informatiques, le responsable hiérarchique de Paul n'aura qu'à valider la fonction ou les rôles métier attribués à Paul,

sachant que les habilitations informatiques correspondantes ont déjà été standardisées et définies par ailleurs. La solution de gestion des rôles assure ainsi une connexion efficace et sûre entre les dimensions métier et informatique dans la mesure où elle permet de spécifier les besoins de provisioning et d'audit en utilisant une terminologie métier, sans entrer dans les arcanes des habilitations informatiques détaillées.



Dans ce document, nous nous efforcerons :

- d'examiner les motivations et les enjeux stratégiques justifiant actuellement le déploiement d'une solution de gestion des rôles ;
- d'étudier les bénéfices associés à l'implémentation d'une solution de gestion des rôles ;
- de décrire les fonctionnalités de gestion des rôles du logiciel Sun™ Identity Manager et Sun™ Role Manager dans le cadre d'une intégration de gestion des identités et des accès intégrée par Accenture ;
- d'explorer différents scénarios montrant comment la solution de Sun intégrée à l'aide d'Accenture permet d'atteindre les principaux objectifs des entreprises.

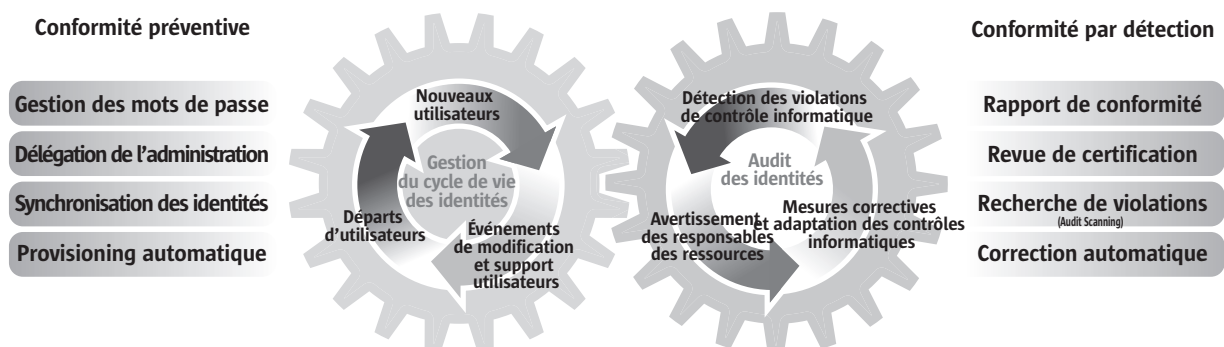
## Chapitre 2

# Les enjeux clés de la gestion des rôles

## Gouvernance, gestion des Risques et Conformité (GRC)

Les affaires de corruption et autres scandales qui ont frappé certaines des plus grandes entreprises publiques ont entraîné un durcissement des contraintes réglementaires, doublé d'une surveillance plus serrée de la part des organismes de réglementation. Depuis la fin des années 90, le législateur a réagi à ces malversations financières ainsi qu'à la menace croissante du vol d'identité en déployant un véritable arsenal de textes régissant l'intégrité de l'information et la protection des données personnelles. En voici quelques exemples :

- La loi Sarbanes-Oxley de 2002 est sans doute l'instrument de réglementation le plus célèbre, le plus important et souvent le plus redouté des États-Unis. Cette loi oblige toutes les sociétés cotées aux États-Unis à protéger l'intégrité des données financières par plusieurs moyens précis, notamment en évitant le risque qu'un même utilisateur ne bénéficie d'un cumul injustifié de ses droits d'accès sur certains types de données.
- La loi de sécurité financière (LSF), aussi appelée Loi Mer du nom du ministre des Finances en poste Francis Mer, a été adoptée par le Parlement français le 17 juillet 2003 afin de renforcer les dispositions légales en matière de gouvernance d'entreprise. Comme la loi américaine Sarbanes-Oxley, la loi de sécurité financière repose principalement sur une responsabilité accrue des dirigeants, un renforcement du contrôle interne et une réduction des risques de conflits d'intérêts.
- La loi n° 78-17 informatique et libertés mise en place en 1978 et modifiée en 2004 constitue le cadre législatif de la protection des données personnelles en France et décrit les missions de la Commission Nationale de l'Informatique et des Libertés (CNIL) en charge du respect de cette loi.



*La convergence des fonctions de provisioning et d'audit des identités permet de réduire les risques de non-conformité en créant un cycle d'audit permanent qui rend possible la détection et la prévention des violations de gouvernance et de conformité de façon continue et durable.*

Une solution de gestion des identités et des accès flexible et complète fournit à l'entreprise les outils nécessaires à une parfaite maîtrise de sa conformité réglementaire :

- Les fonctions de provisioning et d'audit des identités et des accès permettent de couvrir les demandes d'accès tout en détectant les risques associés à ces accès, notamment le cumul injustifié des droits d'accès et le non-respect de la ségrégation des tâches.
- Le contrôle des accès à leur niveau le plus fin est essentiel pour établir une ligne de défense contre les risques de violations de politiques ou de directives réglementaires.
- La gestion des rôles simplifie grandement la remise des preuves de conformité aux organismes d'audit en permettant de décrire les activités de provisioning, d'audit et de contrôle des accès en termes métier plutôt qu'en termes informatiques.

## Le coût de la GRC

Le coût est l'un des aspects les plus rebutants de la Gouvernance, de la gestion des Risques et de la Conformité. Plus les organismes de réglementation et d'audit gagnent en compétence et en expertise, plus la conformité devient coûteuse et difficile à réaliser. Depuis quelques temps déjà, entreprises, consultants et journalistes économiques tirent la sonnette d'alarme au sujet de l'augmentation du coût d'obtention de la conformité :

- Déjà en 2004, CIO magazine prédisait que la multiplication des réglementations se traduirait par une augmentation du coût de la conformité. Parmi toutes les entreprises aujourd'hui soumises à des réglementations multiples, combien considèreraient que cette prédiction ne s'est pas réalisée ?
- Plus récemment, BusinessWeek indiquait : « Si l'on ne peut nier les bienfaits des nouvelles réglementations sur les entreprises qui ont été provoquées par les affaires Enron, WorldCom ou autres, ce grand nettoyage a un coût. Et pour le moment, en ce qui concerne les sociétés cotées, ce coût ne semble pas diminuer avec le temps. »
- Plus proche de nous, le cabinet indépendant Mazars précisait dans son étude 2006 : « Les coûts de mise en conformité sont jugés très, voire trop, élevés et les ressources humaines sont fortement mobilisées. »

Concernant l'impact financier de la mise en conformité, les entreprises européennes considèrent en moyenne à 56% que les avantages de Sarbanes-Oxley (SOX) n'en compensent pas les coûts et 85% estiment que la charge de travail est nettement plus importante qu'initialement prévue.

Pourquoi le coût de la conformité est-il si élevé ? Parmi les principaux éléments de réponse, on peut citer le durcissement du contexte réglementaire, une surveillance plus étroite des organismes de réglementation et d'audit, et le besoin croissant d'élargir l'accès aux clients et aux partenaires de l'entreprise – encore accentué par la tendance à l'externalisation et à la mondialisation.

Source de risque, cette ouverture nécessite de robustes garde-fous pour sécuriser les données et les applications critiques de l'entreprise, mais aussi pour assurer sa conformité à la réglementation en matière d'accès aux informations. Dans un tel environnement, la conformité devient extrêmement coûteuse, à fortiori si elle repose entièrement sur des procédures manuelles et si l'entreprise excède une certaine taille.

Il est toutefois possible de réduire une grande partie de ces coûts en déployant une solution complète d'IAM et de gestion des rôles.

Les entreprises ont pris conscience que le volet « provisioning » de la gestion des identités entraîne une baisse des coûts. Plus précisément, une solution convergente de provisioning, d'audit et de gestion des rôles réduit les coûts de la Gouvernance, de la gestion des Risques et de la Conformité. En effet, une solution automatisée accélère les processus de provisioning, réduit les ressources (métier et IT) nécessaires et élimine les erreurs manuelles coûteuses.

Lors d'une vérification manuelle, les auditeurs perdent souvent un temps précieux à décrypter la liste brute des habilitations informatiques actives. La connaissance des groupes Active Directory et des annuaires (technologie LDAP) ne faisant pas partie des compétences inhérentes à leur fonction, cette reconstitution périodique se solde par un véritable gaspillage de temps et d'argent. Quant aux habilitations conférant un accès illimité à l'utilisateur, elles augmentent les risques de violation du principe de ségrégation des tâches – et sont sources de pénalités lors des audits externes.

L'automatisation du processus périodique de vérification des habilitations – au cours duquel les responsables doivent valider les accès aux ressources et aux applications octroyés à leurs subalternes directs – constitue un excellent exemple de la charge de travail évitée grâce à la gestion des rôles. Dans la mesure où les habilitations soumises pour approbation lui sont présentées en termes de rôles métier, le responsable pourra statuer sur ces accès de façon rapide et fiable puisqu'il saura aisément les relier à son contexte opérationnel et son domaine d'expertise.

Une solution de gestion des rôles réduira considérablement ces différents risques et permettra à l'entreprise de gagner en productivité, et de réduire ses coûts.

## L'automatisation des processus de la GRC : une nécessité

Plus l'organisation grandit et se mondialise, plus la gestion de la Gouvernance, des Risques et de la Conformité dans cette organisation devient problématique. Aussi inefficace que coûteux, les processus d'audit et de contrôle de conformité manuels augmentent les risques d'erreur humaine, ne fournissent pas de trace de contrôle adéquate et accroissent les risques d'agissements inappropriés ou délictueux de la part d'employés malveillants. Sans automatisation, une organisation peut consacrer des semaines voire des mois à la détection des violations d'accès et leur traitement manuel. Et rien n'assure que toutes les violations seront décelées et corrigées. Par ailleurs, les changements d'affectation des employés constituent également un facteur de risque supplémentaire dès lors que les accès correspondants ne sont pas actualisés ou désactivés comme il convient – ce qui peut aboutir à des violations des règles en matière d'accès ou de ségrégation des tâches.

L'automatisation des processus de la GRC permet de combattre efficacement la quasi-totalité de ces risques :

- Le provisioning automatique permet de centraliser le contrôle de ressources et d'applications historiquement isolées, de façon à superviser beaucoup plus efficacement leur accès.
- L'application d'une politique d'audit au moment du provisioning permet de garantir la conformité réglementaire en prévenant toute violation de cette politique.
- L'intégration d'une solution de gestion des rôles étend l'automatisation en simplifiant les processus de gestion des habilitations. Ainsi, la gestion des rôles réduit par exemple considérablement le risque de voir un responsable occasionner, par inadvertance, une violation des règles de ségrégation des tâches en validant une liste brute d'habilitations formulées dans des termes informatiques n'ayant que peu ou pas de rapport avec la fonction réelle de l'employé concerné.

## Chapitre 3

# La solution intégrée de gestion des rôles de Sun en partenariat avec Accenture

L'association des logiciels Sun Identity Manager et Sun Role Manager fournit à l'entreprise la seule solution réellement intégrée de gestion du provisioning et de l'audit au niveau des rôles métier. Issue de la collaboration Sun-Accenture, elle permet d'atteindre un objectif majeur : la haute performance de la Gouvernance, la gestion des Risques et la Conformité dans le contexte spécifique de l'entreprise.

## La gestion des rôles

Le logiciel Sun Identity Manager déploie le provisioning et l'audit à l'échelon des rôles métier, autorisant ainsi une gestion plus efficace, plus économique et mieux maîtrisée de ces processus. L'intégration avec la technologie Sun Role Manager permet de faire appel à des rôles prédéfinis pour le provisioning et l'audit.

## La définition et l'exploration des rôles

Le logiciel Sun Role Manager est le seul outil de gestion des rôles à réaliser l'exploration et la définition des rôles (role mining) selon une stratégie organisationnelle descendante et ascendante. Cette double approche garantit une définition des rôles adaptée aux besoins de l'entreprise tout en évitant une prolifération incontrôlée de ces rôles.

## Une parfaite visibilité des risques de non-gouvernance ou de non-conformité.

Sun Identity Manager propose un tableau de bord de gouvernance et de conformité récapitulant à tout moment les principales mesures ainsi que les violations, exceptions et anomalies en cours.

Les responsables peuvent ainsi fonder leurs prises de décisions sur une parfaite connaissance des failles de sécurité et des défauts de gouvernance et de conformité potentiellement relevés à un moment donné.

## Un reporting de gouvernance et de conformité exhaustif

Le logiciel Sun Identity Manager comprend une bibliothèque de rapports préconfigurés reprenant les principales données d'audit des identités. La solution inclut en outre des rapports de violation de politique, d'action corrective et d'exception, tout en permettant la conception de rapports d'audit personnalisés.

## Des fonctions de provisioning et d'audit des identités extensibles pour les environnements orientés extranet

Avec Sun Identity Manager, l'entreprise dispose d'une infrastructure de gestion des identités applicables à ses applications et ses portails extranet. Les fonctions d'extranet et d'administration fédérée des identités contribuent à accélérer la fourniture de nouvelles applications et de nouveaux services aux clients, sans pour autant sacrifier la sécurité ou les contrôles de gouvernance et de conformité. Cette solution a été validée dans des environnements comportant quelques millions d'utilisateurs.

## Un accompagnement dans toutes les phases d'un projet d'intégration

L'intégration des solutions IAM de Sun telles que Sun Identity Manager et Sun Role Manager est réalisée en partenariat avec Accenture, leader mondial en conseil, intégration de systèmes et outsourcing.

Accenture conseille ses clients, principalement les grands groupes internationaux du CAC 40, dans la mise en œuvre de solutions adaptées à leurs besoins métier. Fort de cette expérience, Accenture a su développer une méthodologie et une expertise afin de garantir le succès de ses projets.

La sécurité du SI est l'une des priorités d'Accenture pour accompagner l'entreprise dans les différentes phases d'un projet d'intégration : du cadrage au déploiement en passant par la conception et la mise en œuvre. Accenture considère la sécurité du SI dans sa globalité afin de prendre en compte tous les aspects stratégiques, procéduraux, organisationnels, réglementaires et technologiques du projet.

C'est ainsi qu'Accenture, de part sa double expérience métier et sécurité, a défini la gestion des rôles comme un ensemble de contrôles des processus métier pour la Gouvernance, la gestion des Risques et la Conformité de l'entreprise. Cette architecture intégrée permet de rationaliser les opérations, de réduire les coûts et de reprendre le contrôle des accès utilisateurs tout en offrant un retour sur investissement important.

## Une intégration optimisée avec les ERP de l'entreprise

Leader reconnu dans le déploiement de solutions ERP complexes, Accenture accompagne l'entreprise dans l'intégration optimisée des solutions IAM de Sun avec les ERP déployés, permettant la construction d'une solution globale de gestion des identités et des accès. La définition des rôles métier au sein de l'entreprise est une tâche complexe qui requiert la prise en compte des habilitations d'accès aux ERP à leur niveau le plus fin. L'expérience d'Accenture en la matière permet d'apporter une valeur ajoutée et un retour sur investissement rapide.

## Chapitre 4

# Exemples d'utilisation de la solution : la gestion des rôles en conditions réelles

Les scénarios suivants se basent sur des contextes typiques rencontrés dans les entreprises à ce jour. Il s'agit de carences précises relevant de la gestion des identités et des accès résolues par les solutions Sun Identity Manager et Sun Role Manager en partenariat avec Accenture.

## Scénario 1 : garantir la ségrégation des tâches dans une grande entreprise industrielle

**Situation** : Marie, comptable en charge des comptes clients, accepte un nouveau poste dans la société et va désormais travailler sur les comptes fournisseurs. Lorsqu'elle commence son nouveau travail, elle se voit rapidement accorder l'accès aux ressources informatiques qui lui sont nécessaires pour remplir ses nouvelles fonctions.

Cependant, elle continue d'avoir accès aux ressources associées à son ancien poste.

Ce faisant, la société ne respecte pas la ségrégation des tâches exigée par la politique de gouvernance mise en place, et se met en infraction avec la loi Sarbanes-Oxley, aux termes de laquelle l'accès conjoint aux systèmes Comptes clients et Comptes fournisseurs constitue un conflit d'intérêt. Cette violation continue de passer inaperçue jusqu'à ce qu'un auditeur externe demande à l'ancien responsable de Marie, au service Comptes clients, de confirmer les droits d'accès des utilisateurs. Le responsable indique que Marie a quitté le service quelques mois auparavant.

**Le problème** : Comme le provisioning est automatisé mais pas l'audit, Marie a accès à deux ensembles de systèmes et de ressources, ce qui représente un risque pour l'intégrité des données financières de la société. Même si elle n'accède plus jamais aux systèmes liés à son ancien poste, le fait qu'elle en ait la possibilité constitue une menace. Pire encore, c'est finalement un auditeur qui se rend compte du problème alors qu'il effectue une vérification de routine des droits d'accès. Les conclusions de l'audit risquent d'être négatives pour la société, qui pourrait être accusée de violation des dispositions de la loi Sarbanes-Oxley sur la ségrégation des tâches. En outre il s'agit là d'un cas de violation de la politique de gouvernance en place par le management de l'entreprise.

**Solution** : En adoptant Sun Identity Manager avec l'aide d'Accenture, la société automatise le provisioning et l'audit des identités à l'échelon des rôles métier à leur niveau le plus fin. Grâce aux rôles prédéfinis fournis avec le logiciel Sun Role Manager et personnalisés selon le contexte métier, tout employé qui quitte un service pour un autre peut obtenir instantanément l'accès aux ressources nécessaires à ses nouvelles

fonctions – il suffit pour cela de lui assigner un nouveau rôle métier. Dans le même temps, les ressources associées à son ancien poste sont automatiquement annulées avec le retrait de son ancien rôle métier. Ceci permet d'éliminer tout risque de violation des dispositions sur la ségrégation des tâches et l'interdiction du cumul injustifié de droits d'accès.

## Scénario 2 : automatiser la vérification des accès dans une grande compagnie d'assurance

**Situation** : La compagnie utilise 500 applications différentes, toutes vitales pour son activité, et 80 % des employés doivent pouvoir accéder à ces applications en fonction de leur mission. Les rôles ne cessent d'évoluer en raison des promotions, des transferts ou mutations, et les droits d'accès doivent être modifiés en conséquence.

**Le problème** : Les dirigeants et les auditeurs doivent certifier que les droits d'accès des utilisateurs aux applications sont intègres. Pour ce faire, des rapports sont générés manuellement et envoyés au management et aux responsables des applications, qui doivent les vérifier et les valider. En raison du nombre d'applications, de l'évolution constante des rôles et, dans certains cas, de la lenteur de la réponse des personnes chargées de la validation, ce processus peut prendre une année entière. Pendant ce temps, la compagnie est menacée puisque les violations de gouvernance et de conformité passent complètement inaperçues.

**La solution** : La compagnie peut accélérer le processus de vérification des droits d'accès avec l'aide d'Accenture en mettant en œuvre Sun Identity Manager, qui sera chargé de suivre automatiquement les approbations, d'avertir les responsables lorsqu'une vérification doit être effectuée et, en l'absence de réponse des auditeurs, de signaler le problème à la hiérarchie. Par ailleurs, Sun Identity Manager génère des rapports utilisables à des fins d'audit, dans lesquels sont consignées toutes les approbations et toutes les mesures correctives. Grâce à l'automatisation des processus, qui simplifie considérablement la vérification des droits d'accès, Sun Identity Manager permet une réduction sensible du coût et de la durée de la mise en conformité.

## Scénario 3 : protéger la confidentialité des données personnelles des collaborateurs dans une entreprise technologique d'envergure mondiale

**Situation** : Alexandre quitte son poste d'agent de liaison avec les partenaires en charge des prestations sociales au sein du service des Ressources Humaines pour prendre un poste au service Marketing de la même société. Alors qu'il ne devrait plus avoir accès aux données personnelles qu'il pouvait consulter lorsqu'il travaillait au service des RH, il conserve cet accès jusqu'à ce qu'un employé du service informatique remarque le problème en réalisant un audit. Il faut encore attendre

plusieurs jours pour qu'une personne chargée du provisioning soit informée de la situation et annule les droits d'accès. Pendant ce temps, Alexandre a bien diverti ses nouveaux collègues du service Marketing en faisant circuler le dossier de leur Directeur !

**Le problème** : Par ses agissements, Alexandre viole non seulement les règles de la société sur le respect de la vie privée des collaborateurs, mais également les dispositions sur la confidentialité de la loi informatique et libertés – la réglementation régissant tous les environnements dans lesquels des personnes ont accès aux informations à caractère personnel des individus.

À cause d'Alexandre, la société pourrait être condamnée à une amende pour violation des dispositions de la loi informatique et libertés.

**La solution** : La société décide de faire appel à Accenture quelques mois plus tard pour mettre en œuvre Sun Identity Manager. Les fonctions convergentes de provisioning, d'audit des identités et de gestion des rôles de cette solution permettent de contrôler de façon précise les accès aux données personnelles des employés.

La prochaine fois qu'un collaborateur quittera la section prestations sociales du service des RH pour rejoindre un autre service, ses droits d'accès aux dossiers d'assurance maladie des employés seront automatiquement annulés et le collaborateur se verra assigner un rôle métier correspondant à sa nouvelle affectation.

## Chapitre 5

### Conclusion

Une solution avancée d'IAM conjuguant des fonctions de provisioning, d'audit des identités et de gestion des rôles s'avère vite indispensable pour aider l'entreprise à se conformer autant à ses propres dispositions qu'à la réglementation. Outre la conformité, les bénéfices sont : une maîtrise des coûts, un retour sur investissements rentabilisant rapidement le projet et des gains en efficacité. Une telle solution réunit en effet tous les atouts permettant à l'entreprise de gérer la Gouvernance, les Risques et la Conformité tout en restant compétitive et en gardant ses budgets IT sous contrôle.

Pour en savoir plus sur la solution complète de gestion des identités et des rôles de Sun, rendez-vous sur [www.sun.fr/identity](http://www.sun.fr/identity)

Pour en savoir plus sur la haute performance en Sécurité du SI avec Accenture, rendez-vous sur [www.accenture.com/security](http://www.accenture.com/security)

