Conformité Bâle III : Apport de la gestion des identités et des accès

EVIDEN

Ce livre blanc décrit comment une solution de gestion des identités et des accès contribue à maîtriser les risques opérationnels.

25 est.1999 Years of Evidian IAM products

Gérez vos risques opérationnels liés aux accès des utilisateurs

Dans les banques plus que dans d'autres secteurs, un accès non autorisé à l'informatique a un risque élevé de causer des dommages financiers.

Un moyen de contrer ce risque est la gestion des identités et des accès, un ensemble de solutions qui permettent de gérer les droits d'accès avec précision. En administrant rationnellement les accès à l'informatique, les banques réduisent leur exposition aux risques opérationnels.

Pour tirer pleinement parti de la gestion des identités et des accès, une banque peut l'intégrer dans son système de gestion des risques opérationnels, rendant ainsi ce dernier plus efficace.

L'accord Bâle III a introduit l'inclusion des risques opérationnels dans l'évaluation des exigences minimales de fonds propres des banques. Il définit le risque opérationnel comme «le risque de pertes provenant de processus internes inadéquats ou défaillants, de personnes et systèmes ou d'événements externes". En 2010-2011, l'accord de Bâle III a été introduit pour renforcer les exigences de fonds propres dans le sillage de la crise financière de 2008.

Parmi les méthodes d'évaluation de ces risques proposées par les accords, les Approches de Mesure Avancées (AMA) autorisent l'établissement financier à évaluer lui-même les risques opérationnels liés à son activité.[1]

Pour cela, la banque doit mettre en place un dispositif de gestion du risque opérationnel et une entité chargée de sa mise en place et de sa gestion. Le système de mesure interne du risque opérationnel s'appuie notamment sur les données suivantes :

- **données sur les pertes réellement subies,**
- **données sur les incidents opérationnels susceptibles d'être générateurs de coûts (« loss data »).**

La gestion des identités et des accès peut équiper utilement une équipe de gestion des risques opérationnels. Dans une seule interface, elle centralise l'information sur tous les accès de la banque, ce qui facilite la mise en place rapide de contrôles.

Pour une banque, Bâle III peut être une opportunité d'améliorer significativement sa gestion des identités et des accès. Une telle refonte peut être une source importante de retour sur investissement en termes de productivité des utilisateurs et de la direction informatique. Elle permet également de mettre en oeuvre facilement des procédures critiques en milieu bancaire, telles que le 'déprovisionnement', la séparation des tâches ou la gestion basée sur les rôles.

[1] Voir le document de la Banque des règlements internationaux de juin 2011 « Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches » http://www.bis.org/publ/bcbs196.pdf

L'accès aux données informatiques : un point critique

Une bonne méthodologie de gestion des risques opérationnels est indispensable pour mettre en oeuvre une Approche de Mesure Avancée (AMA). Elle est également un prérequis pour mettre en place une approche standardisée.

Une grande partie des risques opérationnels définis par les accords de Bâle concerne **l'accès à des données informatiques par des personnes physiques.** En effet, les actifs bancaires sont de nos jours essentiellement dématérialisés et les flux financiers numérisés.

- **Hétérogénéité des supports**

  Les données financières résident sur de nombreux systèmes et types d'applications. Ceuxci peuvent être accessibles par des moyens classiques ou par Internet.

- **Diversité des méthodes d'autorisation d'accès**

  La plupart des méthodes d'autorisation natives produisent des informations sur les accès. Mais la consolidation et l'audit sont malaisés car les formats ne sont pas standardisés.

- **Complexité technique**

  Le savoir-faire d'une équipe de gestion des risques opérationnels est souvent de type organisationnel. Cette équipe ne peut se concentrer sur les aspects techniques informatiques pointus.

Parmi les sept types de risques définis par les accords de Bâle, la gestion des identités et des accès concerne principalement quatre d'entre eux :

Type de risques	Description (*)	Sous-catégorie concernée principalement par la gestion des identités et des accès
Fraude interne	Pertes dues à des actes visant à frauder, étourner des biens ou à tourner des règlements, la législation ou la politique de l'entreprise (à l'exception des atteintes à l'égalité et des actes de discrimination) impliquant au moins une partie interne à l'entreprise.	• Activité non autorisée • Vol et fraude
Fraude externe	Pertes dues à des actes visant à frauder, détourner des biens ou contourner la législation de la part d'un tiers.	• Vol et fraude • Sécurité des systèmes
Clients, produits et pratiques commerciales	Pertes résultant d'un manquement, non intentionnel ou dû à la négligence, à une obligation professionnelle envers des clients spécifiques (y compris exigences en matière de fiducie et de conformité) ou de la nature ou conception d'un produit.	• Conformité, diffusion d'informations et devoir fiduciaire
Exécution, livraison et gestion des processus	Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou des relations avec les contreparties commerciales et fournisseurs	• Saisie, exécution et suivi des transactions • Gestion des comptes clients

(*) Source : Annex 9 of the Basel II Accords – "Detailed loss event type classification".

Apport d'une solution de gestion des identités et des accès

Dans la mise en place d'une AMA, une solution de gestion des identités et des accès peut apporter des avantages importants :

Réduction immédiate des risques opérationnels, en diminuant les possibilités de failles d'accès aux données informatiques.

Information accessible et auditable sur (a) les accès autorisés ou illicites et (b) l'attribution des droits d'accès par les administrateurs. Cette information facilite la mesure du risque opérationnel par l'entité concernée et peut être directement utilisée par les outils de reporting déjà en place.

Possibilité de **réaction immédiate** sur détection d'une source de risque opérationnel. En effet, ces outils disposent d'une console centralisée de gestion de tous les droits d'accès. Après diagnostic d'un risque, la faille détectée (politique de droits d'accès trop large, erreur d'attribution de droits etc.) peut donc être immédiatement comblée.

Simplification des concepts techniques. Dans une solution de gestion des identités et des accès, les aspects purement techniques sont masqués pour permettre aux administrateurs de se concentrer sur l'attribution des droits d'accès. Le processus d'attribution de ces droits est donc simplifié et auditable.

Le présent document aborde plusieurs de ces aspects, et indique comment utiliser au mieux la gestion des identités et des accès en milieu bancaire.

Le tableau ci-dessous résume, de façon non limitative, l'apport possible d'une telle solution à la maîtrise de risques opérationnels. Dans le cadre d'un projet, le déploiement de ces modules peut se faire de façon progressive.

Type de risques	Sous-catégorie principalement concernée	Gestion des identités	Secure SSO	Provision-nement
Fraude interne	Vol et fraude	✓	✓	
	Activité non autorisée	✓	✓	
Fraude externe	Vol et fraude	✓	✓	
	Sécurité des systèmes	✓	✓	✓
Clients, produits et pratiques commerciales	Conformité, diffusion d'informations et devoir fiduciaire	✓		✓
Exécution, livraison et gestion des processus	Saisie, exécution et suivi des transactions	✓		✓
	Gestion des comptes clients	✓		✓

La diversité des méthodes d'accès est source de risques opérationnels

Envisagée sous les deux angles jumeaux des utilisateurs et des administrateurs, l'absence d'une méthode unifiée de gestion des identités et des accès est source de risques opérationnels

Risques opérationnels liés aux utilisateurs

Ces risques sont principalement liés à la multiplicité des mots de passe qu'un employé doit utiliser lors de son travail quotidien. Par exemple :

- Si une source d'information ne peut être consultée qu'avec par un mot de passe, cet obstacle fera que l'utilisateur aura tendance à ne pas s'y référer. C'est une source de risque opérationnel de type "*gestion des processus*" : mauvais suivi des données de référence, erreur comptable ou d'affectation d'une entité etc..
- Si les mots de passe sont trop nombreux, l'utilisateur aura tendance à les noter sur un support facilement accessible (Post-It™ par exemple). Cela facilite la *fraude interne*.
- Une alternative courante, les mots de passe communs à une équipe, permettent à un employé d'accéder à des données client qui ne le concernent pas. C'est une source potentielle de risques de type « *Clients, produits et pratiques commerciales* ».

Certaines solutions proposent d'uniformiser les mots de passe d'un utilisateur sur l'ensemble des ressources auxquelles il accède. C'est clairement une source de risques opérationnels de type "fraude interne" car il suffira à une personne de pénétrer la sécurité d'un seul système (application ancienne par exemple) pour avoir accès frauduleusement à toutes les ressources avec le mot de passe ainsi obtenu. De plus les politiques de choix des mots de passe utilisés de toutes les applications de la banque peuvent ne pas être compatibles.

Comment réduire ces risques ?

Ces risques peuvent être notablement réduits par l'utilisation d'une solution sécurisée d'authentification unique (en anglais single sign-on ou SSO) telle que celle incluse dans *Evidian IAM Suite*.

Avec une solution de SSO sécurisée, les utilisateurs n'auront à se souvenir que d'un seul couple identifiant/mot de passe ; tous les autres sont renseignés de façon invisible à chaque accès à une application. Des solutions de type biométrie et/ou carte à puce peuvent encore renforcer une solution de SSO.

Evidian IAM Suite masque à l'utilisateur les mots de passe réels d'une application donnée. Ces mots de passe peuvent donc être tous différents et non intuitifs ; pénétrer la sécurité d'une application ne compromet donc pas les autres ressources. De plus, *Evidian IAM Suite* permet à la banque de définir et de déployer une politique spécifique de mots de passe.

Risques opérationnels liés à l'administration des droits d'accès

Il est de plus en plus difficile de gérer l'attribution des droits d'accès de manière satisfaisante. Bien que les effectifs des administrateurs soient constants ou en baisse du fait des réductions de coûts, leur tâche est de plus en plus complexe :

- les droits d'accès concernent des ressources très diverses telles des sites Web, applications mainframe etc.
- dans le même temps, les mouvements de personnels (démissions, mutations, concentration bancaire etc.) impliquent une mise à jour régulière et constante.

Cela crée des risques opérationnels, par exemple :

- L'attribution des droits d'accès est souvent déléguée aux ingénieurs systèmes qui considèrent cela comme une tâche secondaire. Cette étape manuelle est donc parfois faite avec retard ou avec des erreurs de manipulation. C'est une source de risque opérationnel de type "gestion des processus".
- Quand un employé quitte la banque, il est fréquent que ses droits ne soient pas supprimés. Il est en effet difficile de faire l'inventaire des autorisations qui lui ont été accordées pendant sa carrière. Il aura donc encore accès aux systèmes alors qu'il n'est plus employé. C'est une source de fraude externe.
- Enfin, des mots de passe trop nombreux sont souvent perdus ou oubliés, générant des appels au help-desk. Devant le volume de ces appels (jusqu'à 30% selon le cabinet d'analystes Gartner) il est nécessaire de déléguer la possibilité de changer un mot de passe à de nombreuses personnes. Cela peut être une source de risques de fraude interne.

Comment réduire ces risques ?

Ces risques peuvent être notablement réduits en utilisant une solution de « provisionnement » et de gestion des identités. L'attribution (et la suppression) des droits d'accès se fait facilement à partir d'une console centrale, et cela sans intervention manuelle au niveau des ressources elles-mêmes. Cette attribution se fait en fonction de critères organisationnels, par des personnes sûres et sans requérir de connaissances techniques. Bien entendu, on doit conserver l'historique de toutes ces opérations d'administration à des fins d'audit.

Idéalement, cette solution doit pouvoir s'intégrer nativement avec les annuaires d'entreprise afin de réduire le nombre d'interventions manuelles, source d'erreurs potentielles. La mise à jour des informations sur les utilisateurs sera alors faite par le service Ressources Humaines, et non par les responsable de la sécurité d'accès.

La gestion des identités et des accès doit être indépendante des technologies

L'évolution rapide d'un système d'information montre qu'un système de gestion identités et des accès doit être extrêmement adaptable.

- Évolution permanente des technol ogies (Java EE, certificats etc.)
- Nécessité d'intégrer un SI nouveau en cas de concentration bancaire
- Développement de nouvelles applications, achats de licences de progiciels

Il est donc nécessaire que la façon de gérer les identités et les accès soit indépendante des technologies et des applications. Dans le cas contraire, la multiplication des consoles de gestion des droits d'accès rend le processus très difficile à définir, à implémenter et à auditer.

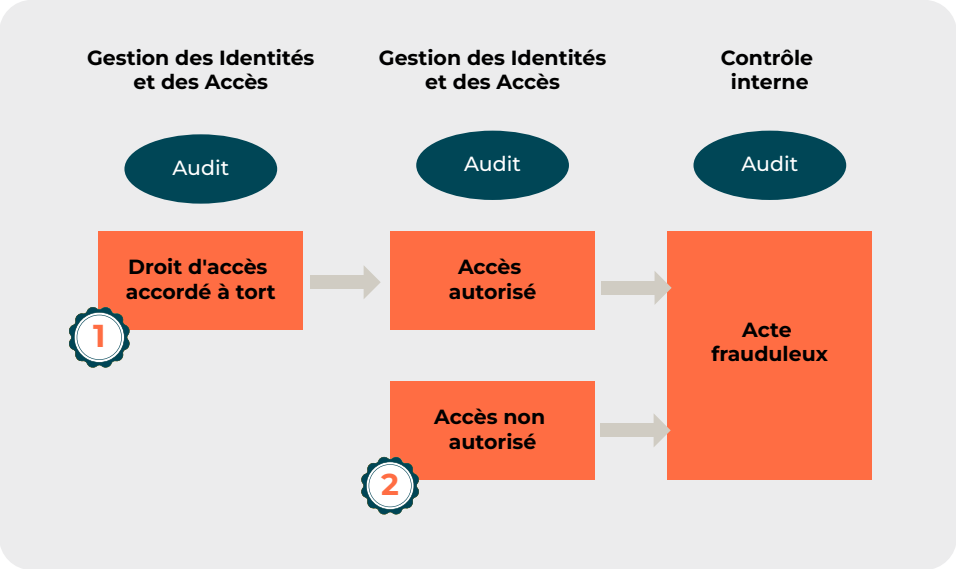
La séparation des rôles dans le processus d'attribution des droits d'accès

Pour être facilement auditable, le processus d'attribution des droits d'accès doit être clairement défini et comporter le moins possible de manipulations manuelles. *Evidian IAM Suite* s'appuie sur les définitions d'utilisateurs et de l'organisation déjà réalisées dans la banque. Il exploite en effet directement les annuaires LDAP de l'entreprise, sans nécessiter d'opérations d'import.

Les rôles sont donc clairement définis et les informations auditables :

Rôle	Qui ?	Où auditer ?
Définition de l'organisation, création, modification et suppression des utilisateurs	Organisation préexistante. Généralement la direction des ressources humaines	Annuaires LDAP
Attribution des droits aux utilisateurs ainsi définis.	Gestions des droits utilisateurs ; organisation centralisée avec possibilité de délégation	Base Evidian IAM Suite
Définition des ressources techniques dont les droits d'accès doivent être gérés	Direction informatique	Base Evidian IAM Suite
Génération de données d'audit sur les accès et les opérations d'administration	Effectué automatiquement par Evidian IAM Suite	Base d'audit Evidian IAM Suite

Les processus d'attribution des droits (demande, qualification, approbation etc.) peuvent donc être facilement définis et audités même s'ils sont très détaillés et complexes.



De cette façon, les informations nécessaires à l'audit comme à l'enquête sur l'origine d'un incident opérationnel sont bien localisées. Dans le schéma ci-dessus, on constate qu'un acte frauduleux peut résulter, soit d'un accès non autorisé (vol de mot de passe par exemple), soit d'une mauvaise attribution de droits d'accès (intentionnelle ou non).

Les données d'audit de la gestion des identités et des accès doivent donc couvrir les deux aspects :

1. audit des attributions de droits et

2. audit des accès.

Retour sur investissement

Les obligations de régulation : une opportunité

La mise en place d'une Approche de Mesure Avancée (AMA) est généralement décidée au niveau de la Direction Générale pour des raisons de stratégie d'entreprise :

- Réduction et maîtrise des fonds propres obligatoires,
- Réduction des coûts d'assurance,
- Démonstration d'une bonne maîtrise des risques auprès des clients et investisseurs.

Une AMA est nécessairement coûteuse en termes d'organisation et de processus, mais la gestion des identités et des accès peut alléger une partie de ce coût.

D'abord, la gestion des identités et des accès contribue à diminuer le nombre d'incidents opérationnels générateurs de pertes. Par les processus de mesure AMA mis en place, la banque peut mesurer cet impact.

Ensuite, une telle solution améliore la productivité des employés. Quand des entreprises d'autres secteurs d'activité (et donc non concernées par Bâle III) s'équipent, en gestion des identités et des accès, elles le font non seulement pour réduire leurs risques opérationnels, mais aussi pour obtenir un retour sur investissement direct.

Cette seconde source de réduction des coûts est facilement démontrable en termes de gains de productivité pour trois types d'employés :

1. utilisateurs,

2. help desk,

3. administrateurs système.

Une solution de gestion des identités et des accès peut donc généralement être rentabilisée rapidement - même sans tenir compte de la réduction des incidents opérationnels qu'elle entraîne.

Mesure du retour sur investissement en termes de productivité

Evidian a développé une méthodologie permettant d'évaluer le retour sur investissement d'une solution *Evidian IAM Suite* en termes de productivité. Voici quelques exemples de domaines concernés :

Utilisateurs	✓ Temps gagné à ne plus rentrer des mots de passe multiples. ✓ SComme il n'y a qu'un seul mot de passe à retenir, les oublis de mots de passe – et le temps perdu à contacter le help desk – sont notablement réduits. ✓ Un nouvel utilisateur ou un utilisateur changeant de fonction dispose immédiatement de ses droits d'accès. Il n'a donc pas à attendre plusieurs jours qu'on lui en attribue
Help-desk	✓ Les pertes de mots de passe représentent jusqu'à 30 % des appels au help-desk. La mise en place d'une solution de gestion des identités et des accès, telle que Evidian IAM Suite, permet de réduire considérablement ces coûts.
Administrateurs systèmes	✓ Les procédures pour déclarer un nouvel utilisateur sont très rapides, et ne nécessitent qu'une simple opération sur la console Evidian IAM Suite. ✓ Supprimer tous les comptes d'un utilisateur qui quitte la banque ne prend également que quelques secondes.

Pour une évaluation adaptée à votre organisation, contactez Evidian à l'adresse info@evidian.com.

Données d'audit

Les accords Bâle requièrent (paragraphe 669 c) une forte granularité du système de mesure du risque opérationnel.

Les données d'audit générées par *Evidian IAM Suite* sont extrêmement détaillées. Elles couvrent notamment les domaines suivants :

Audit sur l'activité des utilisateurs

- Accès autorisé à une application
- Accès refusé pour cause de mot de passe/ identifiant
- Accès refusé car en dehors des heures et dates autorisées (configurable)
- Compte bloqué car trop de ten tatives refusées, etc.

Audit sur l'attribution des droits d'accès

- Création, modification et suppression d'un utilisateur, d'une ressource, d'un groupe d'utilisateurs ou de ressources
- Inclusion d'un utilisateur ou d'une ressource à l'intérieur d'un groupe
- Attribution de droits d'accès (à une ressource ou un groupe de ressources) pour un utilisateur ou un groupe d'utilisateurs
- Création et modification de profils
- Attributions de droits spécifiques à un administrateur de sécurité (basé sur les rôles).
- Opérations de changement de mot de passe, etc.

Pour mieux documenter les incidents générateurs de pertes, les historiques (logs) doivent stocker l'identité réelle de l'utilisateur et le lieu de la tentative d'accès aux applications. Cette information n'est généralement pas présente dans le log des applications. Mais elle est présente dans le log de Evidian IAM Suite.

Log Application :

« Quelqu'un a accédé au compte GMAR_01 le 02/03/2009 à 1:02 du matin »

Log IAM Suite :

« L'employé George Martin a accédé au compte GMAR_01 en utilisant la station PC_027 le 02/03/2009 à 1:02 du matin »

La réduction des risques opérationnels grâce à Evidian IAM Suite

Approche modulaire

Les accords Bâle III permettent d'implémenter des Approches de Mesure Avancées (AMA) sur des zones géographiques ou des domaines fonctionnels donnés.

De façon similaire, la modularité d'*Evidian IAM Suite* rend possible son déploiement sur des zones sélectionnées d'une banque (région, filiale, type d'activité, etc.). Elle permet également de n'activer que certaines des fonctions possibles, telles que l'authentification unique sécurisée, le provisioning ou la gestion des identités.

Evidian IAM Suite peut s'implémenter de façon modulaire, lors d'un projet à plusieurs phases. Ainsi, une banque mettra en oeuvre et intégrera graduellement à son infrastructure de gestion des risques opérationnels des fonctions de gestion des identités et des accès.

Intégration au sein d'un pôle de gestion des risques opérationnels

En rendant possible une gestion efficace des identités et des accès, *Evidian IAM Suite* peut immédiatement réduire les risques opérationnels liés aux accès aux ressources informatiques.

Evidian IAM Suite consolide les données d'audit sur l'attribution des droits d'accès et leur utilisation au sein de la banque. Cela simplifie notablement l'audit, le reporting et le diagnostic.

De plus, les opérations d'attribution de ces mêmes droits d'accès sont également consolidées sur une même console, quelles que soient les plates-formes concernées (serveurs, applications, Web etc.). Cela permet d'effectuer immédiatement une correction en cas de découverte d'un incident opérationnel.

Evidian IAM Suite facilite ainsi la prise en compte des risques liés aux accès à l'information par le pôle de gestion des risques opérationnels défini par Bâle III.

Annexe A : Couverture des exigences des accords de Bâle

Le tableau ci-après, non limitatif, reprend plusieurs des critères qualitatifs nécessaires pour implémenter des Approches de Mesure Avancées (paragraphe 666II met en regard l'apport de *Evidian IAM Suite* concernant le risque opérationnel lié à la gestion des identités et des accès.

Exigence (a) :

"[Une banque] doit disposer d'une fonction gestion du risque opérationnel indépendante, responsable de la conception et de la mise en oeuvre du dispositif de gestion du risque opérationnel de l'établissement. Cette fonction est responsable de la codification des politiques et procédures de l'établissement concernant la gestion et le contrôle du risque opérationnel ; de la conception et de la mise en oeuvre de la méthodologie de mesure du risque opérationnel de l'établissement ; de la conception et de la mise en oeuvre du système de notification du risque opérationnel ; de l'élaboration de stratégies permettant d'identifier, de mesurer, de surveiller et de contrôler/d'atténuer le risque opérationnel."

Coverage (a):

Codification des politiques et procédures de l'établissement concernant la gestion et le contrôle du risque opérationnel	La mise en place d'*Evidian IAM Suite* permet à l'équipe de gestion du risque opérationnel d'avoir un endroit unique où consulter les procédures d'accès aux données et les données historiques sur les accès et les attributions de droits. De plus, cet environnement peut être utilisé pour définir et implémenter toutes les politiques d'accès à l'informatique. Cela permet de faciliter et d'accélérer la mise en oeuvre des politiques et procédures.
Conception et mise en oeuvre de la méthodologie de mesure du risque opérationnel de l'établissement	*Evidian IAM Suite* produit des données historiques sur les accès à l'informatique et l'attribution des droits quelle que soit la plateforme technique. Le travail de synthèse de ces informations afin de mesurer le risque opérationnel est donc grandement facilité. De plus, les méthodologies de mesure mises en place avec *Evidian IAM Suite* sont indépendantes des technologies sousjacentes.
Conception et mise en oeuvre du système de notification du risque opérationnel	*Evidian IAM Suite* dispose de procédures d'alertes configurables en cas de situation critique (tentative d'intrusion etc.) Cela permet utilement de compléter le système de notification mis en place dans l'établissement.
Élaboration de stratégies permettant d'identifier, de mesurer, de surveiller et de contrôler/d'atténuer le risque opérationnel	Le risque opérationnel lié aux accès aux données informatiques est mesurable grâce aux informations d'audit produites par Evidian IAM Suite. En utilisant Evidian IAM Suite, les administrateurs peuvent intervenir immédiatement pour remédier à un risque opérationnel nouvellement découvert. En effet, il dispose de consoles centralisées pour modifier les politiques de droits d'accès sur l'ensemble de la banque, quelles que soient les plates-formes techniques.

Exigence (b):

"Le système interne de mesure du risque opérationnel doit être étroitement associé à la gestion quotidienne des risques de l'établissement. Les données qu'il produit doivent faire partie intégrante de ses processus de surveillance et de contrôle du profil de risque opérationnel. Ainsi, ces informations doivent tenir une place prépondérante dans la notification des données sur les risques, dans les rapports à la direction, dans l'allocation interne du capital et dans l'analyse des risques. La banque doit disposer de techniques pour allouer les fonds propres pour risque opérationnel aux principalesunités et pour inciter à une meilleure gestion du risque opérationnel dans l'ensemble de l'établissement."

Couverture (b):

Le système interne de mesure du risque opérationnel doit être étroitement associé à la gestion quotidienne des risques de l'établissement	La gestion quotidienne des risques liés à l'accès à l'informatique est assurée par Evidian IAM Suite. Les politiques de droits d'accès, suppressions et attributions de comptes et autres opérations sont effectuées à partir de la console de gestion. Cela est valable pour l'ensemble des parties de la banque où *Evidian IAM Suite* a été déployé.
Les données qu'il produit doivent faire partie intégrante de ses processus de surveillance et de contrôle du profil de risque opérationnel.	Ce sont les données d'audit produites par Evidian IAM Suite qui sont utilisées directement par la fonction de gestion du risque opérationnel.

Exigence (c) :

"L'exposition au risque opérationnel et les pertes subies doivent être régulièrement notifiées à la direction de l'unité concernée, à la direction générale et au conseil d'administration. La banque doit disposer de procédures lui permettant de prendre les mesures nécessaires à la lumière des rapports à la direction."

Couverture (c) :

Evidian IAM Suite peut être utilisé comme une source d'information pour les procédures de notification à la direction. Il produit régulièrement des données d'audit utilisables par les outils de mesure et de rapports. *Evidian IAM Suite* permet également de mettre en place rapidement les mesures correctrices d'attribution de droits d'accès nécessaires pour contrer un risque opérationnel détecté.

Exigence (d):

"Le système de gestion du risque de la banque doit être accompagné d'une documentation correcte. La banque doit avoir mis en place des procédures permettant d'assurer le respect d'un ensemble documenté de politiques, contrôles et procédures internes concernant le système de gestion du risque opérationnel, qui doit comporter des règles destinées à remédier aux infractions."

Couverture (d):

Comme *Evidian IAM Suite* est indépendant des technologies sous-jacentes. Les procédures destinées à remédier aux infractions liées aux accès frauduleux sont donc faciles à documenter. Elles sont en effet toutes réalisées en utilisant la même interface, celle de la console *Evidian IAM Suite.*

Exigence (e):

"Les auditeurs internes et/ou externes doivent examiner périodiquement les processus de gestion et les systèmes de mesure du risque opérationnel. Ces examens doivent porter sur les activités des unités et sur la fonction indépendante de gestion du risque opérationnel."

Couverture (e) :

L'examen des processus de gestion du risque opérationnel lié aux droits d'accès est simplifié, car *Evidian IAM Suite* concentre sur la même plate-forme la gestion des accèsà des environnements très divers (Web, applications indows, mainframes, environnements client/serveur etc.) Ainsi, les droits d'accès sont gérés par un nombre limité d'acteurs (ressources humaines, direction de la sécurité). Cela rend le processus plus facilement auditable.

La chaîne de mesure du risque opérationnel lié aux droits d'accès est simplifiée car les informations sont concentrées en un seul point. Les examens sont donc facilités.

Exigence (f):

"La validation du système de mesure du risque opérationnel par les auditeurs externes et/ou les autorités de contrôle doit comporter les éléments suivants :

- vérification du bon fonctionnement des processus de validation interne ;
- vérification de la transparence et de l'accessibilité des flux de données et

des processus liés au système de mesure des risques. En particulier, les auditeurs et les autorités de contrôle doivent être en mesure d'avoir facilement accès aux spécifications et aux paramètres du système, lorsqu'ils le jugent utile et conformément à des procédures appropriées."

Couverture (f) :

La gestion des droits d'accès à l'ensemble des moyens informatiques de la banque est faite entièrement à partir de la console Evidian IAM Suite. Il est donc possible aux auditeurs d'accéder à tout moment à cette console et de vérifier sa bonne configuration et son paramétrage.

Annexe B : Mise en oeuvre nationale des accords de Bâle la Commission Bancaire

Les pays membres sont tenus d'utiliser les accords de Bâle comme une base pour réviser les réglementations locales. Nous donnons ci-dessous un exemple en Europe.

En 2003, la Commission Bancaire française a émis un questionnaire afin de permettre aux établissements financiers d'évaluer leur préparation aux critères des nouveaux accords de Bâle. Le tableau ci-dessous présente les réponses qu'un outil de gestion des identités et des accès permet d'apporter à plusieurs questions.

Gestion, identification et évaluation

Elément du questionnaire	Contribution d'Evidian IAM Suite
(1) L'organe délibérant de votre établissement a-t-il approuvé la mise en place d'un dispositif de surveillance dédié au risque opérationnel ?	La mise en place d'*Evidian IAM Suite* permet très simplement d'alimenter le dispositif de surveillance avec une information pertinente concernant les accès à l'information.
(4) La Direction Générale dispose-t-elle d'états de synthèse adaptés permettant la surveillance du risque opérationnel ?	La fourniture d'états de synthèse ne peut être dépendante de la source d'information. Par conséquent, *Evidian IAM Suite* a pour vocation de produire des données facilement intégrables dans une infrastructure de reporting existante.
(27) Ces analyses ont-elles conduit à l'élaboration d'une typologie du risque opérationnel conforme aux 7 facteurs de risques définis par le Comité de Bâle ?	Les données sur les risques opérationnels fournies par *Evidian IAM Suite* concernent quatre des sept types de facteurs de risque : ✓ fraude interne, ✓ fraude externe, ✓ clients, produits et pratiques commerciales, ✓ exécution, livraison et gestion des processus.
(31) Votre établissement dispose-t-il d'une base de données historique recensant les pertes et incidents ?	*Evidian IAM Suite* peut fournir des données sur les incidents opérationnels sous forme relationnelle ou d'export lisibles par des outils de rapport standard. Ces extraits peuvent être stockés pendant plusieurs années.

Reporting interne

Elément du questionnaire	Contribution d'Evidian IAM Suite
(33) Votre établissement a-t-il mis en place un reporting interne sur le risque opérationnel ?	*Evidian IAM Suite* permet de gérer la sécurité des accès, et produit des données d'audit concernant les accès et les opérations d'attribution des droits. Les données produites par *Evidian IAM Suite* sont directement exploitables par des outils de reporting standard.
(35) Ce reporting reflète-t-il et identifie-t-il tous les domaines à risques ?	Les données produites par Evidian IAM Suite concernent : ✓ les incidents liés aux tentatives d'accès non autorisés (mots de passe erronés, accès en dehors des heures de travail etc.), ✓ les données sur les accès autorisés, ce qui permet de diagnostiquer après coup un incident d'exploitation, ✓ les données sur la gestion des droits, ce qui permet d'identifier les opérations d'administrations erronées ou frauduleuses.
(38) Ce reporting comporte-t-il des indicateurs d'alerte qui mettraient en évidence toute augmentation du risque ou toute possibilité de pertes futures ?	Des alertes sont produites par Evidian IAM Suite sur une gamme d'événements concernant les tentatives d'accès non autorisés.

Dispositif de réduction

Elément du questionnaire	Contribution d'Evidian IAM Suite
(45) Votre dispositif de contrôle des systèmes d'information s'assure-t-il de la maintenance d'accès sécurisés aux actifs et aux données ainsi que des procédures permettant leurs sauvegardes ?	Les serveurs rendant possible l'accès sécurisé aux ressources peuvent être installés en configuration à tolérance de panne. Cela garantit un accès hautement disponible aux serveurs et applications critiques.

Annexe C : Gestion des identités et détection d'intrusion

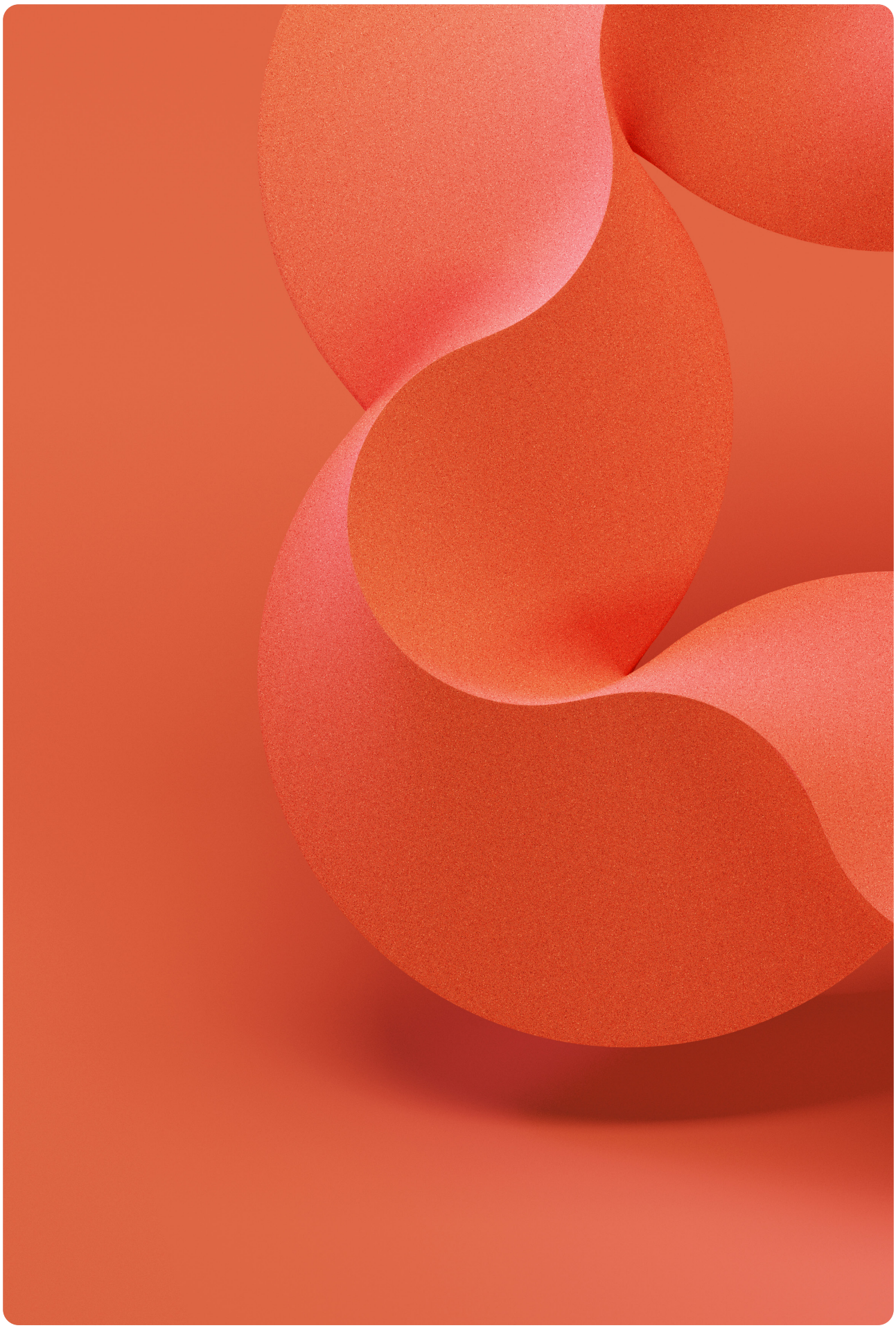
Une gestion centralisée des identités et des accès permet de simplifier notablement le travail de l'équipe du pôle de gestion du risque opérationnel. Elle est essentiellement complémentaire avec des outils de détection d'intrusion, lesquels sont insuffisants pour assurer une couverture complète des risques informatiques :

- Une grande partie des incidents opérationnels concerne des accès utilisant des mots de passe volés ou utilisés à mauvais escient. Ils ne sont donc pas le fait d'une intrusion par des moyens techniques. Un outil de gestion des identités et des accès, tel qu'*Evidian IAM Suite*, permet de connaître très rapidement la source de l'accès, et les conditions dans lesquelles les droits d'accès ont été attribués à tort.

- De nombreux incidents opérationnels sont le fait de personnes travaillant à l'intérieur de l'entreprise, et ont lieu dans l'intranet de la banque. Dans ce cas, la cause de l'incident n'est pas une tentative d'accès externe.

- Un outil de détection d'intrusion permet de centraliser les données d'alerte, mais pas les moyens d'action pour remédier à ces alertes. Après détection d'un incident opérationnel, il faudra reconfigurer un outil précis (firewall, routeur etc.) avec ses propres outils d'administration.

À l'inverse, Evidian IAM Suite, on the other hand, allows immediate correction of the source of the incident from a single console, whatever the platform concerned (mainframe, web site, etc.).



Connect with us

eviden.com