IXerp l'Art de décider
Services Informatiques

PARTAGE & CONNAISSANCE
La Newsletter destinée à ceux qui désirent en savoir plus !
n°28 - Juillet 2009

Enjeux et Objectifs des Autorisations sur SAP

Les autorisations : Pourquoi ?

Le concept d'autorisation s'applique à tout système d'information (SI).

Il s'agit d'autoriser des utilisateurs à accéder au système, puis aux données contenues dans ce système. (On parle aussi d'habilitation, terme plus spécifique qui désigne purement l'autorisation d'accès octroyée à un utilisateur).

En effet, n'importe qui ne doit pas avoir accès à n'importe quelle donnée dans le SI.

Ceci pour des raisons de confidentialité d'une part, et de sécurité d'autre part.

L'entreprise se doit donc de paramétrer son SI pour assurer la protection de ses actifs et la confidentialité de son passif, en octroyant des droits d'accès ad hoc aux utilisateurs de ce SI.

Cette démarche de sécurisation d'accès aux données au niveau applicatif est désignée sous le terme de « gestion des autorisations ».

Fonctionnellement, cette gestion est transverse.

Elle impacte en effet toutes les fonctions et tous les métiers de l'entreprise.

Que dit la loi française ?

La CNIL[1] a statuer que les entreprises doivent respecter des lois spécifiques pour la protection des salariés, protection des accords conclus entre partenaires sociaux, fournisseurs, … les empêchant de diffuser quelque information que ce soit définie dans le cadre desdites lois.

La sécurité des systèmes d'information (SSI) doit être considérée globalement afin d'éviter d'omettre de prendre en compte des risques qui pourraient avoir un impact inacceptable sur les activités de l'entreprise.

Cette vision globale est nécessaire à la mise en place d'un véritable Système de Gestion de la Sécurité des Systèmes d'Information (SGSSI)

Il permettra de planifier, mettre en œuvre, vérifier et améliorer la SSI, et ce, de manière itérative.

La norme internationale ISO 27001 spécifie un Système de Gestion de la Sécurité des Systèmes d'Information (SGSSI).

Ce SGSSI est structuré en quatre étapes récurrentes (planifier, mettre en œuvre, vérifier, améliorer), afin de respecter le principe de la roue de Deming, issue du monde de la qualité.

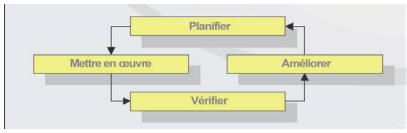

Schéma récapitulatif

C.N.I.L
Commission Nationale de l'Informatique et des Libertés, est une autorité indépendante qui a pour mission d'informer, de garantir les droits d'accès et de protéger les fichiers informatiques.

La sécurité financière : Une notion protéiforme
C'est la connaissance, la maîtrise et la couverture des risques liés à l'activité économique et financière. Ces risques sont multiples et l'exigence de sécurité s'inscrit plus largement dans l'émergence contemporaine de la « société assurantielle ».

Outre Atlantique : Sarbanes-Oxley

Suite aux scandales des affaires Enron et Worldcom survenus en 2001, le congrès américain vote la loi Sarbanes-Oxley dite « SOX » en 2002, visant à renforcer les

systèmes de contrôle interne et externe des entreprises cotées en bourse et d'assurer ainsi une plus grande fiabilité de l'information. Par la même, la loi SOX fait peser une plus forte responsabilité pénale sur les dirigeants avec notamment des sanctions renforcées.

Les systèmes d'information sont directement impactés par les sections **404** (mise sous contrôle des rôles opérationnels), **302** (traçabilité comptable) et **409** (remontée d'informations en temps réel) de ladite loi .

En Europe, les grands groupes d'envergure internationale se mettent donc peu à peu en conformité avec les recommandations de la loi SOX ; mise en conformité qui concerne pour l'essentiel la section 404 : mise sous contrôle des rôles opérationnels, avec respect strict des règles de séparation des tâches.

Dans ce cadre, les audits ne doivent surtout pas négliger la possibilité de failles dans le SI susceptibles de remettre en cause la sécurité des processus dans l'entreprise.

La gestion des autorisations intervient alors spécifiquement dans un **audit plus global**. Elle permet de révéler des lacunes et erreurs de gestion des habilitations, et donc d'identifier des risques encourus par l'entreprise à tout niveau.

LES BONNES QUESTIONS A SE POSER !

Qui a le droit d'accès à quelle donnée ?
Quels dangers pour quelle autorisation d'accès ?
Ce sont les problématiques de la gestion des autorisations
Gestion sans laquelle le système d'informations risque d'être totalement inefficient.

Les Autorisations sous SAP

Une autorisation permet de :

- Renseigner les données maîtres utilisateurs dans le système
- Définir les données accessibles par les utilisateurs

La mise à niveau des autorisations permet de bénéficier des résultats suivants :

1 - Mise en conformité effective de la gestion des profils et des droits, avec les exigences SOX.

2 - Mise en oeuvre d'une matrice de rôles respectant les principes de séparation des tâches (SOD).

3 - Personnalisation et amélioration des outils SAP liés à la gestion des autorisations.

4 - Mise en place d'une procédure de traitement des failles détectées par les auditeurs.

5 - Homogénéisation des rôles permettant de simplifier la maintenance et l'évolutivité des autorisations.

Retrouvez notre dossier «La gestion des autorisations selon IXERP» sur www.ixerp.com

Les Mardis de l'ERP redémarrent ! Et vous ?

Mardi 15 Septembre 2009
Salons Hoche - Paris 8e

« La Déclaration d'Echange de Biens »

IXerp
l'Art de décider

Renseignements au 01 73 04 92 34

La Newsletter IXERP
Redacteur : stephane.bensimon@ixerp.com
Tel : 01 73 04 92 34 - Fax : 01 79 75 93 37
Disponible sur www.ixerp.com