

L'audit du système informatique

L'audit du système informatique porte sur le matériel informatique et le logiciel, particulièrement les applications. Pour le matériel, on vérifie que l'équipement est approprié aux objectifs poursuivis. Pour le logiciel, on vérifie que l'entrée, le traitement, le stockage et la sortie des données s'effectuent correctement.

Un audit peut être interne ou externe. Dans le second cas, le choix des consultants est crucial pour la réussite de l'audit. Un bon choix permet de bénéficier des compétences parfois considérables que les consultants ont accumulées au fil du temps. Par contre, le coût d'un audit externe est plus élevé que celui d'un audit interne.

L'objectif fondamental d'un audit consiste à vérifier et améliorer la qualité des procédures en place pour le contrôle du fonctionnement du système informatique. On cherche à contrôler les procédures de contrôle.

Un audit s'appuie généralement sur un processus d'analyse et d'évaluation long et compliqué. Il donne lieu à un rapport qui présente les faiblesses constatées. Voici un exemple de fiche d'audit :

Auteur et date	Paul Martin, 2 septembre 2009
Faiblesse constatée	Pas de procédure de contrôle périodique des sauvegardes de données
Commentaire	L'ensemble des données de plusieurs jours ou de plusieurs semaines sont susceptibles d'être perdues sans possibilité de récupération
Niveau de risque	Élevé
Urgence	Haute
Probabilité d'occurrence	Moyenne
Effet sur l'audit	Non
Destinataire et date	Jean Dupont, 7 septembre 2009
Responsable de l'action	Jean Dupont
Action corrective	Établir et mettre en oeuvre une procédure de test périodique des backups
Délai d'action	30 septembre 2009

La notion de traçabilité des transactions est importante. Au temps où on travaillait manuellement, il était simple de suivre chaque transaction de sa naissance à sa terminaison (*audit trail*). Avec la gestion informatisée des transactions, par contre, certaines étapes de traitement restent invisibles, ce qui complique le processus d'audit et augmente les risques d'erreur. C'est pourquoi les progiciels de gestion actuels comprennent généralement des moyens étendus de traçabilité des transactions.

Quelques formes d'audit

Un audit peut être général ou se concentrer sur un aspect du système informatique.

Les audits financiers ont historiquement été les premiers. Dans le contexte des systèmes informatiques, ils consistent à analyser et évaluer la pertinence financière des choix informatiques effectués dans l'organisation qui fait l'objet de l'audit. Ces choix concernent le matériel, le logiciel, mais aussi les processus de travail et tout autre aspect de l'informatique de l'organisation.

Les audits sur la qualité des données vérifient que les données de l'organisation qui fait l'objet de l'audit sont exactes, complètes et non ambiguës. Ils s'appuient sur deux sources d'informations principales : le personnel et les données stockées en mémoire de masse.

Ces audits sont importants dans tout type d'organisation. Au début des années 1980, le FBI émettait jusqu'à 12'000 mandats d'arrêt invalides par jour, mettant autant de personnes en danger d'être arrêtées sans cause.

Les audits applicatifs portent sur un logiciel particulier, par exemple un progiciel de gestion intégré. Ils contrôlent l'intégrité des données, la validité des informations, l'exactitude des traitements (par exemple, le calcul de la TVA), la traçabilité des transactions, les procédures de mise à jour et de consolidation des données, la maintenance du logiciel concerné (gestion des patches, gestion des updates, etc.), les méthodes et les programmes d'interfonctionnement (interoperability), etc.

Les audits sur la sécurité sont de plus en plus importants parce que les télécommunications rendent les systèmes plus vulnérables qu'auparavant. Ils portent sur les contrôles d'accès au système informatique et aux données, le chiffrement, l'authentification des auteurs des messages, les procédures de récupération en cas de défaillance du système, le plan de reprise sur sinistre (*disaster recovery*), etc.