Conférence RSA Security : CA fédère ITIL + Cobit + ISO/IEC

Computer Associates, ayant été lui-même, au coeur de la tourmente sur la transparence des comptes (cf. le feuilleton 2003 et 2004), s'est senti parmi les plus concernés s'agissant de l'application des nouvelles règles en matière de données financières et de transparence sur les comptes.

L'éditeur propose un « mapping » -ou sorte de réconciliation / consolidation permettant de rapprocher les trois principales régulations en vigueur: ITIL, COBIT et ISO17799:2005 Responsables financiers, commissaires aux comptes, auditeurs, mais aussi DSI n'ont pas le choix: il faudra progressivement être conformes aux nouvelles règles sur la présentation des données financières et comptables. Un vrai casse-tête pour qui veut suivre les « standards ». Computer Associates, qui, après ses démêlés avec les autorités de régulation financière, n'a plus le choix que d'être un modèle de référence, se propose donc de « fédérer » ou consolider les trois principaux « standards » en la matière -standards définis par l'ISACA (association internationale des auditeurs et contrôleurs de gestion), dont le correspondant en France est l'AFAI. Petit rappel: 1- **ITIL** (Information Technology Infrastructure Library): ses règles ont, en grande partie été inspirées tout au long des années 1990 par la doctrine de Margareth Thatcher (ex Premier ministre du Royaume-Uni surnommé, on s'en souvient, « la Dame de fer »). « *Il est prévu un rafraîchissement de l'ITIL, qui doit conduire à un rapprochemnt avec les règles du COBIT*« , commente Yves Le Roux, responsable de la stratégie technologie chez Computer Associates France. 2- **COBIT** (Control Objectives for Information and related Technology, de l'association Information Systems Audit and Control Association): ses dispositions concernent directement la gouvernance des systèmes d'information, « *au sens large du terme, donc incluant les données financières, comptables… Il existe pas moins de 34 'process' pour 318 points de contrôle*« . Une 4è édition est en préparation, la première datant de 1996. 3- **ISO/IEC 17799:2005**: cet ensemble de règles a été mis à jour en juin 2005. On y compte 11 chapitres dits de « sécurité » (un nouveau chapitre s'y est ajouté, en même temps que des rajouts/suppressions de points de controles, et la mise à jour de la documentation s'y rapportant). Pour fédérer toutes ces règles, provenant de trois organismes différents, Computer Associates préconise de suivre les travaux de l'association internationale ISACA. « *Faire le « mapping » des points de contrôle définis par ces trois grandes organisations, c'est ce que nous avions commencé à faire*« , explique Yves Le Roux. « *Nous nous fions désormais à l'ISACA, une association neutre, qui n'est pas l'expression d'une personne ni d'un lobby mais bien la résultante d'un groupe de travail indépendant, international*« . Une première synthèse devrait être prête pour la fin 2005. Un travail fastidieux! « *ITIL ne couvre bien qu'une partie de COBIT: 10 des 34 'process' [évoqués plus haut]. En pratique, nous avons mis en place des matrices ou sortes de tableaux de bord de correspondance qui aident à établir des corrélations entre les procédures décrites, s'agissant par exemple des SLA utilisées pour ITIL*« , explique Yves Le Roux. (A suivre)