# Explications concernant les nouvelles lignes directrices de l'OFCOM relatives à la sécurité et la disponibilité des infrastructures et des services de télécommunication

Le concept de ces lignes directrices est fondé sur les principes de la gestion de la sécurité de l'information sur lesquels sont basés des standards existants.

Il est premièrement recommandé aux FST (fournisseurs de services de télécommunication) de développer et de gérer une politique en matière de sécurité qui constitue la base de la gestion de la sécurité de l'information. L'objectif de celle-ci est la préservation et la sécurisation des ressources sensibles au sein de l'organisation. Elle décrit notamment la vision de la direction d'entreprise relative à la sécurité et tient compte des menaces à considérer pour définir le périmètre à sécuriser.

Le FST est ensuite invité à mettre en place un système de gestion de la sécurité (ISMS) selon les exigences de la recommandation X.1051 qui a été développée dans le but d'être en mesure de démontrer la capacité d'un FST à maîtriser les aspects de sécurité afin de promouvoir la confiance des parties prenantes en ses pratiques.

L'objectif de cette recommandation semble correspondre parfaitement à celui de nos lignes directrices puisque cette dernière adapte les principes du standard BS 7799-2 (specification for information security management systems) au contexte des télécommunications modernes.

Le processus prévu par ce document reprend le principe de l'amélioration continue en suivant les 4 phases récurrentes « PLAN-DO-CHECK-ACT » prévue par le standard BS 7799-2 mais encore par d'autres systèmes de gestion tel que la norme ISO 9001 prévue pour la gestion de la qualité ou encore la norme ISO 14001 relative au domaine de l'environnement. Par ailleurs, ce modèle en 4 phases reflète parfaitement les principes de la directive de l'OCDE sur la sécurité des systèmes d'information et des réseaux (2002 OECD Guidance on the Security of Information Systems and Networks).

En phase de planification (PLAN), il est prévu de définir les objectifs. Le FST devrait notamment identifier et évaluer les risques puis déterminer des objectifs de contrôle susceptible de les traiter. Puis, en phase d'exploitation (DO), des procédures et des contrôles sont mis en œuvre pour atteindre le objectifs définis.

Il s'ensuit une phase d'évaluation et de révision (CHECK) de l'ISMS permettant d'estimer l'efficacité du système, d'apprécier l'ampleur du risque résiduel et de prendre en compte l'impact de certains événements sur la sécurité de l'information.

La dernière phase (ACT) invite les FST à améliorer régulièrement le système de gestion de la sécurité.

Comme dans le cadre des documents BS7799-2 et ISO 9001, une documentation du système de gestion de la sécurité est exigée. Une telle documentation pourrait servir de base à d'éventuelles activités de l'OFCOM en matière de surveillance.

En plus de cette recommandation relative à la mise en place du système de gestion de la sécurité, les lignes directrices proposent de se référer aux documents UIT-T X.1051, UIT-T E.408 et ISO 17799 pour ce qui concerne les procédures et les contrôles à mettre en œuvre dans le cadre de l' ISMS. De telles références répondent aux souhaits des FST consultés qui sont unanimement opposés à la publication d'un nouveau document sur le sujet mais plutôt en faveur de l'utilisation de l'ISO 17799 auquel ils se réfèrent d'ores et déjà. Ce document qualifié de « code des bonnes pratiques » est en fait une liste détaillée et commentée de mesures de sécurité favorisant l'interprétation commune.

La référence des récents documents UIT-T X.1051 et E.408 dans nos lignes directrices paraît judicieuse puisque cet organisme de standardisation du domaine des télécommunications prévoit de se baser sur ces publications pour l'élaboration d'un futur document relatif au domaine de la sécurité des réseaux ( ITU-T Study Group 17, TD 2048 Rev. 3, Proposal for a new Project – Security baseline for Network Operators ).

Par ailleurs, les lignes directrices recommandent également aux FST d'élaborer une planification de la continuité (BCP, Business continuity Plan) ainsi qu'une planification de la reprise des activités après un sinistre (DRP, Disaster Recovery Plan) ce qui correspond là encore au cadre prévu par les principes de base de la gestion de la sécurité.

La planification de la continuité a pour but d'organiser et de gérer la réponse à une panne afin d'en venir à bout et de minimiser les effets de celle-ci. La planification de la reprise des activités après un sinistre, quant à elle, décrit les procédures à mettre en œuvre permettant de recouvrer une exploitation normale.

Finalement, les lignes directrices proposent aux FST de mettre en œuvre leurs procédures et leur infrastructure conformément aux standards reconnus en matière de sécurité de l'information et des infrastructures. Compte tenu des importants développements qui peuvent être constatés au sein des différents organismes de normalisation, l'OFCOM pourrait publier et actualiser une liste des documents de référence en annexe aux lignes directrices.

26.10.05/OFCOM/jec