

Politique de sécurité globale et politiques sectorielles de sécurité l'expérience du Groupe France Télécom

Présentation Club 27001 – 20 septembre 2007

Christiane Payan – Secrétariat général – Direction de la Sécurité Groupe



sommaire

- les fondamentaux : gouvernance, globalité, amélioration continue
- la gestion de la conformité et les références normatives
- politiques et systèmes de management de sécurité : la nouvelle approche
- de la politique de sécurité de l'information à la politique de sécurité globale
- la sécurité globale dans le Groupe FT : politique et organisation
- l'élaboration des politiques sectorielles de sécurité des fonctions Corporate
- la méthode d'analyse et d'appréciation des risques : le choix d'EBIOS
- les objectifs de sécurité

les fondamentaux

- ❑ la démarche sécurité s'inscrit dans un contexte où la normalisation et la certification sont de plus en plus partie intégrante de la **gouvernance d'entreprise**.

- ❑ l'approche est désormais **globale** :

sécurité des systèmes d'information et des réseaux

sécurité des personnes (collaborateurs et clients)

sécurité des biens physiques

sécurité de l'environnement

- ❑ la politique de sécurité implique une **démarche d'amélioration continue** fondée sur un **système de management de la sécurité**, auditable et basé sur l'analyse et la gestion des risques.

une démarche d'entreprise fondée sur la mesure de la conformité et sur des processus d'évaluation

- ❑ la **gestion de la conformité** implique l'élaboration de **référentiels internes de sécurité** qui reposent sur des standards reconnus : les normes sous-tendent la politique de sécurité au niveau stratégique comme dans ses déclinaisons au niveau fonctionnel et opérationnel.
- ❑ la conformité répond aussi aux obligations légales et réglementaires.
- ❑ le management de la sécurité s'articule avec les programmes renforçant la culture de bonne gouvernance et de **contrôle interne**.
- ❑ les obligations liées au Sarbanes-Oxley Act jouent un rôle majeur pour la sensibilisation des managers et de tous les collaborateurs.
- ❑ la politique de sécurité globale a été précédée par et s'articule avec des politiques spécifiques : sécurité de l'information, archivage, gestion des crises, santé et sécurité au travail, charte de déontologie..., qui s'inscrivent dans une démarche de cohérence et de complémentarité.

références normatives : rappel de quelques caractéristiques majeures

- ❑ émergence et développement de normes de sécurité, en général issues des TIC et souvent transposées de normes nationales
- ❑ élaboration progressive d'un ensemble de standards pour la gestion de la sécurité à travers la série ISO 27000X (une dizaine en préparation d'ici 2008)
- ❑ avec un recentrage des aspects techniques vers la méthodologie, les principes directeurs, les systèmes de management
- ❑ dans une démarche générale d'amélioration continue, de plus en plus **transverse**, avec une forte **implication managériale** et une prise en compte de la sécurité globale

le groupe France Télécom prend ces normes comme référence pour son approche de la sécurité, et tout particulièrement la norme 27001 pour l'implémentation du système de management de la sécurité.

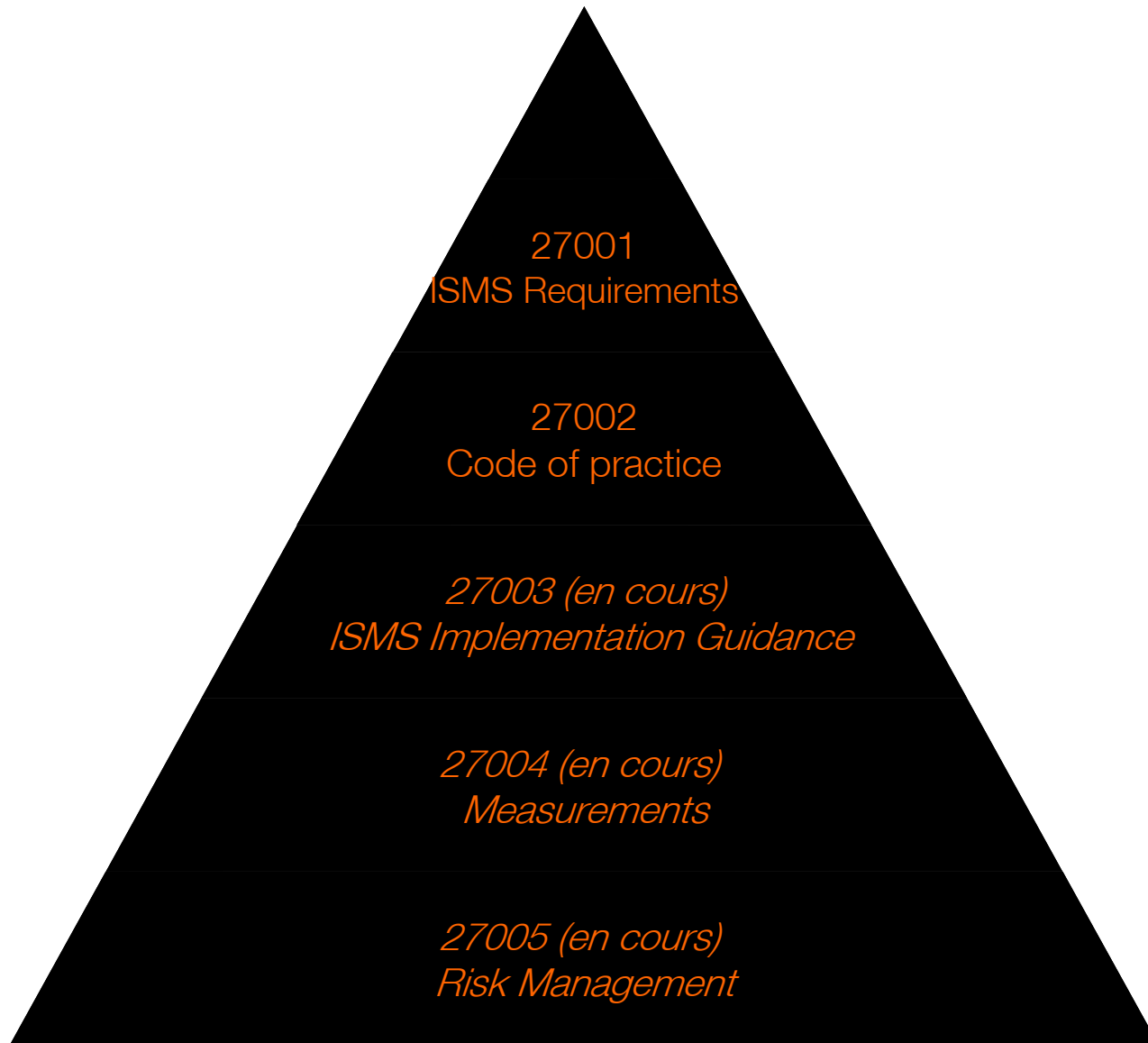
politiques et systèmes de management de la sécurité

Choix d'une approche globale s'appuyant sur le modèle de gouvernance

Plan Do Check Act

- ❑ à partir de la norme ISO 27001 et de la norme technique ISO 27002 une stratégie de gouvernance de la sécurité peut se mettre en place qui implique toute l'entreprise, ligne managériale, ensemble des collaborateurs internes et externes
- ❑ obligeant à élaborer, à réviser, à mettre en cohérence une série de documents qui constitueront le référentiel de sécurité
- ❑ avec une mise en œuvre adaptée aux besoins de l'organisation et aux différents métiers et fonctions
- ❑ avec différents niveaux d'implémentation : stratégique, fonctionnel, opérationnel
- ❑ et des procédures de suivi pour mesurer la conformité du système de management de la sécurité par des audits internes ou externes

rappel : la famille ISO 27000X



présentation de la nouvelle approche sécurité du groupe France Télécom

un bref historique

2004 : Politique de Sécurité de l' Information du Groupe (PSIG), complétée en 2006 par la politique d'archivage et records management du Groupe et par la politique de prévention et gestion des crises (avec d'autres documents de référence liés : charte de déontologie par ex.)

depuis le 1^{er} juillet 2007 la **Politique de Sécurité Globale pour le Groupe** (PSG) a remplacé la PSIG.

actuellement la PSG est en cours de déclinaison au niveau fonctionnel :

ses principes doivent être déclinés en politiques sectorielles de sécurité pour le Groupe pour les fonctions Corporate métiers et pour les périmètres transverses de portée Groupe (gestion de crises, gestion des identités et habilitations, archivage, etc.).

le document fondateur : La Politique de Sécurité Globale pour le Groupe

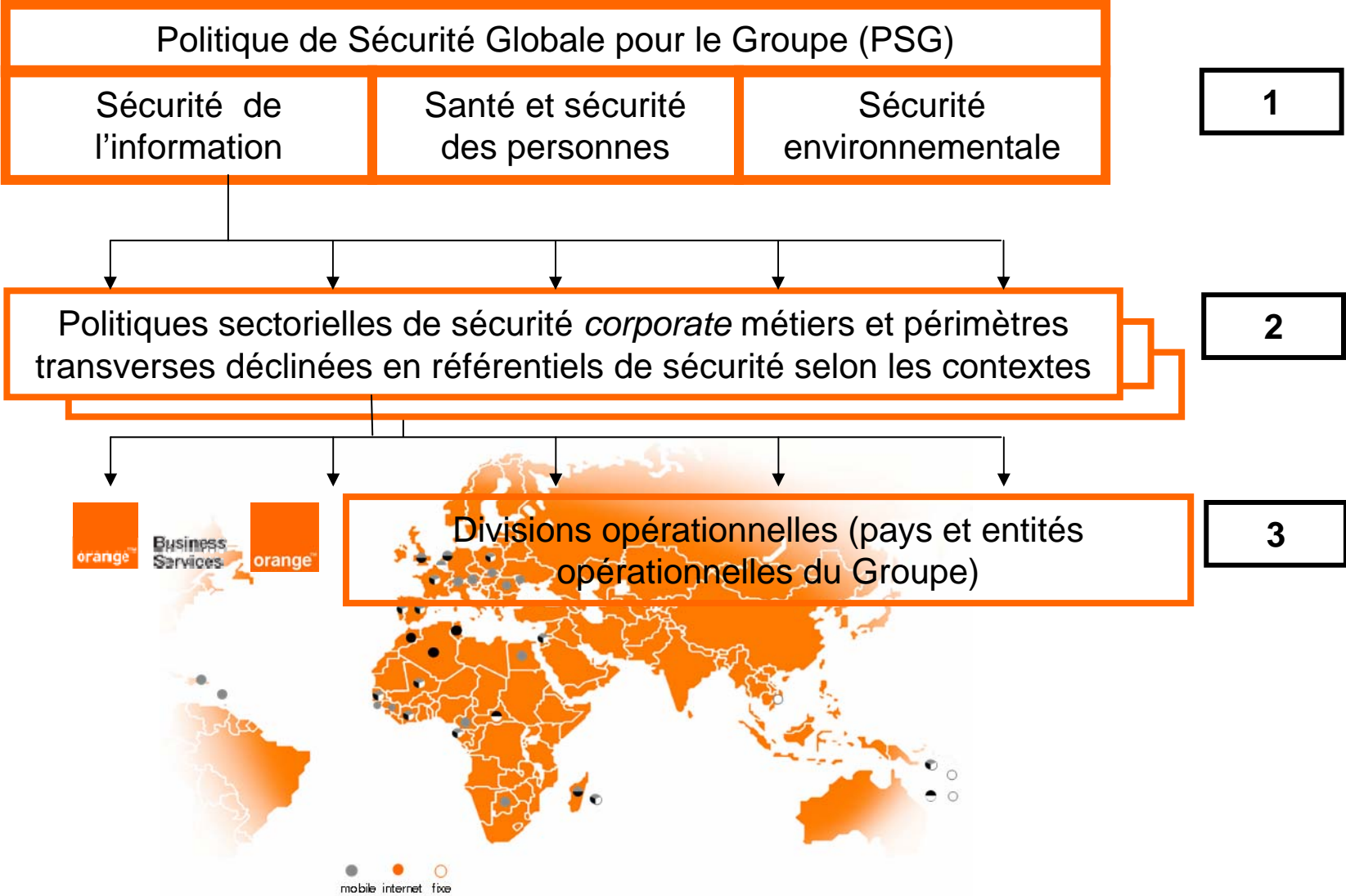
Sans sécurité, pas de création de valeur.

Le groupe France Télécom se doit d'offrir à ses clients le meilleur niveau de sécurité des connexions et des services qu'il leur procure. En contribuant à **la maîtrise de leurs risques**, en leur apportant simplicité et transparence, nous gagnons leur **confiance** et leur **fidélité**. **La sécurité est une source d'avantage compétitif** : notre Groupe doit en tirer parti en position de leader.

Plus que jamais, la sécurité est notre affaire à tous.

*(extrait de la
Politique de Sécurité Globale
du Groupe France Télécom,
entrée en vigueur le 1^{er} juillet 2007)*

la sécurité globale dans le Groupe France Télécom



organisation de la sécurité globale

- ❑ la Direction de la Sécurité du Groupe (DSEC) anime et coordonne les actions de sécurité,
- ❑ la DSEC pilote plus spécialement la politique et le système de management « sécurité de l'information ».
- ❑ des porteurs de sécurité sont désignés par les directeurs au niveau des CODIR des divisions .
- ❑ le réseau des Coordinateurs de Sécurité Globale (CSG)
 - > un CSG par Fonction Support (un ou plusieurs secteurs métiers)
 - > un Directeur de la Sécurité à Orange Business Services
 - > un Directeur de la Sécurité par Grand Pays (FR, POL, UK, SP)
 - > un CSG par Division multi-pays et par filiale

SMS : le déroulement des étapes selon la norme 27001

1. Le périmètre (scope)
2. L'inventaire des actifs (assets)
3. Risques (recensement, analyse, options envisageables)
4. Décision par les managers (refus, acceptation, transfert, réduction)
5. Sélectionner les mesures de sécurité adaptées à la réduction des risques retenus
6. Edicter les principes de sécurité (et donc la politique) puis les règles
7. Validation de la politique par les niveaux pertinents
8. Déploiement de la politique avec boucle de progrès
9. Mesures d'appropriation et de performance

Utilisation d'une méthode d'analyse
et de gestion du risque

élaboration des politiques sectorielles de sécurité des fonctions corporate (en cours)

- un engagement pris fin 2006 dans le cadre du plan d'action SOX 302 d'environnement de contrôle interne : élaborer en 2007 les politiques sectorielles de sécurité de l'information des fonctions corporate pour décliner la PSIG – Politique de Sécurité de l'Information du Groupe ;
- un objectif renouvelé avec la publication fin juin 2007 de la Politique de Sécurité Globale du Groupe qui prévoit des politiques sectorielles de sécurité au sein des métiers (RH, SI-Réseaux, Finances, Marketing stratégique, etc.) et sur des périmètres transverses de portée Groupe (sûreté et sécurité des biens physiques, gestion de l'identité...).
- dans le cadre d'une démarche de mise en œuvre du système de management de la sécurité et d'élaboration de référentiels et d'outils de reporting.

une façon de mutualiser la démarche

- ❑ à partir du ou des documents de référence de niveau stratégique, les secteurs (métiers) doivent élaborer des documents d'appropriation à leur niveau.
- ❑ pour cela, ils se positionnent sur les **éléments essentiels** (processus, acteurs...) de façon à obtenir des principes et des règles **les plus pérennes possibles**.
- ❑ cette approche peut être déclinée en tant que de besoin à différents niveaux par toute entité opérationnelle autonome en fonction de contraintes locales (par ex. Pays).

la démarche commune : impulsion et coordination DSEC, mais pilotage par la fonction concernée

- ❑ les politiques sectorielles de sécurité respectent les principes de la PSG et en déclinent les différents chapitres en les complétant : la DSEC en vérifie la conformité et la cohérence avec le Référentiel sécurité du Groupe.
- ❑ elles reposent sur l'expression par chaque fonction de ses besoins de sécurité spécifiques, avec :
 - l'évaluation du contexte et des enjeux
 - la définition du périmètre concerné
 - l'identification des éléments essentiels
 - l'analyse des risques avec le soutien du pôle interne d'expertise EBIOS
 - l'identification des types d'impact
- ❑ elles s'accompagnent d'actions de sensibilisation des collaborateurs.

la démarche au niveau de chaque fonction

les principes de sécurité découlent du **choix du management**.

le projet de **PSS** est piloté par le **porteur de sécurité de la fonction** et le **coordonnateur de sécurité globale** (CSG).

chaque fonction :

- définit le contexte de son projet et le périmètre retenu : le domaine et les sous-domaines métier de l'entité au sein du Groupe et ses relations avec les autres métiers ;
- ses objectifs par rapport aux clients internes ou externes, partenaires et interlocuteurs ;
- ses actifs et éléments essentiels (processus, actifs informationnels, données métier, acteurs, outils, bâtiments...)
- apprécie ses risques particuliers : identification des menaces, des vulnérabilités et des failles de sécurité, des mesures existantes, hiérarchisation des risques, choix du type de traitement.

les grandes étapes

- ❑ identification du contexte et des enjeux
- ❑ définition du périmètre
- ❑ identification des éléments essentiels (actifs principaux)
- ❑ appréciation des risques selon l'échelle de qualification des préjudices (4 niveaux)
- ❑ formulation des objectifs de sécurité
- ❑ production des principes et règles de la politique
- ❑ cohérence et héritage avec les autres documents de référence
- ❑ élaboration du référentiel documentaire

identification du contexte

- ❑ définition du contexte du projet et du périmètre :
- ✓ le **domaine métier** de l'entité au sein du Groupe, ses objectifs business (enjeux et orientations, contraintes),
- ✓ les **actifs matériels et immatériels** (processus, informations, acteurs, outils, bâtiments,...)
- ❑ le projet d'élaboration d'une PSS
 - > l'organisation (commanditaire, Copil, Chef de projet,...)
 - > la contractualisation entre le secteur et les experts(*) en analyse de risque
 - > les livrables : politique sectorielle, liste des éléments essentiels, analyse de risques

(*) *Ces experts sont là pour faire parler les responsables métiers et leur faire prendre position sur les jalons principaux de l'analyse de risques.*

identification des éléments essentiels

- ❑ description des processus métier
- ❑ identification des données « métier »
- ❑ identification des « propriétaires » (responsables des actifs)
- ❑ validation de l'expression de besoin de sécurité par la ligne managériale
- ❑ organisation projet : comité de pilotage, groupes de travail ad hoc
 - interview des acteurs
 - production de l'expression de besoin de sécurité
 - validation par le comité de pilotage

appréciation des risques (méthode EBIOS)

- ❑ analyse des menaces auxquelles chaque élément essentiel est exposé (selon la personne légitime pour en parler...)
- ❑ identification des vulnérabilités de chaque élément essentiel
- ❑ identification des menaces
- ❑ hiérarchisation des risques
- ❑ organisation projet retenue :
 - > interview des acteurs
 - > production du livrable « Risques »
 - > validation de l'analyse de risques et des objectifs de sécurité par le comité de pilotage