CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Conformité et analyse de risques

la conformité chez DOCAPOST
Retour d'expérience

Cercle National des Armées, 13 décembre 2012
Olivier Corbier, RSSI DOCAPOST

DOCAPOST en quelques mots

- Holding opérationnelle du Groupe La Poste regroupant les activités de « gestion des processus de relation d'affaires»

Numérisation, vidéocodage
Éditique, logistique déportée
Services courriers
Back-offices complexes

Dématérialisation
Échanges de données sécurisées
Archivage électronique
Autorité de certification, d'horodatage

Éditeur de logiciels
Conseil

- Clientèle essentiellement grands comptes
  - Banque/Finance, Assurance, Industrie, grande distribution, Telco, Energie, Santé, Organismes publics …
- Promesse client :
  *« La sécurisation de vos processus par la **qualité**, la **sécurité**, le respect des **normes** et contraintes **réglementaires**, et le **développement durable** maîtrisé. »*

La conformité : les référentiels applicables

(liste non exhaustive)

- Référentiels métiers
  - Labels **FNTC-TA** : Tiers-archivage à valeur probatoire → ***label***
  - **GS1** : échanges électroniques, EDI → ***certification***
  - **RGS** : Certification et d'horodatage →***référencement***
  - **CNIL (recommandation) :** vote par correspondance électronique
- Normes ou obligation règlementaires sectorielles
  - **CGI** 289bis, **CCRLF** 97/02, **PCI-DSS**
- Activités certifiées
  - ISO **9001** : toutes les activités industrielles
  - ISO **27001** : archivage électronique ***(traitement, hébergement, gestion)***
- Démarches transverses au groupe : ISO 14001 (environnement), ISO 26000 (responsabilité sociétale),

Manager la conformité

- Il ne s'agit pas « d'avantages produits », mais bien de fonctionnalités essentielles de nos offres
- S'ajoutent des conformités techniques plus ou moins obligatoires (référencement de l'AC par les navigateurs par exemple)
- Nécessité d'assurer une veille
  - Devoir de conseil auprès de nos clients
  - La législation évolue (relativement) vite
- De vrais risques de non-conformité
  - Clauses de rupture dans les contrats
  - Impossibilité d'exercer une activité, d'adresser un marché
  - Obsolescence technologique ou juridique
  - Faire face à un volume soudain de migrations

Organisation, gouvernance de la conformité

- Très forte implication de la Direction
- S 'appuie sur un département QSE (qualité, sécurité, environnement) constituée d'experts qualité, ou d'auditeurs internes
- Qui managent aussi les certifications 9001
- La traduction en processus opérationnels clairement définis et supervisés
- Les risques de non-conformité sont remontés au niveau stratégique

- Le RSSI a-t-il encore quelque chose à faire ?

Besoins de sécurité des SI

- Quelques remarques en général
  - Les activités sont cloisonnées, et la conformité contribue à renforcer ce cloisonnement
  - **Mais** elles sont de plus en plus interopérables et interconnectées (intégration des offres)
  - Des projets internes d'optimisation … donc de mutualisation
    - Processus, et ressources (support) mutualisés
    - Homogénéisation (pratiques, compétences, référentiels)
- Quelques remarques en particulier
  - Les référentiels sont pas définition figés; et même complets, ne peuvent prétendre à l'exhaustivité
  - La composante IT est très forte, avec très peu d'externalisation, et une grosse activité SaaS

La quadrature du cercle ?

1. La conformité ne règle pas toutes nos préoccupations en sécurité des SI
2. « obligations de conformités » multiples
   - Des référentiels quelquefois contraignants *(quand ils ne sont pas contradictoires)*
   - Des grilles de lecture hétérogènes *(auditeurs de compétences différentes, rapport d'audit structurés différemment)*
   - Forte tendance à « geler » les périmètres (o*n est conforme = on bouge plus)*

- Mais la gestion des changements est indispensable
  - Réorganisation interne, (optimisation, croissance externe)
  - Évolutions technologiques des offres en mode SaaS

Démarche SSI Groupe

- Cohérence indispensable (voire cohésion)
- Démarche d'amélioration continue
  - Imposée par certains référentiel
  - Adresser correctement la gestion des changements
- Des processus SSI transverses
  - Outillage technique
  - Cartographie et classification
  - Expertise technique

- DONC :
  - Un SMSI qui doit pouvoir être décliné selon les périmètres, et consolidé au niveau groupe
  - Un outillage complet en management des risques : analyse de risques complète, risques individualisés et risques projets

La conformité : de forts leviers pour le RSSI

- Implication de la Direction
- S'inscrit dans une gouvernance
  - des ressources disponibles (département QSE, service juridique)
  - Définition et formalisation des responsabilités
  - Formalismes existants (enregistrements au sens 9001)
- Matérialise le travail accompli (labels, certificats), fort vecteur de motivation des équipes
- Impose des échéances → remet les projets SSI dans la liste des actions prioritaires
- la plupart des référentiels abordent aujourd'hui la gestion des risques

Gérer les risques et la conformité : comment ?

- Se doter d'un modèle de risque « référent »
  - Consistant, rationnel, rigoureux, intelligible
  - Description des concepts, de la terminologie
  - Déterminer et expliquer les automatismes (grilles de décisions)
  - Le doter de tables de références minimales, et les faire évoluer
- Documenter les correspondances, les équivalences et les différences terminologiques avec les autres référentiels
- Décliner le modèle dans tous les processus, par exemple :
  - Constitution et suivi des plans d'actions
  - Gestion des incidents et des problèmes
  - Classification des informations
  - Cadrage des projets
  - Monitoring et Indicateurs

Un modèle de risque transcendant ?

- Pour autant il ne doit pas être trop précis
  - Les précisions seront apportées là où elles sont nécessaires
  - doit réussir à englober les modèles et concepts proches,
- … ni trop rigide
  - Doit pouvoir évoluer au gré des nouvelles versions de référentiels, ou au gré des évolutions du contexte
  - Garder à l'esprit que c'est un outil
- Des avantages certains
  - Intégrer les résultats d'audit plus directement dans une gestion cohérente (réutilisation des rapports)
  - Produire des tableaux de bord détaillés et consolidés
  - Communication sur les risques plus aisée (collaborateurs formés, règles d'appréciation acceptées, …)
- Et puis … il permettra de sécuriser le SI !!!

Conclusions

- Gérer la conformité $\neq$ gérer la SSI
- Le RSSI ne doit pas se priver des leviers que cela peut lui offrir (rester pragmatique)
- Le management des risques est non seulement le seul moyen de gérer correctement la SSI, mais c'est aussi un outil incomparable d'assurer le management de la conformité; il doit pour cela s'appuyer sur un modèle robuste, parfaitement compris et expliqué