De l'importance d'une veille continue dans la revue d'une PSSI

Xavier PANCHAUD, Sécurité des SI Groupe

Paris

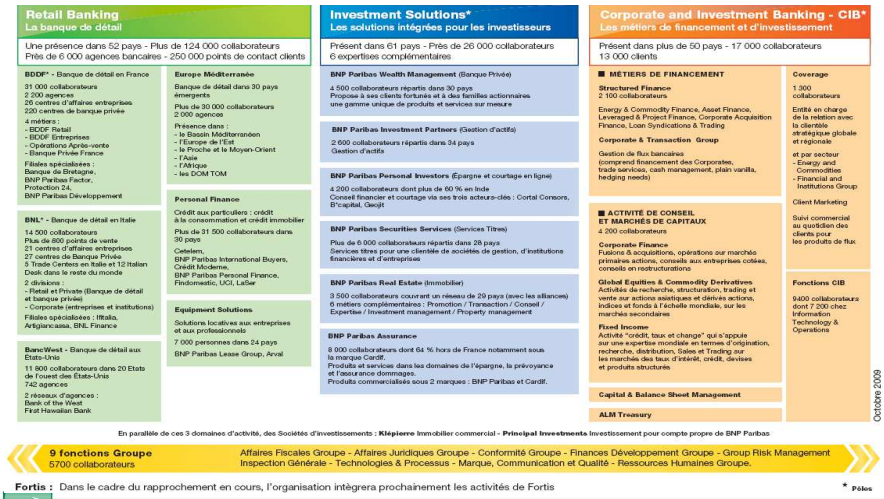
3 juin 2010

Agenda

- **Chiffres clés**
  - Les forces de BNP Paribas
  - Fonction Groupe : « Information Technologies & Processes » (ITP)
  - Culture corporate d'ouverture et de cohésion fondée sur 4 valeurs communes
- Présentation « SSI Groupe »
  - Carte d'identité
  - Présentation des Activités
- L'usage de la veille
  - Rappel : La démarche de revue d'une PSSI
  - Quelle veille pour quels besoins ?
  - Besoins ponctuels ou continus ?
  - Risques de la démarche
- Cas pratiques
  - Mise à jour des exigences sur la messagerie
- Conclusion

Organisation du Groupe

Trois domaines d'activité, organisés en « **pôles** » ou « **entités opérationnelles** » ou « **métiers** », répartis sur différents « **territoires** » (pays ou régions).
Neuf « **fonctions** » assurent un appui transversal à l'ensemble des activités.
Les collaborateurs de ces domaines travaillent **ensemble** pour être au plus près des besoins du client.



Fonction Groupe : « Information Technologies & Processes » (ITP)

5 missions intégrées

- **Production IT** — sur un périmètre de production mutualisée*
- **Achats** — Périmètre Groupe
- **Immobilier d'exploitation** — Périmètre France
- **Sécurité Globale** — SI, personnes, sites — Périmètre Groupe
- **Assurance pour compte propre** — Périmètre Groupe

- Un lien fonctionnel fort entre le responsable ITP et les correspondants métiers/fonctions
- Un COMEX pour chaque mission qui définit les objectifs, suit les réalisations et contrôle les coûts

2 missions de gouvernance pour le compte de la Direction Générale

- Suivi de la cohérence des principaux projets de développements IT via des CSSI**
- Définition et contrôle des normes, standards et architecture Groupe

Cohérence des développements IT

Amélioration des processus

- 4 axes : internationalisation & mutualisation; standardisation; ACE Lean 6 sigma; autres optimisations
- Suivi de la cohérence des principaux projets d'optimisation via des CSOP***

Missions de prestations de service pour certaines entités du Groupe

Développement IT des SI des Fonctions Groupe

Appui technique en immobilier d'exploitation — Hors France

BNP PARIBAS

* Fonctions centrales, Retail Banking (hors filiales non majoritaires), IS (sauf BP2S NY et Singapour), Métiers de financement (France et Europe), ALM trésorerie

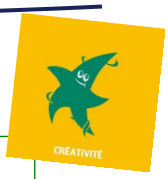
** CSSI : Comités de Suivi des Systèmes d'information *** CSOP : Comités de suivi de l'Optimisation des Processus

Culture corporate d'ouverture et de cohésion fondée sur 4 valeurs communes

Réactivité

- *Être **rapide** dans l'évaluation des situations et des évolutions comme dans l'identification des **opportunités** et des **risques***
- *Être **efficace** dans la prise de décision et dans **l'action***

Créativité



- *Promouvoir les **initiatives** et les **idées** nouvelles*
- ***Distinguer** leurs auteurs*

Engagement

- ***S'impliquer** au service des clients et de la réussite collective*
- ***Être exemplaire** dans ses comportements*

Ambition

- *Goût du **challenge** et du **leadership***
- *Volonté de gagner **en équipe** une **compétition** dont **l'arbitre est le client***

Agenda

- Chiffres clés
  - Les forces de BNP Paribas
  - Fonction Groupe : « Information Technologies & Processes » (ITP)
  - Culture corporate d'ouverture et de cohésion fondée sur 4 valeurs communes
- **Présentation « SSI Groupe »**
  - Carte d'identité
  - Présentation des Activités
- L'usage de la veille
  - Rappel : La démarche de revue d'une PSSI
  - Quelle veille pour quels besoins ?
  - Besoins ponctuels ou continus ?
  - Risques de la démarche
- Cas pratiques
  - Mise à jour des exigences sur la messagerie
- Conclusion

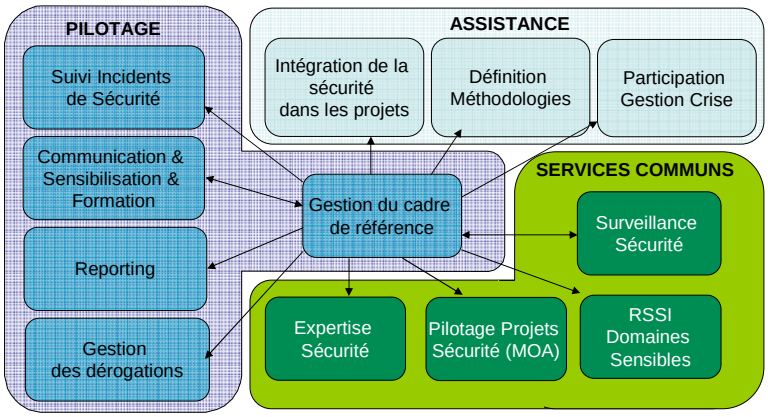
Carte d'identité

- **OBJECTIF** : maîtrise démontrée du risque sécurité lié aux SI conformément
  - Aux lois et règlements de l'industrie bancaire et financière
  - Les valeurs du groupe BNP Paribas : éthique, développement durable, valeur de la marque, maîtrise du risque opérationnel...
  - L'appétence au risque propre à chaque métier dans chaque implantation
- **PÉRIMÈTRE** : tout le groupe sur l'ensemble de ses territoires
- **COUVERTURE** : la sécurité de l'information comme définie par l'ISO 27001
- **MOYENS** : un cadre de management de la sécurité (politique, procédure, scorecard, gouvernance projet, veille...) et des actions permanentes
- **EFFECTIFS** : sécurité groupe + un réseau de BISO / CISO + une communauté et des acteurs opérationnels repartis (~500 pers.)

La maîtrise du risque de sécurité lié aux SI, c'est :

- Une dimension de la stratégie de Sécurité Globale
- La contribution au processus global de gestion des risques opérationnels
- Un moyen de contrôle permanent
- Une valeur du groupe BNP Paribas et de des métiers

Présentation des Activités



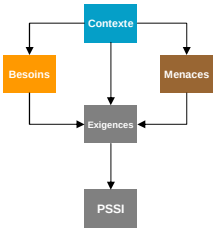
Une activité reposant sur 3 piliers

Agenda

- Chiffres clés
  - Les forces de BNP Paribas
  - Fonction Groupe : « Information Technologies & Processes » (ITP)
  - Culture corporate d'ouverture et de cohésion fondée sur 4 valeurs communes
- Présentation « SSI Groupe »
  - Carte d'identité
  - Présentation des Activités
- **L'usage de la veille**
  - Rappel : La démarche de revue d'une PSSI
  - Quelle veille pour quels besoins ?
  - Besoins ponctuels ou continus ?
  - Risques de la démarche
- Cas pratiques
  - Mise à jour des exigences sur la messagerie
- Conclusion

Rappel : La démarche de revu d'une PSSI

- Le contexte
  - Les référentiels existants
  - L'organisation interne
- Les besoins
  - Les contraintes réglementaires
  - Les spécificités locales
- Les menaces
  - Connaissance de l'existant
  - Recensement des incidents
- Les exigences



Bâle 2, SOX, …

Types d'usage, spécificités métier…

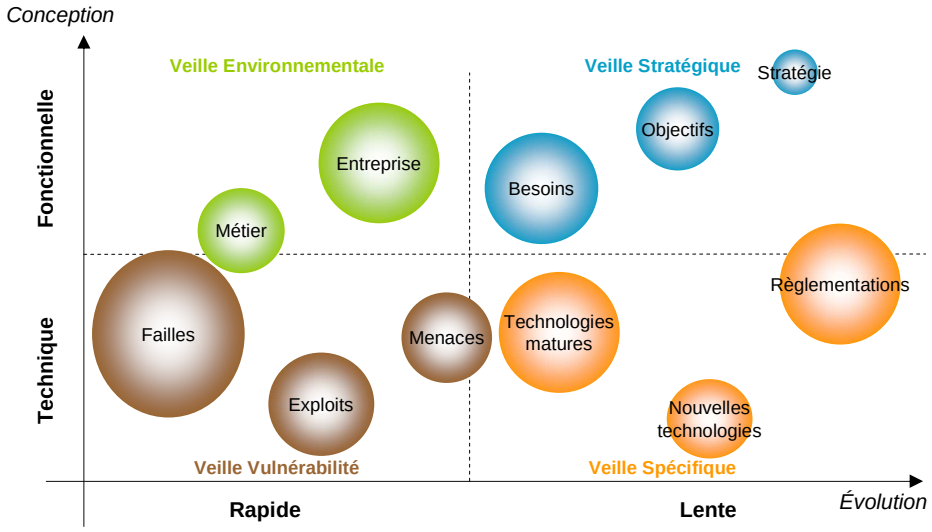
Maîtrise de ses processus, Cartographie de ses actifs, …

Définition des processus et actifs critiques

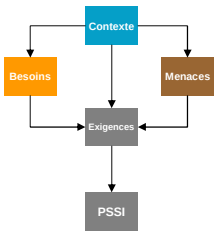
Adaptation en fonction de l'organisation (Fraude, détournement de données, dégradation)

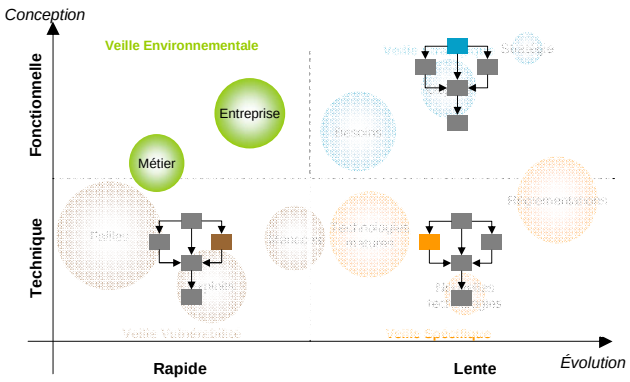
Bonnes pratiques ISO 27002

Quelle veille pour quels besoins ?



Quelle veille pour quels besoins ?





Besoins ponctuels ou continus ?

- Des besoins ponctuels
  - Dans les actions stratégiques
    - Lors de la révision des documents
  - Et technique
    - Lors de la création de nouveaux documents
- Une veille continue
  - Pour le suivi des vulnérabilités
    - Pour la mise à jour des documents à très forte teneur technique
  - Et de l'image de l'entreprise
    - Pour suivre l'évolution des risques portés par l'entreprise

Varie en fonction du type de document

Risque de la démarche

- Se focaliser sur une seule des veilles
  - Baser son modèle sur une démarche réactive

    Veille sur les menaces
    - Impliquant de nombreux changements lourds à formaliser
    - Reportant la PSSI dans un domaine purement technique
    - Limitation du périmètre d'application
  - S'orienter vers une démarche attentiste

    Veille sur les besoins ou le contexte
    - Basée uniquement sur les concepts à long terme
    - Difficilement exploitable par les opérationnels en charge de sa déclinaison
    - Décalée de la réalité

Agenda

- Chiffres clés
  - Les forces de BNP Paribas
  - Fonction Groupe : « Information Technologies & Processes » (ITP)
  - Culture corporate d'ouverture et de cohésion fondée sur 4 valeurs communes
- Présentation « SSI Groupe »
  - Carte d'identité
  - Présentation des Activités
- L'usage de la veille
  - Rappel : La démarche de revue d'une PSSI
  - Quelle veille pour quels besoins ?
  - Besoins ponctuels ou continus ?
  - Risques de la démarche
- **Cas pratiques**
  - Mise à jour des exigences sur la messagerie
- Conclusion

Mise à jour des exigences sur la messagerie

- Exigences de sécurité sur la messagerie (email)
  - À partir d'une analyse EBIOS simple
  - Des thèmes clés, prioritisés :
    - Protection des informations
    - Contrôle d'accès
    - Protection et maintenance de l'infrastructure et du client
    - Traçabilité
- Quelle veille lancer ?
  - Choix des mots clés
    - Messagerie, Messagerie d'entreprise, Menaces, Atteinte, Protection
  - Choix des sources
    - Presses spécialisés… Veille du CERT-IST

Mise à jour des exigences sur la messagerie

- Premiers résultats

- Qui amènent d'autres recherches plus ciblées

Mise à jour des exigences sur la messagerie

- Lotus Notes : 5 failles critiques en 2010, 6 failles critiques en 2009
- BlackBerry : Des vulnérabilités exploitées par l'envoi d'un PDF malicieux en pièce jointe, utilisé pour une attaque de déni de service ou l'exécution de code à distance

- Spam sur messagerie instantanée : une nouvelle variante d'un ancien vers informatique, 4 mai 2010
- Maîtrise des infrastructures : Seulement 11% des entreprises interrogées procèdent au filtrage de contenu des données synchronisées entre les smartphones et les ordinateurs des employés
- Mots de passe : la vitesse des attaque par brute force multipliée par 10 voire 100 grâce aux cartes graphiques

- Spam : sur 1000 mails - 2 phishing, 3 virus, 900 spam, 95 vrais mails, Mars 2010
- Erreur humaine : 50 % des employés du panel avouent déjà avoir envoyé des informations sensibles à un mauvais destinataire
  - L'auto-complétion de l'adresse : en Angleterre, un policier a envoyé accidentellement un fichier Excel sensible et non protégé à un journaliste (contenant des casiers judiciaires de milliers de personnes), Mars 2010
- Social engineering : Accès à des comptes Twitter personnels dont ceux de Barack Obama et de Britney Spears
- Mots de passe : 1/3 des internautes ont un mot de passe commun pour tous leurs sites

- Maîtrise des infrastructures : ICQ vendu par AOL à un fonds d'investissement russe, Digital Sky Technologies, 29 avril 2010

Vulnérabilité Spécifique Environnementale Stratégique

Mise à jour des exigences sur la messagerie

- Évolutions
  - Veille stratégique
    - Complétude du spectre
      - messagerie instantanée, messagerie mobile et modèle externalisé
  - Veille vulnérabilité
    - Mise à jour des guides pratiques
      - à usage des administrateurs messagerie
    - Position Paper
      - venant pérenniser des messages d'alertes
  - Veille spécifique
    - Affinage des seuils
  - Veille environnemental
    - Outil de communication pour accompagner la diffusion du document
    - Révision de certaines exigences devenues désuètes
      - Robustesse des moyens d'authentification par exemple

Agenda

- Chiffres clés
  - Les forces de BNP Paribas
  - Fonction Groupe : « Information Technologies & Processes » (ITP)
  - Culture corporate d'ouverture et de cohésion fondée sur 4 valeurs communes
- Présentation « SSI Groupe »
  - Carte d'identité
  - Présentation des Activités
- L'usage de la veille
  - Rappel : La démarche de revue d'une PSSI
  - Quelle veille pour quels besoins ?
  - Besoins ponctuels ou continus ?
  - Risques de la démarche
- Cas pratiques
  - Mise à jour des exigences sur la messagerie
- **Conclusion**

Outil d'évolution continue

- Veille permettant une coordination des résultats identifiés
  - Présentant souvent le résultat d'une menace dans un contexte défini, pour un besoin spécifique
- Facilitant la mise en lumière des objectifs de la PSSI
  - Pour accompagner :
    - Sa promotion
    - Son évolution