

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

Xavier PANCHAUD, Sécurité des SI Groupe

Paris

3 juin 2010



BNP PARIBAS

Information Technology & Processes

## 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



BNP PARIBAS

Information Technology & Processes

# 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.

Retail Banking La banque de détail	Investment Solutions* Les solutions intégrées pour les investisseurs	Corporate and Investment Banking - CIB* Les métiers de financement et d'investissement
<p>Une présence dans 52 pays - Plus de 124 000 collaborateurs Près de 6 000 agences bancaires - 250 000 points de contact clients</p> <p><b>BDDF*</b> - Banque de détail en France 31 000 collaborateurs 2 500 agences 26 centres d'affaires entreprises 220 centres de banque privée 4 métiers : - BDDF Retail - BDDF Entreprises - Opérations Agence-vente - Banque Privée France</p> <p>Filières spécialisées : Banque de Bretagne, BNP Paribas Factor, Protection SA, BNP Paribas Développement</p> <p><b>BNL**</b> - Banque de détail en Italie 14 500 collaborateurs Plus de 800 points de vente 21 centres d'affaires entreprises 27 centres de Banque Privée 3 Trade Centres en Italie et 12 Italian Desk dans le reste du monde 2 divisions : - Retail et Private (Banque de détail et Banque Privée) - Corporate (entreprises et institutions)</p> <p>Filières spécialisées : Italea, Art&amp;Finance, ENL Finance</p> <p><b>BankWest</b> - Banque de détail aux Etats-Unis 11 800 collaborateurs dans 20 Etats de l'Ouest des Etats-Unis 742 agences 2 réseaux d'agences : Bank of the West First Hawaiian Bank</p>	<p>Présent dans 61 pays - Près de 26 000 collaborateurs 6 expertises complémentaires</p> <p><b>BNP Paribas Wealth Management</b> (Banque Privée) 4 500 collaborateurs répartis dans 30 pays Propose à ses clients fortunés et à des familles adossées une gamme unique de produits et services sur mesure</p> <p><b>BNP Paribas Investment Partners</b> (Gestion d'actifs) 2 600 collaborateurs répartis dans 14 pays Gestion d'actifs</p> <p><b>BNP Paribas Personal Investors</b> (Epargne et courtage en ligne) 4 200 collaborateurs dont plus de 60 % en Inde Conseil financier et courtage via ses trois acteurs-clés : Coral, Corsors, E-capital, Odegi</p> <p><b>BNP Paribas Securities Services</b> (Services Titres) Plus de 6 000 collaborateurs répartis dans 28 pays Services titres pour une clientèle de sociétés de gestion, d'institutions financières et d'entreprises</p> <p><b>BNP Paribas Real Estate</b> (Immobilier) 3 500 collaborateurs couvrant un réseau de 29 pays (avec les alliances) 9 métiers complémentaires : Promotion / Transaction / Conseil / Expertise / Investment management / Property management</p> <p><b>BNP Paribas Assurance</b> 8 000 collaborateurs dont 64 % hors de France notamment sous la marque Cardif. Produits et services dans les domaines de l'épargne, la prévoyance et l'assurance dommages. Produits commercialisés sous 2 marques : BNP Paribas et Cardif.</p>	<p>Présent dans plus de 50 pays - 17 000 collaborateurs 13 000 clients</p> <p><b>MÉTIER DE FINANCEMENT</b></p> <p><b>Structured Finance</b> 2 100 collaborateurs Energy &amp; Commodity Finance, Asset Finance, Leveraged &amp; Project Finance, Corporate Acquisition Finance, Loan Syndications &amp; Trading</p> <p><b>Corporate &amp; Transaction Group</b> Gestion de flux bancaires Emploi de financement des Corporates, trade services, cash management, plain vanilla, hedging needs)</p> <p><b>ACTIVITÉ DE CONSEIL ET MARCHÉS DE CAPITALIS</b> 4 200 collaborateurs</p> <p><b>Corporate Finance</b> Fusions &amp; acquisitions, opérations sur marchés primaires actions, conseils aux entreprises cotées, conseils en restructurations</p> <p><b>Global Equities &amp; Commodity Derivatives</b> Activités de recherche, structuration, trading et vente sur actions européennes et américaines, indices et fonds à l'échelle mondiale, sur les marchés secondaires</p> <p><b>Fixed Income</b> Activité "credit, taux et change" qui s'appuie sur une expertise mondiale en termes d'organisation, recherche, distribution, Sales et Trading sur les marchés des taux d'intérêt, crédit, dérivés et produits structurés</p> <p><b>Capital &amp; Balance Sheet Management</b></p> <p><b>ALM Treasury</b></p>
<p><b>Europe Méditerranée</b> Banque de détail dans 30 pays émergents Plus de 30 000 collaborateurs 2 000 agences Présence dans : - le Bassin Méditerranéen - l'Europe de l'Est - la Proche et le Moyen-Orient - l'Asie - l'Afrique - les DOM TOM</p> <p><b>Personal Finance</b> Crédit aux particuliers : crédit à la consommation et crédit immobilier Plus de 31 500 collaborateurs dans 30 pays Cetelem, BNP Paribas International Buyers, Credit Moderne, BNP Paribas Personal Finance, Finobmeteo, UCI, Lufax</p> <p><b>Equipment Solutions</b> Solutions locatives aux entreprises et aux professionnels 7 000 personnes dans 24 pays BNP Paribas Lease Group, Arval</p>	<p><b>Coverage</b> 1 300 collaborateurs Etre en charge de la relation avec la clientèle stratégique globale et régionale et par secteur - Energy and Commodity - Financial and Institutions Group</p> <p><b>Client Marketing</b> Suivi commercial au quotidien des clients pour les produits de flux</p> <p><b>Fonctions CIB</b> 9400 collaborateurs dont 7 200 chez Information Technology &amp; Operations</p>	

En parallèle de ces 3 domaines d'activité, des Sociétés d'investissement : Klépierre Immobilier commercial - Principal Investments Investissement pour compte propre de BNP Paribas

9 fonctions Groupe 5700 collaborateurs Affaires Fiscales Groupe - Affaires Juridiques Groupe - Conformité Groupe - Finances Développement Groupe - Group Risk Management Inspection Générale - Technologies & Processus - Marque, Communication et Qualité - Ressources Humaines Groupe.

Fortis Dans le cadre du rapprochement en cours, l'organisation intégrera prochainement les activités de Fortis \* Pôles

**BNP PARIBAS** Information Technology & Processes

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

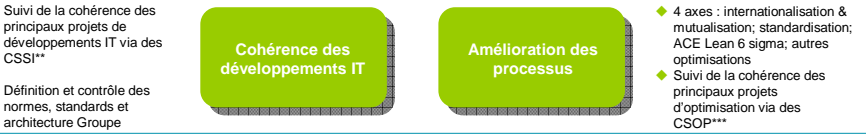
### 5 missions intégrées



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



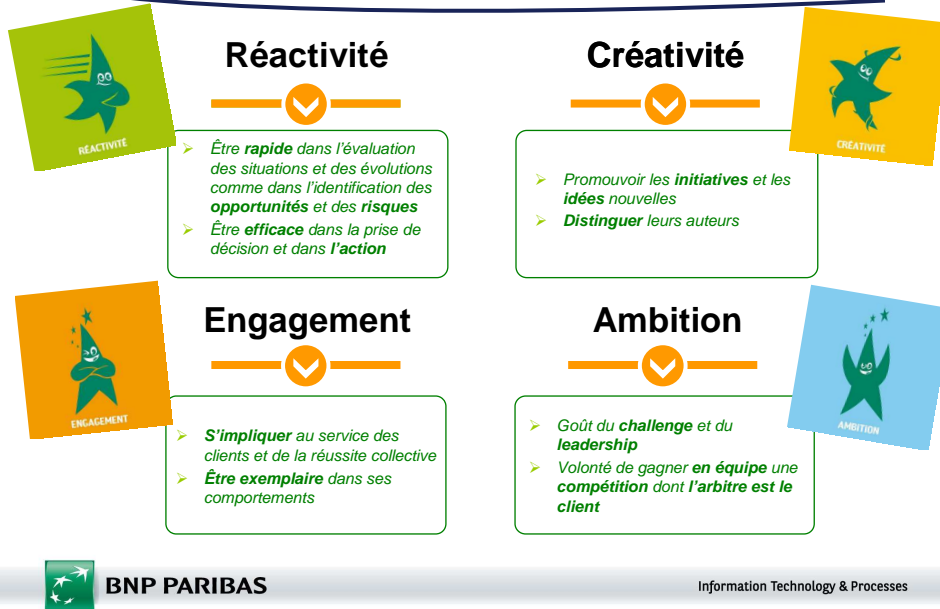
### Missions de prestations de service pour certaines entités du Groupe



**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



## 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 :

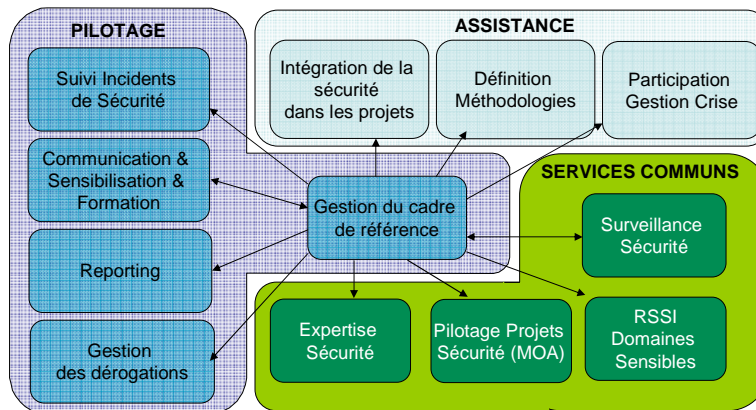
- Une dimension de la stratégie de Sécurité Globale
- La contribution au processus global de gestion des risques opérationnels
- Un moyen de contrôle permanent
- Une valeur du groupe BNP Paribas et de des métiers



BNP PARIBAS

Information Technology & Processes

## Présentation des Activités



Une activité reposant sur 3 piliers



BNP PARIBAS

Information Technology & Processes

# 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

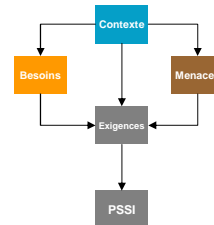


BNP PARIBAS

Information Technology & Processes

## Rappel : La démarche de revue 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

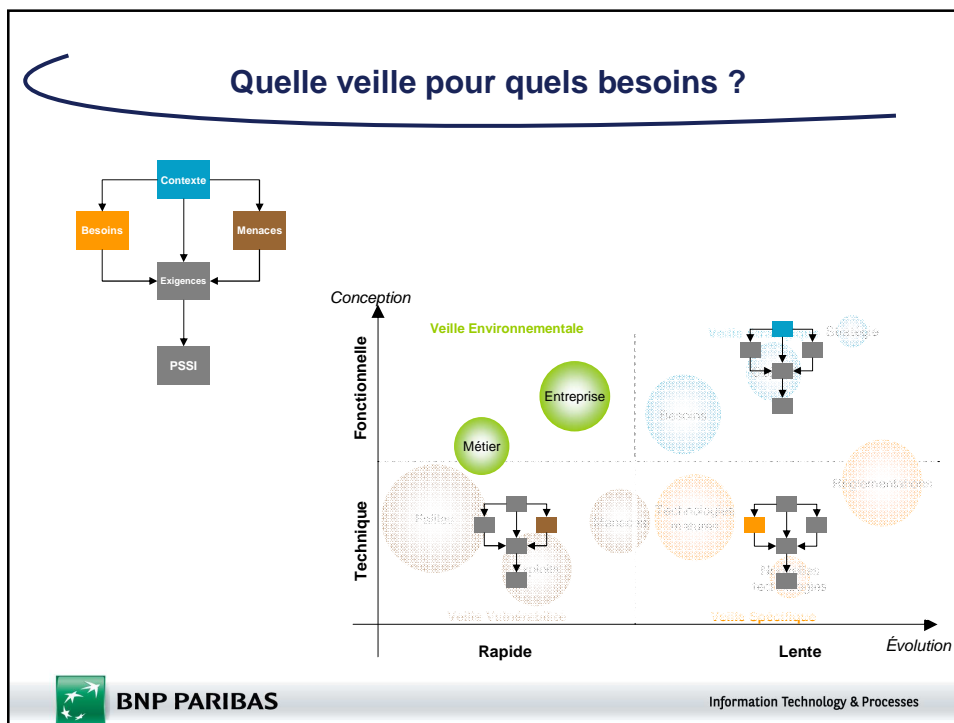
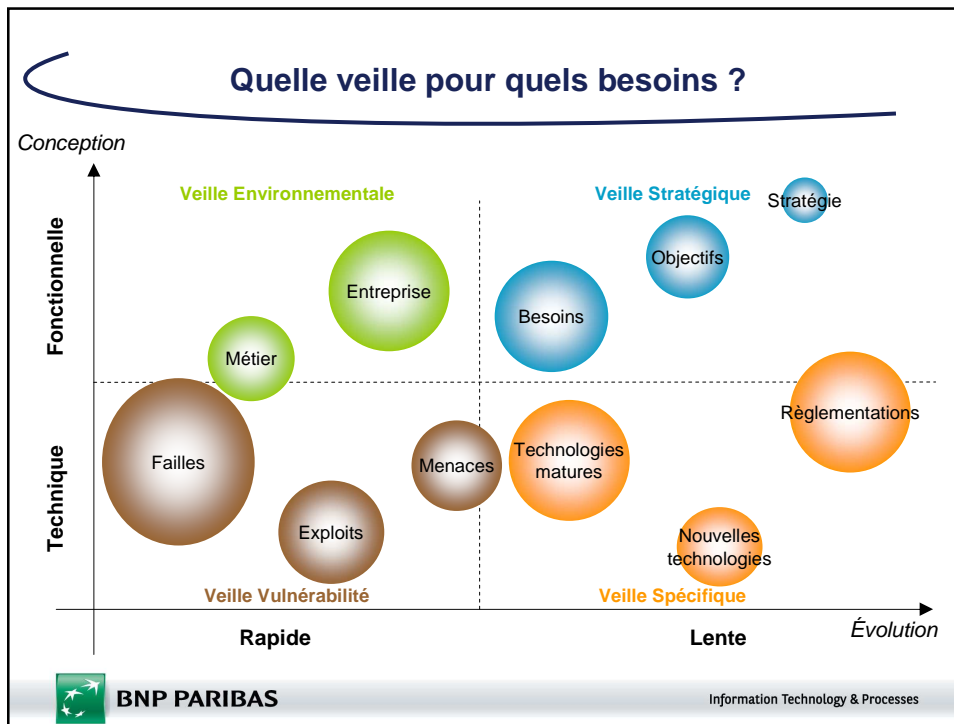
Adaptation en fonction de l'organisation (Fraude, détournement de données, dégradation)

Bonnes pratiques ISO 27002



BNP PARIBAS

Information Technology & Processes



## 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



BNP PARIBAS

Information Technology & Processes

## 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



BNP PARIBAS

Information Technology & Processes



## Mise à jour des exigences sur la messagerie

- Premiers résultats



- Qui amènent d'autres recherches plus ciblées



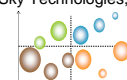
BNP PARIBAS

Information Technology & Processes

## 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



BNP PARIBAS

Information Technology & Processes

## 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



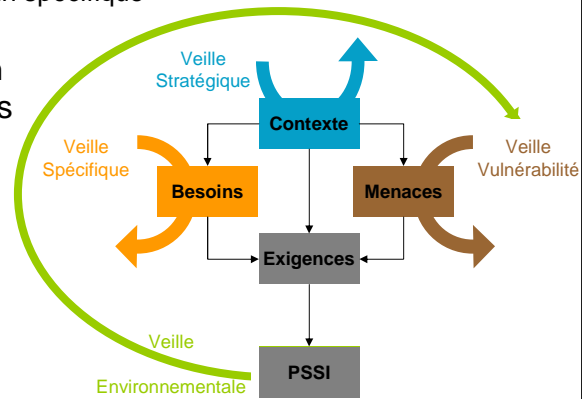
## Agenda

- 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



BNP PARIBAS

Information Technology & Processes



BNP PARIBAS

La banque d'un monde qui change

