La cyber sécurité
un enjeu de stabilité financière

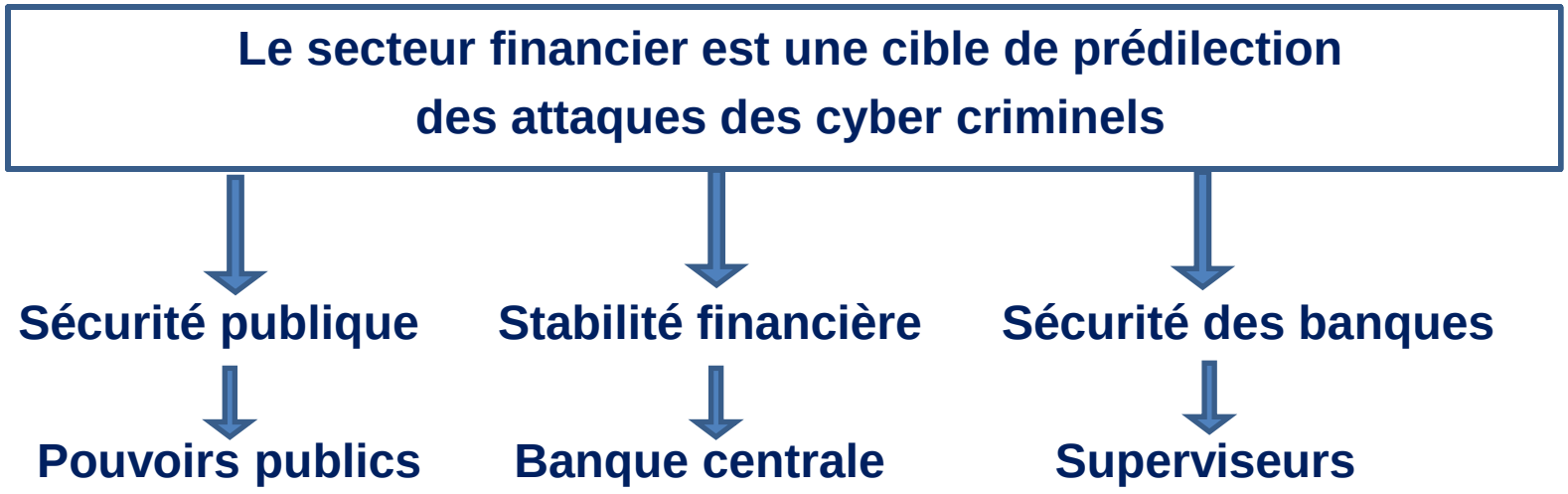
Paris, le 7 décembre 2017

Frédéric VISNOVSKY Secrétaire général adjoint

1. La cyber sécurité, un enjeu de stabilité financière (1/8)

Le secteur financier est particulièrement exposé avec le développement soutenu de la dématérialisation : les évolutions technologiques ont permis de réduire certains risques opérationnels (notamment d'exécution) mais avec

- l'expansion des réseaux et des technologies,
- l'ouverture des systèmes d'information aux échanges extérieurs,
- la croissance des transactions électroniques,…



1. La cyber sécurité, un enjeu de stabilité financière (2/8)

Entités	Impacts possibles pour les entités	Impacts possibles pour le système financier
Banques	▪ Pertes financières pour les clients et la banque ▪ Risque de réputation ▪ Indisponibilités pour les contreparties et les clients pendant un certain temps ▪ Atteinte à l'intégrité des données/pertes de données	▪ Limités, mais dépendant de la durée d'indisponibilité et de la taille/importance de la banque ▪ Perte de confiance des clients
Systèmes de paiement	▪ Risque de réputation ▪ Pertes financières	▪ Impacts significatifs pour les participants de marché
Contreparties centrales	▪ Interruption des marchés ▪ Impossibilités de règlements ▪ Risque de réputation et éventuelles pertes financières	▪ Impacts significatifs pour les participants de marché
Banques centrales	▪ Risque de réputation ▪ Indisponibilité des systèmes de paiement et de règlement	▪ Impacts significatifs pour les participants de marché
Tiers fournisseurs de services	▪ Indisponibilité des services ▪ Atteinte à l'intégrité des données/pertes de données	▪ Impacts systémiques en fonction de la concentration des services du prestataire
Entreprises d'investissement et assurances	▪ Risque de réputation ▪ Pertes financières	▪ Limités

1. La cyber sécurité, un enjeu de stabilité financière (3/8)

L'organisation de la robustesse de la Place financière en France

Un Groupe de Place avec 5 objectifs :

- **Améliorer l'efficience** : consolider les dispositifs internes des établissements en situation de stress
- **Maîtriser les externalités** : besoin de coordination et de solidarité entre acteurs
- **Gérer l'incertitude** : le caractère évolutif des menaces exige une actualisation permanente des scénarios et des répondes à y apporter
- **Améliorer la capacité** de la Place financière de Paris à surmonter les chocs affectant des fonctions critiques telles que les systèmes de paiement, la gestion de la liquidité, le financement de l'économie
- **Renforcer l'attractivité** de la Place financière de Paris en montrant sa capacité à faire face à une crise opérationnelle majeure

Assurer la continuité en cas de crise

- Détecter et identifier les alertes pour mettre en place les mesures appropriées
- Etablir un état des lieux de la Place financière et informer les membres
- Etablir un dialogue permanent avec les services de l'Etat
- Prendre les décisions et les plans d'actions suite à une consultation collective
- Gérer la communication de crise

La cyber attaque est l'un des 8 scénarios de crise identifiés par le Groupe de Place

1. La cyber sécurité, un enjeu de stabilité financière (4/8)

Le risque IT dans les préoccupations des superviseurs car l'IT est essentiel dans l'activité bancaire et pour les clients

Un risque multi forme : sécurité, continuité, réputation, conformité, confidentialité

Des obligations légales et réglementaires :

- Code monétaire et financier : LCB-FT
- Arrêté du 3 novembre 2014 (ex CRBF 97-02)
- Pratiques utiles : rapport Lagarde, Livres blancs de la Commission bancaire (informatique en 1996 et internet en 2000), étude sur le Cloud computing (2013)

Les outils de supervision :

- Contrôles sur place
- Rapports internes des banques
- Analyses transversales

Et la cyber criminalité ?

- Le senior supervisory group (SSG) a inscrit le sujet à son agenda
- L'une des priorités dès 2015 de la BCE

Définir une approche convergente au sein des superviseurs

1. La cyber sécurité, un enjeu de stabilité financière (5/8)

Un élément de préoccupation des instances internationales

- **Autorité bancaire européenne (EBA) :** task force sur le risque IT créée en 2015
  - Compléments publiés en mai 2017 aux lignes directrices sur les évaluations prudentielles (dites SREP) sur le risque IT
    - Les lignes directrices SREP définissent le risque IT : « le risque actuel ou potentiel de pertes en raison du caractère inapproprié ou de la défaillance du matériel et du logiciel des infrastructures techniques, susceptible de compromettre la disponibilité, l'intégrité, l'accessibilité et la sécurité de ces infrastructures et des données »
    - Principaux éléments complémentaires apportés pour les SREP 2018 :
      - Évaluation de la gouvernance et de la stratégie
      - Évaluation des principaux risques : a) disponibilité et continuité, b) sécurité, c) évolution des systèmes, d) intégrité des données, e) externalisation
  - Projet de recommandation de mai 2017 sur le Cloud computing : convergence des attentes des superviseurs
  - Travaux prévus : lignes directrices sur la cyber sécurité

1. La cyber sécurité, un enjeu de stabilité financière (6/8)

- **Comité de Bâle :**
  - BCBS 239 sur les principes aux fins de l'agrégation des données sur les risques et de la notification des risques (janvier 2013)
    - Principe 2 : architecture des données et infrastructure informatique « toute banque devrait concevoir, mettre en place et gérer une architecture des données et une infrastructure informatique permettant de renforcer ses capacités d'agrégation des données de risque et ses pratiques de notification des risques, non seulement en situation normale mais aussi en période de tensions ou de crise, sans manquer aux autres Principes ».
  - Revue des principes pour une saine gestion des risques opérationnels (en attente) : définition du risque IT dans le risque opérationnel

1. La cyber sécurité, un enjeu de stabilité financière (7/8)

➢ Mécanisme de Supervision Unique (MSU) :

- Revue thématique sur la cyber sécurité (2015)
- Suites données : reporting sur les incidents de cyber sécurité (phase pilote en 2016 avec 18 banques, extension en juillet 2017)

Incidents classification is based on impact

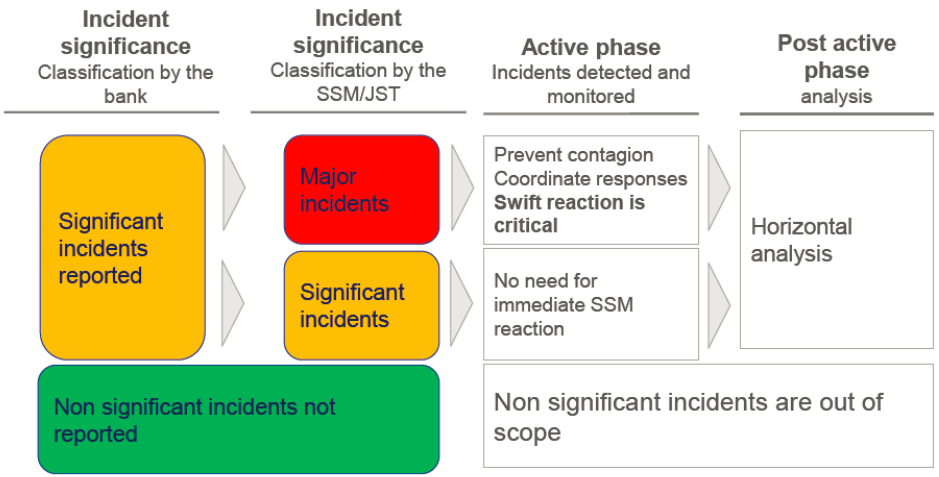
Significant incident

- Potential impact of 5 MEUR or 0.1% of CET1;
- or publicly reported;
- or escalated to CIO;
- or notified to other Authorities;
- or Disaster Recovery and/or Business Continuity;
- Or expert Judgment on financial impact, business disruption or reputational risk.

Major incident

- potential impact 25 MEUR or 0.5 % of the CET1
- Expert judgment from JST and CIG:
  - *Disruption of service;*
  - *Reputational damage;*
  - *Legal costs;*
  - …

Cybercrime incident reporting structure



- 2016 : revue thématique sur l'outsourcing de l'IT
- Travaux prévus : attentes des superviseurs sur les risques IT, mise en œuvre des lignes directrices EBA dans le SREP

1. La cyber sécurité, un enjeu de stabilité financière (8/8)

- **G7 Cybersecurity Experts Group (CEG)**
  - Développer des principes pour renforcer la cyber sécurité du secteur financier des pays du G7 :
    - Octobre 2016 : publication des éléments fondamentaux pour la cyber sécurité dans le secteur financier (https://www.tresor.economie.gouv.fr/Ressources/File/429227)
    - Octobre 2017 : éléments fondamentaux pour l'évaluation de la cyber sécurité (http://www.mef.gov.it/inevidenza/documenti/PRA_BCV_4728453_v_1_G7_Fundamental.pdf)

- **G20 (FSB) :** revue des cadres nationaux en matière de cyber sécurité

2. Les actions de l'ACPR (1/9)

- **Questionnaire cyber sécurité adressé à 82 établissements contrôlés par l'ACPR (hors établissements dans le champ de contrôle du MSU)**
  - Auto évaluation du dispositif
  - Suit le cadre développé par le NIST (National Institute of Standards and Technology)
  - Objectif de classer les banques pour adapter les actions de supervision

- **Travaux en cours : attentes de l'ACPR en matière de risques IT**

2. Les actions de l'ACPR (2/9)

Les enseignements du questionnaire cyber sécurité

- **Nos objectifs**
  - Améliorer la connaissance des profils de risque de cyber sécurité des **établissements moyens et petits**
  - Sensibiliser et accompagner le développement de dispositifs de cyber sécurité robustes

- **La méthode :**
  - Auto évaluation (méthodologie de l'Institut national des standards et de la technologie – NIST)
  - 4 niveaux de maitrise dans l'aptitude à gérer les risques cyber sécurité
  - 6 axes d'analyse (gouvernance, identification, protection, détection, réaction, rétablissement)

- **Les enseignements** : des marges de progrès qui feront l'objet d'un suivi rapproché en 2018

Gouvernance	2,39 / 4
Identification	2,01 / 4
Protection	1,98 / 4
Détection	1,52 / 4
Réaction	1,54 / 4
Récupération	1,71 / 4

2. Les actions de l'ACPR (3/9)

Une pratique d'évaluation par des contrôles sur place

✓ **Des contrôles sur place des principaux groupes bancaires français, avec une double approche :**

- Évaluation de la prise en compte du risque de cyber sécurité
- Revue de la cyber sécurité dans un environnement de banque internet

\+ **Des tests d'intrusion menés avec des experts du CERT de la Banque de France**

UNE FORTE EXPERTISE

Depuis 1995, une équipe dédiée pour les risques liés aux systèmes d'information composée d'environ 10 auditeurs.

Une expertise renforcée par :

- une bonne connaissance des systèmes informatiques des banques françaises et des sujets touchant aux organisations, fraudes, qualité des données, continuité d'activité, sécurité internet, services de paiement, etc.
- la participation à différents travaux internationaux (groupe d'experts du G7 sur la cyber sécurité notamment).
- la coopération avec l'ANSSI et le CERT de la Banque de France

2. Les actions de l'ACPR (4/9)

Un champ large des missions de contrôle

- Besoin d'une approche élargie : tous les systèmes IT peuvent faire l'objet de cyber attaques
- Mais il est impossible de revoir des milliers d'applications
- Une approche ciblée est possible :
  - L'implication du management est primordial
  - L'évaluation de la sécurité n'est significative que sur un environnement limité : les groupes peuvent avoir des centaines de sites bancaires sur Internet, l'examen peut être effectué sur un seul
- La sécurité physique constitue un élément essentiel

2. Les actions de l'ACPR (5/9)

La pratique des tests d'intrusion

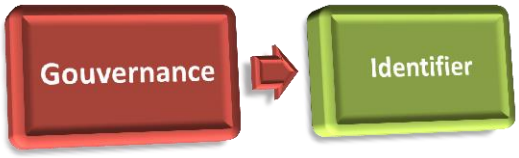
- ✓ **Objectifs : évaluer le niveau de protection des applications et des infrastructures informatiques dans un environnement de banque internet.**
- ✓ **Cibles:**
  - ➢ Faiblesses des serveurs et des plate formes administratives
  - ➢ Failles dans les logiciels
  - ➢ Sécurité des réseaux
  - ➢ Protection des codes d'authentification

Les engagements du chef de mission :

- ❖ Tests effectués dans des environnements de pré-production
- ❖ Défauts identifiés testés sur l'environnement de production
- ❖ Tests uniquement dans les heures ouvrées
- ❖ Tests en présence de la banque
- ❖ Retours quotidiens

2. Les actions de l'ACPR (6/9)

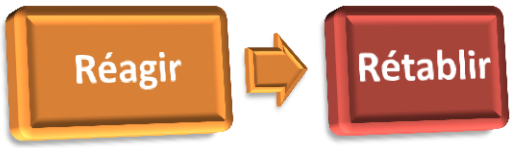
Les points d'attention identifiés en matière de cyber sécurité



- Besoin de renforcer l'implication du management
- Inventaires à actualiser des logiciels et réseaux
- Système IT hétérogènes et inter connectés
- Obsolescence et complexité des systèmes IT

- La gestion des accès est un élément majeur
- Meilleure identification des informations sensibles

- Qualité des capteurs
- Détection dans l'ensemble des systèmes IT



- Dispositifs de réaction et de rétablissement pas nécessairement adaptés aux cyber attaques

2. Les actions de l'ACPR (7/9)

Un prochain document de discussion de l'ACPR sur les attentes en matière IT

Principaux messages du document

- Le risque informatique est une **préoccupation majeure** des autorités de supervision :
  - toute l'activité des établissements est dépendante de leur IT et ces environnements sont devenus très complexes à gérer
  - les dommages informatiques peuvent avoir des conséquences particulièrement graves (pannes, cyberattaques)

- Les travaux des **instances internationales** sur le risque informatique se sont intensifiés depuis 2015 mais l'ancrage du risque informatique dans le risque opérationnel reste à clarifier.

- Une **définition du risque informatique** : le « risque informatique » (ou « risque des technologies de l'information et de la communication - TIC » ou « risque du système d'information ») correspond au risque de perte, avérée ou potentielle, résultant d'une organisation inadéquate, d'un défaut de fonctionnement, ou d'une insuffisante sécurité du système d'information, compris comme l'ensemble des équipements systèmes et réseaux et des moyens humains destinés au traitement de l'information de l'institution.

2. Les actions de l'ACPR (8/9)

Un document de l'ACPR sur les attentes en matière IT

Une catégorisation du risque informatique en trois grands domaines

Facteurs de risque retenus → **Mesures utiles ou nécessaires**

1. **Risques liés à une mauvaise organisation** : regroupent les situations de décision et de pilotage global insuffisant, pouvant conduire à une mauvaise gestion informatique, à un support insuffisant des besoins des métiers, voire à une mauvaise gestion du risque informatique en général.

2. **Risques de mauvais fonctionnement** : visent tout ce qui peut porter atteinte au bon fonctionnement du système d'information et altérer ainsi la capacité d'un établissement à réaliser ses activités. En particulier, la catégorisation retient les risques de mauvais pilotage des projets et des changements systèmes, d'atteinte à la continuité de l'exploitation et de qualité insuffisante des données (données relatives aux clients, ou devant être communiquées au superviseur ou propres aux établissements et n'ayant pas vocation à être diffusées).

3. **Risques de sécurité insuffisante** : visent en général toutes les atteintes à la confidentialité et à l'intégrité des données et systèmes gérés par l'établissement. Il s'agit des facteurs de risque liés à la mauvaise protection des actifs du système informatique et ceux liés à des systèmes de détection insuffisants, ou à une capacité de réaction aux attaques trop faible.

2. Les actions de l'ACPR (9/9)

Un document de l'ACPR sur les attentes en matière IT

Quel usage de cette définition et de cette catégorisation par les établissements ?

1. Les établissements sont libres d'utiliser leur propre catégorisation ou de choisir celle indiquée par l'ACPR.
2. Il convient en tout état de cause qu'ils couvrent l'entièreté du champ des risques identifiés, sauf à ce que leur organisation ou leur modèle d'affaire ne le justifie pas.
3. Lorsque tout ou partie du système d'information d'un établissement est sous-traité, cela ne signifie pas que l'établissement n'est plus exposé à ces risques informatiques. Il doit en conséquence continuer à les identifier et les maîtriser dans le cadre de sa gestion du risque opérationnel et de son dispositif de contrôle interne

Plus de détail à venir dans le document de discussion à publier

Merci de votre attention
et retrouvez les analyses de l'ACPR sur notre site internet : www.acpr.banque-france.fr