Cyber sécurité et risque informatique : les enjeux pour les établissements financiers

Réunion d'Information Réflexion :

"Cyber sécurité enjeux et bonnes pratiques"

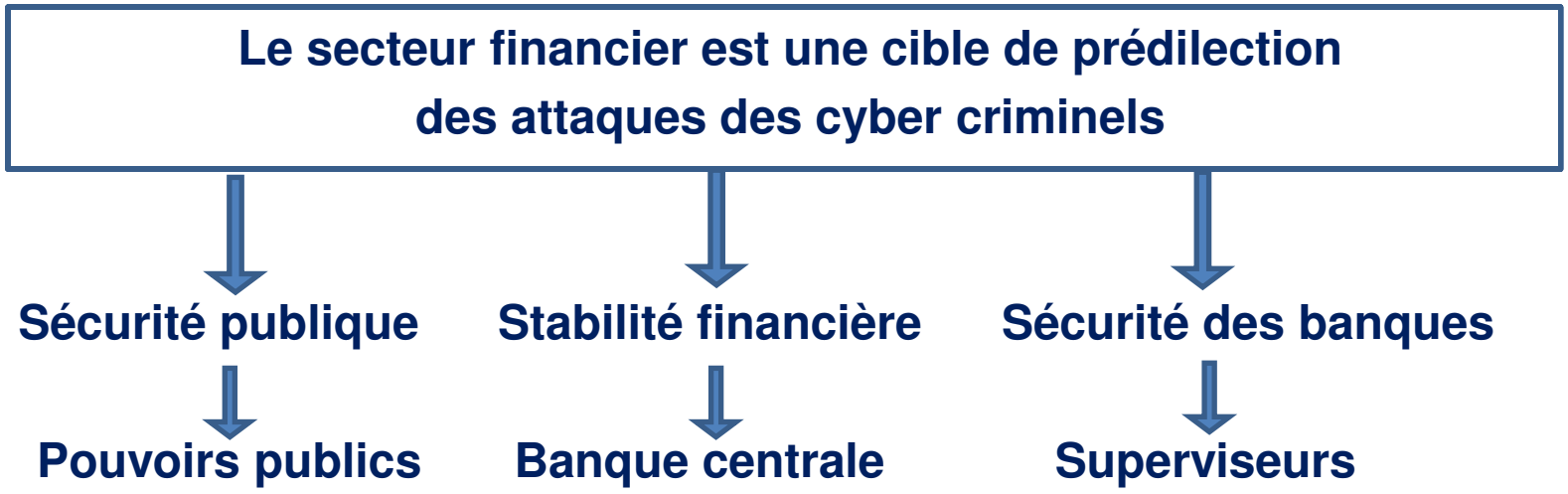
Paris, le 15 juin 2018

Frédéric VISNOVSKY Secrétaire général adjoint

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

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

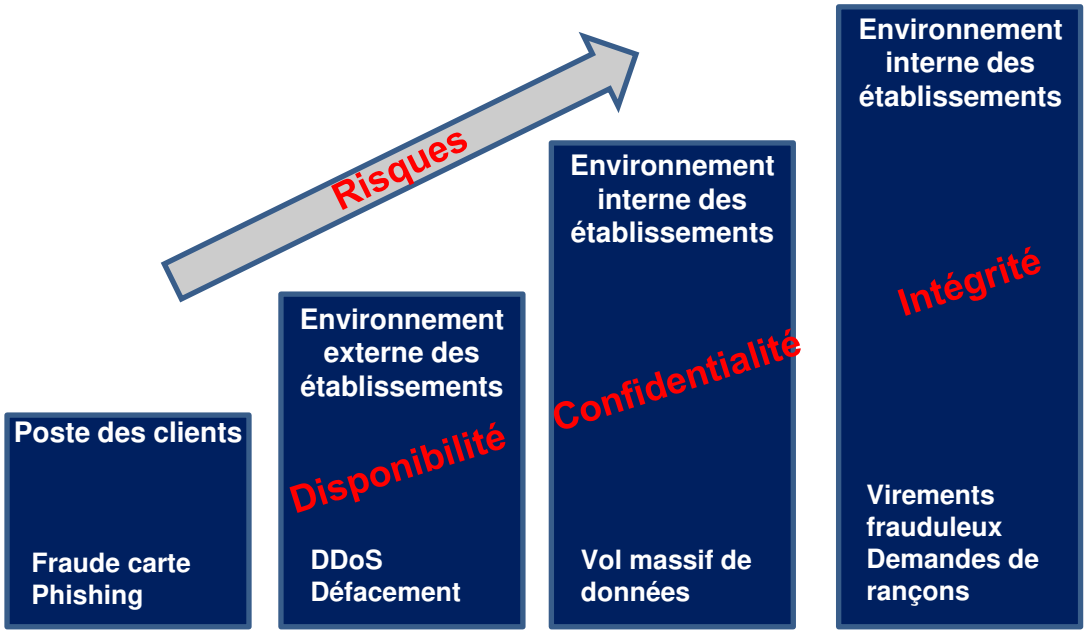
- l'expansion des réseaux et des technologies,
- l'ouverture des systèmes d'information aux échanges extérieurs,
- la croissance des transactions électroniques,…



1. La cyber sécurité, un enjeu de stabilité financière (2/5)



- Les systèmes des établissements sont visés
- L'impact financier augmente
- Le risque de réputation est plus fort

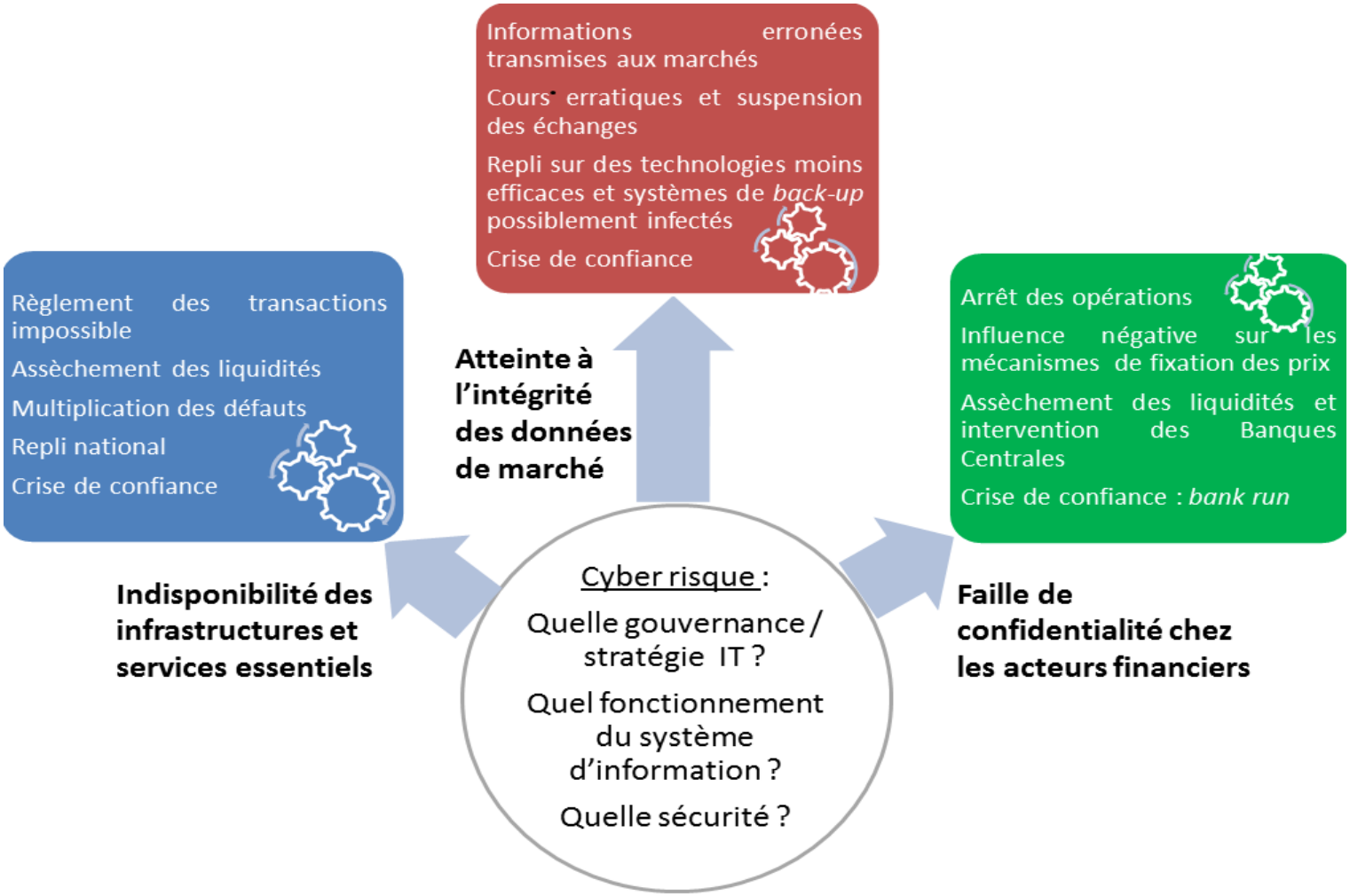


1. La cyber sécurité, un enjeu de stabilité financière (3/5)

Évolution de la nature du risque	Interconnexions entre les systèmes d'information	Innovations technologiques et prépondérance des prestataires
• Des attaques qui visent les environnements informatiques des institutions (et plus seulement les équipements des clients) pour les voler et/ou pour les détruire • Des procédés qui eux-mêmes se complexifient : *Dark Net, social engineering, Exploit Kits*, puissance de calcul informatique plus forte, préparation inadéquate des employés en interne à l'utilisation des outils informatiques…	• Entre les acteurs : présence au sein d'un même groupe, relations interbancaires, (ré)assurance, externalisation, caractère intrinsèquement systémique de certains acteurs... • Nature transfrontalière des outils/ infrastructures utilisés (Internet, réseau SWIFT, chambres de compensation…) eux-mêmes systémiques	• Arrivée de nouveaux intermédiaires et technologies (FinTech ou GAFA/BATX), zones de fragilités supplémentaires possibles en lien avec les institutions financières • Croissance du recours à l'externalisation par des services de *Cloud Computing/Big Data*, impliquant des flux numérisés d'informations essentielles qui peuvent être interceptées et moins aisément contrôlables par les entités clientes souvent tributaires de leurs prestataires

Source : Banque de France - Évaluation des risques du système financier français • Décembre 2017

1. La cyber sécurité, un enjeu de stabilité financière (4/5)



Source : Banque de France - Évaluation des risques du système financier français • Décembre 2017

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

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

Un Groupe de Place avec 5 objectifs :

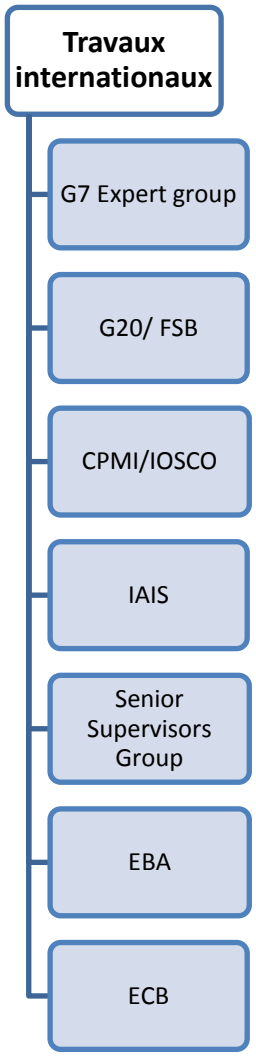
- **Améliorer l'efficience** : consolider les dispositifs internes des établissements en situation de stress
- **Maîtriser les externalités** : besoin de coordination et de solidarité entre acteurs
- **Gérer l'incertitude** : le caractère évolutif des menaces exige une actualisation permanente des scénarios 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

2. Les actions des superviseurs et de l'ACPR (1/7)



- **Renforcement des principes normatifs sur les risques cyber**
  - Autorité Bancaire Européenne :
    - Lignes directrices pour l'évaluation des risques informatiques (2017)
    - Recommandations sur l'usage du *Cloud computing* (décembre 2017)
    - Mise en chantier des « lignes directrices pour le risque informatique » (incluant la cybersécurité) en 2018
  - ACPR :
    - Recommandations sur l'usage du *Cloud computing* (Juillet 2013)
    - Élaboration d'un document de réflexion sur les risques informatiques et leur maîtrise chez les banques et assurances (Mars 2018)

- **Renforcement des actions de supervision depuis 2015**
  - BCE (Mécanisme de Supervision Unique) :
    - Enquête thématique début 2015
    - Lancement d'inspections sur place
    - Collecte des incidents de cybersécurité (démarrage en août 2017)
  - ACPR :
    - Questionnaire de maturité sur l'organisation et la maîtrise des risques informatiques dans les organismes d'assurance (2016)
    - Questionnaire d'auto-évaluation sur la cybersécurité (83 établissements de crédit « moins significatifs » interrogés en 2017)
    - Questionnaire sur la sécurité des SI dans les organismes d'assurance (2017)
    - Enquêtes sur place en banques et assurances
    - Accord de coopération renforcée entre l'ANSSI et l'ACPR (janvier 2018)

2. Les actions des superviseurs et de l'ACPR (2/7)

- **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 établissements pour adapter les actions de supervision



2. Les actions des superviseurs et de l'ACPR (3/7)

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 des superviseurs et de l'ACPR (4/7)

Une pratique d'évaluation par des contrôles sur place

✓ **Des contrôles sur place des principaux établissements 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 des superviseurs et de l'ACPR (5/7)

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 des superviseurs et de l'ACPR (6/7)

La pratique des tests d'intrusion

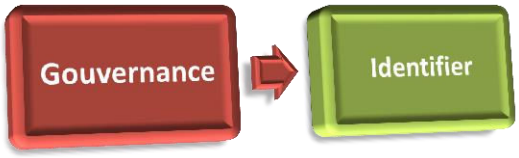
- ✓ **Objectifs : évaluer le niveau de protection des applications et des infrastructures informatiques dans un environnement de banque internet.**
- ✓ **Cibles:**
  - ➢ Faiblesses des serveurs et des plate formes administratives
  - ➢ Failles dans les logiciels
  - ➢ Sécurité des réseaux
  - ➢ Protection 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 des superviseurs et de l'ACPR (7/7)

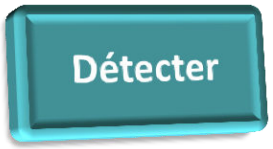
Les points d'attention identifiés en matière de cyber sécurité



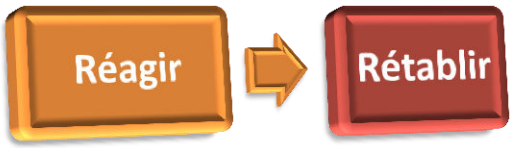
- Besoin de renforcer l'implication du management
- Inventaires à actualiser des logiciels et réseaux
- Système IT hétérogènes et inter connectés
- Obsolescence et complexité des systèmes IT



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



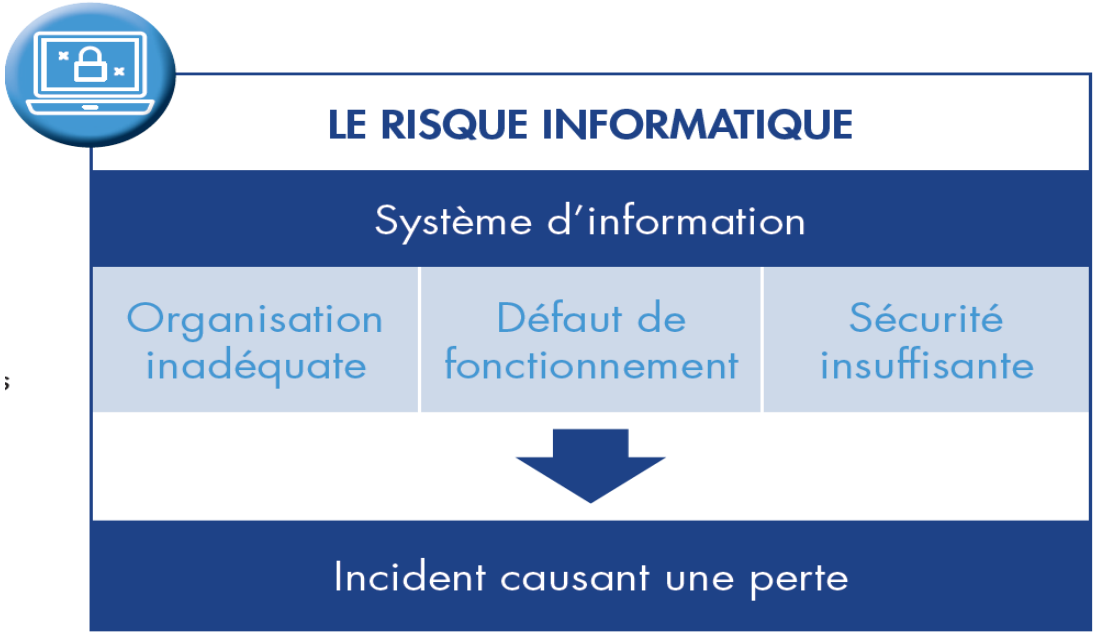
- Qualité des capteurs
- Détection dans l'ensemble des systèmes IT



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

3. - Le document de réflexion de l'ACPR (1/5)

Une catégorisation du risque informatique en trois grands domaines



Pour chaque processus

Facteurs de risque retenus

↓

Mesures utiles ou nécessaires

3. - Le document de réflexion de l'ACPR (2/5)



Exemples :

IMPLICATION DES INSTANCES DIRIGEANTES

- Mauvaise perception des enjeux
- Décisions inappropriées
- Pilotage insuffisant

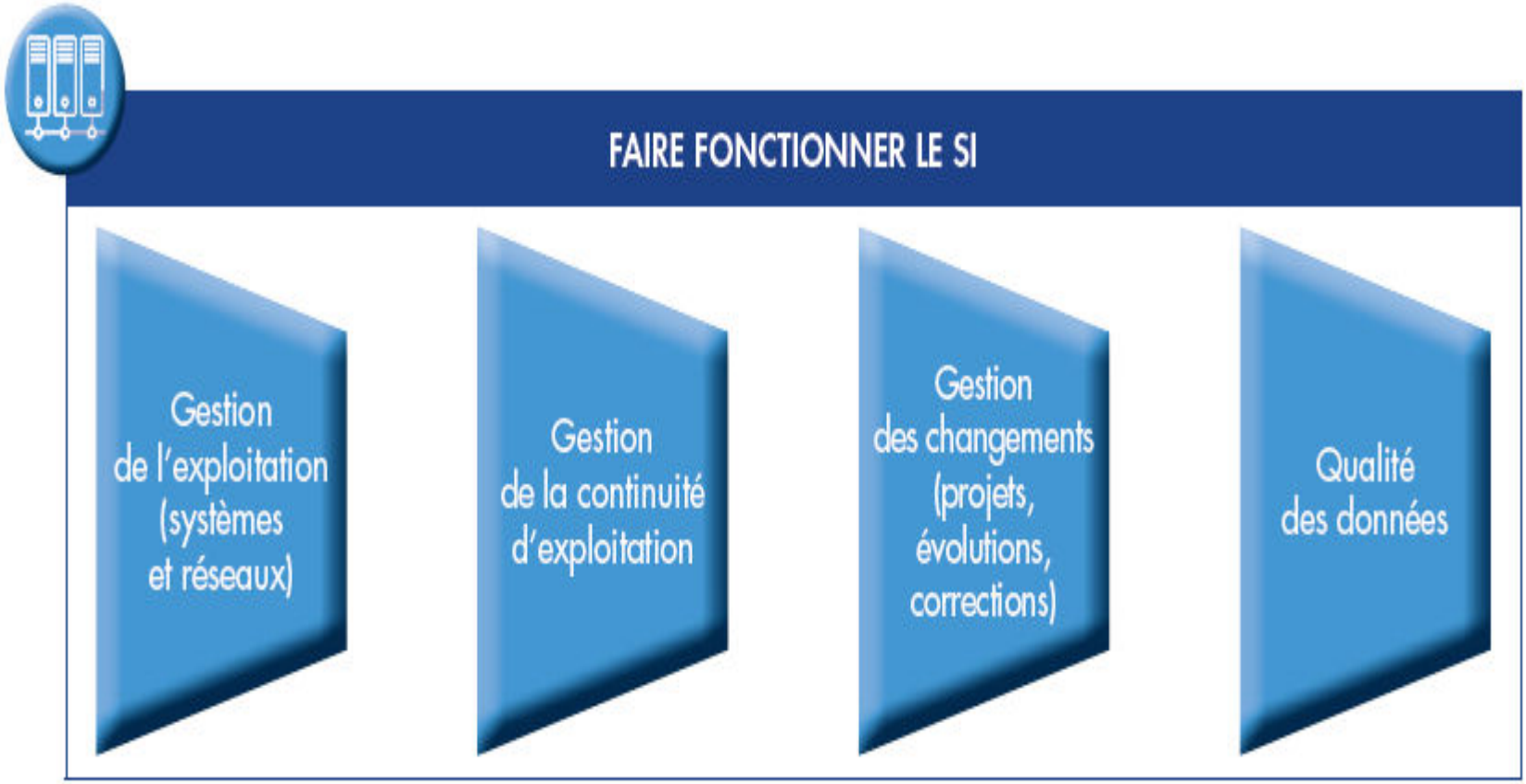
RATIONALISATION DU SYSTÈME D'INFORMATION

- Maîtrise de l'architecture du système d'information (urbanisation)
- Cohérence des normes informatiques
- Maîtrise de l'obsolescence

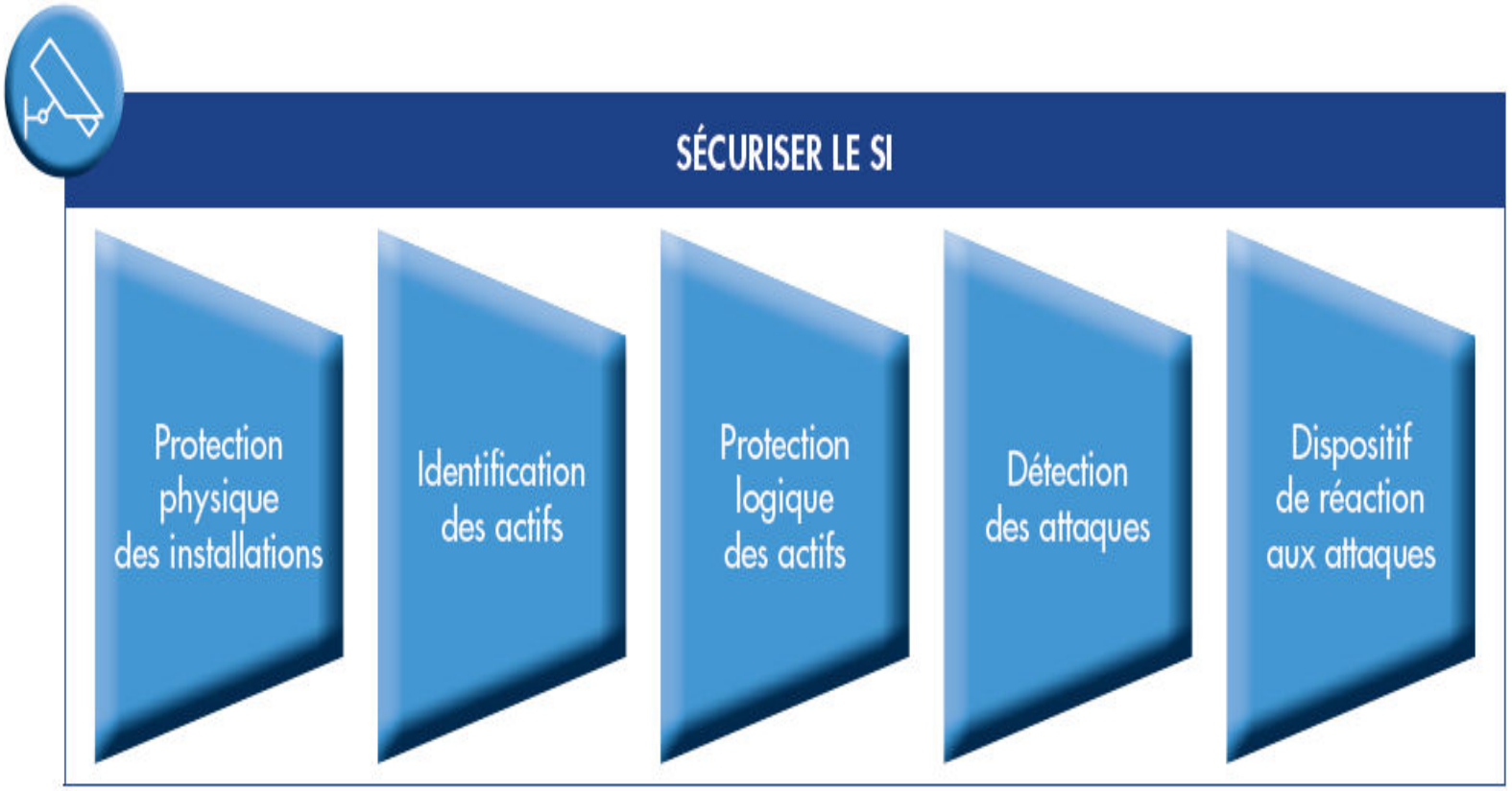
AMÉLIORER LA GESTION DES RISQUES

- Cartographie des risques
- Dispositif de contrôle permanent
- Recensement et gestion des incidents de risque opérationnel
- Dispositif de contrôle périodique

3. - Le document de réflexion de l'ACPR (3/5)



3. - Le document de réflexion de l'ACPR (4/5)



3. - Le document de réflexion de l'ACPR (5/5)

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

Observations et commentaires attendus d'ici le 15 juin 2018

Référence : ACPR, Document de réflexion n°1-2018

Envoyer vos commentaires (réf. DR/1-2018) à : commentaires-doc@acpr.banque-france.fr

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