ACPR
BANQUE DE FRANCE

LA CONFÉRENCE DE L'ACPR

- La qualité des données et la robustesse des systèmes d'information : un défi pour les secteurs de la banque et de l'assurance

Jeudi 16 juin 2016

Palais Brongniart

Introduction

Bernard Delas,
vice-président de l'ACPR

Sommaire

Conférence animée par Bertrand Peyret, directeur de la 2e direction du Contrôle des assurances à l'ACPR

1. **La qualité des données en assurance et en banque**
   - **La qualité des données en assurance**
   - **La qualité des données en banque : la vision de la BCE**
   - **La qualité des données en banque : le point de vue de l'ACPR**
2. **Présentation de l'enquête de l'ACPR sur les systèmes d'information**
3. **Les risques liés aux systèmes d'information et notamment la cyber-sécurité**
   - **Les risques liés à l'usage des technologies de l'information**
   - **Cyber-sécurité : état des menaces et attentes des superviseurs**

Sommaire

Sommaire

1. **Une amélioration partielle de la qualité des données prudentielles envoyées à l'ACPR**

2. **Un dispositif de gestion de la qualité des données au périmètre souvent incomplet**

3. **Un défaut d'urbanisation des systèmes d'information pénalisant la qualité des données**

Sommaire

1. **Une amélioration partielle de la qualité des données prudentielles envoyées à l'ACPR**
2. **Un dispositif de gestion de la qualité des données au périmètre souvent incomplet**
3. **Un défaut d'urbanisation des systèmes d'information pénalisant la qualité des données**

Une amélioration de la qualité des données reçues par l'ACPR

- **Les organismes d'assurance ont fourni les efforts nécessaires pour être en capacité d'effectuer les remises en XBRL :**
  - Adoption d'un format type sans dérogation possible
  - Des contrôles intra et inter QRT renforcés
- **La qualité des premières remises Solvabilité II est encourageante :**
  - 97% des remises solo « D1S » actuelles sans anomalie (au 25/05, 92% des remises attendues ont été réalisées – date de remise demandée : 20/05)
  - Aucune anomalie pour les remises solo « QRS » (au 25/05, 11% des remises attendues ont été réalisées – date de remise demandée : 26/05)
  - 83% des remises groupe « D1G » actuelles sans anomalie (au 25/05, 11% des remises attendues ont été réalisées – date de remise demandée : 01/07)

Des progrès réalisés dans les dispositifs de gestion de la qualité des données

- **Une meilleure identification des données** utile à la fabrication des états règlementaires et en particulier au calcul des SCR/MCR et des provisions (Articles 219, 244 et 265 du règlement 2015/35 UE)
- **Une priorisation** des données utilisées en fonction de **leur matérialité** dans le calcul des états règlementaires
- **Une responsabilisation des acteurs** concourant à leur production (Articles R.354-6 du Code des Assurances)
- Une formalisation et, parfois, une industrialisation des **contrôles de qualité de ces données** (Articles 219, 231, 244 et 264 du règlement 2015/35 UE et article R351-13 du Code des Assurances)
- La définition d'**objectifs / seuils** sur la qualité à atteindre (Articles 219, 231, 244 et 264 du règlement 2015/35 UE)

Ces progrès ont été identifiés indépendamment du choix de l'utilisation de la formule standard ou d'un modèle interne

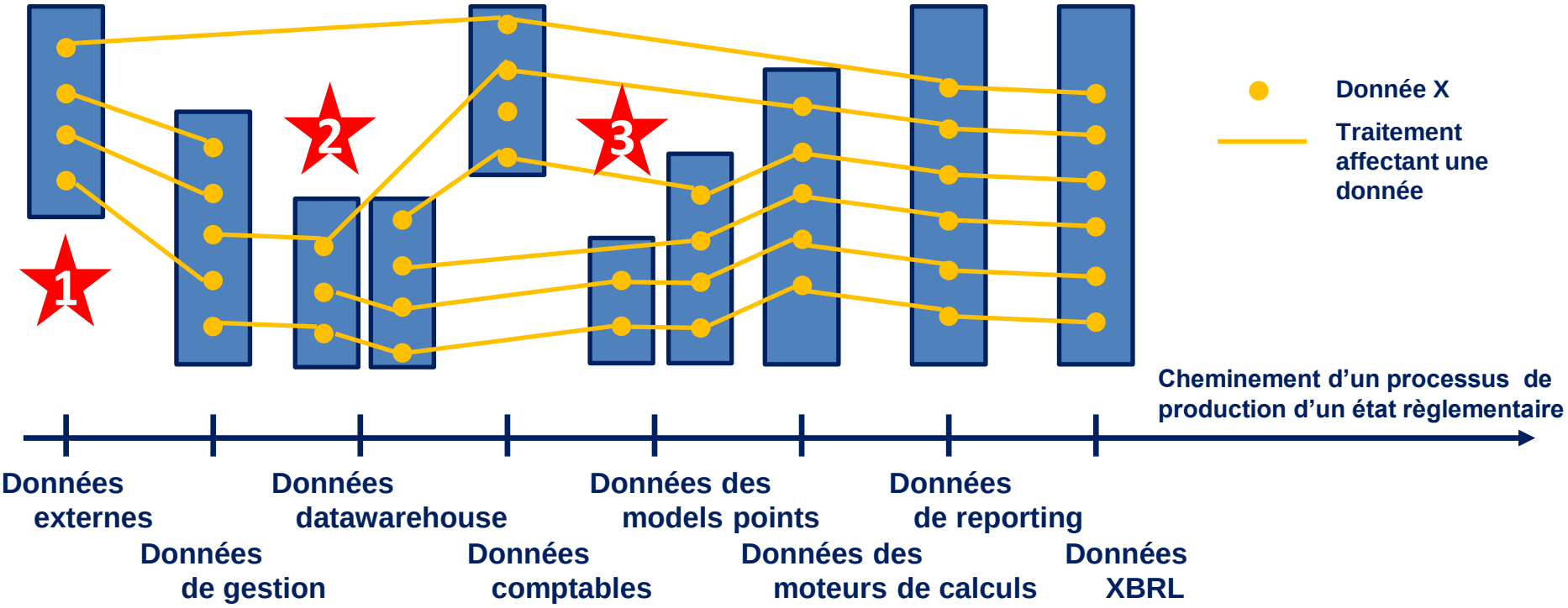
Sommaire

1. Une amélioration partielle de la qualité des données prudentielles envoyées à l'ACPR

2. **Un dispositif de gestion de la qualité des données au périmètre souvent incomplet**

3. Un défaut d'urbanisation des systèmes d'information pénalisant la qualité des données

Seule la connaissance et la maîtrise du cheminement global des données peuvent garantir l'atteinte d'un objectif de qualité de données



Trois principaux écueils ont été régulièrement rencontrés

Un dispositif de gestion de la qualité des données principalement restreint à l'aval des processus

1. **Les données provenant de partenaires externes** ne font pas toujours l'objet d'une même attention concernant leur qualité que les données internes à l'organisme (Articles 19, 219, 237 du règlement 2015/35 UE)

2. Au niveau des **systèmes de gestion et datawarehouses internes** :
   - **La saisie des données** (contrats / sinistres) fait l'objet de peu de contrôles de qualité
   - Les traitements sur les données effectués dans ces systèmes amonts sont souvent peu maîtrisés voire font l'objet de **rupture de la piste d'audit** (Article A343-1 du Code des Assurances)

Ces deux écueils sont d'autant plus prégnants en cas d'exploitation de « big data »

Des traitements actuariels manuels souvent mal maîtrisés

- **De nombreux traitements actuariels ne sont pas automatisés**, que ce soit dans l'extraction des données utilisées ou dans leur manipulation (ex : construction des triangles)

- **Ces processus manuels ne sont pas toujours fiabilisés** :

  - Utilisation d'outils *ad hoc* non standardisés
  - Gestion des habilitations lâches sur ces outils
  - Traitements non documentés/justifiés
  - Non utilisation du principe des 4 yeux pour les contrôles
  - …

  (Articles 219, 244 et 265 du règlement 2015/35 UE)

Sommaire

1. Une amélioration partielle de la qualité des données prudentielles envoyées à l'ACPR

2. Un dispositif de gestion de la qualité des données au périmètre souvent incomplet

3. **Un défaut d'urbanisation des systèmes d'information pénalisant la qualité des données**

Un défaut d'urbanisation des systèmes d'information pénalisant la qualité des données

- **Le système d'information de nombreux organismes est éclaté et peu structuré,** ce qui constitue un frein à la mise en place d'une architecture de données de qualité :
  - Difficulté à mettre en place un dispositif de contrôle adapté et à atteindre les caractères **exhaustif, exact et approprié** de la donnée (Article R351-13 du Code des Assurances ; articles 19, 20, 219, 231 et 264 du règlement 2015/35 UE)
  - Problème de **disponibilité de la donnée**, complexifiant le respect des délais de livraison des états règlementaires mais également l'atteinte des exigences en matière de **lutte contre le blanchiment et le financement du terrorisme** (Article A310-8 du Code des Assurances)

Les principaux points d'attention

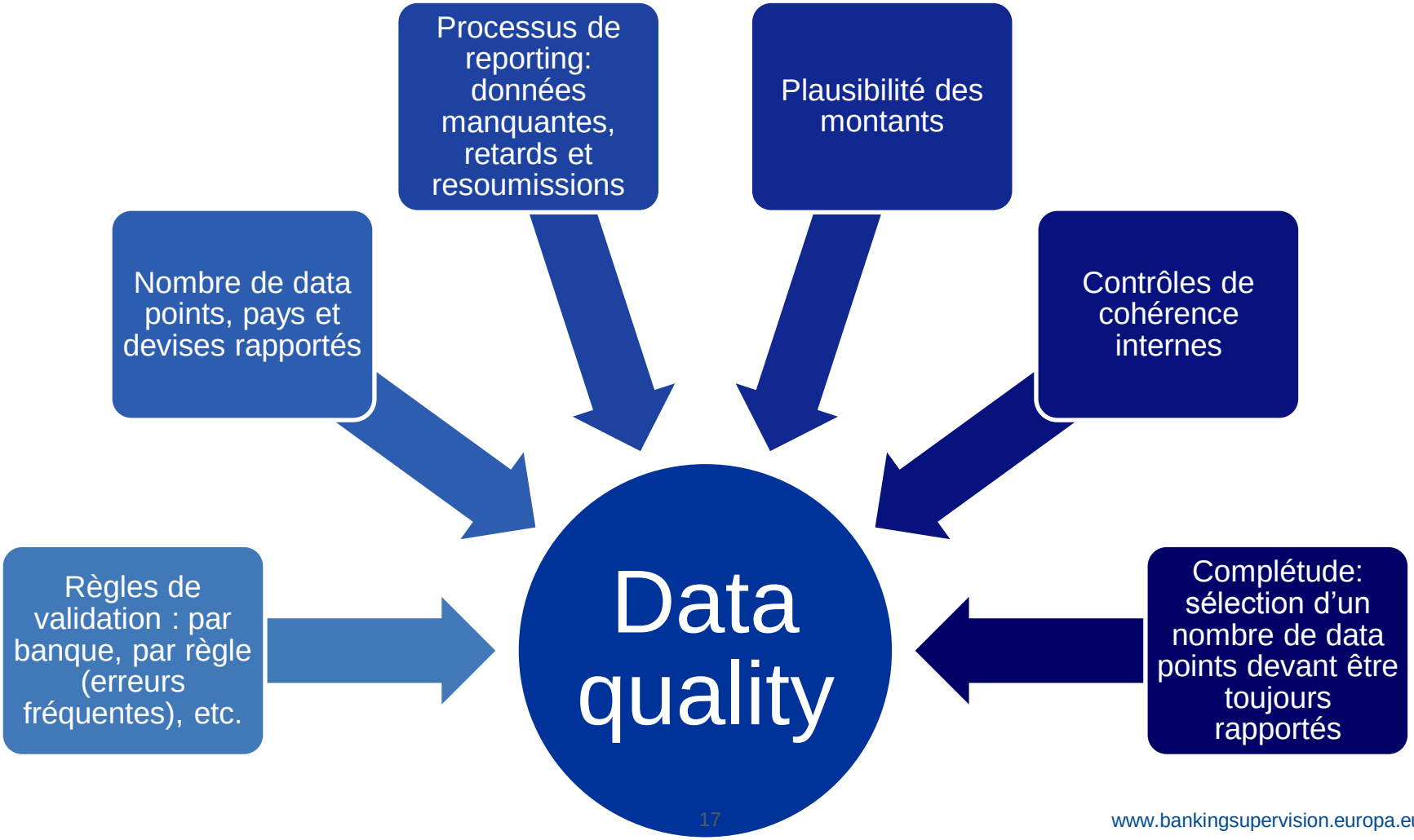
- La qualité des données est un sujet qui concerne l'ensemble des directions de l'entreprise, pas seulement l'informatique
- Les contrôles très en aval des processus de production (ex : contrôles intra et inter QRT) sont insuffisants pour garantir la qualité des données
- Une vision transverse du parcours de la donnée, transcendant les différents silos de l'entreprise, est nécessaire pour en effectuer une évaluation correcte
- L'automatisation des processus de production des données reste le moyen le plus efficace pour en garantir la fiabilité et la traçabilité

Sommaire

1. **La qualité des données en assurance et en banque**
   - La qualité des données en assurance
   - **La qualité des données en banque : la vision de la BCE**
     - **Giancarlo Pellizzari, Head of Supervisory Statistics Division, spécialiste de la qualité des données à la BCE**
   - La qualité des données en banque : le point de vue de l'ACPR
2. Présentation de l'enquête de l'ACPR sur les systèmes d'information
3. Les risques liés aux systèmes d'information et notamment la cyber-sécurité
   - Les risques liés à l'usage des technologies de l'information
   - Cyber-sécurité : état des menaces et attentes des superviseurs

Une approche globale sur le contrôle de la qualité des données

- **Plusieurs angles sont utilisés pour effectuer cette évaluation.**



Produits

En production

Tableaux de base

- Produits 3 fois par date de remise
- Servant de base pour les analyses

En process

Tableau de bord individuel par institution

- Incluant un rating de cette institution

En process

Système de mise en évidence automatique de certaines banques (outliers)

- RAG

En production

Rapport d'évaluation de la qualité des données

- Produit pour chaque date de remise
- Partagé avec le Supervisory Board

En process

Système de scoring immédiat de la qualité des rapports

- Basé sur les 5 dimensions

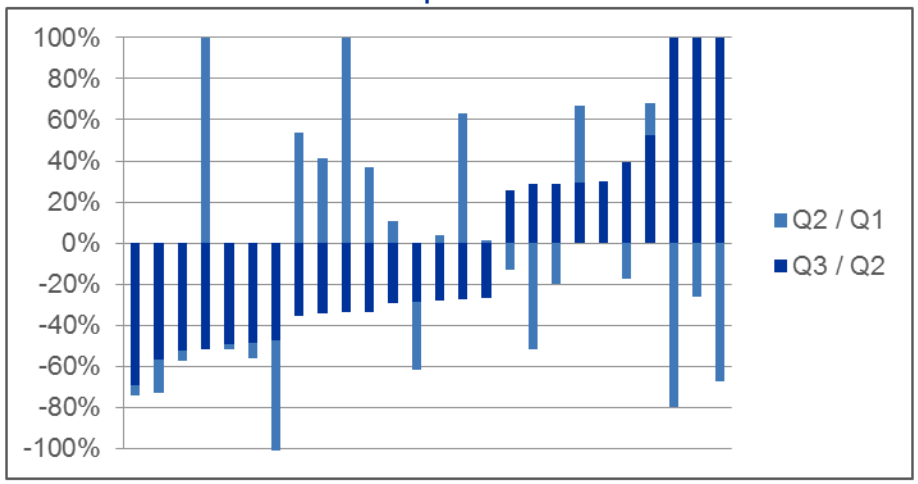
En production

Analyses thématiques

- Au sein de l'EGDQ
- Suite à des demandes spécifiques des JSTs (BCBS 239 par exemple)

Exemples

Variation des dépôts de clients “retail”



Niveau de complétude par business

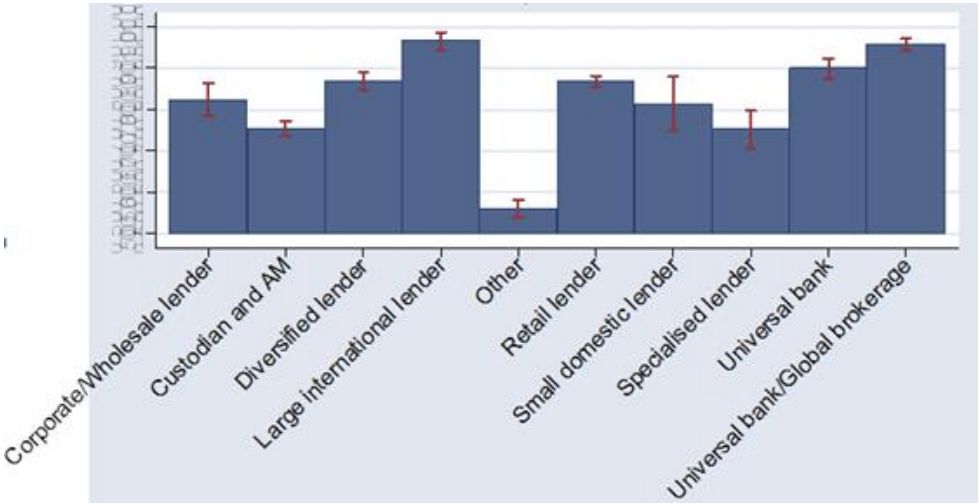


Tableau de bord individuel

Period: **Name:**

LEI:
Country:
Accounting framework:
Significance:
Scope:

SA/IRB (IM)
Credit risk SA / IRB
Securitisation SA / IRB
Market risk SA / IM

1. SUBMISSION OF THE ITS DATA

	COREP	LE	LCR	NSFR	FINREP	AE
Status of data submissions	Accepted	Accepted_Manually	Pending	Rejected	Accepted_Manually	Accepted_Manually
Delay in the submission	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
Cumulated number of delays						
Days of delay						
Number of resubmissions before final						
Number of failed validation rules						
% over total number of VR						
Percentile in total sample						

2. COMPLETENESS AND ACCURACY OF THE DATA

	COREP	LE	LCR	NSFR	FINREP	AE
Number of data points						
Change from last period						
Number of countries reported						
Change from last period						
Number of currencies reported						
Change from last period						
Number of group institutions reported						
Change from last period						
% of missed data points *(1)*						
Percentile in total sample						

(1) DG-S SUP has identified a number of data points which should be reported in all cases by all institutiongs, regardless of their characteristics (size, business model, ...).

Chart 1. Failed validation rules by module

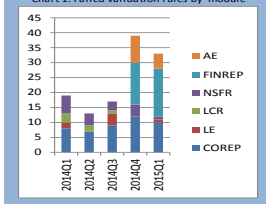


Chart 2. Dispersion of failed validation rules across SUBA

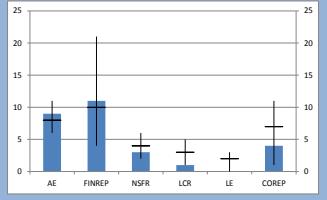
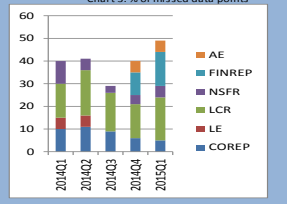


Chart 3. % of missed data points



3. INTERNAL CONSISTENCY OF THE DATA *(to be discussed with DG-IV)*

Example: Leverage ratio is lower than the capital ratio	Yes/No
Example: Capital ratio including Pillar 2 adjustments is not equal (larger) to capital ratio without them	Yes/No
Example: SA/IRB templates are reported according to metadata available	Yes/No
Example: Tier 1 and 2 capital in COREP and NSFR is reported with the same amounts	Yes/No
Check 5	Yes/No
Check 6	Yes/No
Check 7	Yes/No
Check 8	Yes/No
Check 9	Yes/No
Check 10	Yes/No
Total number of failed internal consistency checks	
Average number of failed internal consistency checks in SUBA for the period	

DATA QUALITY RATING OF THE INSTITUTION

	Institution	Sample
1. Submission process		
2. Completeness and accuracy		
3. Internal consistency		
TOTAL		

Objectif :

Recevoir 100% des rapports dans les délais et sans erreurs !

Sommaire

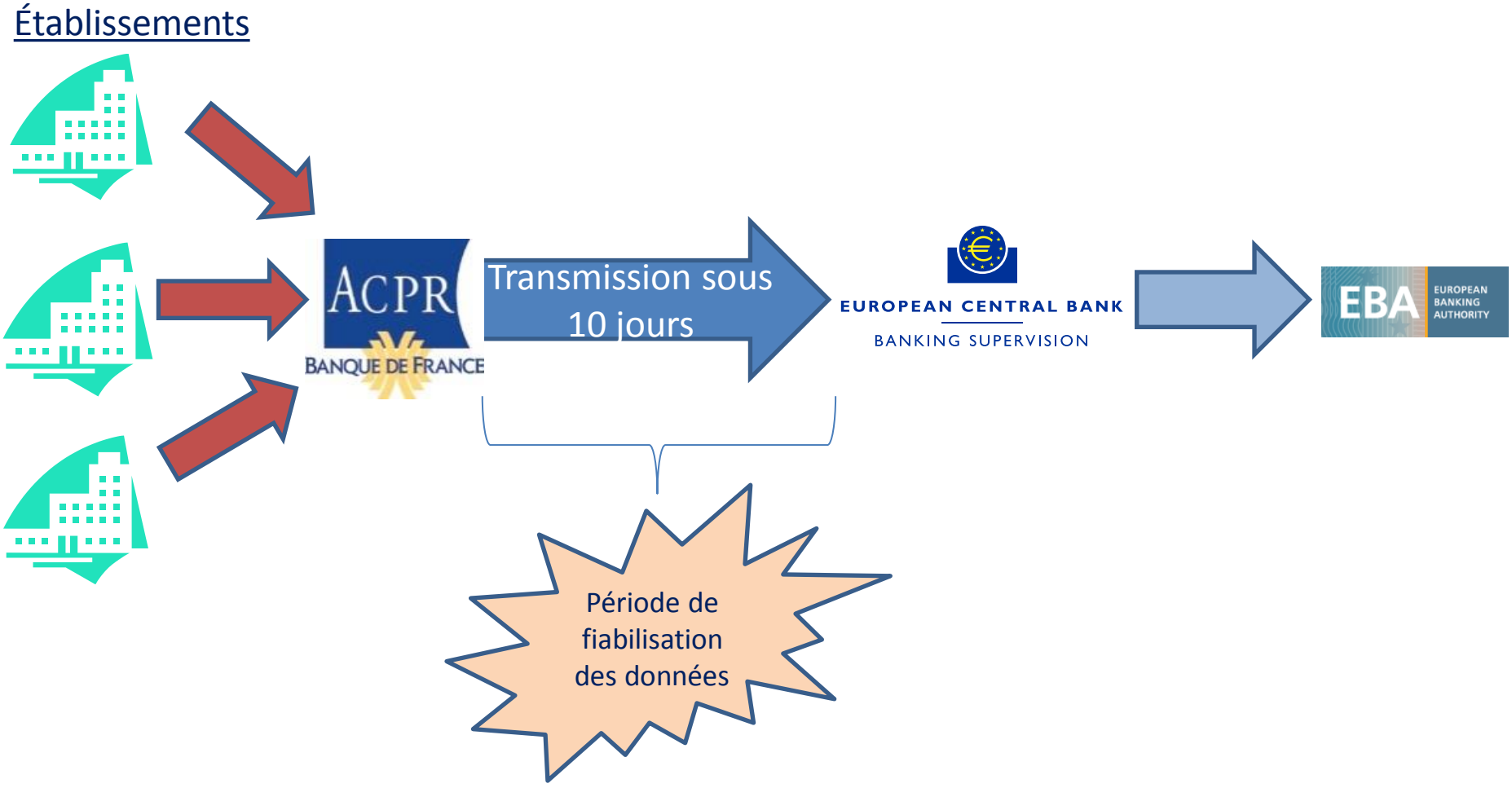
Sommaire

1. Rappel du processus de collecte et de transmission à la BCE et à l'ABE

2. Une amélioration de la qualité des données prudentielles transmises à l'ACPR

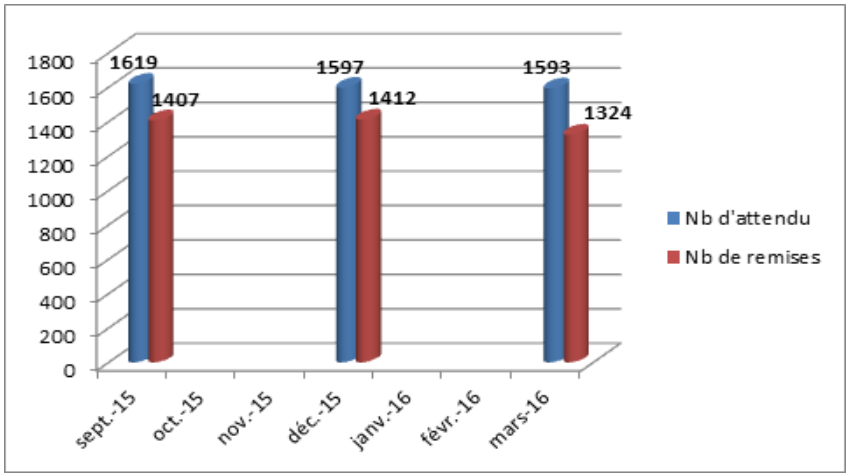
3. Une démarche globale d'amélioration de la qualité des données

1. Rappel du processus de collecte et de transmission à la BCE et à l'ABE

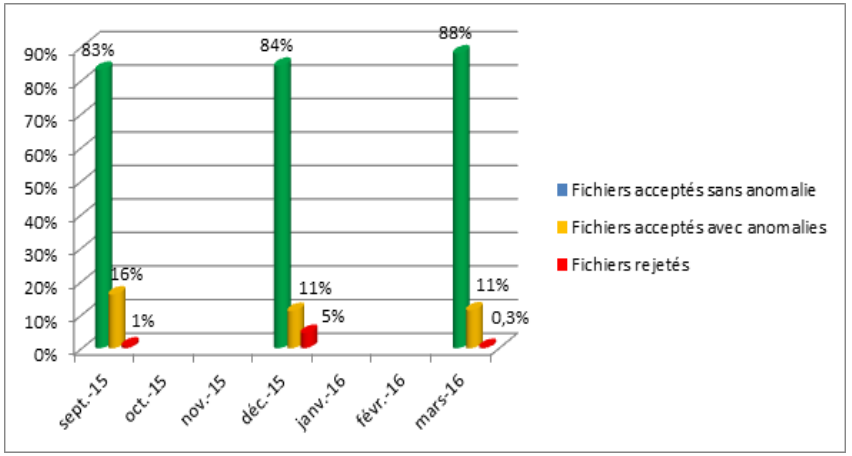


2. Une amélioration de la qualité des données prudentielles envoyées à l'ACPR

Évolution de la complétude des données pour les SI / LSI (Prise de référence à la date limite d'envoi des données à la BCE)



Évolution de la qualité des données pour les SI / LSI (Prise de référence à la date limite d'envoi des données à la BCE)



Mais qui reste perfectible en regard des autres pays

3. Une démarche globale d'amélioration de la qualité des données

- **Un renforcement des contrôles et des rejets alignés sur ceux de la BCE et de l'ABE dès les prochaines remises avec une tolérance proche de zéro**

- **Implication forte des différents acteurs des établissements dans la production de données fiables**

- **Délai de réaction des établissements pour fiabiliser les données à améliorer**

Sommaire

1. La qualité des données en assurance et en banque
   - La qualité des données en assurance
   - La qualité des données en banque : la vision de la BCE
   - La qualité des données en banque : le point de vue de l'ACPR
2. **Présentation de l'enquête de l'ACPR sur les systèmes d'information**
   - **Thierry Auran, chef du service des Contrôles sur place spécialisés à l'ACPR**
3. Les risques liés aux systèmes d'information et notamment la cyber-sécurité
   - Les risques liés à l'usage des technologies de l'information
   - Cyber-sécurité : état des menaces et attentes des superviseurs

Enquête sur les systèmes d'information (SI) et la qualité des données (QDD)

- **3 thèmes** : QDD, SI et sécurité du SI.
- Chacun de ces trois sujets fait l'objet d'une quinzaine de questions tantôt fermées, tantôt **d'auto-évaluation selon l'« échelle de maturité » suivante :**

Catégorie	Définition	En deux mots
+ + (très mature)	Les normes écrites couvrent tous les objectifs "clé" identifiés. Elles s'accompagnent de toutes les modalités d'application induites, décrivent leur pilotage ainsi que leur amélioration continue, et sont respectées. Elles sont réajustées de manière régulière et proactive.	Normes cohérentes appliquées et en amélioration
+ (mature)	Les normes écrites couvrent les principaux objectifs "clé" identifiés, ainsi que les modalités d'application qu'ils induisent. Leur mise en place, déjà effective ou en cours de déploiement, fait l'objet d'un suivi, de contrôles, et d'une capitalisation centralisée. Elles sont réajustées de manière réactive, quand le besoin s'en manifeste.	Normes cohérentes appliquées
- (peu mature)	Les normes écrites les plus structurantes sont globalement finalisées, cohérentes et validées. Cependant, elles ne mettent pas à la disposition des collaborateurs l'ensemble des principes, des règles ou des outils nécessaires à leur pleine application sur les périmètres prévus.	Présence de politique écrite
-- (très peu mature)	Les normes écrites sont partielles, peu nombreuses ou inexistantes. Elles ne sont ni standardisées, ni généralisées, ni massivement respectées. La performance reste difficilement prévisible ainsi que peu contrôlée, et son succès repose très majoritairement sur quelques collaborateurs qualifiés de "clé", tandis que la plupart des employés sont peu ou mal informés des responsabilités	Mode "héros"

Enquête sur les systèmes d'information (SI) et la qualité des données (QDD)

- A vocation à être récurrente
- Une très bonne participation (situation au 26 mai) :
  - **Les réponses remises couvrent 306 organismes dont la plupart des entreprises appartenant au 20 plus grands groupes**
  - 130 mutuelles, 100 SA, 36 SAM, 25 IP ont répondu
  - Représentant environ 235 Md€ de chiffre d'affaires soit plus de 85% du marché de l'assurance et de la réassurance

Enquête sur les systèmes d'information (SI) et la qualité des données (QDD)

1. Premiers résultats de l'enquête en QDD

2. Premiers résultats de l'enquête en gouvernance du SI

3. Premiers résultats en sécurité du SI

1. Premiers résultats de l'enquête en QDD

- Plus de 50% des entreprises (mais moins de 40% en part de chiffre d'affaires) encore peu matures en politique de qualité de données

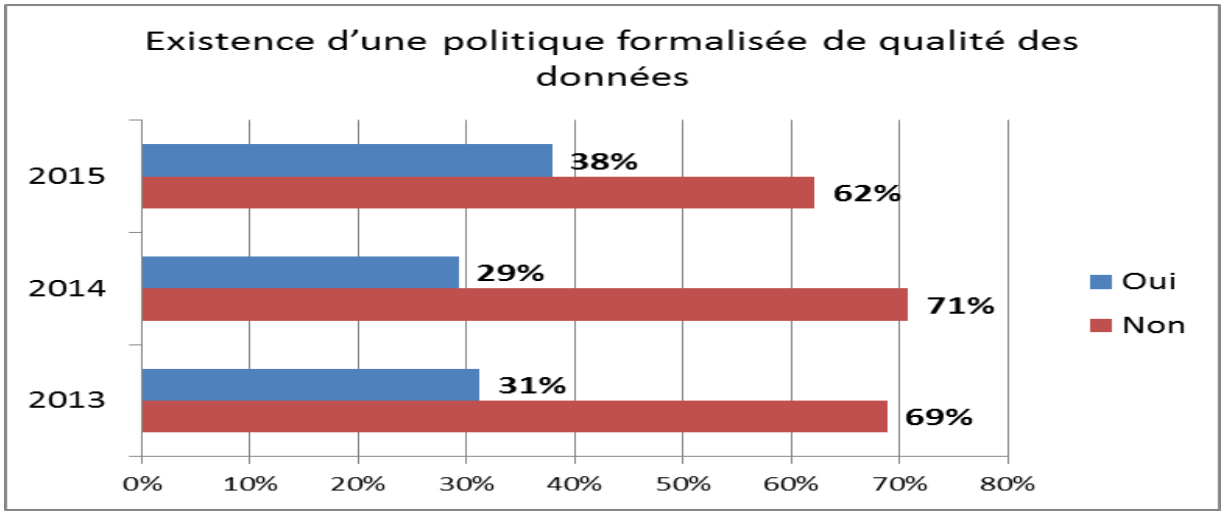
Auto évaluation de la maturité en politique et gouvernance de la QDD

Part 2016 (en nombre)	++ (très mature)	+ (mature)	- (peu mature)	-- (très peu mature)	NR	Ensemble
IP	4%	24%	48%	24%	0%	100%
Mutuelle ou union	5%	38%	44%	12%	2%	100%
SA	14%	37%	42%	6%	0%	100%
SAM	8%	58%	31%	3%	0%	100%
Ensemble	**8%**	**39%**	**42%**	**10%**	**1%**	**100%**

- Seuls 10% indiquent n'avoir pas de politique de qualité de données (soit 2% du chiffre d'affaires)
- 5% déclarent ne pas évaluer la qualité des données utilisées dans les provisions techniques (ce qui n'est pas conforme à l'article art. 272 du règlement 2015/35)

1. Premiers résultats de l'enquête en QDD

- **Rappel sur les résultats des enquêtes de préparation à Solvabilité II (2013-2015)**



- **Les progrès enregistrés en 2016 s'expliquent par l'entrée en application du régime Solvabilité II**

1. Premiers résultats de l'enquête en QDD
D'autres réserves à apporter

- Parmi les entreprises « matures » et « très matures », environ 27% font état de dispositifs d'évaluation de la QDD examinés selon une fréquence insuffisante (dans un contexte d'entrée en application de la directive), que cela soit par le contrôle interne ou par l'audit interne

- Les indicateurs relatifs à la QDD ne sont pas suivis par les organes dirigeants dans 43% des entreprises

- **Parmi les 24 entreprises se déclarant « très matures » (« ++ »), seules 13 soumettent des indicateurs de QDD à leurs organes dirigeants**

- Les diligences réglementaires (art. 272 du règlement 2015/35) en matière d'évaluation de la QDD portent sur plus de 75% des provisions techniques chez seulement 54% des répondants

2. Premiers résultats de l'enquête en SI

- 77% des répondants se considèrent matures (« ++ » et « + »), ce qui représente 92% du chiffre d'affaires des répondants

Auto évaluation de la politique et la gouvernance du SI

Part en % (2016)	Très matures (++)	matures (+)	Peu matures (-)	Très peu matures (--)	Ensemble
Nombre	14%	63%	21%	2%	100%
CA	28%	64%	7%	0%	100%

- De même, 87% indiquent être matures pour la gestion opérationnelle de l'exploitation du SI, et 76% pour la gestion opérationnelle des projets SI

- Enfin, 91% (99% en termes de CA) des répondants affirment être matures en connaissance de risque SI, **et 75% prendre en compte les impacts des risques SI sur les métiers** (art. 259 du règlement 2015/35)

2. Premiers résultats de l'enquête en SI
Des réserves à apporter

- Pour 9% des répondants, le directeur des SI (DSI) ne fait partie :
  - ni des organes dirigeants,
  - ni d'un comité traitant l'ensemble des sujets stratégiques SI en présence des organes dirigeants

- Ce chiffre se réduit à 6% pour le périmètre des entreprises se déclarant matures (« + » ou « ++ »)

- 41% des entreprises déclarées « très matures » en connaissance de risques ne recensent pas les types de cyber attaques qui les menacent

3. Premiers résultats de l'enquête en SSI

- 78% des entreprises (96% du chiffre d'affaires) se déclarent matures (« + » ou « ++ ») en politique de sécurité du SI

Autoévaluation en maturité en gouvernance de la sécurité SI

Part en nombre (2016)					
Nature juridique	Très peu matures (--)	Peu matures (-)	Matures (+)	Très matures (++)	Ensemble
IP	4%	4%	72%	20%	100%
Mutuelle ou union	5%	28%	55%	12%	100%
SA	1%	11%	74%	14%	100%
SAM	0%	17%	81%	3%	100%
Ensemble	**3%**	**19%**	**66%**	**12%**	**100%**

- Les répondants disposent d'un responsable de la sécurité opérationnelle du SI (RSI) pour 77% d'entre eux, et d'un responsable de la sécurité du SI (RSSI) pour 79%

- Seuls 3% déclarent ne pas avoir de politique de sécurité du SI (soit 1% du chiffre d'affaires des répondants – 16% n'en avaient pas en 2013). La progression entre 2013 et 2016 peut s'expliquer par l'entrée en application du régime Solvabilité II (art 258 du règlement 2015/35 qui pose des exigences en terme d'objectifs de sécurité du SI)

3. Premiers résultats de l'enquête en SSI
Des réserves à apporter

- Chez seulement 33% des répondants, le RSSI est indépendant du DSI (fort taux d'abstention pour la réponse à cette question)

Part des organismes déclarant un RSSI indépendant du DSI								
(2016)	Oui		Non		NR		Ensemble	
	nombre	CA	nombre	CA	nombre	CA	nombre	CA
IP	56%	51%	32%	46%	12%	3%	100%	100%
Mutuelle ou union	28%	32%	49%	64%	23%	5%	100%	100%
SA	37%	46%	61%	54%	2%	0%	100%	100%
SAM	19%	46%	75%	54%	6%	0%	100%	100%
Ensemble	**33%**	**45%**	**55%**	**54%**	**13%**	**1%**	**100%**	**100%**

- Seulement 62% des répondants recensent les cyber menaces dont ils peuvent être victimes
- Parmi les entreprises « matures » et « très matures », 21% font état de dispositifs d'évaluation de la SSI examinés selon une fréquence insuffisante, que cela soit par le contrôle interne ou par l'audit interne

3. Premiers résultats de l'enquête en SSI
Les cyber attaques

- **82% des entreprises ont été victimes d'attaques**. Près de 90% (en CA, près de 60% en nombre) ont été victimes d'attaques par usurpation d'identité

En fonction du type d'attaques, % d'organismes visés depuis le 1er janvier 2015		
Type d'attaques	**Nombre**	**En part de CA**
Déni de service	31%	43%
Par logiciel piégé / malveillant	69%	87%
Par usurpation d'identité ou d'ingénierie	57%	89%
Par rançonnage sur ses données	57%	69%

- La part élevée de la pratique des tests d'intrusion est cohérente avec les déclarations de maturité en sécurité SI

% de tests d'intrusion ou des identifications de vulnérabilités menés		
Nature Juridique	**Nombre**	**En part de CA**
IP	91%	99%
Mutuelle ou union	74%	92%
SA	95%	99%
SAM	97%	100%
Total général	**86%**	**99%**

- 86% des victimes d'attaques ont effectué des tests d'intrusion depuis le 1er janvier 2015

3. Premiers résultats de l'enquête en SSI
Les plans de continuité pour les services SI critiques

Auto évaluation de la capacité des services critiques du SI à basculer, durant un incident majeur, sur un site de secours

Part (en nombre) 2016	++	+	-	--	Ensemble
Autre	0%	80%	20%	0%	100%
IP	68%	32%	0%	0%	100%
Mutuelle ou union	29%	51%	15%	5%	100%
SA	45%	52%	3%	0%	100%
SAM	56%	39%	3%	3%	100%
Ensemble	**41%**	**48%**	**8%**	**2%**	**100%**

- 89% des organismes se déclarent matures (« + » et « ++ »)
- Amélioration par rapport à l'enquête de préparation à Solvabilité II de 2013 : seuls 2% (« -- ») ne disposent toujours pas de procédures (contre 25 % en 2013)

Les premiers enseignements

- **Des progrès sont déclarés sur l'ensemble des 3 sujets**. Des efforts ont été accomplis en matière de mise en place de politiques/procédures

- Toutefois, il convient de noter que :
  - L'évaluation de la maturité est moins élevée en gouvernance de QDD
  - L'évaluation de la QDD ne se fait pas complètement ou seulement sur une partie de la chaîne.
  - Des faiblesses dans l'identification des risques SI demeurent
  - Les cyber attaques sont nombreuses. Il convient de donner au RSSI les moyens et l'indépendance suffisants
  - Plus généralement, en recoupant les réponses et en comparant avec les constats des contrôles sur place, il apparaît qu'un grand nombre d'entreprises semblent surévaluer leur niveau de maturité

Questions/réponses

PAUSE

Sommaire

1. La qualité des données en assurance et en banque
   - La qualité des données en assurance
   - La qualité des données en banque : la vision de la BCE
   - La qualité des données en banque : le point de vue de l'ACPR
2. Présentation de l'enquête de l'ACPR sur les systèmes d'information
3. **Les risques liés aux systèmes d'information et notamment la cyber-sécurité**
   - **Les risques liés à l'usage des technologies de l'information**
     - **François Phillipe, responsable de mission au service des Contrôles sur place spécialisés à l'ACPR**
   - Cyber-sécurité : état des menaces et attentes des superviseurs

1. **De quoi parle-t-on ?**

2. Dans quel environnement évolue-t-on ?

3. Quelles réponses apporter

Qu’est ce que le risque SI ?

- **C’est un risque inclus dans le risque opérationnel ; c’est-à-dire le risque résultant d’une inadaptation ou d’une défaillance imputable à des procédures, personnels et systèmes internes ou à des événements extérieurs.**

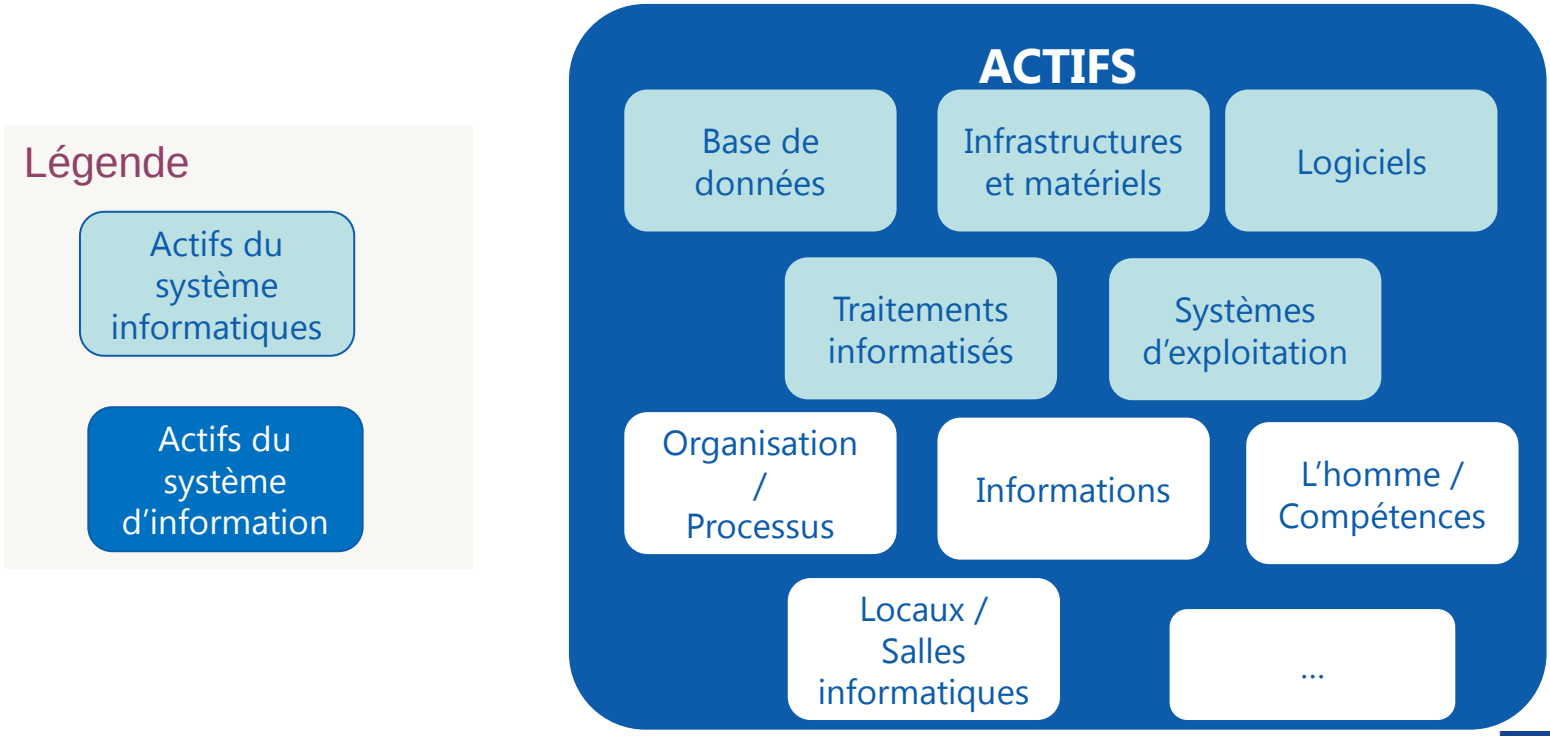
- **Les instances internationales évoluent vers une définition spécifique**

  - Banque : EBA, BCBS, BCE
    - EBA SREP guidelines (Dec 2014): ‘Information and communication technology (ICT) risk’ means the current or prospective risk of losses due to the inappropriateness or failure of the hardware and software of technical infrastructures, which can compromise the availability, integrity, accessibility and security of such infrastructures and of data.”
  - Assurance : non caractérisé spécifiquement mais qui découle de la définition du risque opérationnel Solvabilité II

- **Désignés comme « risques informatiques » ou « risques des systèmes d’information », le superviseur retient une acception large (technique et organisation)**

Qu’est ce que le risque SI ?

- **Risque : « Effet de l’incertitude sur l’atteinte des objectifs » - Référentiel ISO.**
- **Risque SI : effet de l’incertitude liée aux actifs SI sur l’atteinte des objectifs stratégiques métier (raison d’être du SI).**

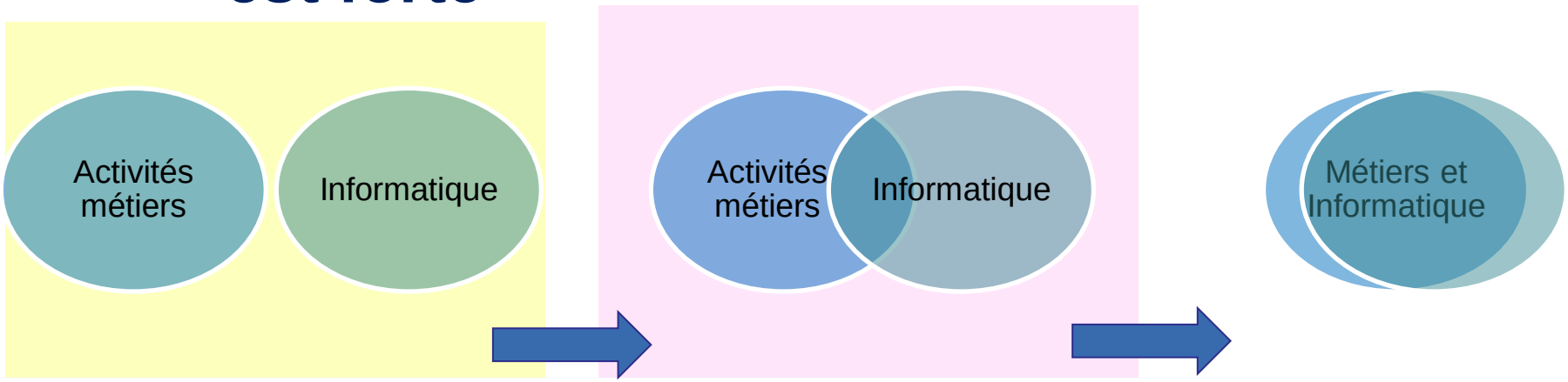


1. De quoi parle-t-on ?

2. **Dans quel environnement évolue-t-on ?**

3. Quelles réponses apporter

Dans un cadre où l'articulation SI et métier est forte



- **Activités métiers et informatiques souvent étroitement imbriquées. L'informatisation des métiers peut conduire à une internalisation de la fonction informatique, l'une et l'autre générant des risques spécifiques :**
  - Aux métiers qui passent outre la DSI
  - Aux DSI au service des filiales métier qui ne respectent pas les règles groupe
- **Une imbrication qui nécessite :**
  - Un SI de plus en plus robuste (disponibilité, performance, sécurité)
  - Une gestion du risque SI en cohérence avec les risques métiers et qui ne peut plus se limiter à un exercice technique à part

Dans un cadre recelant des défis croissants

- **Intensification de l'ouverture des SI**
- **Digitalisation des services déjà lancée**
- **Apparition de nouvelles technologies**
- **Augmentation des cas de cyberattaques et de leurs impacts croissant sur les organismes**
- **Enfin des dispositions règlementaires renforcées**
  - Banque : arrêté du 3 novembre 2014 relatif au contrôle interne
  - Assurance : notamment les articles 258, 259, 260, 269, 273, 294 et 295 du règlement délégué 2015/35.

Alors que le chemin vers la maturité en matière de gestion du risque SI est encore long pour certaines organisations

- **Une appropriation de la démarche de gestion des risques SI**
- **Une intégration de la gestion du risque SI avec les autres risques opérationnels**
- **Un dispositif de pilotage des risques SI à développer**

1. De quoi parle-t-on ?

2. Dans quel environnement évolue-t-on ?

3. **Quelles réponses apporter**

Attente : une gouvernance du risque SI à asseoir

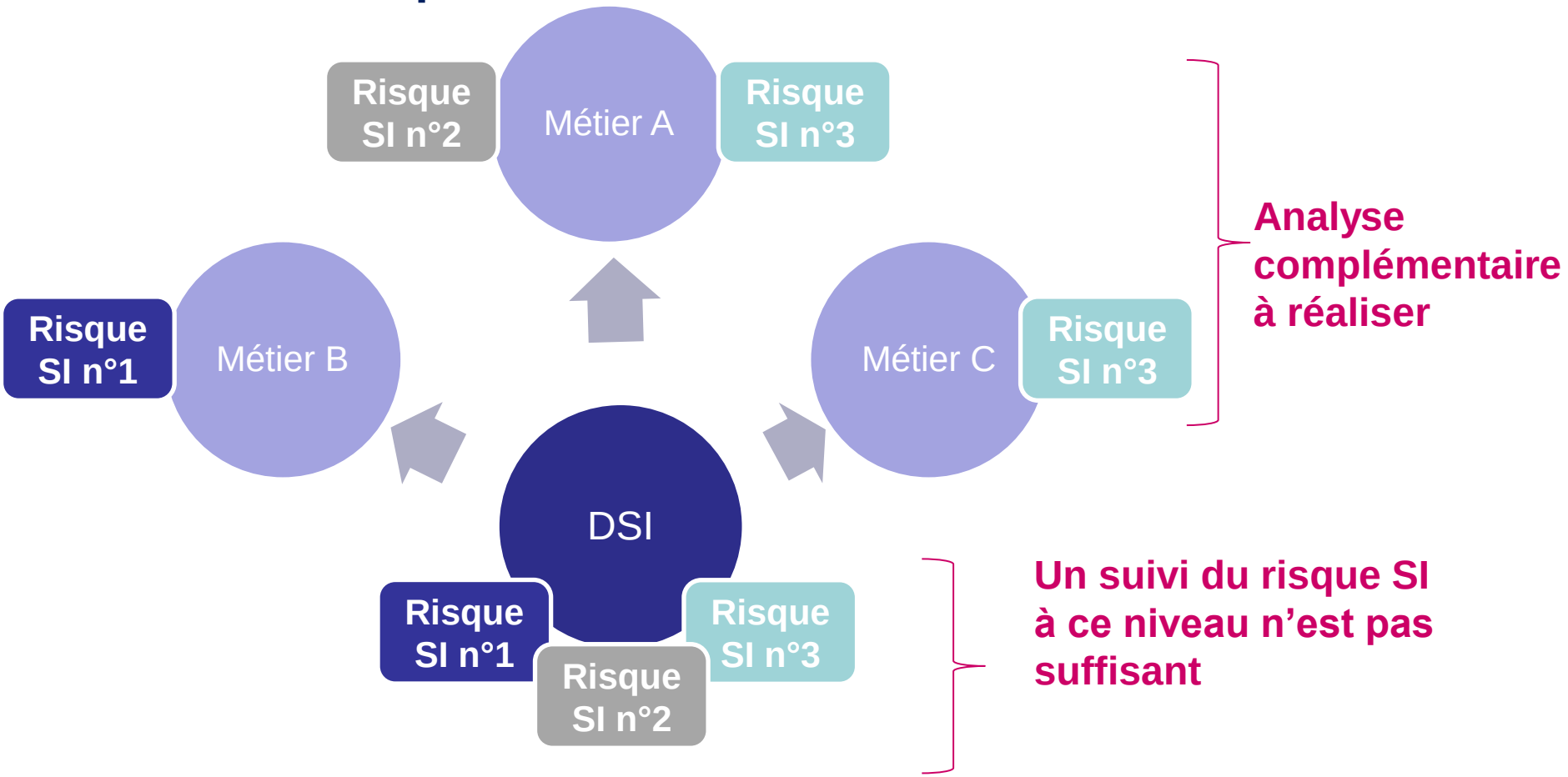
- **L'organisation du système de gestion des risques SI doit permettre :**
  - À l'organe exécutif et à l'organe d'administration ou de surveillance de disposer d'une vision suffisante du niveau de risque :
    - Qualité et exhaustivité de l'information qui leur est remontée
    - Attribution claire aux comités spécialisés (risques, audit – contrôle interne) qu'ils soient distinct (banque) ou non (assurance).
  - La clarification des rôles et responsabilités
  - Une sensibilisation régulière des opérationnels mais aussi des dirigeants
- **La gouvernance du risque SI peut avoir des spécificités mais doit s'intégrer à la gouvernance des risques de l'entreprise.**
- **Le système de gestion du risque SI doit être mieux défini et documenté.**

Attente : une identification des risques SI à étendre

- L'approche d'identification des risques doit permettre une identification exhaustive des risques indépendamment de leur criticité.
- La création d'un base des incidents métier et informatique à jour doit contribuer à l'identification des risques SI.
- Les activités SI externalisées doivent entrer dans le périmètre d'identification des risques SI.
- Les risques SI doivent être identifiés dans un référentiel unique pour permettre une vision globale.

Attente : une identification des risques SI à étendre

- **L'identification des risques SI doit être articulée avec les risques métier**



Attente : une évaluation des risques SI à mettre en cohérence

- L'évaluation doit porter sur les risques SI brut et pas uniquement sur le risque résiduel, et prendre en considération le métier impacté.

- Les méthodologies d'évaluation des risques SI définissent des échelles de cotation adaptées mais aussi des limites et des seuils pour chaque risque SI.

- Les règles et mesures de traitement du risque SI (acceptation, refus, réduction …) doivent être définies et documentées.

Attente : un pilotage des risques SI à développer

- **Comme pour tout risque opérationnel, un dispositif de pilotage des risques SI doit être défini et reposé sur des indicateurs clés (*Key Risk Indicators*).**

- **La révision des risques SI doit être effectuée au fil de l'eau et doit faire l'objet d'une revue annuelle « d'inventaire » intégrant les choix stratégiques de l'entreprise.**

- **Le pilotage des risques SI doit permettre de fournir une vision prospective (et non historique) du risque SI et devenir un élément des processus décisionnels.**

Récapitulatif : Les principaux points d'attention

- **Un renforcement de la gouvernance des risques SI au niveau**
  - Des plus hautes instances décisionnelles
  - De la Direction des risques
  - Et parfois même au niveau de la Direction des Systèmes d'Information

- **Une approche des risques SI à mieux intégrer à l'approche générale des risques opérationnels**

- **Accroître le niveau de maturité de gestion des risques SI pour que celle-ci devienne un outil de pilotage pouvant dépasser les frontières de l'informatique**

Sommaire

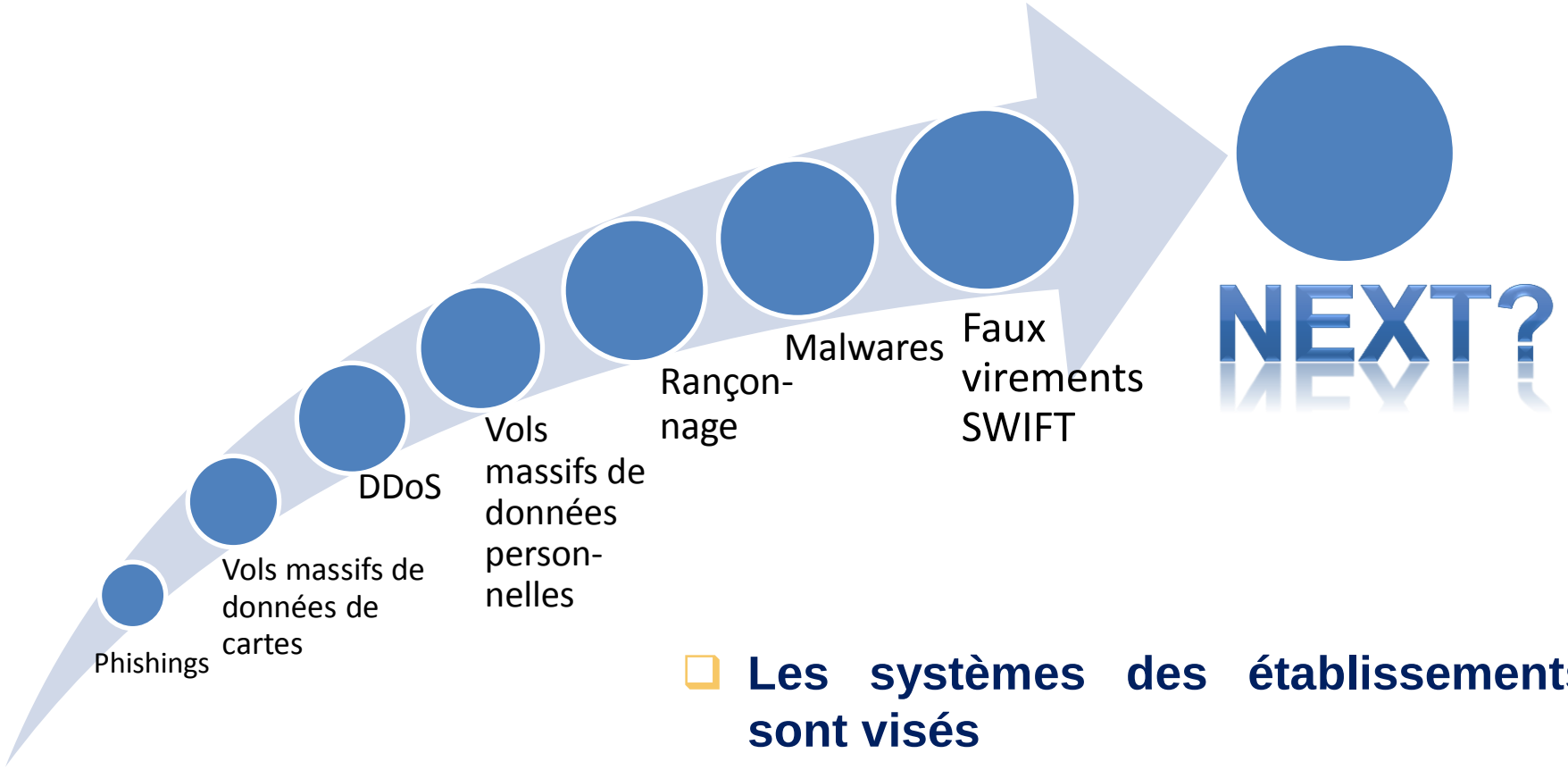
1. La qualité des données en assurance et en banque
   - La qualité des données en assurance
   - La qualité des données en banque : la vision de la BCE
   - La qualité des données en banque : le point de vue de l'ACPR
2. Présentation de l'enquête de l'ACPR sur les systèmes d'information
3. **Les risques liés aux systèmes d'information et notamment la cyber-sécurité**
   - Les risques liés à l'usage des technologies de l'information
   - **Cyber-sécurité : état des menaces et attentes des superviseurs**
     - **Marc Andries, inspecteur de la Banque de France, responsable de la cellule d'évaluation des risques des systèmes d'information à la Délégation au contrôle sur place de l'ACPR**

1. **État de la menace : un niveau préoccupant**

2. **Les différentes actions conduites par les superviseurs**

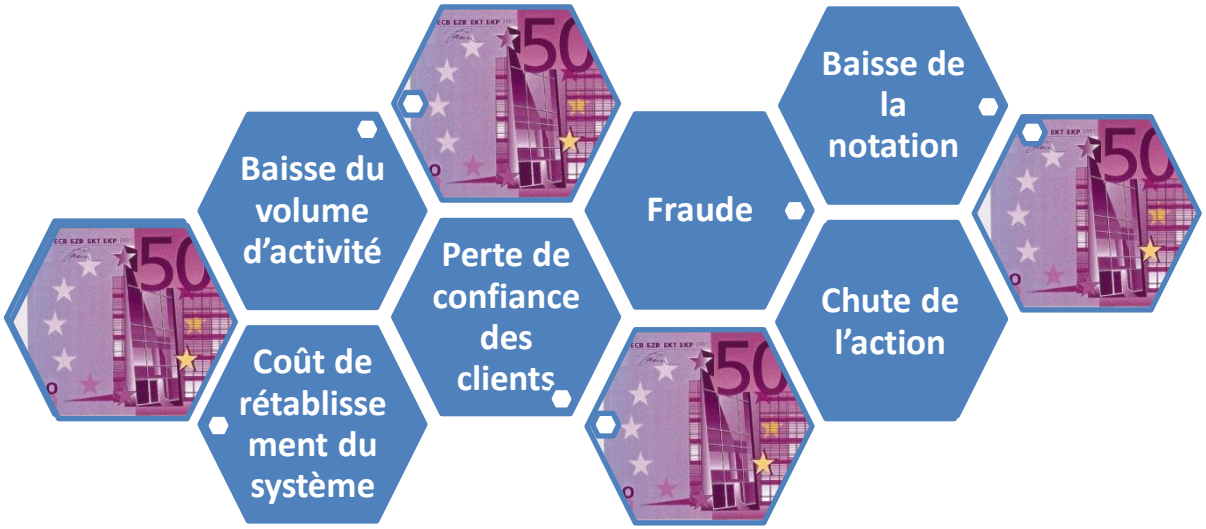
3. **Enjeux pour la profession et attentes du superviseur**

1. État de la menace : un niveau préoccupant



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

1. État de la menace : conséquences majeures



Bloomberg Business Week – Octobre 2014 – Les actions de Target ont chuté de 10% après cette fuite, se traduisant par une perte de 6 milliards de dollars. Les ventes lors de la période de Noël, moment où a eu lieu la fuite, ont diminué de 5,5%. Le PDG et le DSI (directeur des systèmes d'information) ont démissionné. Pour la toute première fois, un PDG d'une entreprise classée dans Fortune 500 s'est vu contraint à démissionner suite aux dommages d'une cyber-attaque.

AFP - 15 mars 2016 - Le gouverneur de la banque centrale du Bangladesh, Atiur Rahman, a démissionné mardi après le vol de 81 millions de dollars par des hackers, l'une des plus grosses fraudes bancaires de ce type dans l'histoire.

LA TRIBUNE

Cyberattaques : les PDG commencent à perdre leur poste !

ACPR BANQUE DE FRANCE

2. Les différentes actions conduites par les superviseurs

Prise en compte des menaces

- Priorité de contrôle de la BCE en 2015
  - Revue thématique par auto-évaluation des banques « significatives » (123)
  - Conduite d'enquêtes sur place (une dizaine)
    - L'ACPR en a conduit plusieurs en réalisant pour la première fois des tests d'intrusion
    - L'ACPR s'appuie sur son expertise de contrôle de la sécurité des systèmes d'information
    - Coopération avec le CERT BDF
  - Suivi des recommandations

- L'ACPR va étendre la démarche par une revue thématique en 2016 sur les établissements « moins significatifs »

Mise en place d'un suivi

- La BCE va mettre en œuvre un suivi des incidents de cybersécurité
  - Pilote en cours
  - Incidents significatifs (impact financier et autres cas)

2. Les différentes actions conduites par les superviseurs

- **Élaboration de normes et standards pour la profession**
  - Participation active de l'ACPR et la Banque de France à différents groupes internationaux
    - Travaux de l'IAIS sur les cyber risques en assurance (consultation papers)
    - Travaux de CPMI-IOSCO sur la cyber-résilience des infrastructures de place
    - Travaux du G7
    - Travaux à venir du Senior Supervisors Group
    - EBA évaluation des risques informatiques, Cloud computing…
  - Coopération avec l'ANSSI pour la mise en œuvre des compétences prévues par la LPM de 2013
- **Développement d'une approche transversale du risque informatique**
  - Travaux EBA et Bâlois sur le risque informatique
  - Organisation d'un réseau d'experts au sein de l'ACPR (banque et assurance)

3. Enjeux pour la profession et attentes du superviseur

Les enjeux de la cyber-sécurité requièrent :

- Un engagement direct des dirigeants des établissements et des conseils d'administration

- Une meilleure répartition des rôles et responsabilités, notamment pour mieux asseoir la responsabilité du RSSI :
  - Assurer son indépendance
  - Un droit de veto en cas de risque majeur pour la sécurité

- Des investissements importants dans la sécurité, avec une portée générale plutôt qu'une approche au cas par cas

3. Enjeux pour la profession et attentes du superviseur

- **Les points d'attention techniques du superviseur :**
  - L'obsolescence et la complexité des systèmes informatiques « legacy »
  - La gestion des droits d'accès, notamment pour les administrateurs
  - La classification des données et des systèmes
  - La ségrégation des environnements sensibles
  - La mise en œuvre d'une détection globale des incidents de sécurité
  - Les situations d'externalisation de données, comme le *Cloud computing*

Pour conclure

- La menace atteint des niveaux très préoccupants et doit être prise très au sérieux
- Les superviseurs précisent leurs attentes et renforcent leurs actions de contrôle
- Les instances dirigeantes doivent se mobiliser et renforcer le positionnement et l'indépendance des responsables de la sécurité
- Les budgets de sécurité doivent être préservés ou rehaussés. L'approche doit être globale
- La sécurité technique des environnements sensibles est une priorité
- Une couverture assurantielle peut compléter ces mesures sans jamais s'y substituer

Merci pour votre attention

Questions/réponses

Conclusion

Sandrine Lemery,

première secrétaire générale adjointe de l'ACPR