

# Enjeux prudentiels des données utilisées par les entreprises d'assurance : le point de vue du superviseur

Atelier « Information et assurance »

Institut de Science Financière et d'Assurances – ISFA  
Université Claude Bernard  
Lyon - 17 et 18 mars 2015

# Sommaire

- ❖ **1. Le contrôle de la qualité des données : quels enjeux ?**
- ❖ **2. Des exigences renforcées avec Solvabilité II**
- ❖ **3. Les constats de l'ACPR**
- ❖ **4. *Big Data et Cloud computing* : quels risques ?**

# 1. Le contrôle de la qualité des données : quels enjeux ?

- ❑ La qualité des données est un **élément essentiel du pilotage de l'entreprise** : évaluation des engagements, segmentation, tarification, solvabilité...
- ❑ La capacité de l'organisme à mettre en œuvre une gouvernance des SI/qualité des données est une composante importante de son patrimoine et constitue un **avantage concurrentiel**
- ❑ La qualité de l'information est une **exigence transversale** dans l'entreprise qui concerne les trois « piliers » de la future réglementation Solvabilité II
- ❑ Des **demandes croissantes des autorités** de régulation financière internationales (G20, Comité de stabilité financière, FMI, BCE ...) et des superviseurs nationaux (règles de solvabilité, lutte contre le blanchiment ...)

# 1. Le contrôle de la qualité des données : quels enjeux ?

## □ Quels sont les principaux objectifs ?

- ✓ **Fiabilité** : garantir l'image fidèle des engagements des assureurs et permettre des prises de décisions pertinentes et rapides
- ✓ **Lisibilité et simplicité** : disposer d'une information homogène partagée par tous les acteurs de l'entreprises
- ✓ **Pérennité** : processus d'amélioration continue de la qualité
- ✓ **Contrôle** : partie intégrante du contrôle interne

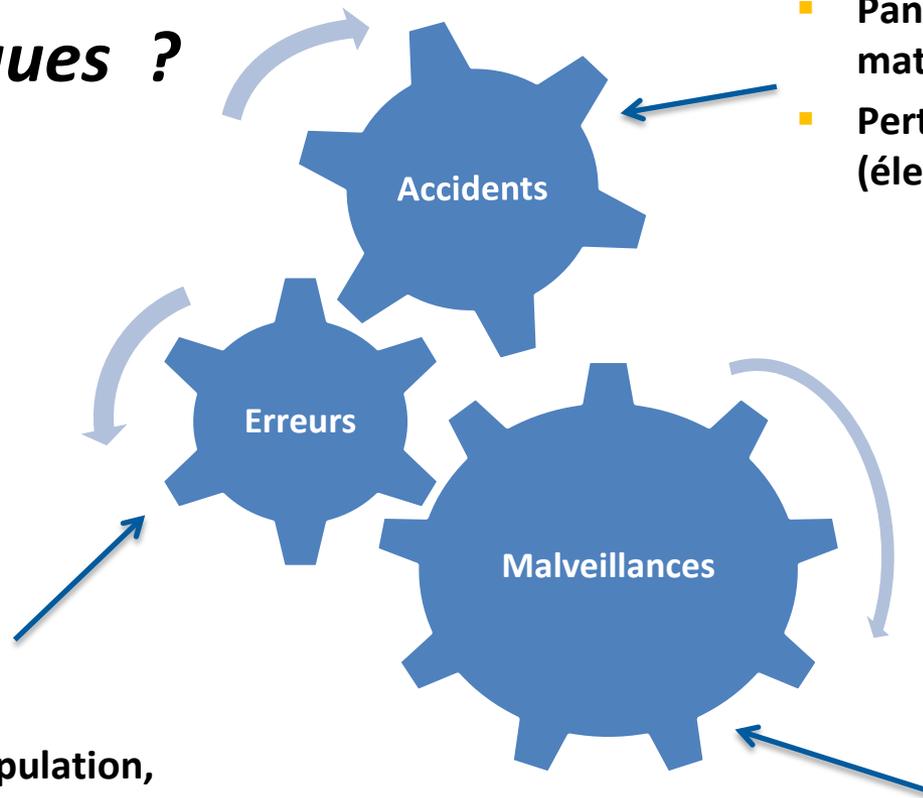
# 1. Le contrôle de la qualité des données : quels enjeux ?

- Le coût élevé de la non-qualité des données :
  - ✓ **Augmentation des coûts opérationnels** (immobilisation inutile de capital) et de la charge réglementaire (production des *reportings* difficile...)
  - ✓ **Baisse de la qualité/pertinence** des analyses
  - ✓ Risque d'initier une **mauvaise stratégie** et de manquer des opportunités commerciales
  - ✓ **Non-conformité** aux exigences réglementaires
  
- Le risque opérationnel lié aux insuffisances des SI est désormais pris en compte par Solvabilité II ; il est potentiellement accru avec le *Big Data*

# 1. Le contrôle de la qualité des données : quels enjeux ?

## *Quels risques ?*

- Conception
- Programmation
- Exploitation (manipulation, paramétrage ...)



- Événements naturels
- Pannes et défaillances des matériels
- Pertes de services essentiels (électricité, télécoms ...)

- Vol
- Sabotage
- Attaques logiques

## 2. Des exigences renforcées avec Solvabilité II

Les exigences réglementaires existant en matière de qualité des données (Solvabilité I)

- ❑ Disposer d'une **piste d'audit** (art. A. 343-1 code des assurances, A. 931-11-9 du Code de la sécurité sociale, § 2.1.2 du règlement CRC n° 2002-06 pour la mutualité)
- ❑ Tenue de registres **des sinistres/polices** (articles A.342-5 et A.342-6 du code des assurances)
- ❑ Justification des **engagements** des entreprises d'assurance à tout moment (art. R. 331-1 du code des assurances)
- ❑ Informations sur la clientèle en matière de **lutte anti-blanchiment** (L.561-5 du code monétaire et financier)
- ❑ Informations relatives à la **protection de l'assuré** (L.32-22 code des assurances, L. 561-6 du code monétaire et financier)

## 2. Des exigences renforcées avec Solvabilité II

Des exigences prudentielles enrichies et des critères de qualité de données formalisés (directive 2009/138 et règlement délégué 2015/35) :

- ❑ **Pour différents usages** : modèle interne (art. 121.3), provisions techniques (art. 82), paramètres spécifiques (art. 104-7), états réglementaires ...
- ❑ **Des critères de qualité explicités** : exhaustivité, pertinence et exactitude (art. 82 sur les provisions techniques et art. 121.3 sur modèle interne)
- ❑ Les données servant à établir **les états réglementaires** doivent être complètes, accessibles, pertinentes, fiables et compréhensibles (art. 35)
- ❑ **Exigence de traçabilité** (art. 19, 219 et 265 du règlement 2015/35 ) tant internes qu'externes

## 2. Des exigences renforcées avec Solvabilité II

### Exhaustivité

- Les données doivent permettre l'identification des principaux groupes de risques homogènes de l'engagement évalué
- Une granularité suffisante pour identifier les tendances et l'évolution des risques sous-jacents
- Des historiques suffisants et disponibles

### Pertinence

- Les données doivent être adaptées et appropriées à l'usage qui leur est destiné (i.e. la valorisation des provisions techniques, l'établissement d'hypothèses, etc... ) et utilisables pour le risque analysé
- Les données reflètent les risques auxquels est exposé l'assureur

### Exactitude

- Absence d'erreurs matérielles ou d'omissions
- Informations stockées de manière adéquate, mise à jour fréquente (notamment si les données sont dupliquées)
- Confiance dans les données qui sont utilisées dans la gestion courante de l'organisme

## 2. Des exigences renforcées avec Solvabilité II : le dispositif de gouvernance des données

- ❑ **Les organismes doivent mettre en place un dispositif de gouvernance des données** : art. 48 sur la fonction actuarielle et art. 19, 20, 244 et 265 du règlement 2015/35 qui précisent notamment les critères de qualité de données, la gouvernance, le répertoire des données...
- ❑ **La gouvernance des données** intègre notamment les objectifs suivants :
  - **Responsabilisation et transversalité** : intégration dans la gouvernance globale de l'organisme en associant plusieurs directions (DSI, métiers)
  - **Harmonisation et cohérence** de l'utilisation des données dans l'entreprise
  - **Agilité** : permettre une prise de décision rapide

## 2. Des exigences renforcées avec Solvabilité II : le dispositif de gouvernance des données



## 2. Des exigences renforcées avec Solvabilité II : le dispositif de gouvernance des données

- ❑ Les dispositifs de **contrôle interne et de conformité** contribuent également au contrôle de la qualité des données (combinaison des art. 41, 46 de la directive et art. 256 du règlement 2015/35)
- ❑ **L'évaluation des données** selon les 3 critères (art. 19 du règlement 2015/35)
- ❑ Les **cas de non-qualité** doivent être identifiés et faire l'objet de plans d'actions documentés

## 2. Des exigences renforcées avec Solvabilité II : le dispositif de gouvernance des données

- ❑ Appréciation de la qualité et la suffisance des données par la **fonction actuarielle** (qui est une des 4 fonctions clés dans Solvabilité II)
- ❑ Extrait de l'art. 48 de la Directive :

*« Les entreprises d'assurance et de réassurance mettent en place une fonction actuarielle efficace afin [...] d'apprécier la suffisance et la qualité des données utilisées dans le calcul des provisions techniques »*
- ❑ Le **rapport de la fonction actuarielle** (art. 272 règlement 2015/35) : au moins une fois par an, un rapport écrit est soumis à l'organe d'administration, de gestion ou de contrôle : *« Ce rapport rend compte de tous les travaux conduits par la fonction actuarielle et de leur résultat, il indique clairement toute défaillance et il émet des recommandations sur la manière d'y remédier. »*

### 3. Les constats de l'ACPR

- ❑ Si la gouvernance des projets de qualité de données a nettement progressé depuis 2 ans, ...
- ❑ ... un certain nombre d'insuffisances retiennent l'attention :
  - **Prise de conscience tardive** de l'importance du sujet (sous-dimensionnement) ayant conduit à reconsidérer l'approche globale du projet Solvabilité II
  - Développements (notamment en modèle interne) réalisés sans rédaction systématique de cahiers des charges, ni de spécifications
  - **Planification du mode permanent insuffisante**
  - **Faible industrialisation** des systèmes d'information ne permettant pas une collecte des données fiable et rapide
  - **Retard dans la rationalisation des systèmes d'information**, lié notamment aux évolutions structurelles du secteur (fusions, changements de systèmes...)
  - **Non-prise en compte de la production des états réglementaires** dans le chantier « qualité des données »

### 3. Les constats de l'ACPR

#### Gouvernance et contrôle interne

- Dispositifs de contrôle parcellaires des données depuis leur collecte jusqu'à leur utilisation
- Absence de vision globale des contrôles sur les données
- Faible intégration des démarches de contrôle interne et de qualité des données
- Contrôle des données à un instant T uniquement

#### Politique de données

- Dictionnaire des données incomplet
- Absence de critère de qualité des données
- Justification des seuils d'acceptation insuffisante
- Absence d'évaluation selon les critères de la Directive

### 3. Les constats de l'ACPR

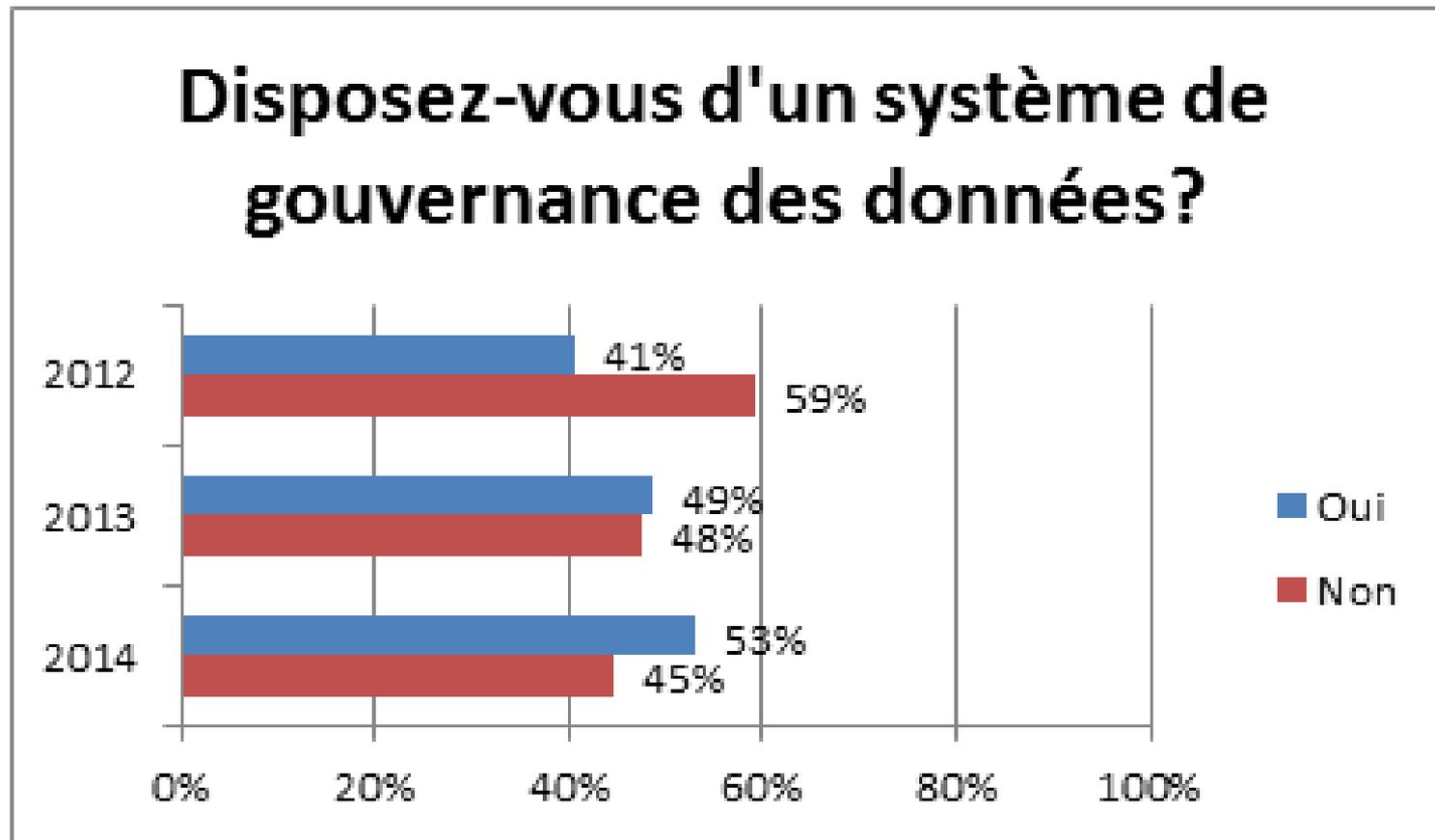
#### Sécurité des données

- Absence de gestion de la sécurité des systèmes d'information
- Externalisation de la production de données pas toujours maîtrisée

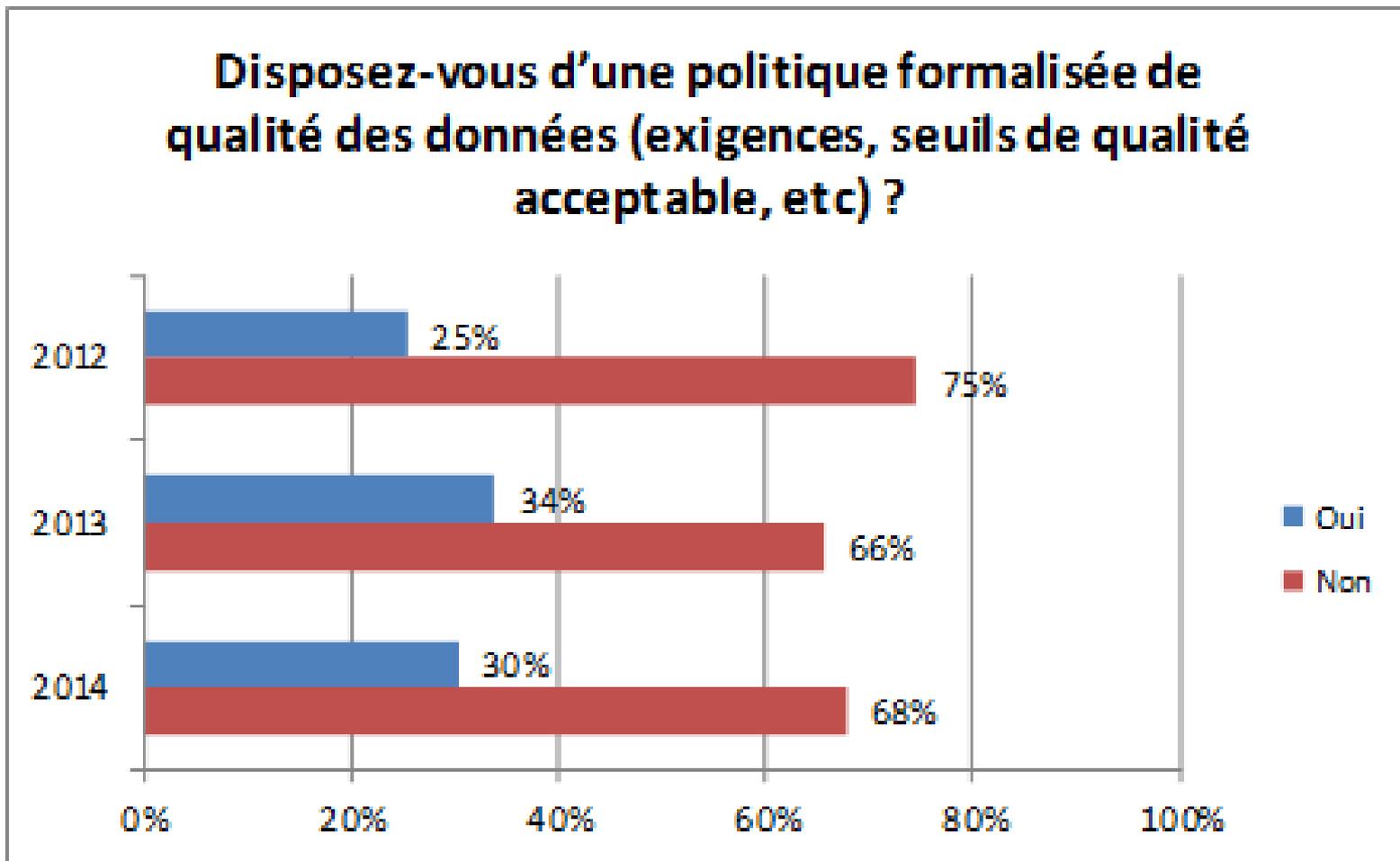
#### Qualité des bases de données

- Les tests réalisés par le contrôle montrent des insuffisances

### 3. Les constats de l'ACPR : l'exercice de préparation de Place (septembre 2014)



### 3. Les constats de l'ACPR : l'exercice de préparation de Place (septembre 2014)



### 3. Les constats de l'ACPR

#### Quelle conclusion (provisoire) ?

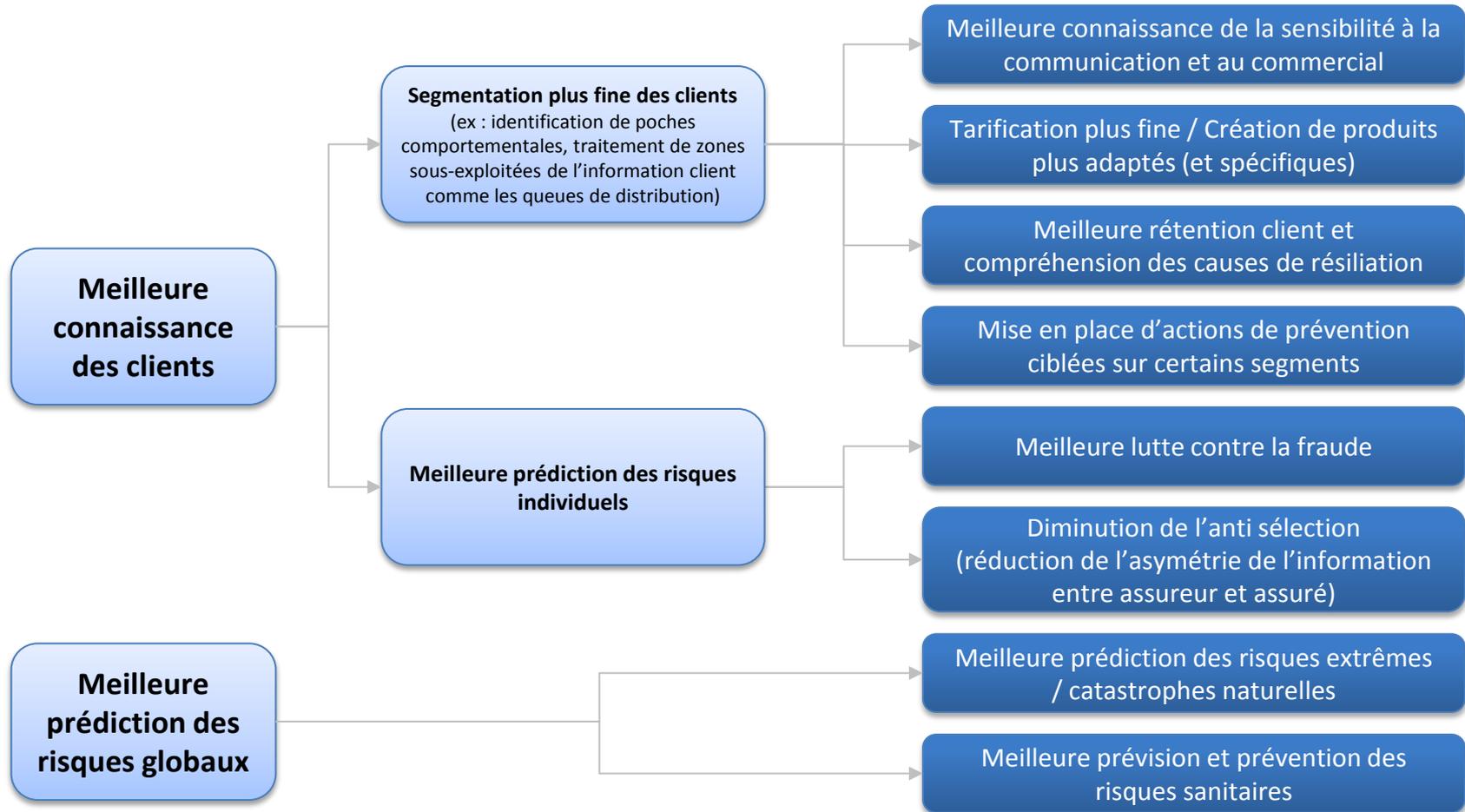
En dépit de progrès notables, les organismes doivent, au-delà des exigences réglementaires, poursuivre leur appropriation d'une gouvernance de la qualité des données en l'intégrant de façon pérenne dans leur stratégie globale

# 4. *Big Data* et *Cloud Computing* : quels risques ?

## □ Le *Big Data*

- Caractérisé par le volume très important et la variété de données ainsi que la vitesse de collecte et de traitement de celles-ci : multiplicité de sources, structurées ou non, internes ou externes (réseaux sociaux, *Open data* ... )
- **Des données nouvelles collectées sur les assurés** : géolocalisation et télématique embarquée, informations publiques sur les sociétés assurées, style de vie des assurés et données médicales, données subjectives ....
- Facteur structurant : amélioration de la **connaissance des clients**, meilleure prédiction des **risques globaux**, impact sur les systèmes d'information ...

# Perspectives ouvertes par le *Big Data* pour le métier de l'assurance



# 4. *Big Data* et *Cloud Computing* : quels risques ?

## □ Le *Big Data*

- Mais de nombreux **risques potentiels** :
  - ✓ éthiques
  - ✓ inégalités de traitement des clients et forte discrimination
  - ✓ remise en question de la mutualisation
  - ✓ gouvernance et qualité des données (normes, piste d'audit...)
  - ✓ confidentialité (notamment avec les solutions de type *Cloud*)
  - ✓ risque juridique et conformité
- Les **points de vigilance** pour l'organisme et le superviseur :
  - ✓ **Confidentialité** : respect des règles de protection de la clientèle (code de la santé publique, Loi informatique et libertés et CNIL) : la collecte d'informations personnelles nécessite l'accord de la personne ou de la structure intéressée

# 4. *Big Data* et *Cloud Computing* : quels risques ?

- Le *Big Data* : les **points de vigilance** pour l'organisme et le superviseur (suite) :
  - ✓ **Structuration des données et continuité d'activité** :
    - forte augmentation du volume d'informations mais baisse de la qualité des données
    - tri nécessaire et identification des données prudentielles, impliquant des changements organisationnels
    - vigilance particulière sur la qualité des données utilisées pour les modèles internes et les plans de continuité de l'activité
  - ✓ **Urbanisme des systèmes d'information** : facteur de complexification des architectures SI avec la création de nouvelles bases de données, voire de nouvelles briques applicatives hétérogènes
  - ✓ **Impact des volumes sur les traitements statistiques et décisionnels**
  - ✓ **Problème de stockage et d'accès à ces données** : risques liés au recours aux services de *Cloud Computing* (cf. infra)
  - ✓ **Cybercriminalité** : vulnérabilité liée aux nouveaux points d'accès

# 4. *Big Data et Cloud Computing* : quels risques ?

## □ *Le Cloud Computing*

- Mode particulier d'externalisation d'un service ou d'une fonction informatique présentant des degrés et des formes multiples (privé interne ou externe, hybride, public)
- Risques sur la **protection des données** : absence récurrente de garantie contractuelle concernant l'intégrité et la traçabilité des données ; risque de transmission des données à des tiers en fonction de la localisation du prestataire et de la loi locale (cf. *Patriot Act*). Anonymisation et chiffrement possibles des données dès l'émission mais risque juridique et de conformité
- **Réversibilité** du dispositif problématique

# 4. *Big Data et Cloud Computing* : quels risques ?

## □ *Le Cloud Computing*

- **Continuité et qualité du service** difficiles à formaliser dans un engagement (absence de pénalité ...)
- Impact fort sur la **gouvernance et l'urbanisme des systèmes d'information** : le donneur d'ordre n'est pas responsable des choix technologiques ... difficultés de coordination des différents services SI interconnectés et de pilotage
- **Capacité limitée à auditer** des opérations externalisées avec les « prestataires de prestataires »

**Merci pour votre attention !**