



# *Les enjeux de la qualité des données*

*Bruno Longet*

*ACPR – Direction des contrôles spécialisés et transversaux*

Séminaire Commission analyse des risques

Fédération Française des Assurances

16 décembre 2016



# Sommaire

1. La qualité des données : quels enjeux ?
2. État des lieux de la qualité des données et des systèmes d'information (enquête ACPR 2016)
3. Principaux constats des contrôles sur place de l'ACPR
4. Éclairage international

# Sommaire

1. La qualité des données : quels enjeux ?
2. État des lieux de la qualité des données et des systèmes d'information (enquête ACPR 2016)
3. Principaux constats des contrôles sur place de l'ACPR
4. Éclairage international

# Le contrôle de la qualité des données : les 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 réglementation Solvabilité II
- ❑ **L'exhaustivité, l'exactitude et le caractère approprié** de la donnée (article R.351-13 du code des assurances ; articles 19, 20, 219, 231 et 264 du règlement 2015/35 UE)
- ❑ **Le risque opérationnel lié aux insuffisances des SI est désormais pris en compte par Solvabilité II** ; il est potentiellement accru avec le *Big Data* et lorsque les activités sont externalisées (*Cloud computing*)

# Le contrôle de la qualité des données : les 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

## 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 contrôle de la qualité des données : les enjeux liés à Solvabilité II

Des exigences réglementaires renforcées 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

# Le contrôle de la qualité des données : les enjeux liés à Solvabilité II

## Le dispositif de gouvernance des données



## Les critères de qualité

### 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

### Exactitude

- 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

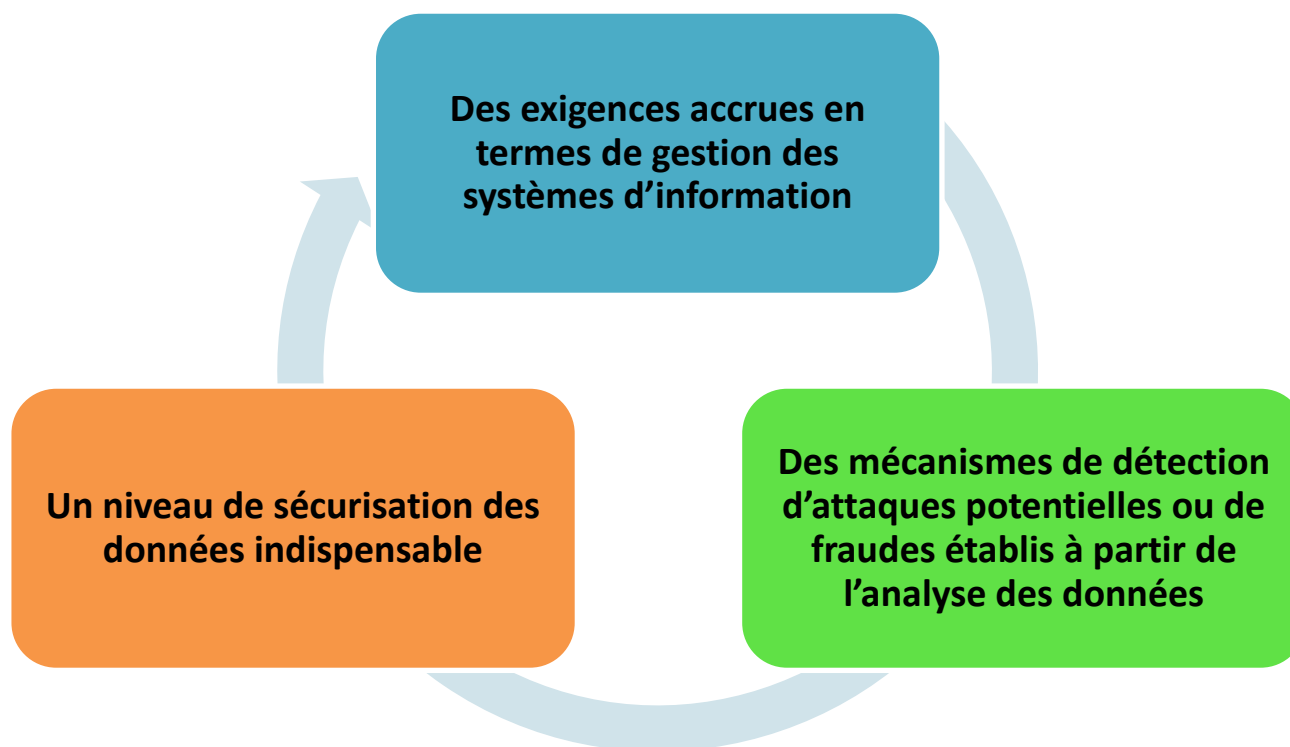
### Pertinence

- 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

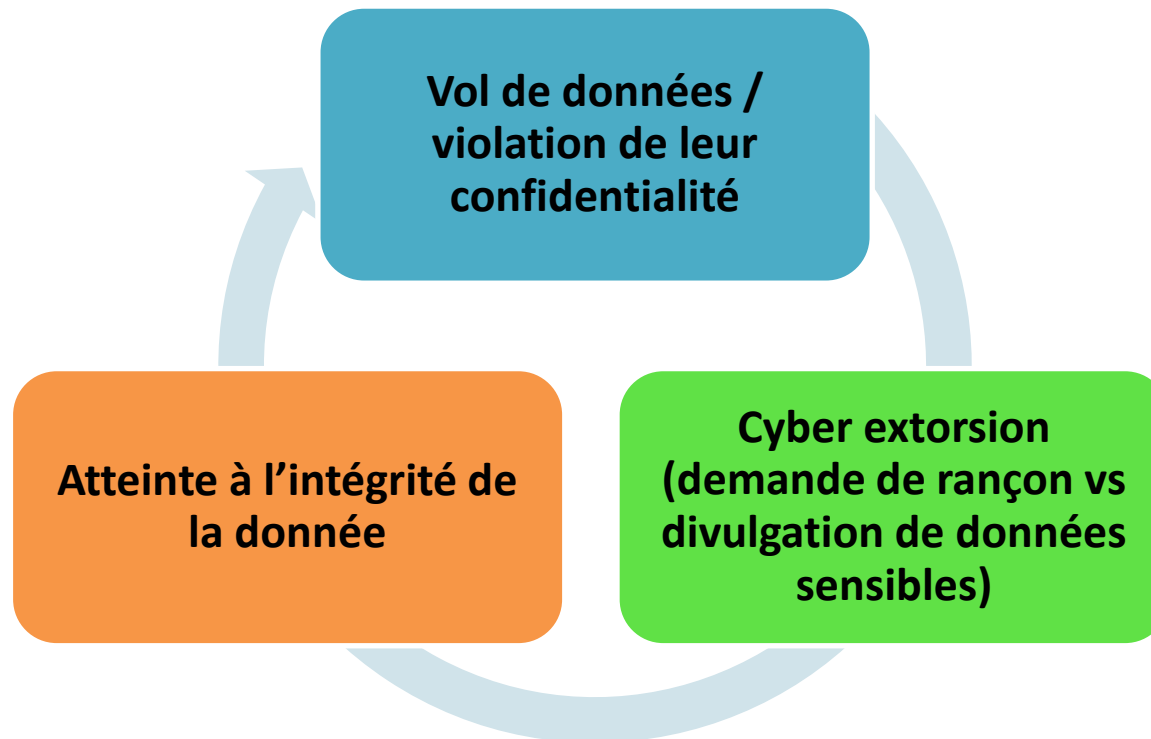


# Le contrôle de la qualité des données : les enjeux

- Une vigilance renforcée est indispensable face aux nouveaux enjeux des systèmes d'information



❑ **Les risques de cyber-attaques comme problématique de la gouvernance des données**



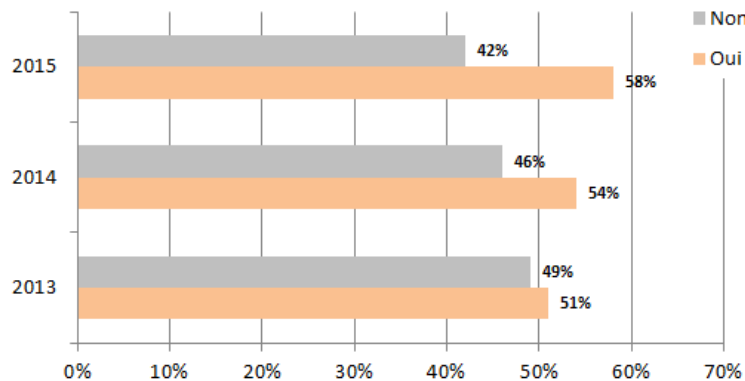
# Sommaire

1. La qualité des données : quels enjeux ?
2. **État des lieux de la qualité des données et des systèmes d'information (enquête ACPR 2016)**
3. Principaux constats des contrôles sur place de l'ACPR
4. Éclairage international

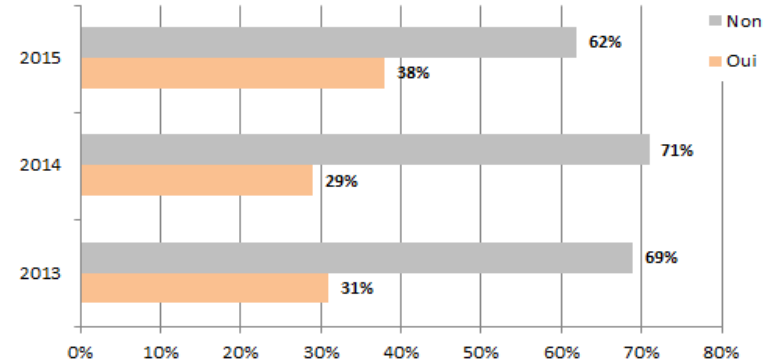
# En dépit des progrès réalisés, la qualité des données des organismes d'assurance n'est pas encore satisfaisante

## □ Pour mémoire, résultats des enquêtes de préparation à Solvabilité II (2013-2015)

Existence d'un système de gouvernance des données



Existence d'une politique formalisée de qualité des données



## □ Résultats de l'enquête ACPR 2016 sur les systèmes d'information et la qualité des données

- Absence de politique de qualité des données (QDD) pour 10 % des déclarants
- Plus de la moitié des organismes se disent encore « peu matures » dans ce domaine
- 5 % déclarent ne pas évaluer la qualité des données utilisées pour le calcul des provisions techniques (non conforme à l'art. 272 du règlement 2015/35)

# En dépit des progrès réalisés, la qualité des données des organismes d'assurance n'est pas encore satisfaisante

- ❑ Résultats de l'enquête ACPR 2016 sur les systèmes d'information et la qualité des données (suite)

**Seule la moitié des organismes évaluent la qualité des données à hauteur de plus de 50 % de leurs provisions techniques** : d'une manière générale, l'évaluation de la QDD n'est réalisée que sur une partie de la chaîne de traitement

**La fréquence d'évaluation de la QDD est insuffisante pour 1/3 des organismes « matures » et « très matures »**

**Les indicateurs de QDD ne sont pas remontés aux dirigeants pour environ la moitié des organismes**

- ❑ La comparaison des réponses au questionnaire avec les constats des contrôles sur place fait ressortir une **surévaluation de leur niveau de maturité par nombre d'organismes**

# La sécurité des SI à l'épreuve des chiffres...

## ❑ Les cyber-attaques

- ✓ Une très large majorité d'entreprises ont été victimes d'attaques, notamment victimes d'attaques par usurpation d'identité
- ✓ Une très large majorité d'entreprises victimes d'attaques ont effectué des tests d'intrusion depuis le 1er janvier 2015
- ✓ 2/3 des répondants recensent les cyber menaces dont ils peuvent être victimes

## ❑ **3/4 des répondants disposent d'un responsable de la sécurité opérationnelle du SI (RSI) et d'un responsable de la sécurité du SI (RSSI)**

## ❑ **Chez seulement 1/3 des répondants, le RSSI est indépendant du DSI (fort taux d'abstention pour la réponse à cette question)**

## ❑ **Une très faible minorité d'organisme ne possède pas politique de sécurité du SI, les 3/4 des entreprises se déclarent (très) matures sur ce sujet**

# Sommaire

1. La qualité des données : quels enjeux ?
2. État des lieux de la qualité des données et des systèmes d'information (enquête ACPR 2016)
3. **Principaux constats des contrôles sur place de l'ACPR**
4. Éclairage international

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

**Une meilleure identification des données utile à la fabrication des états réglementaires et en particulier au calcul des SCR/MCR et des provisions** (articles 219, 244 et 265 du règlement 2015/35 UE)

**Une responsabilisation des acteurs concourant à leur production** (article R.354-6 du code des assurances)

**Une priorisation des données utilisées en fonction de leur matérialité dans le calcul des états réglementaires**

**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**



# Mais d'importantes marges d'amélioration demeurent en matière de gouvernance

- ❑ Prise de **conscience tardive** du sujet
- ❑ **Intégration insuffisante** à la gouvernance d'ensemble et sensibilisation insuffisante de l'AMSB
- ❑ Définition peu fréquente des **acteurs cibles** de la gouvernance
- ❑ **Interactions informatique / métiers insuffisantes**
- ❑ Un **dispositif de gestion** de la qualité des données au périmètre souvent incomplet
- ❑ Un **défaut d'urbanisation** des systèmes d'information pénalisant la qualité des données

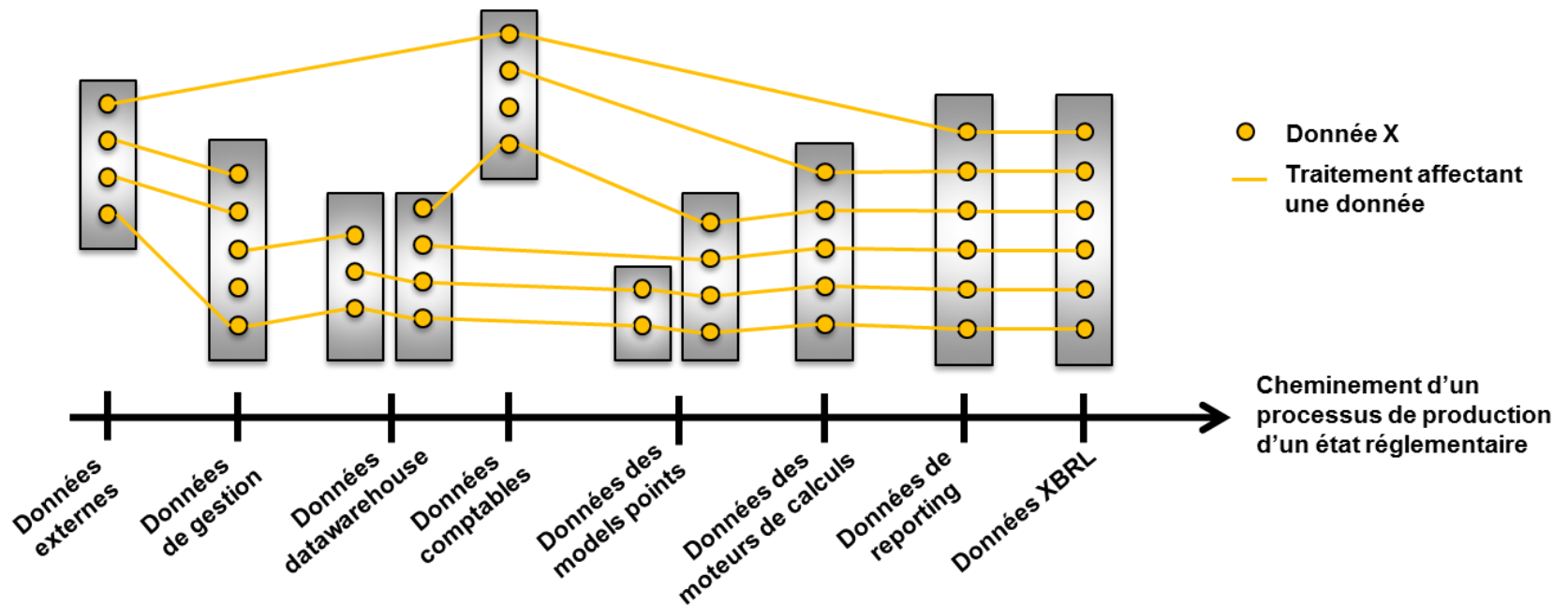
# Le dispositif de gestion de la qualité est souvent limité à l'aval des processus

- ❑ **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)
  - ✓ Les prestations de service doivent être davantage contractualisées...
- ❑ Concernant les **systèmes de gestion et datawarehouses internes** :
  - ✓ **La saisie des données** (contrats / sinistres) fait encore 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 A.343-1 du code des assurances)

**Ces deux écueils sont d'autant plus prégnants  
dans le cas du « big data »**

# Les bonnes pratiques de gestion de la QDD

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



# Des traitements actuariels manuels fréquemment 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)

# Ces faiblesses traduisent 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 l'**exhaustivité, l'exactitude et le caractère approprié** de la donnée
  - ✓ Problème de **disponibilité de la donnée**, complexifiant le respect des délais de livraison des états réglementaires mais également l'atteinte des exigences en matière de **lutte contre le blanchement et le financement du terrorisme** (article A.310-8 du code des assurances)

# La qualité des dernières déclarations reçues par le SG ACPR confirme ces constats

- ❑ **Reporting Day One** : nombreuses resoumissions suite à des problèmes de rejet (cf. LEI)
  
- ❑ **Reporting trimestriel** : trois points d'attention
  - ✓ Organismes solos exemptés de *reporting* trimestriel (QRS) et qui doivent remettre un MCR (10 % d'absents)
  - ✓ Taux d'absence élevé préoccupant concernant le *reporting* trimestriel groupe (plus de 30 %)
  - ✓ Remise des données du T3 problématique (à remettre avant le 25 novembre) : 20 % d'absents (fin novembre) ou invalides (absence de signature électronique) : cf. droits à signer

# Sommaire

1. La qualité des données : quels enjeux ?
2. État des lieux de la qualité des données et des systèmes d'information (enquête ACPR 2016)
3. Principaux constats des contrôles sur place de l'ACPR
4. **Éclairage international**

# Éclairage international

- **Des exigences croissantes concernant la qualité des données et les systèmes d'information**
  - ✓ **des autorités de régulation financière internationales** (G20, Comité de stabilité financière, IAIS, FMI, BCE ...), notamment pour les acteurs systémiques
  - ✓ **de l'EIOPA :**
    - Au sein du *IT Data committee* : groupe de travail EIOPA/superviseurs nationaux sur l'exploitation des données remises : échanges de bonnes pratiques entre superviseurs sur les contrôles qualité des données transmises à l'EIOPA
    - Sujet majeur dans le dispositif de supervision et du processus de contrôle (*Handbooks SRP*)
    - Sujet transversal, traité notamment dans de nombreuses orientations (système de gouvernance, calcul des provisions techniques ...)



# Éclairage international

## □ EIOPA : Orientations sur le système de gouvernance

### ✓ Guideline 47 – Coordination du calcul des provisions techniques

Justification des modifications sur les données affectant le montant des provisions techniques

### ✓ Guideline 48 – Qualité des données

Évaluation de la cohérence des données internes et externes utilisées dans le calcul des provisions techniques au regard des standards de qualité de données. Implication de la fonction actuarielle au niveau des procédures internes permettant l'amélioration de la qualité des données.

### ✓ Guideline 53 – Procédure de contrôle de la qualité des données

Mise en place de procédures de contrôle pour mesurer la qualité des données et identifier toute déficience :

- Exhaustivité des données
- Caractère approprié (données internes et externes)
- Revue indépendante et vérification de la qualité des données

# Éclairage international

## ❑ Pour mémoire du côté bancaire : *Basel Committee of Banking Supervision (BCBS) 239*

### *“Principles for effective risk data aggregation and risk reporting”*

- ✓ Toute banque devrait : concevoir, mettre en place et gérer une architecture des données et une infrastructure informatique lui permettant de renforcer ses capacités d'agrégation des données de risque
- ✓ pouvoir produire des données exactes et fiables sur les risques pour satisfaire aux exigences d'exactitude applicables aux notifications, en temps normal comme en période de tensions ou de crise (**exactitude** et **intégrité**),
- ✓ pouvoir saisir et agréger toutes les données relatives aux risques significatifs encourus par le groupe (**exhaustivité**),
- ✓ rapidement produire, agréger et mettre à jour des données sur les risques tout en respectant les principes d'exactitude, d'intégrité, d'exhaustivité et d'adaptabilité...