Le Cloud Computing ou l'informatique « en nuage »: Approches en matière de réglementation et de contrôle

A2ii – IAIS Consultation téléphonique

28 novembre 2019

Présentatrices

Expert technique

Andrea Camargo
Director, Inspowering
Expert technique, A2ii

Paulo Miller
Head of the Office of studies and Institutional relations
SUSEP, Brazil

Modérateur

Mariella Regh
Access to Insurance Initiative (A2ii)

Financial Stability Institute | BIS

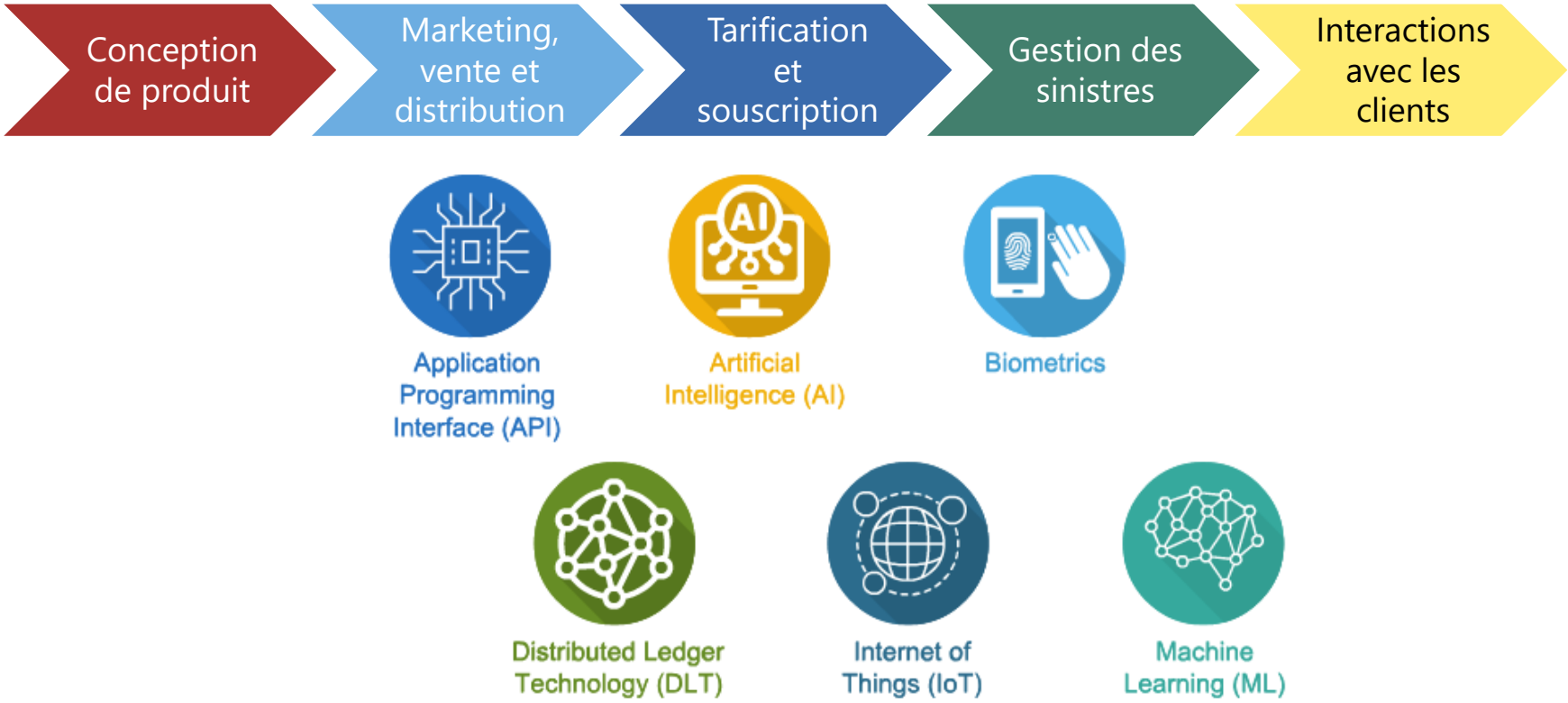
Le *Cloud Computing* ou les services informatiques dématérialisés « dans le nuage » : Approches en matière de réglementation et de surveillance

Consultation téléphonique de l'A2ii/AICA

Le 28 novembre 2019

Denise Garcia Ocampo, Conseillère principale chez FSI*

Entrée du secteur d'assurance dans le monde du numérique



Fournisseurs tiers de technologies et de services informatiques dématérialisés (ex.)

LÉGENDE:

Digital claims prevention Prévention numérique des sinistres

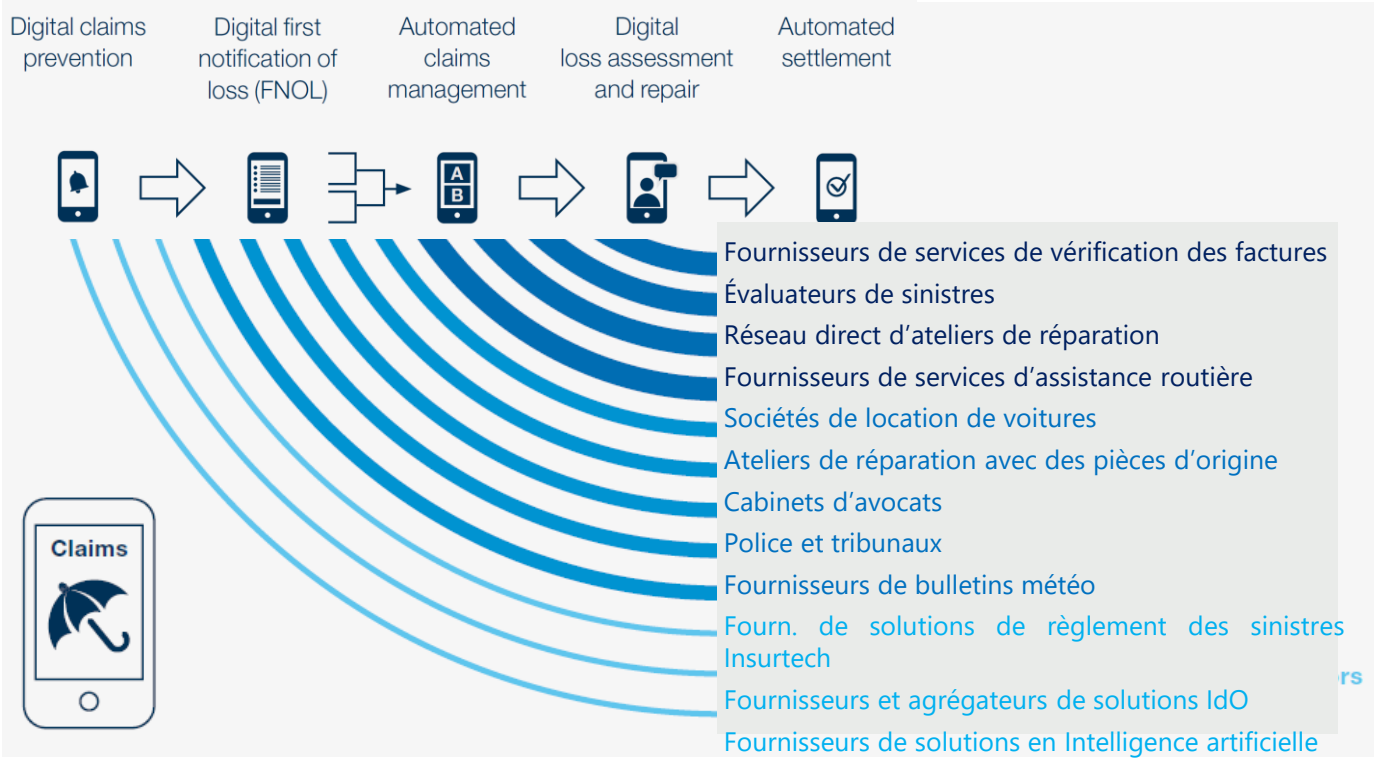
Digital First notification of loss: Premier avis de sinistre envoyé numériquement

Automated claims management: Gestion automatisée des réclamations

Digital loss assessment and repair: Évaluation et réparation des pertes numériques

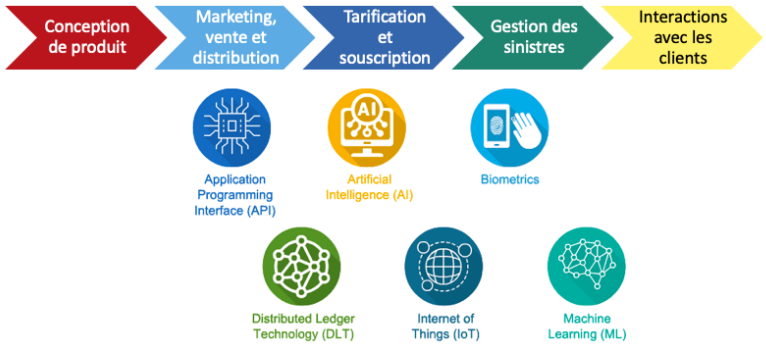
Automated settlement: Règlement automatisé

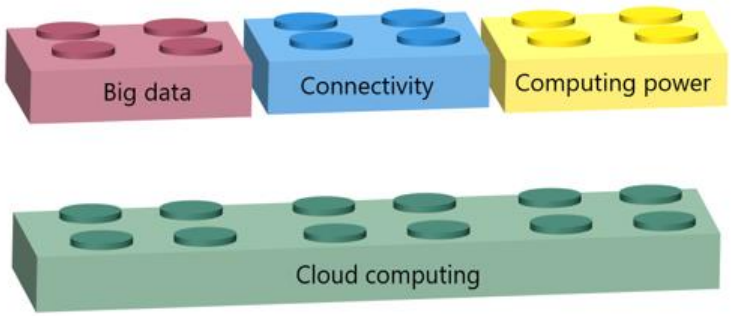
Claims : Déclarations de sinistre



Source: L'assurance numérique en 2018 : Un impact non négligeable grâce aux technologies numériques et de mesures analytiques, McKinsey & Company

L'informatique dans le nuage comme moteur de l'innovation





5 caractéristiques du nuage :

- Libre-service sur demande
- Vaste réseau de service
- Mise en commun des ressources (ou « multilocation »)
- Souplesse et rapidité
- Service entièrement géré

4 modèles de déploiement :

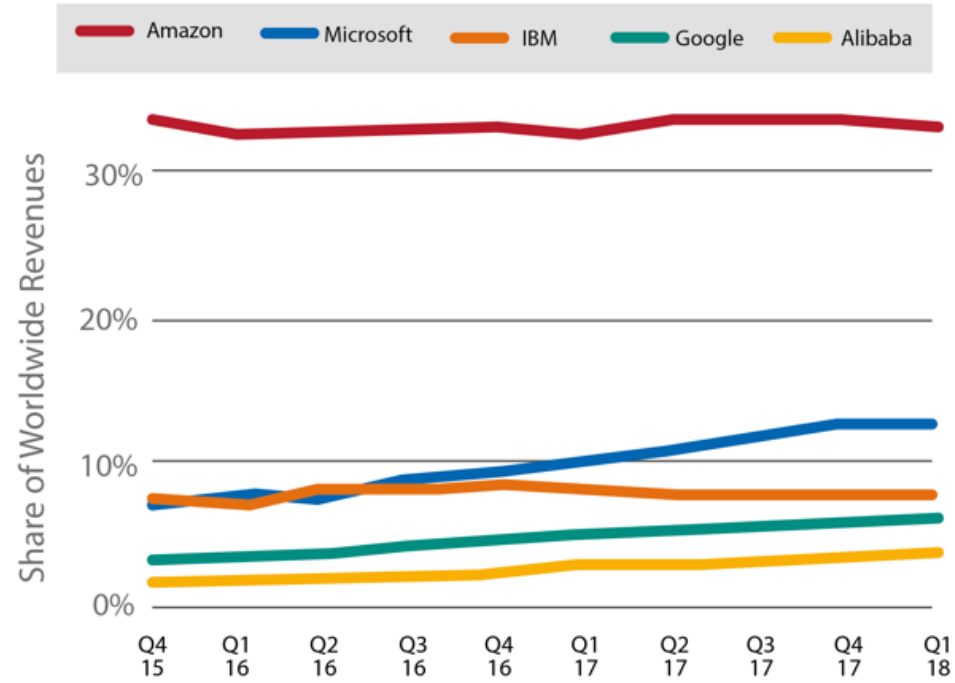
- Nuage grand public
- Nuage hybride
- Nuage collectif
- Nuage privé

3 modèles de services

- L'infrastructure en tant que service
- La plate-forme en tant que service
- Le logiciel en tant que service

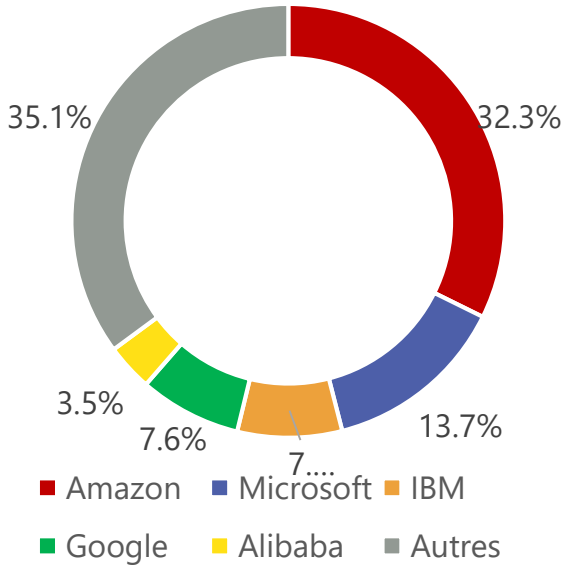
Fournisseurs de services dématérialisés

Market share trend of cloud infrastructure services (IaaS, PaaS & Hosted Private Cloud)



Source: Synergy Research Group

Part de marché, T1 2018



Où se situe ce « nuage » ?

Avantages et risques potentiels des services informatiques dans le nuage

- Rentable
- Efficacité accrue
- Flexibilité
- Évolutivité
- Mise sur le marché plus rapide / catalyseur d'innovation
- Renforcement de la sécurité pour les petites entreprises

- Cybersécurité et protection des données
- Gouvernance
- Aspects juridiques et de conformité
- Concentration
- Recrutement et substituabilité des fournisseurs
- Continuité des activités

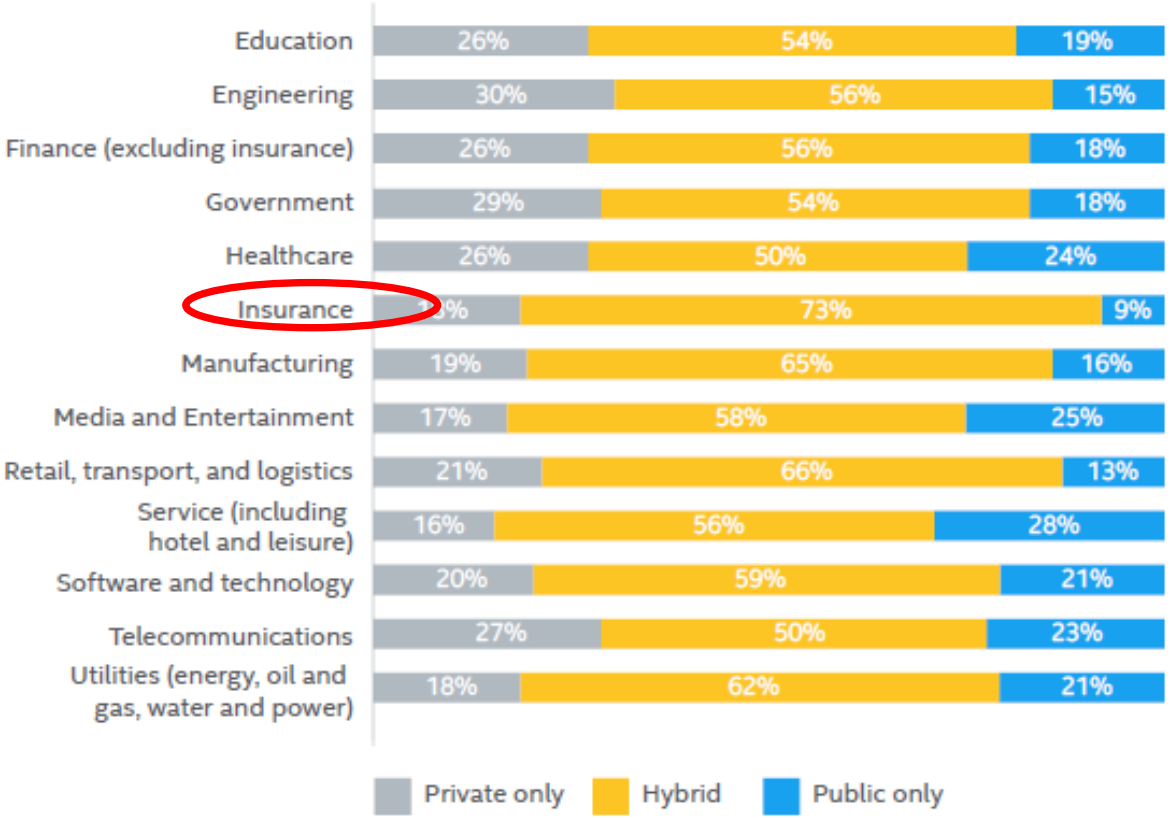
Utilisation du cloud dans le secteur des assurances

L'**adoption de** l'informatique en nuage a connu une **croissance** constante dans tous les secteurs de l'économie.

Dans le secteur de l'**assurance**, les technologies du Cloud sont en général utilisées:

- Énormément par les **nouveaux arrivants** et par un marché de **niche** pour certaines fonctions **critiques**
- Principalement par les **grands établissements** pour effectuer des fonctions **non critique**s

Architecture en nuage par secteur d'activité (2017)



Source: Building trust in a Cloud Sky, Cloud Security Alliance

Document de *FSI Insights* sur les services informatiques dématérialisés

par Juan Carlos Crisanto, Conor Donaldson, Denise Garcia et Jermy Prenio

www.bis.org

Sur la base de renseignements disponibles pour le grand public et d'entretiens menés auprès de 14 autorités établies en Asie, en Europe et en Amérique du Nord, ce document présente des **idées** clés sur les tendances en matière de **traitement prudentiel** de l'informatique dématérialisée dans le secteur de l'**assurance**.

Approches réglementaires

Règlementation et principes de l'autorité de surveillance s'appliquant à l'externalisation dans le nuage

Cadres de l'information	Externalisation		Gouvernance et gestion des risques		Sécurité	
	Principes généraux	Spécifique au Cloud	Principes généraux	Spécifique au Cloud	Principes généraux	Spécifique au Cloud
APRA					*	
OSFI						
EIOPA						
ACPR						
BaFin					*	
HKIA						
IRDAI						
DNB						
SAMA						
MAS[37]						
FINMA						
FCA						
PRA						
NAIC						

*Processus consultatif en cours

Réglementation générale

Disposition portant spécifiquement sur le Cloud

Réglementation générale comportant une disposition spécifique sur le Cloud Computing

Exigences réglementaires relatives aux services informatiques dématérialisés

1. Évaluation de l'importance relative, du caractère critique ou de l'importance
2. **Gouvernance**
3. Procédure de vérification préalable (*Due diligence*)
4. **Évaluation des risques**
5. **Protection des données et sécurité de l'information**
6. Lieu
7. Sous-traitance
8. **Continuité des activités et stratégie de sortie**
9. Surveiller et contrôler
10. Audit et droits d'accès

Gouvernance

Spécifique aux réalités du Cloud

Le Conseil d'administration et la Direction générale doivent:

- définir l'**orientation technologique** et les **objectifs de l'entreprise** en y prenant soin d'y intégrer la possibilité d'externaliser **concrètement** les services vers le « nuage »
- pour ce qui est de la gestion des risques liés à la technologie du Cloud:
    - Répartir les **responsabilités**
    - Définir l'**organigramme** et la **structure opérationnelle**
    - Doter le **personnel** des **qualifications** et des **moyens** adaptés

Évaluation des risques

Spécifique aux réalités du Cloud

L'évaluation des risques sur les **questions liées aux données** devra prendre en compte :

- **l'identification, la classification** et **l'importance** des données stockées et traitées dans le nuage
- l'identification des **dangers** relatifs à la **confidentialité**, à la **disponibilité** et à la **sécurité** de ces données
- l'évaluation des **répercussions** des **fuites de données**

L'APRA recommande d'effectuer des **analyses de scénario** sur tout événement susceptible de compromettre la confidentialité, l'intégrité et la disponibilité des données stockées dans le nuage.

Protection des données et sécurité de l'information

Spécifique aux réalités du Cloud

Les assureurs doivent comprendre la **nature** et la **force** des **contrôles des fournisseurs de services informatiques « dans le nuage »** (sécurité physique des centres de données, mesures de cybersécurité, etc.)

L'APRA, l'ACPR, l'IRDAI, la SAMA et le MAS recommandent que les ententes d'impartition comprennent des politiques et des procédures sur la **classification**, la **séparation**, la **sécurité**, la **conservation**, la **prévention des pertes** de données, mais aussi la **notification** des incidents**, la récupération** et la **destruction** des données.

L'APRA souligne l'importance de **répartir les responsabilités**.

Le BSIF recommande de mettre en place des processus pour que les **cyberincidents soient rapidement signalés.**

Continuité des activités et stratégie de sortie

Spécifique aux réalités du Cloud

Toute entente d'impartition doit inclure la **durée maximale de l'interruption du système** et la **perte maximale de données permise**.

Deux **éléments** clés de la **stratégie de sortie** pour les accords de stockage de données dans le nuage :

- la **suppression** et l'**effacement** complets des données de tous les emplacements où elles sont stockées, gérées ou traitées ;
- La capacité (définie clairement) de l'établissement contrôlé à **réabsorber** l'activité externalisée (reprendre son contrôle).

Les conditions de **réversibilité** doivent être définies à la signature de l'accord d'externalisation, y compris le format des données restituées et/ou leur destruction.

Communication autour du plan de services du Cloud

Communication de la stratégie de cloud à l'autorité			
	Notification		**Consultation ou autorisation**
APRA	Oui, pour les ententes d'impartition comportant de faibles risques inhérents à l'informatique dans les nuages.	**Consultation, pour des dispositions d'externalisation impliquant des activités matérielles lorsqu'il s'agit d'activité offshore et pour des dispositions impliquant des risques inhérents ou exacerbés par les technologies du Cloud, qu'il s'agisse d'activités offshore ou non.**	
OSFI	Non	Non	
EIOPA	Oui, pour les ententes d'impartition portant sur des fonctions critiques ou importantes.	Non	
ACPR	Oui, pour les ententes d'impartition portant sur des fonctions critiques ou importantes.	Non	
BaFin	Oui, pour les ententes d'impartition portant sur des fonctions critiques ou importantes.	Non	
HKIA	Oui, pour les ententes d'impartition de matériel.	Non	
IRDAI	Non	Non	
DNB	Oui, pour les ententes d'impartition de matériel.	**Une certaine forme de consultation est exigée.**	
SAMA	Non	**Autorisation, pour toute externalisation matérielle et pour tout accord de service dans le Cloud.**	
MAS	Non	Non	
FINMA	Non	**Autorisation, pour les accords d'externalisation impliquant des fonctions importantes ou de contrôle en rapport avec le plan d'entreprise.**	
FCA	Oui, pour les ententes d'impartition de matériel.	Non	
PRA	Oui, pour les ententes d'impartition portant sur des fonctions critiques ou importantes	Non	
NAIC	**Non**	**Non**	

Pratiques en matière de contrôle

- Supervision au titre du **risque opérationnel** selon une approche **axée sur le risque**
- Les inspections sur site comprennent l'examen des éléments suivants
  - Les **justificatifs** documentés à l'appui de l'entente d'impartition (processus de vérification préalable, évaluation des risques de l'activité à impartir)
  - Évaluer les **processus** de l'assureur liés à la gestion de la cybersécurité, au contrôle des rapports et des contrôles, et aux plans de continuité des opérations
- Les examens hors site mettent l'accent sur l'évaluation des pratiques de gouvernance et de gestion des risques de l'assureur
  - Fichier de **notification** ou de **validation**
  - Information du **public** (notamment les certifications et les rapports d'assurance du CSP)
  - **Rapports** réglementaires (ex : politique d'externalisation, ORSA, rapports d'externalisation)
  - **Demandes** spécifiques (examens thématiques, questionnaires)

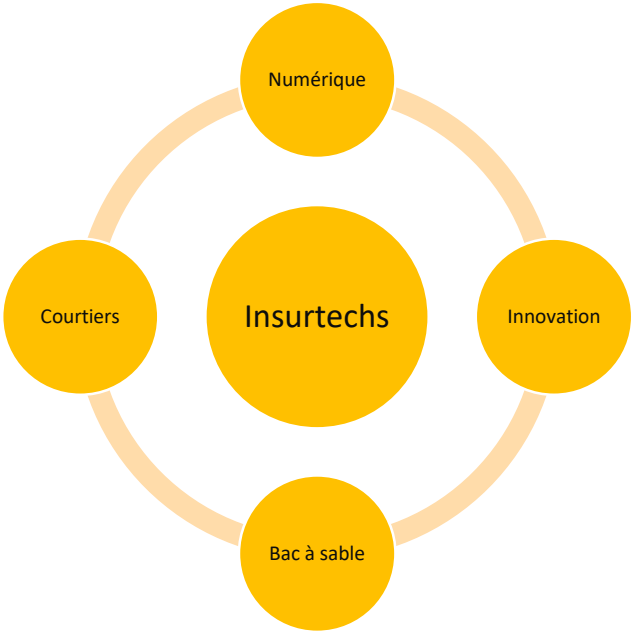
Conclusions

- Il est utile de **clarifier les attentes en matière de réglementation** afin :
  - d'examiner les **risques particuliers** potentiels relatifs aux processus de l'informatique « dans le nuage »
  - De fournir un niveau raisonnable de **certitude réglementaire** en ce qui concerne l'utilisation de ces services dématérialisés
  - **D'assister** les acteurs du marché dans l'**adoption responsable** de cette technologie
- Considérations relatives aux cadres réglementaires : **fondés sur des principes, neutres sur le plan technologique, cohérents** entre les secteurs financiers et appliqués sur une base **proportionnelle**
- La **coopération internationale** entre les autorités du pays d'origine et du pays d'accueil, en particulier par le **partage d'**informations pertinentes sur les **CSP**, est particulièrement importante lorsqu'il s'agit d'assurer un **contrôle** efficace des activités d'informatique dans le nuage.

Aperçu de l'informatique en nuage dans le secteur des assurances au Brésil

Novembre - 2019

Que se passe-t-il au Brésil?



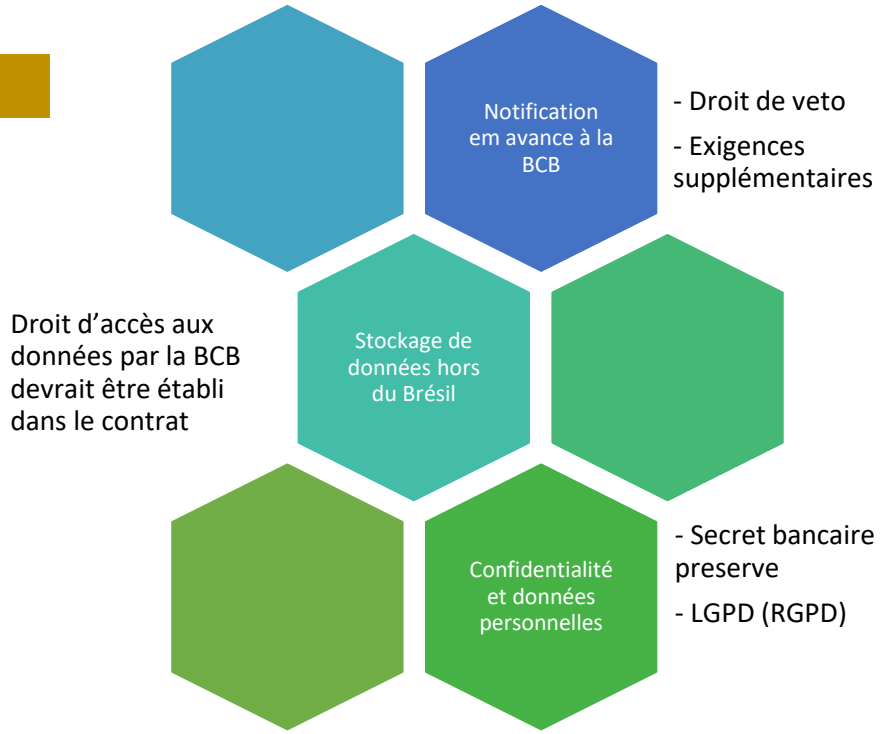
Nuage

- Évolutivité
- Securité
- Tranquillité

SUSEP

Règlement de référence - Banques

Res CMN nº 4.658/2018



SUSEP

Quoi d’autre?

- Concurrence des fournisseurs de services
  - Amazon, Microsoft, Google et ???
  - Problèmes lors de migration entre fournisseurs
- Système d'enregistrement des opérations
- LGPD (RGPD – Loi nº 13.709/2018)
  - Création de l’Agence National de Données Personnelles
  - Exigences supplémentaires

SUSEP

Merci

Merci!

Follow us on Twitter @a2ii_org, Youtube and LinkedIn