access to insurance initiative

Cloud Computing: Regulatory and Supervisory Approaches

A2ii – IAIS Consultation Call

28 November 2019

Expert

Denise Garcia Ocampo

FSI, Senior Advisor

Supervisory Presenter

Gustavo Adolfo Araujo Caldas
Technical Analyst
SUSEP, Brazil

IAIS representative

Alessandro Nardi
International Association of Insurance Supervisors (IAIS)

Moderator

Janina Voss
Access to Insurance Initiative (A2ii)

Financial Stability Institute | BIS

Cloud computing: Regulatory and supervisory approaches

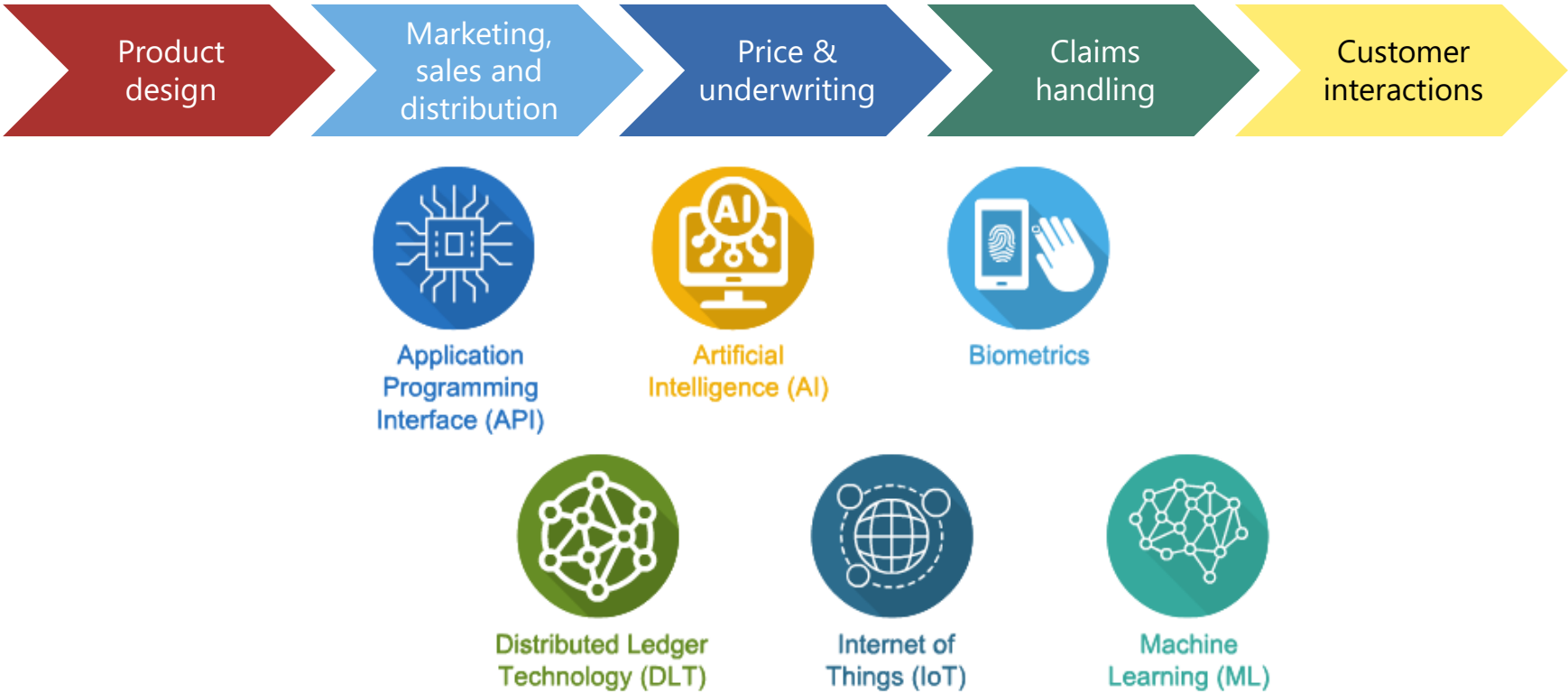
A2ii IAIS Consultation Call

28 November 2019

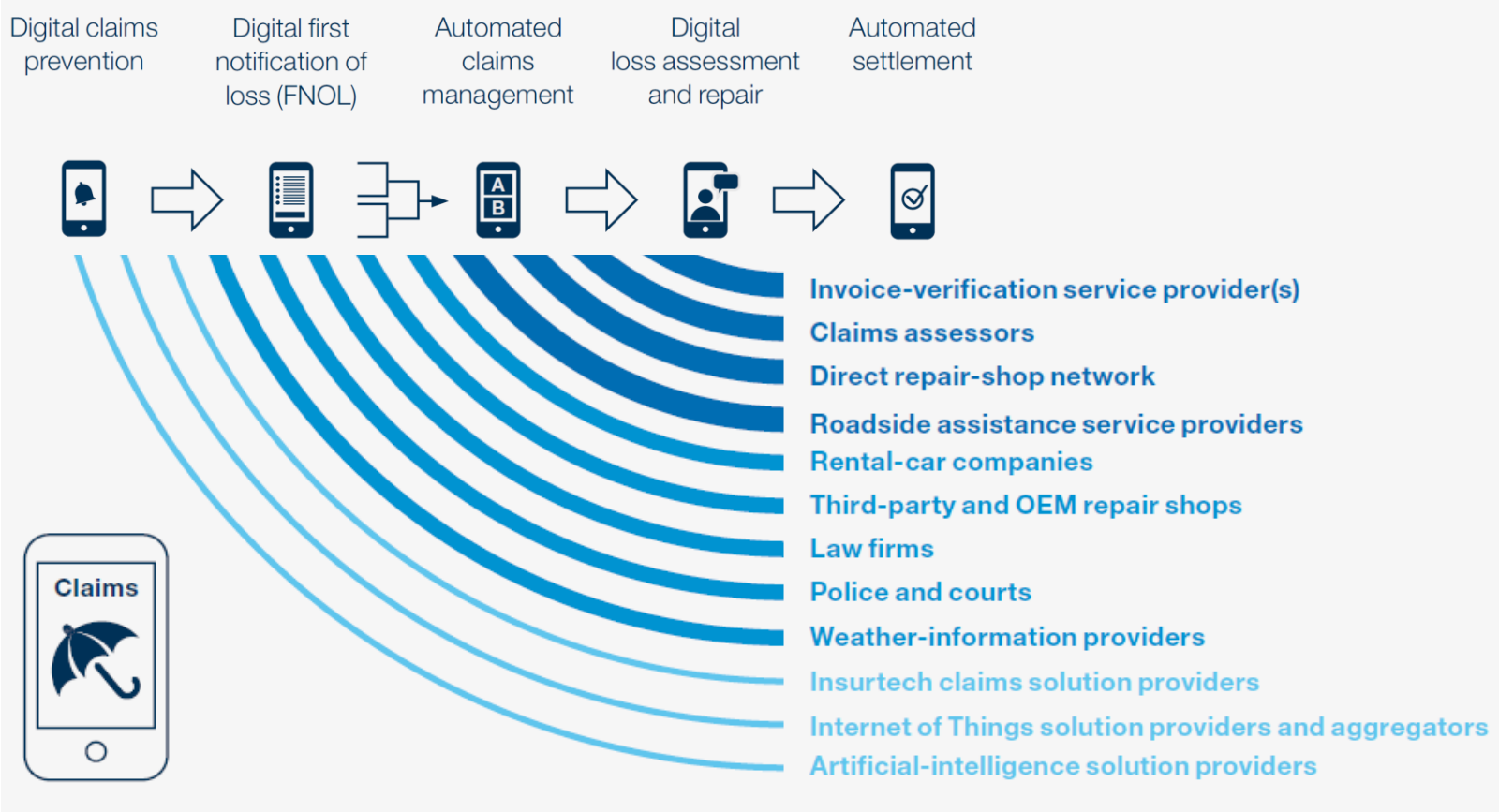
Denise Garcia Ocampo, FSI Senior Advisor*

**The views expressed in this presentation are those of the presenter and not of the BIS or the Basel-based committees.*
The views and the content of this presentation are to be used for the purposes of this meeting and must not be publicly quoted or disseminated without the authorisation of the presenter.

Digitalisation of the insurance business

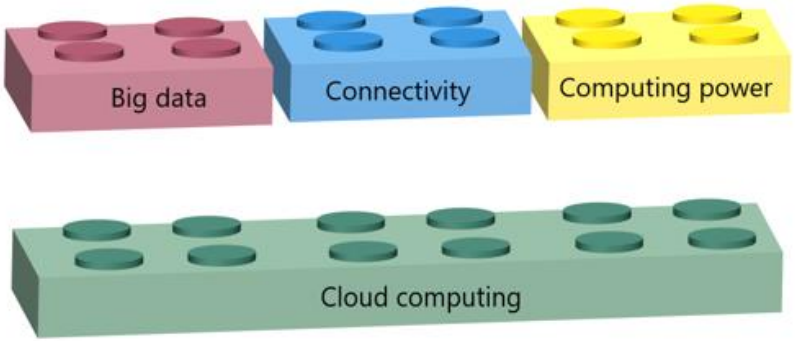


Digitalisation and technological third party providers – example



Source: Digital insurance in 2018: Driving real impact with digital and analytics, McKinsey & Company

Cloud computing as an enabler of innovation



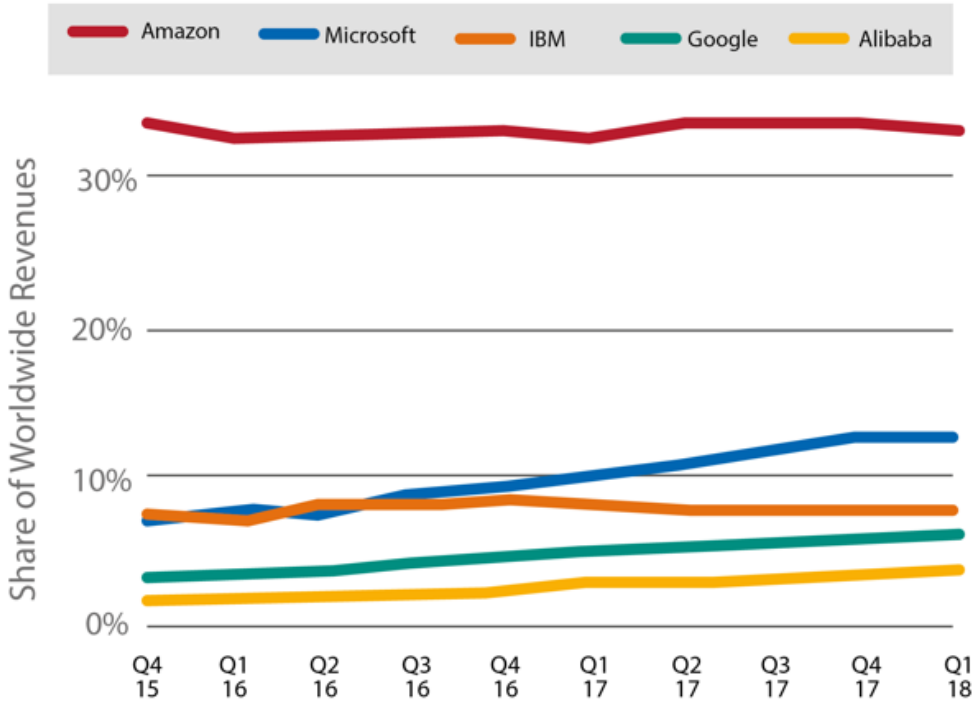
5 Characteristic of CLOUD
- On-demand Self-service
- Broad Network service
- Resource pooling (a.k.a Multi-tenancy)
- Rapid elasticity
- Managed Service

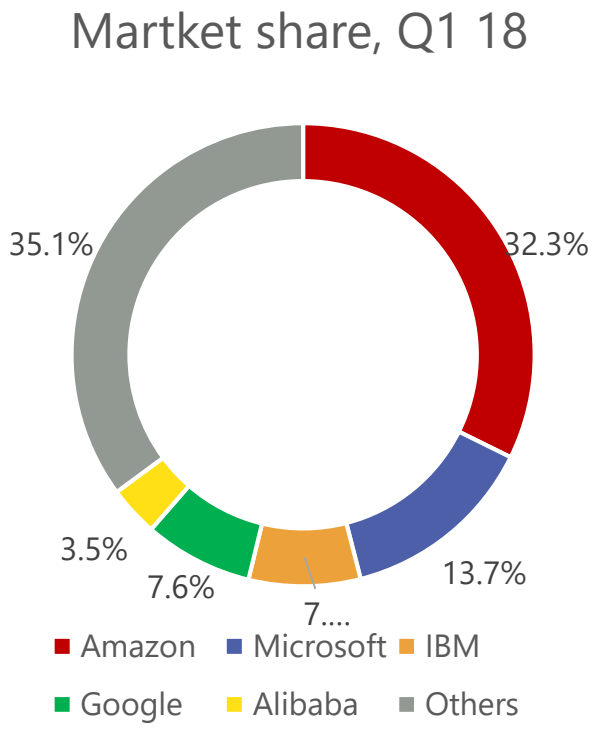
4 Deployment Models
- Public Cloud
- Hybrid Cloud
- Community Cloud
- Private Cloud

3 Service Models
- Infrastructure as a Service
- Platform as a Service
- Software as a Service

Cloud service providers

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





Source: Synergy Research Group

Where is the cloud?

Cloud potential benefits and risks

- Cost-effective
- Increased efficiency
- Flexibility
- Scalability
- Faster time to market – innovation enabler
- Improved security for small companies

- Cyber security and data protection
- Governance
- Legal and compliance
- Concentration
- Provider lock-in and substitutability
- Business continuity

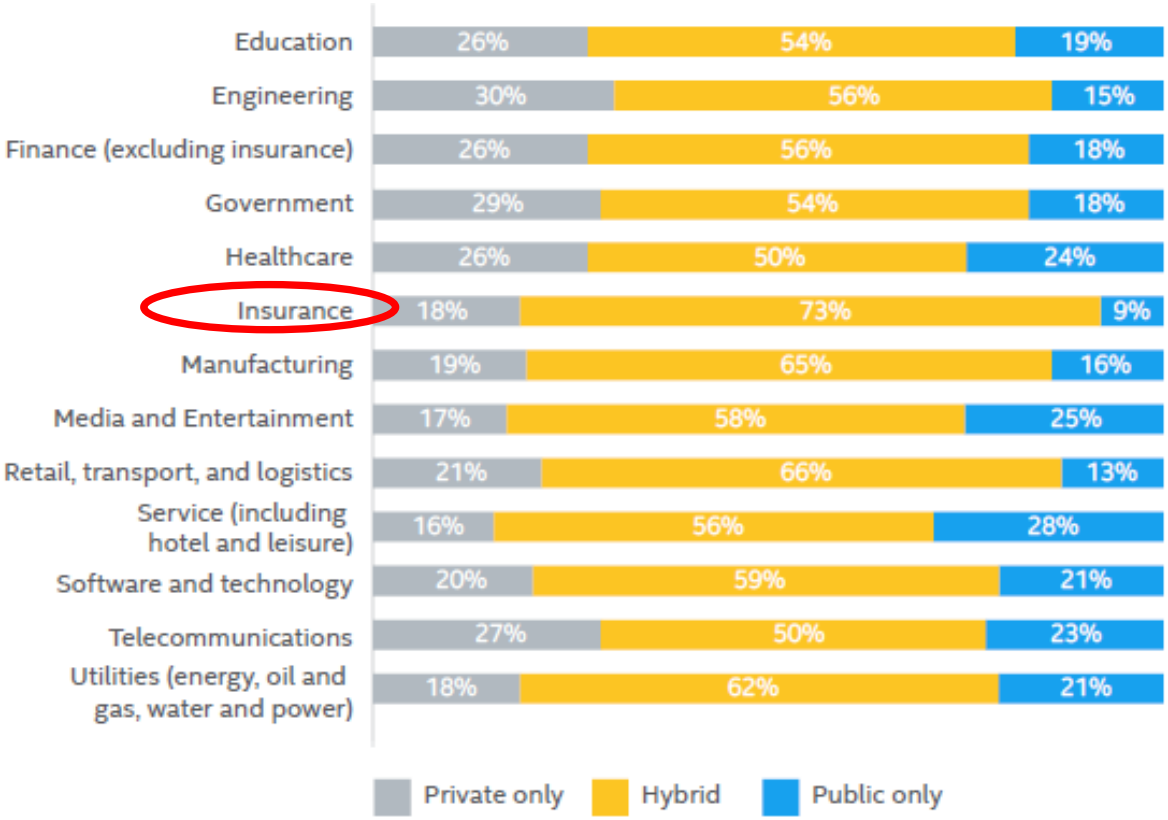
Cloud use in the insurance sector

Adoption of CC has been **growing** steadily in all sectors of the economy.

In the **insurance** sector, in general CC is used:

- extensively by **newcomers** and by a **niche** of the market for **critical** functions
- mostly used by **larger institutions** for **non-critical** functions.

Cloud architecture by industry, 2017



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

FSI Insights paper on cloud computing

by Juan Carlos Crisanto, Conor Donaldson, Denise Garcia and Jermy Prenio

www.bis.org

Based on the public information and interviews to 14 authorities located in Asia, Europe and North America, this paper presents key **insights** on the emerging **prudential treatment** of cloud computing in the **insurance** industry.

Regulatory approaches

Supervisory authority regulations and statements applying to outsourcing to the cloud

Frameworks	Outsourcing		Governance and risk management		Information security	
	General	Cloud Specific	General	Cloud Specific	General	Cloud Specific
APRA					*	
OSFI						
EIOPA						
ACPR						
BAFIN					*	
HKIA						
IRDAI						
DNB						
SAMA						
MAS						
FINMA						
FCA						
PRA						
NAIC						

* Currently under consultation process.

General regulation | Cloud specific statement | General regulation with a specific section on cloud

Regulatory requirements for cloud computing

1. Assessment of materiality, criticality or importance
2. **Governance**
3. Due diligence
4. **Risk assessment**
5. **Data protection and information security**
6. Location
7. Subcontracting
8. **Business continuity and exit strategy**
9. Monitor and control
10. Audit and access rights

Governance

Cloud specific

Board and senior management should:

- define the **technological strategy** and **corporate objectives** including **material** outsourcing to the cloud
- for management of cloud computing risks:
    - allocate **responsibility**
    - define **organisational** and **operational structure**
    - ensure **staff** with sufficient **skills** and **resources**

Risk assessment

Cloud specific

Risk evaluation on **data-related issues** should take into account:

- **identification, classification** and **importance** of data stored and processed in the cloud
- identification of **risks** related to **confidentiality**, **availability** and **security** of such data
- evaluation of **impacts** of data **breaches**

APRA recommends use of **scenario analysis** on events that may compromise confidentiality, integrity and availability of data stored in the cloud.

Data protection and information security

Cloud specific

Insurers should understand the **nature** and **strength** of **cloud service provider's controls** (physical security of data centers, cyber security measures, etc).

APRA, ACPR, IRDAI, SAMA and MAS recommend that outsourcing agreements include policies and procedures on data **classification**, **segregation**, **security**, **retention**, **loss prevention**, incident **notification, recovery** and **destruction**.

APRA emphasises the importance of **allocation of responsibilities**.

OSFI recommends to have processes to ensure **timely notification of cyber incidents.**

Business continuity and exit strategy

Cloud specific

Outsourcing agreement should include **maximum duration of downtime** and **maximum allowable loss of data**.

Two key **elements** of the **exit strategy** for cloud arrangements:

- complete **removal** and **deletion** of data from all locations where it is stored, managed or processed;
- define the supervised institution's ability to **re-absorb** the outsourced activity.

Conditions of **reversibility** must be defined when subscribing the outsourcing agreement including the format of returned data and its destruction.

Communication of cloud computing plan

	Notification	Consultation or Approval
APRA	Yes, for outsourcing arrangements involving cloud low inherent risks.	Consultation, for outsourcing arrangements involving material activities where offshoring is involved and for arrangements involving cloud heightened or extreme inherent risks regardless of whether offshoring is involved.
OSFI	No	No
EIOPA	Yes, for outsourcing arrangements involving critical or important functions	No
ACPR	Yes, for outsourcing arrangements involving critical or important functions	No
BAFIN	Yes, for outsourcing arrangements involving critical or important functions	No
HKIA	Yes, for material outsourcing arrangements	No
IRDAI	No	Approval, for all outsourcing arrangements involving core functions
DNB	Yes, for material outsourcing arrangements	No
SAMA	No	Approval, for material outsourcing and for any cloud service arrangement
MAS	No	No
FINMA	No	Approval, for outsourcing arrangements involving significant or control functions relevant to the business plan
FCA	Yes, for material outsourcing arrangements	No
PRA	Yes, for outsourcing arrangements involving critical or important functions	No
NAIC	No	No

Supervisory practices

- Supervised under **operational risk** following a **risk-based** approach
- On-site inspections include review of:
  - Supporting **documentation** of outsourcing agreement (eg due diligence, risk assessment of activity to be outsourced)
  - Assessing insurer's **processes** related to cyber security management, monitoring reports and controls, business continuity plans
- Off-site reviews focus on assessing insurer's governance and risk management practices
  - **Notification** or **approval** file
  - **Public** information (eg certifications and assurance reports of CSP)
  - Regulatory **reports** (eg outsourcing policy, ORSA, outsourcing reports)
  - Specific **requests** (eg thematic reviews, questionnaires)

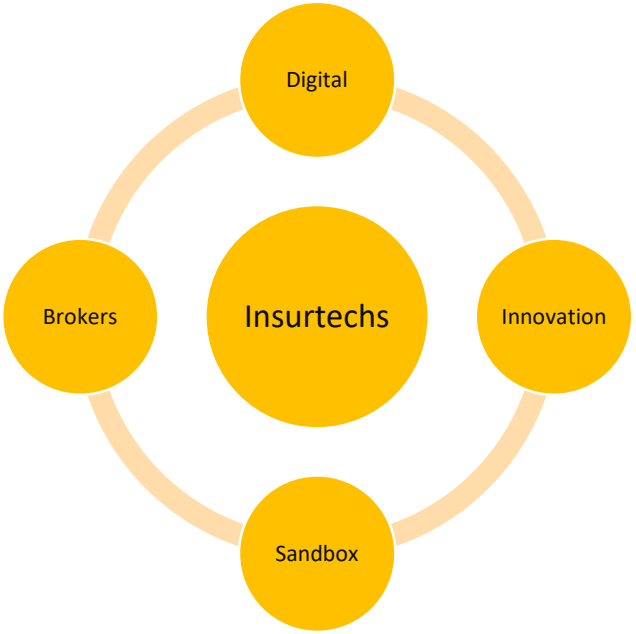
Key findings

- There is value in **clarifying regulatory expectations** in order to:
  - address the potential **specific risks** associated with cloud computing,
  - provide reasonable level of **regulatory certainty** with respect to the use of cloud services
  - **support** market participants in the **responsible adoption** of the technology
- Considerations for regulatory frameworks: **principled- based, technology neutral, consistent** between financial sectors and applied on a **proportionate** basis
- **International cooperation** among home and host authorities, in particular through **sharing** relevant information on **CSP**, is especially important when it comes to ensuring an effective **oversight** of cloud computing activities.

Overview of cloud computing in the brazilian insurance market

November - 2019

Context



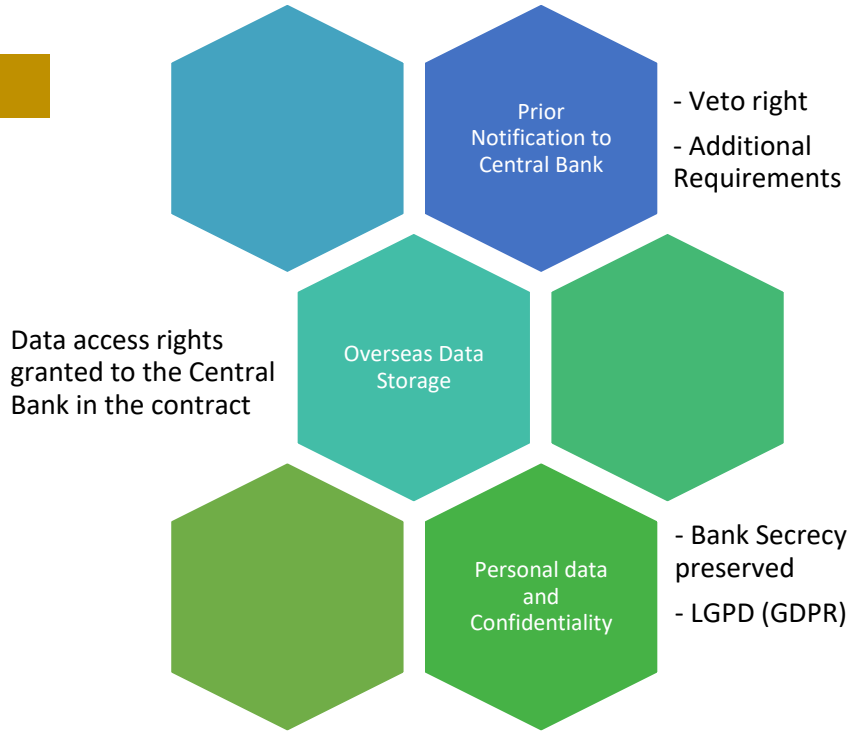
Cloud

- Scalability
- Security
- Focus on business

SUSEP

Benchmark - Banks

Res CMN nº 4.658/2018



SUSEP

What else?

- Service Providers Competition
  - Amazon, Microsoft, Google and ???
  - Migration issues between vendors
- Operations Registration System
- LGPD (GDPR – Law nº 13.709/2018)
  - Personal Data National Agency creation
  - Additional Requirements

SUSEP

Thanks

Thank you

Save the Date: Next Consultation Call on

30 January, 2020

Follow us on Twitter @a2ii_org, Youtube and LinkedIn