Financial Stability Institute | BIS

Putting cloud into a global perspective
*Emerging regulatory approaches**

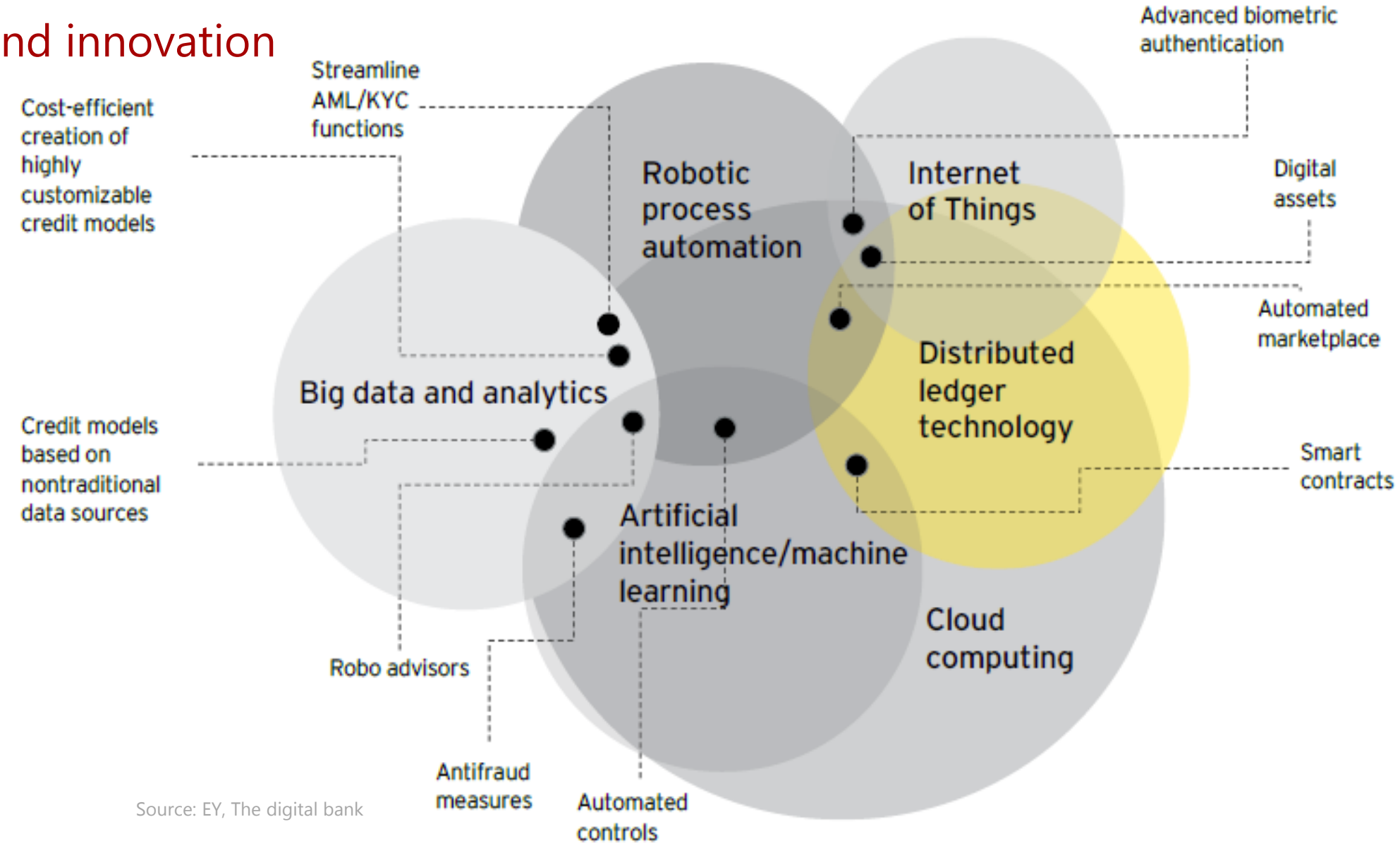
2nd EBF Cloud Banking Conference – Shaping a multi-cloud environment

Brussels, 9 July 2019

Denise Garcia Ocampo, Senior Advisor, FSI

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 conference and must not be publicly quoted or disseminated without the authorisation of the presenter.

Cloud and innovation



Source: EY, The digital bank

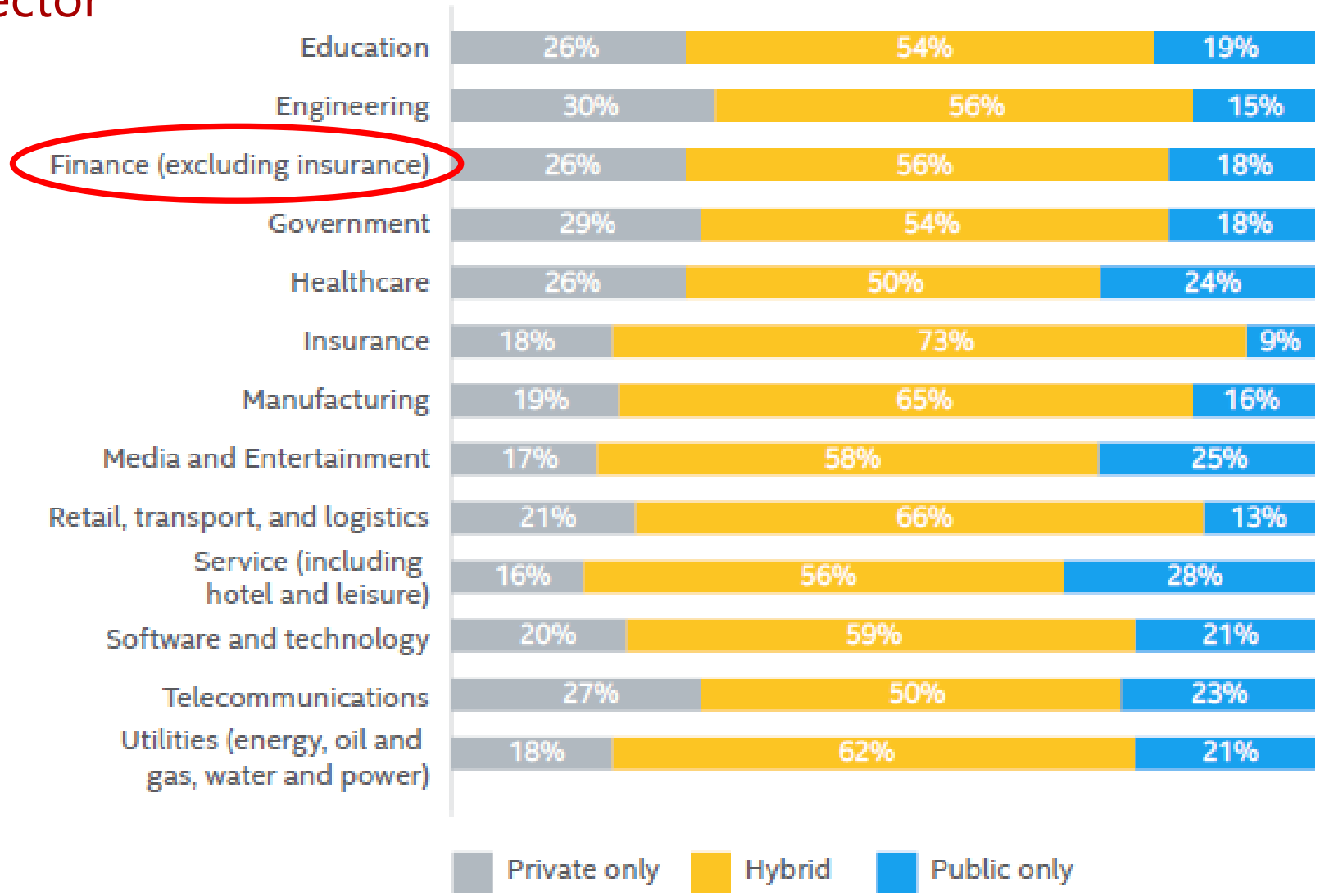
Cloud use in the financial sector

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

In the financial sector, in general CC is used:

- **extensively** by **newcomers** and by a **niche** of the market for **critical** functions
- **moderately** by **larger FI** for **non-critical** functions
- mostly implemented through **hybrid** deployment models and tending to use **multiple** CPS

Cloud architecture by industry, 2017



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

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 and management
- Legal and compliance
- Provider lock-in and substitutability
- Concentration
- Business continuity

Global perspective *(selected authorities)*
FSI Insights paper on regulatory and supervisory approaches to CC

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

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[37]						
FINMA						
FCA						
PRA						
NAIC						

* Currently under consultation process.

General framework | Cloud-specific statement | General framework with a specific section on cloud

Regulatory requirements

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

Assessment of materiality, criticality or importance

General	Cloud specific
Authorities use **different criteria** or consider different factors in assessing whether an outsourced activity or function is material, critical or important. Examples: • potential **impact** of any **failure** or **disruption** of the outsourced activity • **cost** of outsourcing • level of difficulty of finding an **alternative** provider or bringing the activity in-house **Customer-data** specific materiality criteria is not common.	MAS: FI's use of CC that involve the storage in the cloud of **customer information** would be considered as material outsourcing. APRA and ACPR: recommend to consider the **nature, sensitivity and criticality** of customer's data in the materiality assessment.

Data protection and information security

General	Cloud specific
Authorities require the **outsourcing agreement** to ensure that the **CSP** protects any **confidential information** related to the FI, its customers, employees, contracting parties and all other persons, establishing policies and procedures for disclosing information and monitoring security practices.	In general, authorities expect FI to understand the nature and strength of the **CSP's controls** on data **confidentiality, integrity and availability**. APRA, ACPR, IRDAI, SAMA and MAS: recommend that outsourcing **agreements** include policies and procedures on data **classification**, **segregation**, **security**, **retention** and **loss prevention**, **incident notification** and **destruction**. APRA: emphasises the importance of **allocation of responsibilities** (shared responsibility model).

Location

General	Cloud specific
Authorities expect FI to **assess risks** related to offshoring (eg country, compliance, legal risks). FINMA requires that insurers should **maintain** in **Switzerland** all **information** that could be needed for **resolution** purposes.	Most authorities recommend FI to have a **clear understanding** of the legal environment of the jurisdictions in which their data will be **stored, processed and managed**. In some cases, authorities require **authorisation** or **previous consultation** when cloud services are to be provided outside the jurisdiction. • IRDAI: requires that data be **hosted locally**. • APRA: recommends that supervised institutions consider the benefits of **Australian hosted options**, in the absence of any compelling business rationale to do otherwise. • FCA: requires FI to agree with the service provider on a **data residency policy.**

Business continuity and exit strategy

General

Authorities require FI to have arrangements in place to be able to **maintain** their **operations** if a **disruption** in the provision of outsourced services occur.

These arrangements are envisaged to include a business continuity plan and an exit strategy.

Cloud specific

Most authorities expect FI to **assess** their CSP plans and resources in ensuring continuity of operations, including their **recovery and resumption capabilities** (eg max downtime duration; max allowable loss of data)

Some authorities require specifically that FI should **define** and **test contingency plans** and **exit strategy** that takes into account:

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

Audit and access

General	Cloud specific
Authorities require the outsourcing contracts to clearly stipulate the **audit** requirements and **access rights** of the FI, its auditor or appointed representative and the supervisory authority. In general, authorities expect to be able to **request information** from service providers related to the functions or activities that are subject of the outsourcing agreement.	Some authorities have included **cyber** specific **requirements**: • SAMA requires that FI should have the right to perform a **cyber security audit** and a **cyber security examination** at the cloud service provider Some authorities are considering allowing FI to use **pooled audits.**

Communication of CC 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

Regulatory challenges

- 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
  - applied on a **proportionate** basis

Issues under discussion

- Identification of **globally important third party technology providers**
  - **Joint supervision** by **cross-sectoral authorities** from different jurisdictions
  - Establishment of arrangements similar to **supervisory colleges**
- Use of **pooled audits**
- Use of **external certifications**
- Issuing specific provider's **licenses**

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.

Final considerations

- To embrace CC, **financial institutions** must weigh opportunities and risks and set-up a **sound governance system** to **properly manage** cloud projects and to **adequately monitor** the cloud services on an on-going basis, under a clear understanding of the **shared responsibility model**.

- To succeed with the cloud, it is paramount that **CSP** not only tailor their services but also **adapt** their **contractual agreements** to the specific **nature** of the financial sector, given its relevance to the overall economic activity.

- To facilitate innovation in the financial sector, **policy initiatives** need to focus on financial institutions' **operational resilience** in order to maintain sound and safe institutions, protect consumers and maintain financial stability.

Thank you.

Denise.GarciaOcampo@bis.org

www.bis.org/fsi

www.fsiconnect.org