Outsourcing to the cloud and other IT service providers - emerging prudential approaches in the insurance industry

(Forthcoming FSI Insights)

Juan-Carlos Crisanto
Financial Stability Institute
Bank for International Settlements
July 2018
Background

- **Digitalisation** is affecting all areas of the **insurance value chain**

![Value Chain Diagram]

- Some insurance companies are **outsourcing all or parts of the value chain activities** to third-parties as part of innovation business strategies.

- Additionally, in order to enhance flexibility, gain scalability, access cutting-edge technologies and reduce costs, insurance companies are **outsourcing core functions to technological third-parties**, including **cloud providers**.

- **Risk management, actuarial function, internal audit**
- **Investment & HR management**
- **IT system management (data storage & processing)**
- **Back-office operations**
Motivation

- Outsourcing of core functions through cloud computing requires (re)assessing whether traditional (IT) outsourcing framework remains fit for purpose

- **Outsourcing to IT third-parties**, including **cloud providers** (eg collection, storage, process and analysis of personal data) can bring a number of **benefits** but also introduces/exacerbates **risks** related to, among others:
  - Data security (including cyber)
  - Data location and access
  - Integrity of information systems

- In light of the above, the **prudential oversight of cloud computing** is evolving

- Focus of **forthcoming FSI Insights**:
  - Describe **range of regulatory approaches and supervisory practices** to deal with outsourcing to the cloud and other IT providers in the insurance industry
Current IAIS workstreams on digitalisation that include third-party’s risks

- Draft application paper on the **use of digital technology in inclusive insurance**
- Draft issues paper on the **increasing use of digital technology in insurance and its potential impact on consumer outcomes**
- Draft application paper on **supervision of insurer cyber-security**
Forthcoming FSI Insights

● **Scope**
  - Reviewed approaches in 13 jurisdictions
    - General/specific frameworks, integrated/non-integrated authorities, geographical representation

● **Methodology**
  - Public information, pre-filled surveys and interviews

● **Timeline**
  - April – August 2018
Main general observations

- Cloud computing and outsourcing of other IT services to third-parties are generally treated as a form of (IT) outsourcing.
  - Therefore, supervised firms are typically subject to **prudential requirements applicable to (IT) outsourcing**
    - However, some authorities have issued **specific requirements or recommendations** related to third-party cloud computing services
  - Mostly supervised as part of **onsite/offsite frameworks related to operational/IT risks and outsourcing**
    - Nonetheless, in limited cases, **specific reviews** targeted at cloud computing
- With a few exceptions, authorities seem to follow a **principle-based approach** and apply **proportional and risk-based approaches** to their regulatory and supervisory frameworks
Regulatory frameworks

- To complement their general prudential frameworks for outsourcing, some jurisdictions have issued specific requirements or recommendations for IT outsourcing, cloud computing and/or information security (cyber framework)

- Specific requirements or recommendations on cloud computing tend to focus on issues such as:
  - Materiality assessment
  - Risk assessment of data security, confidentiality and availability
  - Rights of information and audit
  - Reversibility of service
  - Business continuity and exit plan
  - Offshoring and sub-contracting
  - Robust legal arrangements
Supervisory approaches

- Most authorities are **notified** about the outsourcing of (material) cloud computing and other IT services either ex-ante or ex-post
  - A few authorities require **authorisation**
- All authorities have **access to information** of outsourced activities mainly through supervised firms
  - A few authorities have **direct powers to supervise** cloud and other IT providers
- Cloud computing is supervised as part of the **offsite/onsite reviews related to IT/operational risk or outsourcing**
  - A few authorities have used **targeted/thematic reviews** on cloud computing
- Most authorities are in the process of applying a systematic approach to monitor the **cross-border dimension** of cloud computing as well as its **implications for financial stability**
Concluding remarks

Although our policy implementation work is still in progress, we could preliminary say:

- **Risks** stemming from outsourcing core functions to cloud providers and other technological third parties **seem not insignificant**

- Insurance authorities are mostly relying on their **general outsourcing rules** but are closely monitoring this issue and several have issued **additional specific requirements or recommendations**

- **Supervisory frameworks** very much rely on approaches to deal with **IT and/or operational risk and/or outsourcing risk** but there is work in progress in several areas including:
  - concentration risk
  - cross-border aspects
  - developing and retaining expertise