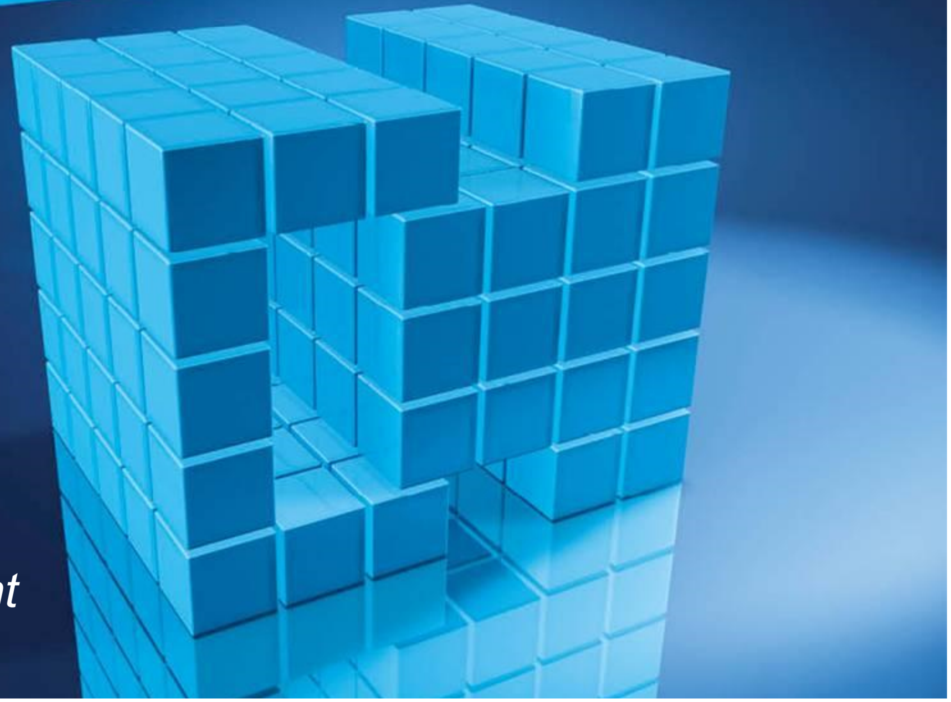
CSSF
COMMISSION
DE SURVEILLANCE
DU SECTEUR
FINANCIER

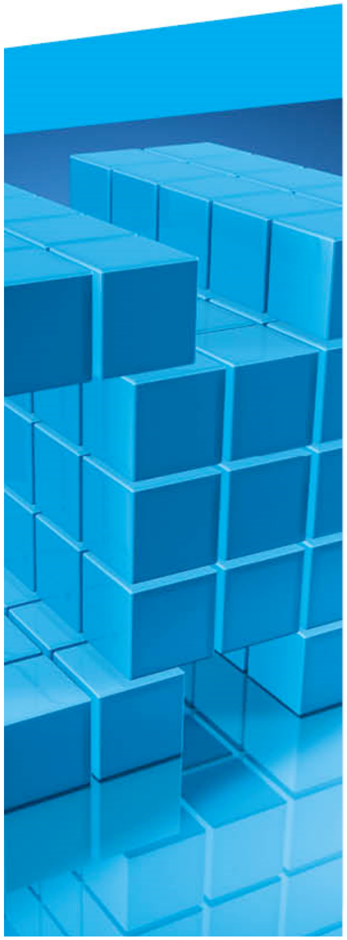
EBA Recommendations on cloud outsourcing: Implementation in Luxembourg

EBA Fintech Knowledge Hub
17 October 2018



Cécile GELLENONCOURT
CSSF, Deputy Head - IT supervision
IT supervision and support PSF Department

COMMISSION
DE SURVEILLANCE
DU SECTEUR
FINANCIER

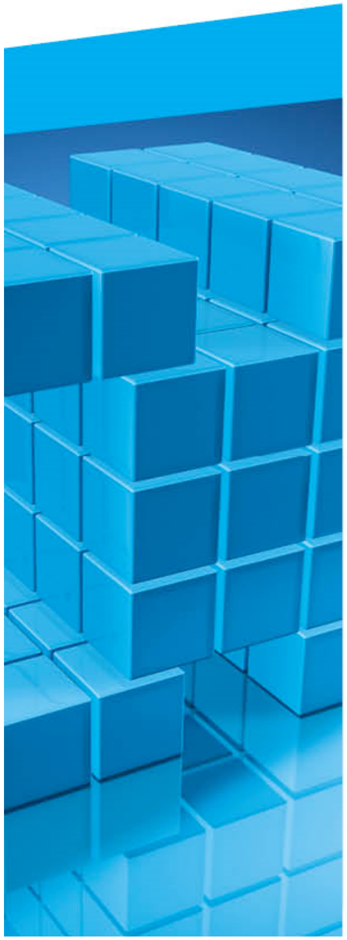


Introduction

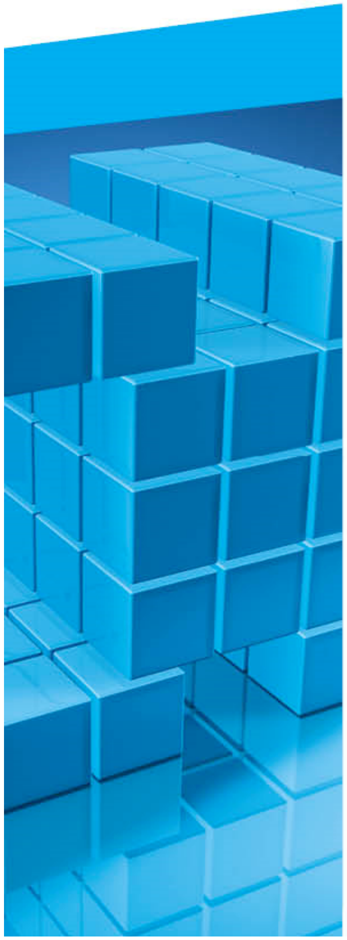
- Beg. of 2016: « Cloud workstream» at CSSF
- End of 2016: « Cloud workstream» at EBA (TFIT)
- Same global objectives:
  - To clarify the supervisory requirements w.r.t. cloud outsourcing
  - Therefore removing uncertainty both for financial entities (FIs) and for Cloud Service Providers (CSPs)
- But with Luxembourg regulation specificities, leading to 2 texts:
  - May 2017: CSSF circular 17/654 on cloud outsourcing (« CSSF cloud circular »)
  - December 2017: EBA Recommendations on cloud outsourcing ("EBA Rec.")

How the EBA Rec. support supervisory messages…

- EBA Rec. strengthen the message with more legal ground and EU harmonisation
- Supervisors' exchanges with CSPs from national level to EU level
- Remove barrier to cloud adoption within group
- While still leaving room for national specificities
  - CSSF global compliance with the EBA Rec.…
  - …even with Luxembourg specificities in the implementation of the Recommendations



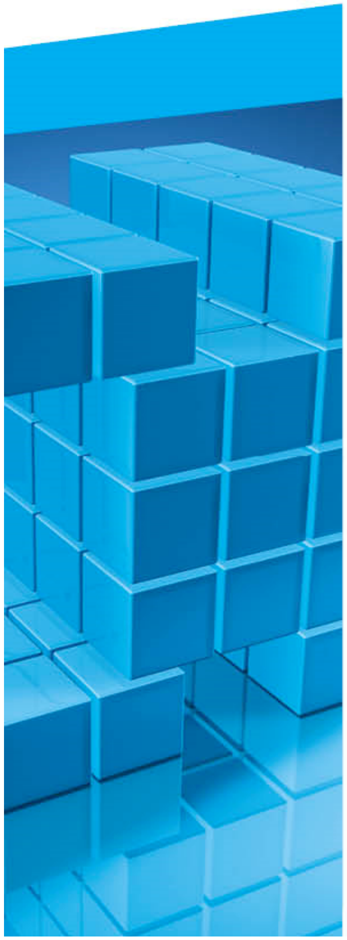
LU specificities in the implementation



- Cloud definition
- Responsibilities and requirements defined according to the “role” played in the outsourcing
- “Cloud officer”

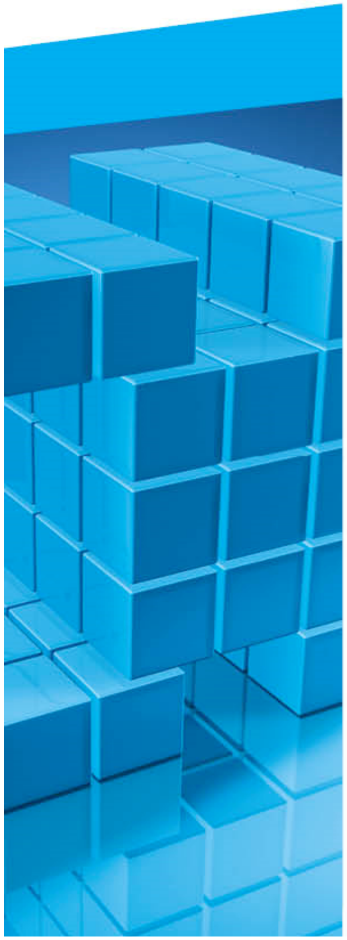
- And some others not covered today
  - Authorisation / notification
  - Contract under EU law
  - …

What is cloud computing



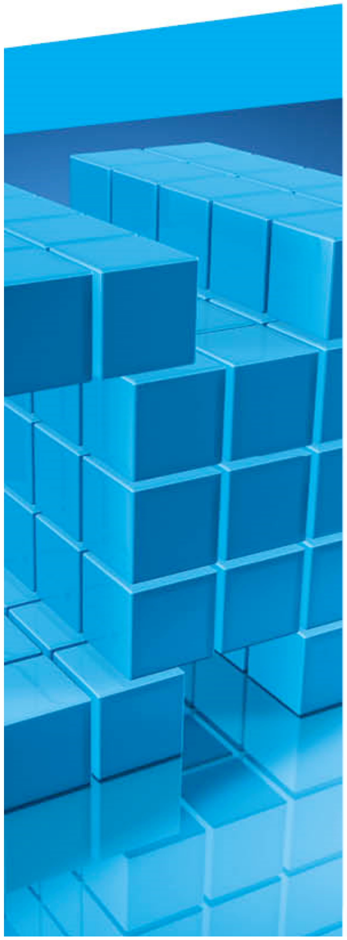
- A Cloud computing infrastructure relies on an IT stack composed of:
  - The **hardware** – servers, disks, network devices, cables, power supplies, etc.;
  - The **logical core (or abstraction layer)** – which contains the standardized services offered by the CSP;
  - The **orchestrator** – which launches the automated processes to deploy Cloud services using predefined “blueprints”;
  - The **management plane (or control plane)** – which is used by the CSP to manage / control the Cloud services and the back-end systems;
  - The **customer’s management interface** – used by the end users to manage the provided services.

Definition of cloud computing: 7 criteria



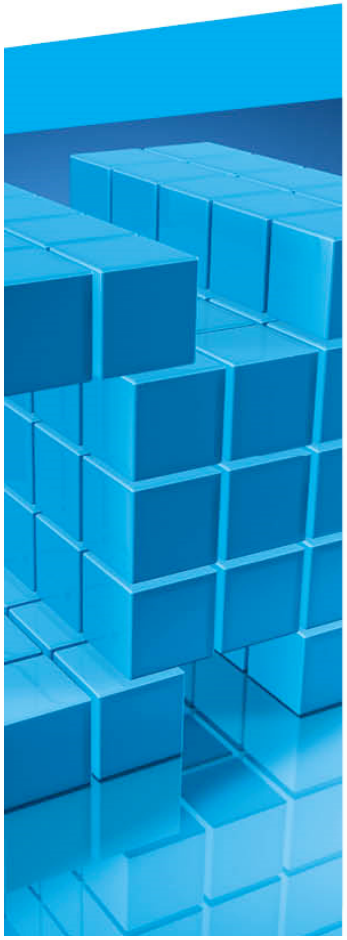
- Cloud definition based on a recognised terminology (NIST, ENISA)
  - 5 criteria / features: on-demand self-service, broad network access, resources pooling, rapid elasticity and measured service
- Cloud definition based on 2 additional criteria justified by the very high degree of automation and industrialisation
  - Apart from exceptional situations**, the provider does not access the data and systems of the consumer** without its prior consent and without monitoring mechanism available to the consumer
  - **No manual interaction of the provider** as regards the day-to-day management of resources

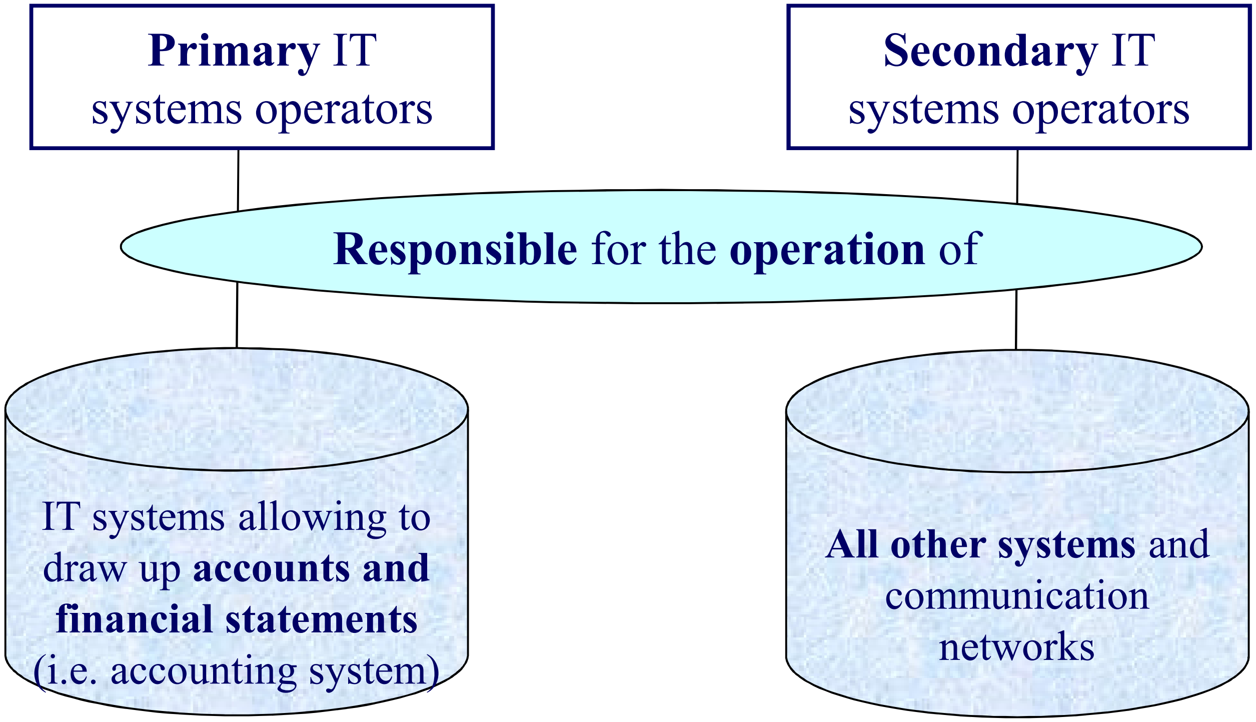
Responsibilities and requirements defined according to the “role”



- Definition of **“roles”** on the basis of the specificities of the cloud (cf. 2 additional criteria) **and** the specificities of the Luxembourg’s regulation
- **Distinguish the provisioning of a cloud from the notion of operating** in the sense of “Support Professional of the Financial Sector” => Support PFS” = IT service providers under CSSF supervision (art. 29-3 and 29-4 of the Law on the Financial Sector)
- **Maintain Support PFS’**s particularities and clarify their role in a cloud context

IT Support PFS





Primary IT systems operators

Secondary IT systems operators

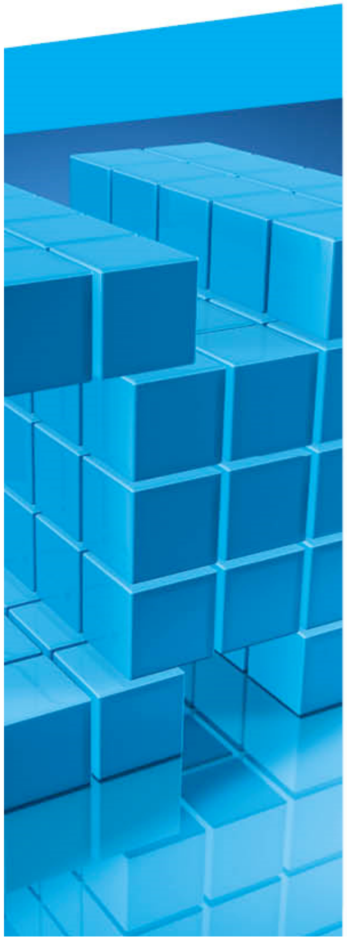
Responsible for the **operation** of

IT systems allowing to draw up **accounts and financial statements** (i.e. accounting system)

All other systems and communication networks

- Are subject to the same legal framework as the financial professionals
- Power of sanction towards Support PFS
- Simple notification if outsourcing to a Support PFS versus non-objection to obtain if other service provider

Responsibilities and requirements defined according to “roles”

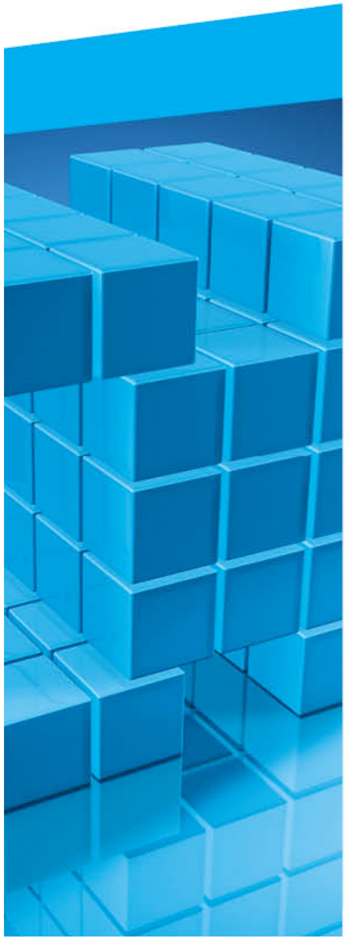


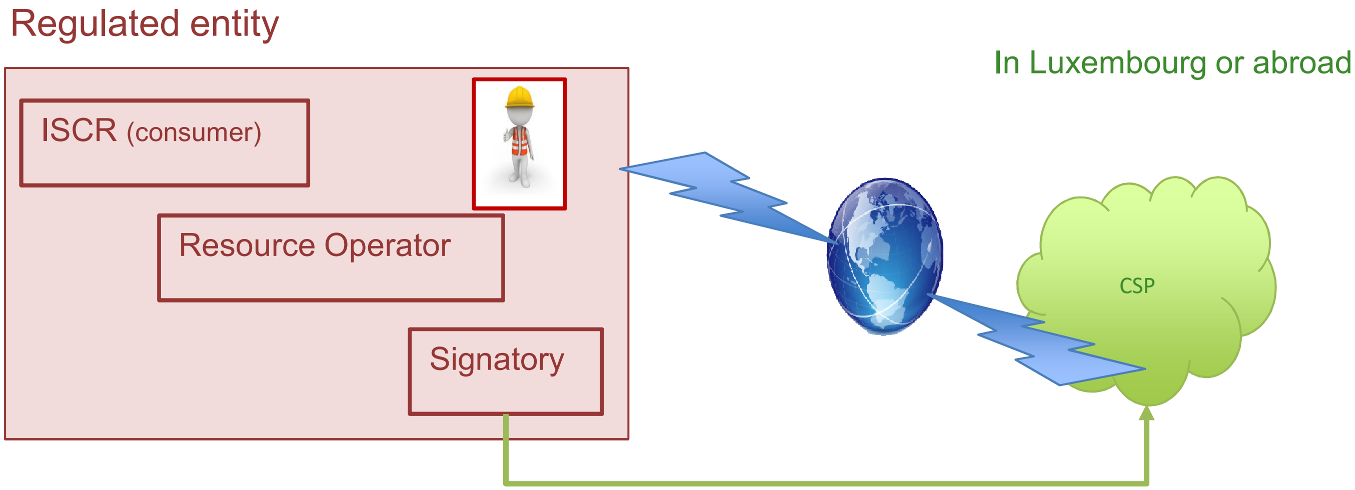
- **Signatory** (of the contract with the cloud service provider)
- Consumer (of resources) ➔ modified in **«ISCR»,** **I**nstitution **S**upervised by the CSSF and **C**onsuming cloud computing **R**esources for the purpose of carrying out its activities
- **Resource Operator**

  → **The resource operator needs a “Cloud Officer”**

  → **The Cloud Officer must be trained on the specific cloud**
- **Cloud computing Service Provider** (CSP)

Direct outsourcing to CSP

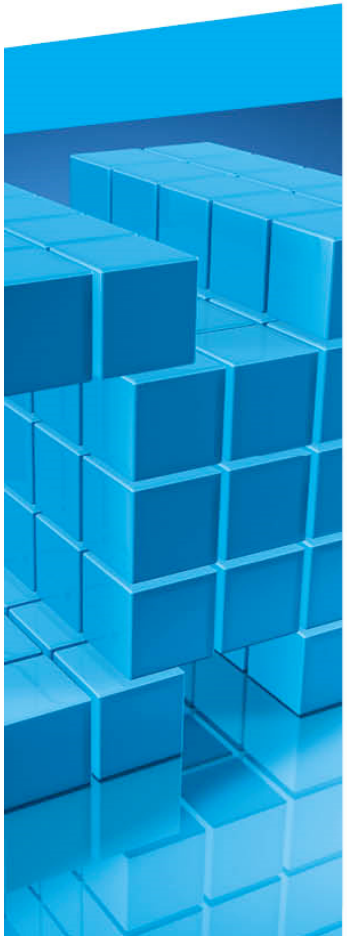


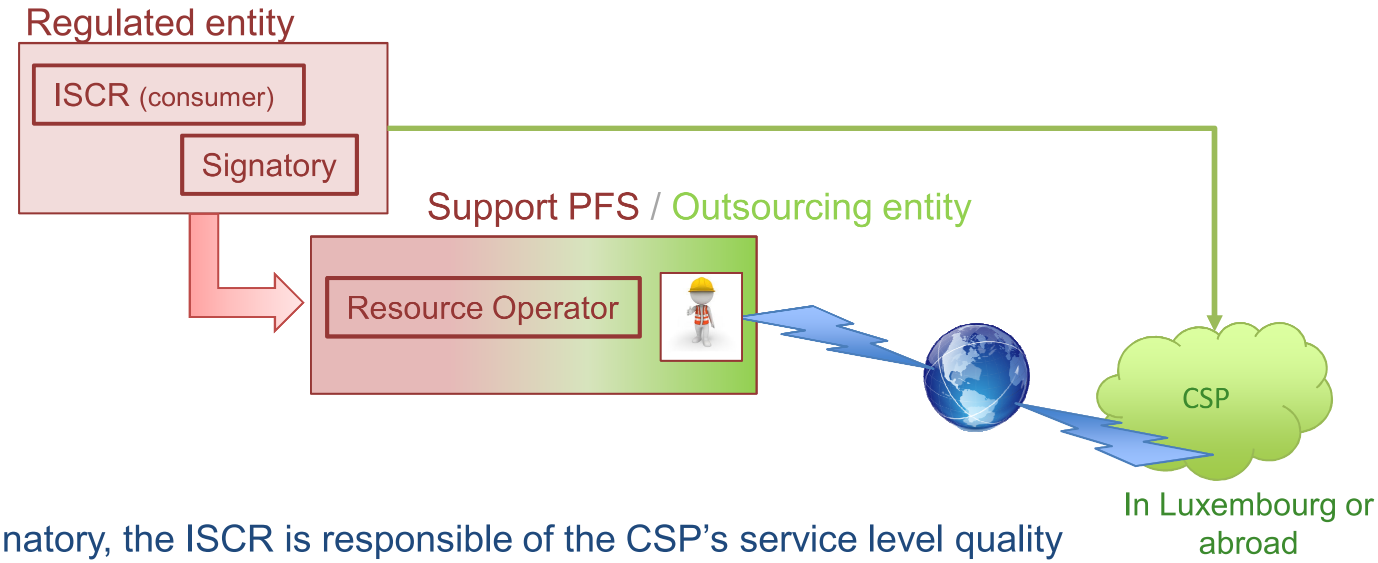


Entity supervised by the Regulator
Entity not supervised by the Regulator

Cloud Officer

Indirect outsourcing to CSP

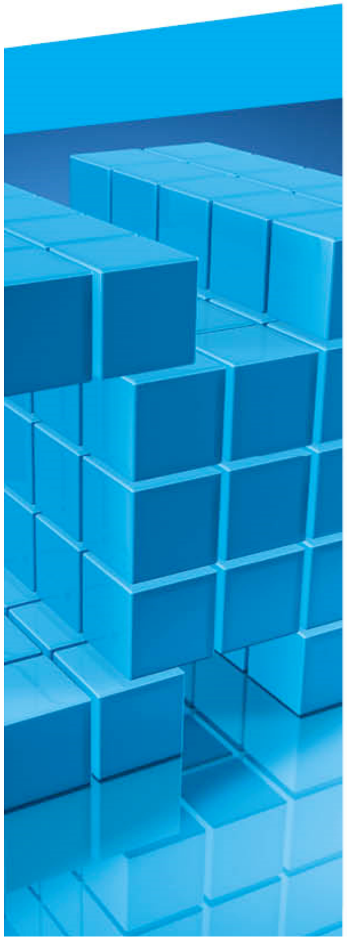




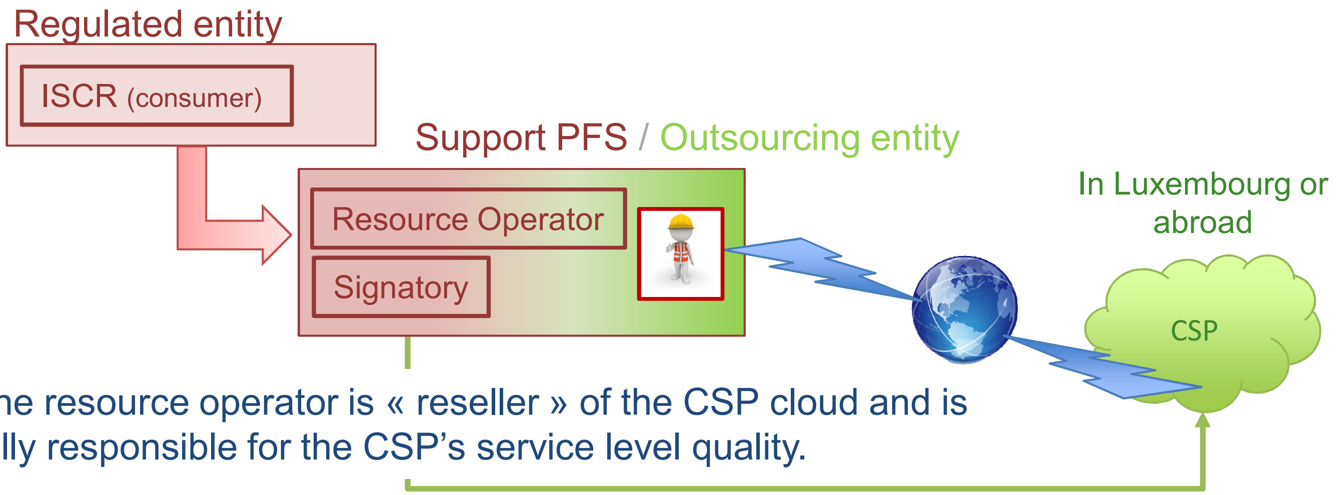
As signatory, the ISCR is responsible of the CSP's service level quality and compliance but can rely on the resource operator's expertise in its assessment of the CSP's service level quality.

Entity supervised by the Regulator
Entity not supervised by the Regulator
Cloud Officer

COMMISSION
DE SURVEILLANCE
DU SECTEUR
FINANCIER



Indirect outsourcing to CSP



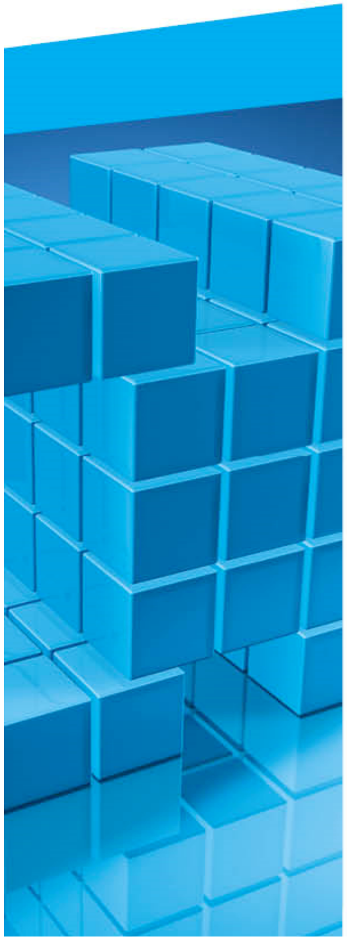
The resource operator is « reseller » of the CSP cloud and is fully responsible for the CSP's service level quality.

The ISCR must verify that the Operator meets the requirements of the cloud circular and that the Operator has done a due diligence on the CSP covering the cloud circular elements.

Entity supervised by the Regulator
Entity not supervised by the Regulator

Cloud Officer

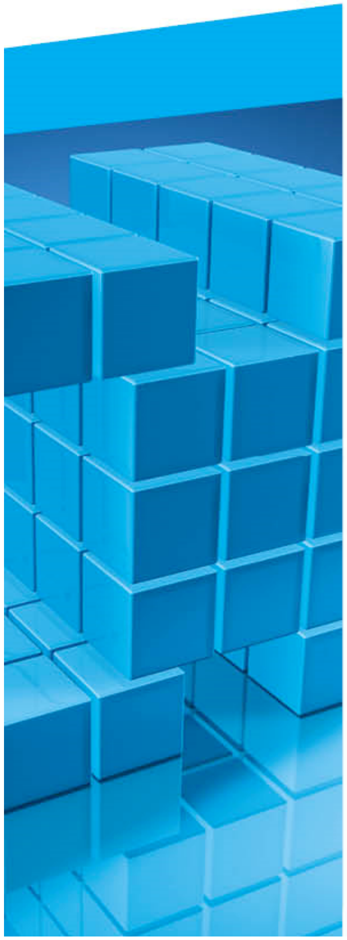
COMMISSION
DE SURVEILLANCE
DU SECTEUR
FINANCIER



Main progresses & remaining challenges observed

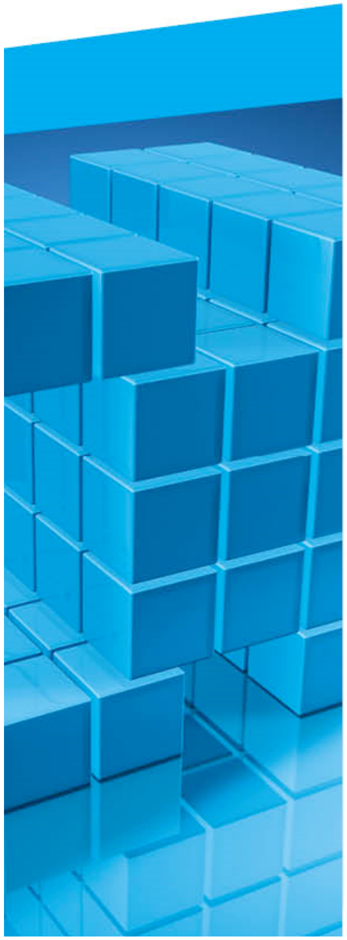
- Authorisation files are often of poor quality but improving
- Too many questions asked about non-material outsourcing in the cloud
  - Project to lower some LU expectations for the non-material outsourcing according to proportionality principle
- Interaction with big CSPs constantly improving leading to better understanding of supervisors' expectations on key aspects (i.e. contractual audit rights)

Conclusion



- Cloud computing is unavoidable
- High professionalism of CSPs who have:
  - Huge resources for development and cybersecurity
  - Very high computing power
  - Willingness to be adopted by the Financial Sector
- 50% of outsourcing authorisation files received are cloud files (but not for core business applications so far)
- EBA and regulators will be in position to size the concentration around major CSPs
- As the systemic risk will grow, it may push the EU to regulate CSPs or at least to fix legal boundaries

COMMISSION
DE SURVEILLANCE
DU SECTEUR
FINANCIER



Thank you for your attention!

Questions?