Outsourcing to cloud service providers: the regulatory perspective

Tom Boedts, General Counsel Febelfin
Belgian Finance Club
25.02.2019

Increased regulatory focus on cloud: why?

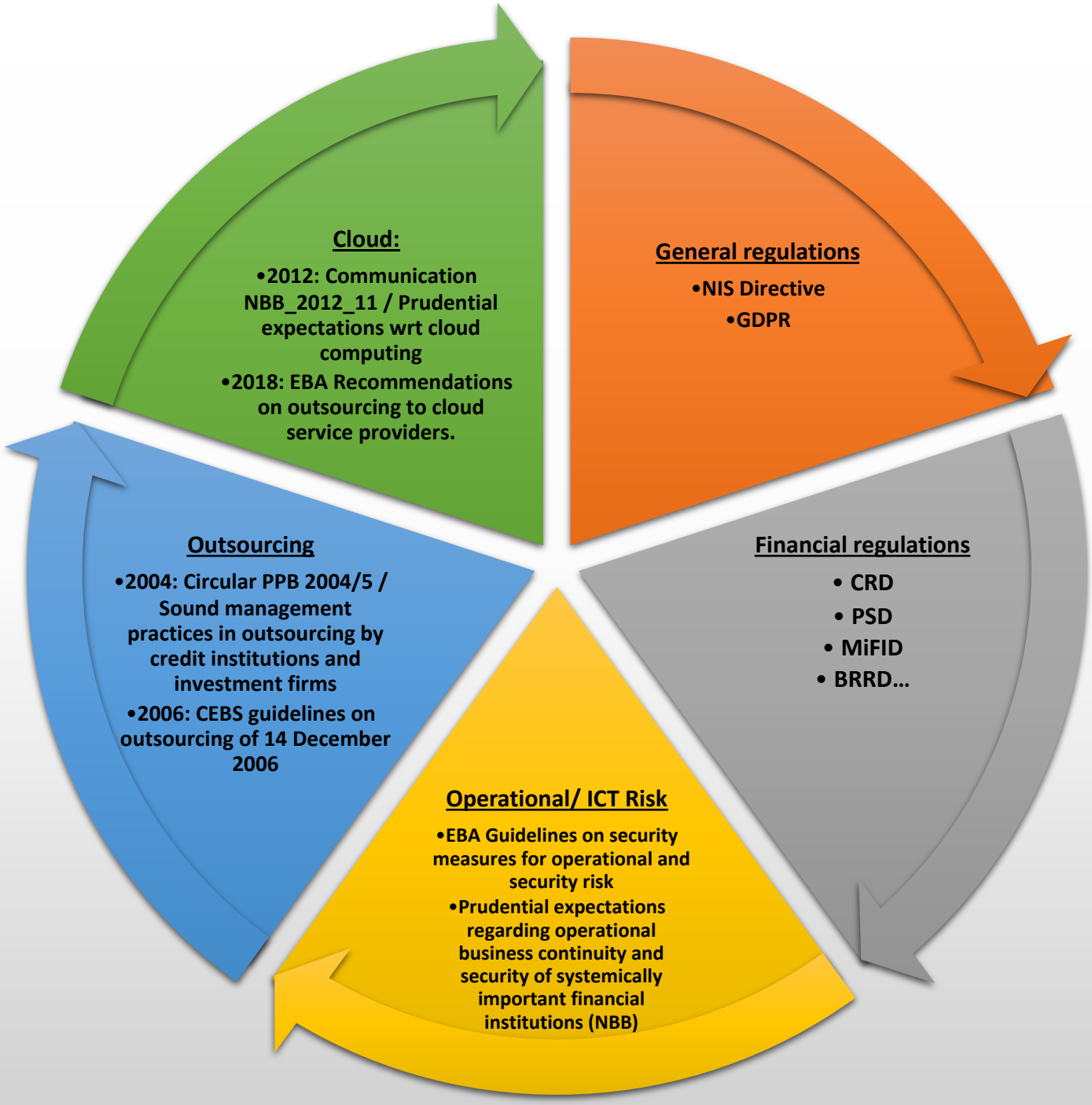
- low interest rate environment : all banks under pressure to reduce costs through digitisation
- new business models: all banks under pressure to put digital and technology at centre of business strategy
- increased reliance on fintech providers

= > Cloud provides easy access to technology needed to reduce costs and digitize business

Risks of cloud outsourcing

- Trust in financial system crucial for economy as whole
- Reputation
- Risks of cloud = risk of outsourcing + ICT risk + data risk
- reliance on less/non regulated/ supervised partners
- relationship with service provider
- concentration risk (multiple outsourcings to same provider, overreliance on small number of suppliers)
- “step in risk” – risk of service provider failing and bank having to step in
- outsourcing to third countries
- recovery and resolution planning
- …

Regulatory framework



Future framework : 2019 EBA Guidelines on outsourcing arrangements


EBA/CP/2018/11
22/06/2018

Consultation Paper

EBA Draft Guidelines on Outsourcing arrangements

- Final Guidelines published *25.02.2019*
- harmonised approach: credit institutions, payment service providers, investment firms, e-money institutions
- integration of outsourcing and cloud requirements

Regulatory expectations as to cloud outsourcing under 2019 EBA Guidelines on outsourcing arrangements

Outsourcing arrangements	• Outsourcing or not • Critical/important or not
Governance famework	• Governance requirements • Outsourcing Policy • Conflicts of interest • Business continuity plans • Internal audit • Documentation
Outsourcing process	• Pre-outsourcing analyses • Contractual arrangements • Oversight • Exit • Information to authorities

1. Set up proper effective governance

Why? ensure effective day tot day management by highest level

- Outsourcing of functions cannot result in the delegation of the management body's responsibilities.
- Institutions remain fully responsible and accountable for complying with all of their regulatory obligations.
- Means:
  - No empty boxes
  - Assign responsibilities, allocate resources,..
  - Create outsourcing function

2. Management to develop outsourcing policy

Why? lack of clear policy, allocation of roles and sound processes increases risk

- Management body should approve and maintain a written outsourcing policy explaining
  - Responsibilities of management, internal control, business
  - Planning, approval process
  - Assessment of service providers
  - Documentation and record keeping
  - …
  - Distinguish between critical and important functions/authorised/intragroup service providers
- ensure its implementation, where applicable, on a consolidated, sub-consolidated and individual basis

3. Manage conflicts of interest

Why? Avoid lack of objectivity / effectiveness in managing outsourcing risk

- Institutions should identify, assess and manage conflicts of interests with regard to their outsourcing arrangements
    - Also for intragroup outsourcing
    - Arm's length conditions!

4. Set up business continuity plans

Why? Prepare for business disruption, disaster recovery, quality deteriorating, insolvency, political risks

- Institutions should have in place appropriate business continuity plans with regard to the outsourcing of critical or important functions.
  - EBA guidelines on internal governance
  - Including testing

5. Involve internal audit function

***Why? Ensuring effectiveness of policy*.**

- The internal audit function's activities should cover, following a risk based approach, the independent review of outsourced activities.
- Audit plan and programme should include in particular the outsourcing arrangements of critical or important functions
- A.o. appropriateness of data protection measures, controls, risk management and business continuity measures implemented by the service provider.

6. Document

Why? Make sure bank and supervisors have clear overview of cloud outsourcing arrangements

- maintain a register of all outsourcing arrangements at institution
- document and record all current outsourcing arrangements
- distinguishing the outsourcing of critical or important functions and other outsourcing arrangements

7. Carry out pre-outsourcing analysis

Why? Make sure service provider is robust

- *Assessment of the criticality or importance* (impact on license, financial performance, continuity, internal control functions, authorised services)

- *Due diligence*

Before entering into an outsourcing arrangement, ensure that the service provider has appropriate and sufficient ability, capacity, resources, organisational structure

- *Risk assessment of outsourcing arrangements*

Identify manage, monitor and report all risks relating to arrangements with third parties

8. Set up contractual arrangements

Why? Make sure bank has sufficient rights against service provider to ensure compliance

- *Written agreement*

The respective rights and obligations of the institution, the payment institution and of the service provider should be clearly allocated and set out in a written agreement.

- *Sub-outsourcing of critical or important functions*

- *Security of data and system*

ensure that service providers comply with appropriate information security standards.

8. Set up contractual arrangements (2)

- *Access, information and audit rights*

Ensure that the service provider grants them and their competent authorities and any other person, including the statuary auditor, appointed by the institution, the payment institution or the competent authorities access, information and audit rights

- *Termination rights*

The outsourcing arrangement should expressly allow the possibility for the institution or payment institution to terminate it

9. Carry out oversight of outsourced functions

Why? Ensure compliance on continuing basis

- monitor on an ongoing basis the performance by the service provider and, where applicable sub-contractors, with regard to all outsourcing arrangements
- update risk assessment
- monitor concentration risk
- evaluate performance
- particular focus on the outsourcing of critical or important functions
- including that the availability, integrity and security of data and information is ensured.

10. Provide for exit strategies

Why? Facilitate exit cloud outsourcing without business disruption

- Exit plans with clearly defined exit strategy for all outsourcing of critical or important functions
- taking into account at least the possibility of the termination of outsourcing arrangements, the failure of the service provider and a material deterioration of the service provided.
- Test plans
- Identify alternative providers

11. Inform supervisors

Why? Enable effective supervision

- make available the register of all existing outsourcing arrangements to the competent authority in a common data base format within each supervisory review and evaluation process (SREP), at least every 3 years and upon request
- inform authorities of outsourcing of critical or important functions
- material changes
- severe events.

2019 EBA Guidelines on outsourcing arrangements

- very much in line with previous guidelines
- principle based approach
- would apply to outsourcing arrangements entered into on or after 30 September 2019
- existing arrangements as to critical/important outsourcings to be updated by next review, no later than 31 December 2021