Cloud Computing in the Banking Sector of the Euro-area

George Papoulias, CGEIT, ITIL Expert, CRISC, CISA, Price2P, COBIT
Senior Management Advisor,
CISO & CDO Office
National Bank of Greece
Vice Chair, itSMF Hellas

ITSDFI Conference, Brno, Czech Republic
16th-17th of May 2018
Digital Transformation of Banks in EU
Europe's Digital Progress (Czech Republic)
The European Banking Cloud Ecosystem
Barriers, Security Threats, Challenges, Concerns
EBF-Cloud Banking Forum
EU Regulatory Requirements
Fintech and Cloud Services Adoption
Cloud Compliance to GDPR
Digital Transformation of Banks in EU

Key Priorities for 2018 and Actions to Be Taken by the European Commission in the Banking Sector:

1. Payments
2. Cloud
3. Data (Data Analytics & Privacy)
4. Cybersecurity
5. Fintech (*Considered as Banks by ECB*)
6. Blockchain Technologies
7. Digital Skills

1. Creation of a clear and consistent EU and global regulatory framework
2. Creation of a proportionate risk-based approach to due diligence and contracts between the CSPs and the banking sector
**Integration of Digital Technology (Czech Republic-EU)**

<table>
<thead>
<tr>
<th>Czech Republic</th>
<th>EU</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESI 2017</td>
<td>DESI 2016</td>
</tr>
<tr>
<td>Value</td>
<td>Rank</td>
</tr>
<tr>
<td>Cloud Enterprises</td>
<td>10%</td>
</tr>
</tbody>
</table>

RFID, use of eInvoices, social media and cloud is below EU average.

The Digital Economy and Society Index (DESI): The Digital Economy and Society Index (DESI) is a composite index that summarizes relevant indicators on Europe’s digital performance and tracks the evolution of EU member states in digital competitiveness.

Source: Europe's Digital Progress Report (EDPR) 2017, Country Profile Czech Republic
Cloud-based Services

Cloud computing allows the sharing of on-demand computer processing resources in a way that promotes efficiencies and economies of scale. Such cost-cutting may be attractive for banks, but concerns over safety and privacy seem to have initially inhibited banks from using cloud computing infrastructure.

Source: Technet
FinTechs have made a significant impact on the financial services industry but they lack scale, access to a larger customer base, and expertise in handling regulations, which is leading to a significant scope for banks and FinTechs to collaborate and operate together.

Additionally, banks are looking at different ways in order to improve their agility as well as provide an enhanced customer experience, in order to give them an edge over their competitors.

Cloud services enable agility and flexibility in banks' middle and back office that would let them digitize their business on an end-to-end basis.

AI and cognitive technologies are being applied in the banking industry primarily for customer relationship management, identity authentication, anti-money laundering, compliance, and risk control.

Augmented reality technology enables banks to provide enhanced customer service using location-based deals and cross-sales opportunities.

Source: Capgemini, Top Ten Trends in Banking, 2017
Security and Innovation is the Way Forward

Banks are strengthening their security systems and investing into innovation by leveraging new technologies such as distributed ledgers, biometrics, and robotic process automation.

01 Distributed ledgers technology will help banks identify opportunities, test proof of concept, and understand regulatory concerns.

02 Biometric authentication will help banks to combat identity thefts, make transactions more secure, and enhance the customer experience.

03 Robotic process automation will provide banks with significant value additions to various areas of the customer lifecycle.

04 Increasing digitization and connectivity has triggered an increase in data breaches, compelling banks to strengthen their security systems.

Source: Capgemini, Top Ten Trends in Banking, 2017
Benefits for Business

- Agile product development
- Improve customer value propositions
- Increase productivity
- Increase IT flexibility and scalability
- Reduce IT Costs (CAPEX vs OPEX)
- Shared resources
- Foster business innovation
- Facilitate Business Agility
- Improve collaboration
- Pay as you go model
- On-demand service delivery
- Faster software deployment
- Foster business innovation
- Improve IT/Business Efficiency
Barriers to Adoption

- Personal Data Protection & Privacy
- Jurisdiction
- Computer Security
- Reliability
- Terms & Conditions
- Standards
- Accessibility
Barriers, Security Threats, Challenges, Concerns

BIGGEST CLOUD SECURITY THREATS
- Unauthorized access: 61%
- Hijacking of accounts, services or traffic: 52%
- Insecure interfaces / APIs: 43%

BARRIERS TO CLOUD ADOPTION
- General Security Risks: 34%
- Lack of staff resources or expertise: 28%
- Integration with existing IT environment: 27%

CLOUD MANAGEMENT CHALLENGES
- Visibility into infrastructure security: 37%
- Compliance: 36%
- Setting consistent security policies: 34%

TRADITIONAL SECURITY TOOLS DON'T WORK IN THE CLOUD
- Our traditional network security tools don’t work in the cloud: 19%
- Limited functionality: 36%
- All capabilities work in the cloud: 21%

Source: Dome9.com
Enterprise Cloud Adoption

The majority of Enterprise Cloud adopters underscore their commitment to moving larger parts of their IT establishment to the cloud, as they expect to derive greater business value from the cloud technologies in the future.

1 Cloud Adoption is Widespread

Cloud is not just another ITfad passing through the night, cloud adoption is broadening as brighter benefits appear on the horizon.

- 57% of Enterprise are using Software as a Service (SaaS) applications
- 38% have adopted Platform as a Service (PaaS) solutions

Applications already migrated or in the process of being migrated to the cloud include:

- Application development/test environments: 54%
- Disaster recovery and storage: 45%
- Email/collaboration: 41%
- Business intelligence/analytics: 35%

2 Cloud is becoming an enabler of top-line growth

Buyers ranked reduced time for provisioning applications and flexible infrastructure as their top cloud adoption drivers.

- 82% of cloud buyers met their flexible infrastructure objectives
- 71% of cloud buyers met their quicker time to market objectives

3 Cloud is evolving from a cost reduction initiative and moving towards an enabler of top-line growth for Enterprises.

Cloud sellers are still pitching cost savings but Enterprises are looking for more.

TOP ADOPTION DRIVERS ACCORDING TO:

<table>
<thead>
<tr>
<th>BUYERS:</th>
<th>SELLERS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced time for provisioning application/infrastructure</td>
<td>Reduced TCO (Total Cost of Ownership)</td>
</tr>
<tr>
<td>Flexible Infrastructure capacity</td>
<td>Flexible infrastructure capacity</td>
</tr>
<tr>
<td>Limited in-house technical resources</td>
<td>Reduced TCO (Total Cost of Ownership)</td>
</tr>
<tr>
<td>Desire to “variableize” cost</td>
<td>Desire to “variableize” cost</td>
</tr>
<tr>
<td>Reduction in TCO (Total Cost of Ownership)</td>
<td>Limited in-house technical resources</td>
</tr>
<tr>
<td>Industry-specific reasons</td>
<td>Industry-specific reasons</td>
</tr>
</tbody>
</table>

Service providers need to adapt to the “Next Gen Buying Center” and shift discussions away from the traditional cost based value proposition.

- 64% were satisfied with the current results from their cloud initiatives
- 88% expect to achieve greater benefits from cloud solutions in the future

SOURCE: Cloud Connect
Specialist insurer Beazley has reported that the number of business email compromises is accelerating, particularly for those organizations using Office 365, the popular cloud-based solution for Office applications and other Microsoft productivity services. The three sectors most affected were financial services, healthcare and professional services.

Source: www.beazley.com/bbr, Beazley Breach Insights 2018
What is limiting enterprises from using cloud computing services?

Factors limiting enterprises from using cloud computing services, by size class, EU-28, 2017

Source: Eurostat, 2017
European Banking Federation (EBF) - Cloud Banking Forum

The EBF on December 2017, launched a new initiative bringing together banking experts and cloud service providers. The EBF Cloud Banking Forum aims to shape clearer and harmonised supervisory approach towards cloud computing to support the swift adoption of public/hybrid cloud by the banking sector.

• Policy hub on cloud computing for Banks & Cloud Service Providers
• EU Institutions invited as observers
• Aiming at high-level policy recommendations for regulators
• Both global and EU cloud service providers to join

Who is the EBF?
• National Banking Associations from 32 countries
• 4.500 banks with 2.3 million employees

“Cloud computing is driving both the digital transformation of banks and the EU Digital Single Market. We need to create a safe and clear regulatory environment so that both banks and supervisors can do their job well. The success of our first Cloud Banking conference and the launch of the EBF Cloud Banking Forum demonstrates that there is a willingness to innovate and a thirst for clear rules in cloud banking.”

Wim Mijs, Chief Executive Officer of the EBF
Composition of the EBF Cloud Banking Forum

✓ Members of the EBF banks’ expert groups on cloud (those implementing cloud solutions for their banks, legal and/or cybersecurity experts from the banking side)

✓ Cloud Service Providers (CSPs) (both from the EU and US) : e.g.  

✓ Observers:

1. EU institutions and agencies (such as the European Banking Authority, the European Central Bank and the European Commission).
2. Trade associations representing CSPs: Digital Europe, CCIA, Business Software Alliance, CISPE
Priorities of the EBF Cloud Banking Forum

1. Access rights & audits, pooled audits and third party audits;
   - Outsourcing contracts must ensure access and audit rights at the service provider for the outsourcing institution and competent authorities
   - Complete access to all its relevant business premises (head offices and operations centres)
   - Unrestricted rights of inspection and auditing related to the outsourced services

2. Life-cycle management/exit strategy and definition of business continuity plan criteria;
   - Appropriate business continuity plans regarding outsourced operational functions
   - Clearly defined exit strategy
   - Be able to transfer outsourced operational functions, reintegrate outsourced operational functions, end the business activities for which the outsourced operational function is needed

3. Qualitative and quantitative criteria for materiality assessment and other risk assessments;
   - Impact on revenue prospects
   - Direct operational impact of outages
   - Impact of the outsourcing based on scenario analysis
   - Risk related to data (e.g. GDPR)
   - Concentration risks
   - Risk that may result from sub-outsourcing

4. Reporting of outsourced activities.
   - Outsourcing institutions should adequately inform the competent authorities of material activities to be outsourced to cloud service providers.
   - The competent authority may ask the outsourcing institution for additional information on its risk analysis for the material activities to be outsourced
   - The outsourcing institution should maintain an updated register of information on all its material and non-material activities outsourced to cloud service providers at institution and group level.
European Banking Authority (EBA)

Recommendations of Cloud outsourcing

- **Materiality assessment**
  - Criticality and risk profile of activities outsourced

- **Duty to adequately inform supervisors**
  - Inform the competent authorities of material activities to be outsourced
  - Register of information with material and non-material activities outsourced

- **Access and audit rights**
  - Written agreement for the right to audit (Pooled audits, Third-party or internal audit reports, High competence level of auditors)

- **The right of access**
  - On-site visit clearance

- **Security of data and systems**
  - Identify and classify activities, processes and data according to sensitivity
  - Ensure protection of data (Encryption)
  - Monitor security measures

- **Location of data and data processing**
  - Risk assessment (legal, compliance, political, privacy)

- **Chain outsourcing**
  - Subcontracting (exclusions of activity types)
  - Information of significant changes to subcontracting (e.g. notification period)

- **Contingency plans and exit strategies**
  - Develop and implement exit plans

The recommendations will apply from the 1st of July 2018

These recommendations apply to credit institutions and investment firms as defined in Article 4(1) of Regulation (EU) No 575/2013 (Capital Requirements Regulation – CRR).

The purpose of these EBA recommendations is to specify the supervisory requirements and processes that apply when institutions outsource to cloud service providers. To that end, these recommendations build on the guidance provided by the CEBS guidelines.

According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these recommendations, or otherwise with reasons for non-compliance, by the 1st of July 2018. In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant.

Source: EBA, FINAL REPORT ON RECOMMENDATIONS ON CLOUD OUTSOURCING
“Fintech Credit Institutions/Banks” Authorization Process

The ECB and National Competent Authorities (NCAs) will consider:

1. Suitability of the members of the management body
   - IT competence of members
   - Fitness and propriety of members
2. Suitability of shareholders
   - Reputation of shareholders
   - Financial soundness of a shareholder
3. Structural organization
   - Credit risk approval and governance
   - IT-related risks
   - Outsourcing, including cloud services
   - Data governance
4. Programme of operations
   - Execution risks arising from the business model
   - Exit plan
5. Capital, liquidity and solvency

Source: ECB, Guide to assessments of fintech credit institution license applications

The ECB considers “fintech banks” to be those with “a business model in which the production and delivery of banking products and services are based on technology-enabled innovation”
IT-related Risks to “Fintech Credit Institutions/Banks”

European Central Bank (ECB) considers two (2) significant risks areas:

1. Cyber risks
   • Propensity by higher levels of outsourcing involves data sharing across broader range of parties increasing vulnerability to cyberattacks
     ✓ service disruption
     ✓ loss of customer data
     ✓ fraudulent financial transactions
     ✓ systems outages

2. Increased reliance on outsourcing, including cloud computing
   • Outsourcing contracts limitations
     ✓ Audit and Access Rights to outsourced activities
   • Dependencies on suppliers (vulnerabilities owing to contractual lock-in clauses)
     ✓ Business Continuity

Risk areas mitigation controls:

1. Cyber risks
   • Specialized staff and internal risk management framework
   • Arrangements to ensure business continuity
   • Safeguards for IT system and network availability

2. Outsourcing, including cloud computing
   • Performance of a comprehensive assessment
   • Minimize dependence on a single cloud service provider
   • Compliance with legal and regulatory requirements
   • Actions in the event of the CSPs systems failure
   • Protection for personal and confidential data in the SLA

The ECB considers “fintech banks” to be those with “a business model in which the production and delivery of banking products and services are based on technology-enabled innovation”.

Source: ECB, Guide to assessments of fintech credit institution license applications
The Cloud in Compliance with GDPR

**LITTLE CHANGE IN GDPR-READINESS LEVELS**

with May 2018 deadline looming

24.6%
of cloud services rated high on GDPR-readiness

**AMONG THE CLOUD SERVICES RATED AS HIGH FOR GDPR-READINESS:**

- **DATA OWNERSHIP TERMS**
  - 38.3%
of cloud services do not specify that the customer owns the data in their terms of service

- **DATA ENCRYPTION AT REST**
  - 57.1%
of cloud services do not support encryption of data at rest

- **DATA BACKUP IN OTHER GEOS**
  - 80.3%
of cloud services replicate data in geographically dispersed data centers

**Steps to Compliance**

1. GDPR compliance (Art 33)
2. Contractual Requirements (Art 28)
3. Obligation To Appoint A DPO (Art 37)
4. Documentation (Art 30)
5. Sub-Processing (Art 28)
6. Return Or Delete (Art 28)
7. Notification (Article 28)
8. Data Transfer (Article 44)
9. Direct Liability (Article 82)

Source: Netskope Cloud Report 2017
To Wrap it up……

Cloud - including the fin-tech ecosystem, is driving a major change in financial services. It is in our in interest to ensure that regulatory compliance and risk management policies support the efficiencies and agility delivered by the Cloud Service Providers while at the same time, do not underestimate the reasons for regulatory compliance. To do so, we must ensure meaningful exchanges between the key stakeholders, so that, innovation is encouraged in a way that allows for the risks to be mitigated.

I look forward to your participation in tomorrow’s round table discussion to exchange ideas about the new European Banking ecosystem affecting banks, CSPs and regulators.
Enjoy next sessions!