# Improving ICT risk management for EU finance

Slavka Eley, *Head of Banking Markets, Innovation and Products, EBA*

*2nd EBF Cloud Banking Conference, 9 July 2019*

# What has been on regulatory side

**2016**

- Monitoring of innovation and risks, increased supervisory attention to ICT risks
- Guidelines for supervisors on ICT risk assessment

**2017**

- Identified a need to provide regulatory clarifications on cloud adoption
- EBA Recommendations on Outsourcing to Cloud service providers

**2018**

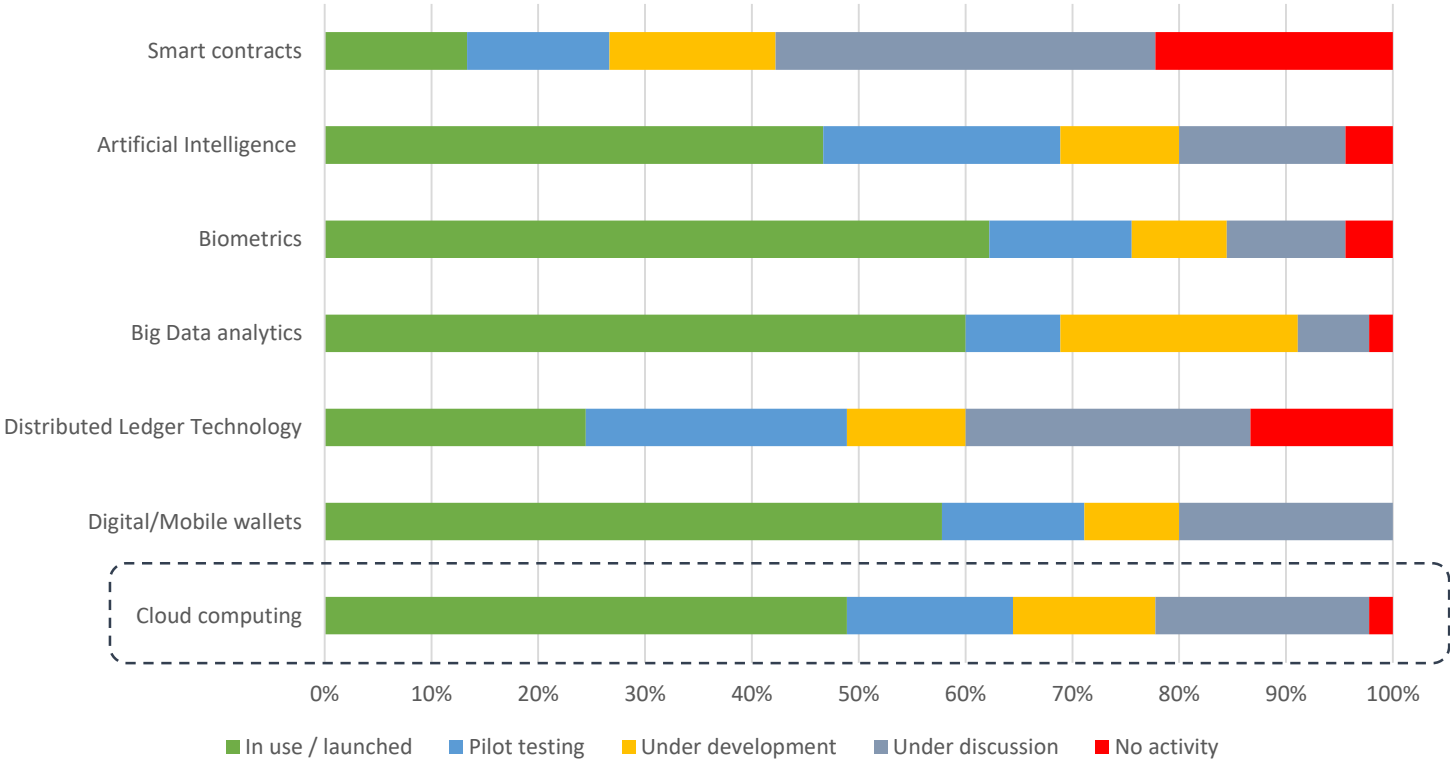
- Guidelines on outsourcing arrangements
- Implementation of EBA Recommendation on outsourcing to cloud – EBA workshop

**2019**

- ESAs advise on legislative improvements in ICT and cybersecurity
- EBA Guidelines on ICT and security risk management
- Monitoring of innovation and trends

# Status of adoption of financial technologies by EU banks

In the context of the EBA Risk Assessment Questionnaire, conducted on a semi-annual basis among banks and market analysts, 50 European banks were asked a series of questions in relation to FinTech. Final results are included in the EBA Risk Assessment Report (H2 2018).




*Source: EBA RAQ H2 2018*

## Benefits of EBA regulatory work for cloud adoption

- EU level convergence
- Clarity of expectations (banks, CSP, supervisors)
- Legal certainty in contracts
- Increased understanding by regulatory and supervisory community
- Facilitated dialogue between industry and supervisors

## Focus going forward

- Operational resilience
- Oversight of critical third party providers

# Draft Guidelines on ICT and security risk management

- **Scope:** payment service providers for their payment services; credit institutions for all activities beyond their payment services; investment firms for all activities.
- These Guidelines integrate the '*Guidelines on security measures for operational and security risks of payment services*' under Article 95 PSD2 (December 2017, EBA GL 2017/17), and elaborate further on certain topics that contribute to mitigating ICT risks in financial institutions. EBA GL 2017/17 will be repealed from the date of application of these Guidelines.
- **Timeline:** Public consultation until **March 2018**. Finalisation in Q3 2019.

CONTENT

- ICT governance and strategy
- ICT risk management framework
- Information security
- ICT Operations management
- ICT Project and Change management
- Business continuity management

# ESA Joint advice to the European Commission on the need for **legislative improvements** for **ICT risk management requirements** in the EU financial sector

## → Overall **operational resilience** including ICT governance and security

- every entity should be subject to general and fundamental requirements on governance and security of ICT (including cybersecurity) to ensure the safe provision of regulated services
- advising on new articles in CRD and PSD2 on **operational resilience** as a requirement relating to governance (ICT security, cyber resilience, contingency planning and business continuity planning) and mandate for Operational resilience guidelines

## → **Oversight of third party providers**

- increased use of third party providers brings new **vulnerabilities** for regulated entities and **concentration** is becoming more relevant from the financial stability perspective (e.g. small number of CSPs)
- advising COM to propose a **legislative solution** for monitoring the activities of third party providers when they are critical service providers


**EUROPEAN BANKING AUTHORITY**

Floor 46, One Canada Square, London E14 5AA

Tel: +44 207 382 1776
Fax: +44 207 382 1771

E-mail: info@eba.europa.eu
http://www.eba.europa.eu