Q&A

## SCOTT MULLINS

Managing Director & General Manager,
Worldwide Financial Services - AWS

# Cloud's role in building a modern and secure European financial services sector

By working with AWS, financial services organizations are optimizing all aspects of their operations – from customer service delivery models to risk management – in order to build a foundation for long-term innovation and growth. As we enter the second decade of AWS adoption in financial services, the use of cloud is broad and varied. In fact, we even see this breadth and variation of cloud adoption within a single customer. As organizations gain experience running applications on AWS, they use that experience to drive additional experimentation and innovation. Standard Chartered Bank is a good example. The bank launched its Nexus banking-as-a service solution and Mox, its new virtual bank in Hong Kong, on AWS.

The bank's award-winning global payments system, SC Pay, and core banking system, eBBS, are cloud-native services, which have resulted in faster and more secure transfer of funds with reduced cost per transaction. Standard Chartered's Financial Markets business, which includes risk management, financing, and investment services, also uses AWS to run algorithms that assess market risk to scale up those workloads during peak demands.

In Europe, but also globally, use of cloud in financial services is gaining momentum, but there are great opportunities for further adoption. And that's not only true of financial services, but of all industries. According to a study commissioned by AWS and published last year by independent consultancy Public First, if you look across all sectors of the economy, only 26% of European companies have taken up key technologies such as the cloud, 25% AI, and 14% big data[1]. This is a long way from the target for 75% of companies to adopt cloud, big data and AI as set out in the European Commission's Digital Decade program[2] so the potential opportunity from technology in the wider EU economy is still very significant. The same study points out that accelerating progress will require a sustained, collective focus – across the public and private sectors – on digital adoption, skills development, infrastructures, entrepreneurship, and digital transformation of businesses and government.

One area in particular that would benefit from this type of sustained, collective focus is operational resilience, which has always been a critical topic in financial services. Indeed, AWS, the financial services industry, and the regulatory community all share a common interest in enhancing operational resilience. The ability to provide continuous service despite potential disruptions, is a key prerequisite for financial stability. Operational resilience is a shared responsibility – AWS is responsible for ensuring that the services used by our customers—the building blocks for their applications—are continuously available, as well as ensuring that we are prepared to handle a wide range of events that could affect our infrastructure.

Our customers can design, deploy, and test their applications on the cloud to achieve the availability and resiliency they need, including for mission-critical applications that require almost no downtime.

Our builds guard against outages and incidents, and accounts for them in the design of AWS services, so that when disruptions do occur, their impact on customers and the continuity of services is as minimal as possible. To avoid single points of failure, AWS minimizes interconnectedness within our global infrastructure. Our global infrastructure is geographically dispersed over five continents and is composed of 31 geographic Regions, which are composed of 99 Availability Zones (AZs). The AZs, which are physically separated and independent from one another, are also built with highly redundant networking to withstand local disruptions. Regions are isolated from one another, meaning that a disruption in one Region does not result in disruption in other Regions. Compared to global financial institutions' on-premises environments today, the locational diversity of AWS's infrastructure greatly reduces geographic concentration risk.

AWS also provides guidance for how customers can design, deploy, and architect financial services industry workloads to improve the resiliency, security, and operational performance, and regularly provides additional educational content on best practices. We refer to these practices as "well architected principles". These principles, to a certain extent, have been adopted widely by several providers, and although they vary

in some form from CSP to CSP depending on the way their infrastructure is built, broadly speaking they guide financial firms to make certain architectural choices depending on their risk appetite for the applications they are looking to run on the cloud.

At AWS, we also make it easier for our customers to translate these principles into actions, via our Well-Architected Tool and Well-Architected Reviews, so we don't just supply the principles, we supply the hands-on guidance needed to translate those principles into actions.

Looking ahead to DORA and the emerging regulatory framework, ensuring that financial firms have full access to technologies like cloud and machine learning is crucial for the future competitiveness of the European financial sector. In particular, any type of localization requirements would not only reduce choice for EU financial organizations, but would also pose risks for the cybersecurity of Europe's most important workloads. This goes directly against the objectives of DORA in terms of enhancing the security and resilience of the financial sector.

For DORA and any future regulatory initiatives, it remains fundamentally important for policy makers and regulators to carefully consider the need to achieve an approach that recognizes the operational resilience, security and innovation benefits of cloud, and enables firms to make the most of that opportunity.

DORA provides the right foundations for a framework that can address ICT risks; however, a lot of the detail is yet to be decided in the regulatory technical standards so it is important that these reflect the specificities of not just cloud but all types of providers. For example, specifically in relation to cloud, it is important to consider the 'digital native' aspects of the technology and the principles that deliver enhanced 'digital native operational resilience'. In this sense, the well architected framework which I referred to before could be leveraged to achieve this.

I would also contend there is a need to re-think regulatory and supervisory practices in light of the digitalization of the sector, for example by considering the shared responsibility model, where the cloud provider looks after the security and resiliency of the cloud, while the financial entity looks after their security and resilience in the cloud. Further, given the fast pace of technological innovation, both regulation and supervision need to be forward looking and flexible enough to adapt to future developments in technology. I believe DORA provides the opportunity to achieve this in order to deliver on its objectives of enhancing digital operational resilience across the EU financial sector.

In relation to the oversight of critical providers, as it is acknowledged in the introductory section of DORA, the framework could potentially lead to synergies that would support the adoption of technology, for example by avoiding duplicative efforts by supervisors and/or firms. However, as I said earlier, we are yet to see how this is implemented in the regulatory technical standards and in practice. More broadly, I'd also add that it is critical that regulators actively facilitate the dialogue among financial firms, service providers and regulators to develop a coherent cross-border framework that continues to support the adoption of technology by financial services firms.

We are seeing differences starting to emerge and are concerned about the potential impact on the ability of financial firms to access services globally at a time when cyberthreats have become a key risk to the financial sector and firms require the latest security toolbox in order to be able to defend themselves against these threats.

*[1] https://awsdigitaldecade.publicfirst.co.uk/*
*[2] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en*