Kaj-Martin Georgsen

Head of Corporate Responsibility & Public Affairs, DNB Bank ASA

A future-proof, customer-centric banking system needs to tap into the cloud

Reaping the benefits of cloud computing is a prerequisite for providing customers with the services they expect in 2020. Banks and regulators need to work closely together to address the requirements for both security, competition and competitiveness.

Physical data centres and other physical IT infrastructure represent are costly, inefficient and often redundant: Since they need to be scaled for peak demand, much capacity will remain idle for most of the year. The result: sunk investment and high maintenance costs.

In realizing this redundant capacity could be leased off to others, Amazon kicked off the cloud revolution which has swept the world of IT in during the last decade, including, to an increasing extent over the last few years, financial institutions.

For banks, in the face of new competition for the end-the benefits of cloud computing are numerous. Moving data and service into public clouds enables us to build new solutions more quickly and deploy at greater scale while reducing costs. At DNB, our P2P payments app Vipps was one of our first major venture into the public cloud in 2016. We haven't looked back since.

Cloud infrastructure allow us to source single-purpose functionality from third parties into both backend and customer-facing applications almost instantly, enabling a more agile development approach. Third-party solutions from smallish fintech partners provide the APIs behind our PSD2 integrations, the voice authentication we are piloting in our call centres, the face recognition for our ID app and the invoice scanner in our mobile bank.

Between these specialized applications and the underlying infrastructure services, today we rely on more than 50 cloud services that allow us greater speed, flexibility and security.

This migration into the cloud does not come without risks. Having fewer companies provide a deeper stack of services inevitably means concentration risks, which regulators are increasingly focusing on. Lock-in effects pose real risks to competition and vendor diversity.

Regulatory authorities are right to be vigilant about these new risks. DNB have maintained a close dialog with our chief regulators, the Norwegian FSA and the Bank of Norway. Our thinking has evolved on both sides of the table as we have gained more experience with the upsides and possible downsides of outsourcing systems of varying degrees of criticality.

Fortunately, thinking has evolved among the cloud providers we work with, too. Thanks to close dialogue with our national regulators and some of the major U.S.-based service providers, we have secured a greater degree of transparency and audit rights than seemed possible a few years ago.

Cloud providers that barely had a national presence in many EU countries, are engaging with both clients and regulators in Europe, and display a better understanding of European concerns about issues such as privacy, competition and security.

Certification and licensing regimes might be useful in certain scenarios, but current rules e.g. for payment providers means licensing regimes are already in place. Taking a risk-based approach, regulators should focus on the main platforms than entail systemic risk, as well as those that provide core financial services.

Applying stringent licensing requirements for all suppliers means erecting barriers to entry for new actors as well as many of our current providers, many of whom are precisely the kind of small, tech-savvy start-ups we should be encouraging.

In seeking to mitigate the risks of the cloud through regulatory measures, EU legislators and regulators need to be careful not to throw the baby out with the bath water. Regulators, cloud providers and financial institutions need to work closely together to ensure the European financial industry is able benefit from the power of the cloud. ●