

WHITEPAPER

Product development and innovation generate the need for cloud-based IT infrastructure for the financial industry



Background

The recent trend development of cloud-based IT infrastructure services (IaaS) has brought enormous opportunities for many companies and organizations who have chosen to outsource all, or parts of, both development and production to such solutions. The benefits are many but predominantly it is about gaining a better cost control. Resources are utilized in a more efficient way when you don't need to invest in over-capacity and when you get access to the most up-to-date technology and security solutions without having to account for the investment.


However, studies and surveys have shown that in many cases the banking and financial sector felt compelled to stand in the background. This is mainly due to the many safety and regulatory aspects incumbent upon the industry, which has lead banks and financial institutions to believe that they can't embrace the latest technologies in their service delivery. In July 2015 American Computer Weekly¹ reported that security, integrity, risk and regulatory expertise represented, in said order, the major obstacles to the sector's willingness to adopt IaaS.

At the same time, there are few industries that are as digitized in their service delivery as the financial sector. In light of recent developments towards more mobile applications, the industry has faced increased requirements on agility in relation to product development. This has also been recognized through research. In 2015 Bankingtechnology.com² referred to an international study where top bank executives claimed that the digitization of their business was the number one business priority over the next five years.

To be able to deliver on customer demands and expectations, the IT infrastructure needs to support these circumstances at all stages. In other words, the IT infrastructure needs to be sufficiently agile to support business innovation.

¹ <http://www.computerweekly.com/news/4500249971/The-obstacles-to-software-as-a-service-adoption-in-banking>

² <http://www.bankingtech.com/283661/digitisation-replaces-regulation-as-top-concern-for-retail-banks/>



Few businesses and industries today would dream of owning and managing their own power plant. As we know, electricity has been delivered as a service simply through the wall socket for ages.

Generation Z is digitized and restless

Most likely we have barely seen the dawn of the digital revolution, where in recent years the development of new services, platforms and devices constantly changes. Soon, a new generation of consumers will come of age and they have never seen a mobile that isn't smart. What this will imply is still not clear, and the only thing we can say with absolute certainty is that these consumers will demand more.

Generation Z is perfectly comfortable navigating the digital landscape, and know how to acquire information about the best applications for any task at hand.

This generates new demands on innovation, development and thus also the IT infrastructure.

Data centers at a crossroads

Today the data center as the aorta of the IT infrastructure stands at a crossroads. The decision that needs to be made is usually not if, but rather when, it needs to be phased out as the midpoint of the entire IT operations. We know for a fact that to manage a data center, although outsourced, is expensive.

Significant investments in excess capacity are often needed in order to meet peaks, and another budget burden is the continuous replacement of old systems. Security is another major concern that consumes enormous resources of time and money. IT infrastructure management is not a core task for the IT department at any service company, much less a bank or an insurance company.

The CIO and the IT department staff should instead devote all their energy on development, simply because it's business critical.

In the wake of new technologies and cloud services being born, the data center function can be likened to a power plant. Few businesses and industries today would dream of owning and managing their own power plant. As we know, electricity has been delivered as a service simply through the wall socket for ages.

Cloud is the new base

The same development is now happening within IT infrastructure. The solution to the cost inefficiency of owning and operating a data center is to locate production, testing and development in the cloud. This is something that the financial sector in general has been hesitant about, but today there are few obstacles. The traditional starting points that have prevented cloud adaptation in the financial sector are now outdated, and the modern cloud providers have every opportunity to make sure that companies in the financial sector can comply with all existing laws and regulations, without sacrificing security and availability.

The dilemma for banks and insurance companies

As outlined above, banks and insurance companies have a number of challenges that businesses outside their industry do not have. It is mainly related to the regulatory requirements that both increase over time, and change frequently. We have Basel and Solvency covering information management and its traceability. In addition, few other industries are as monitored and have as many investigative authorities constantly watching them. Moreover the industry is subject to much higher demands for physical security than other sectors. All together it might be perceived as challenging, since the sector operates in a time when banks are just as exposed to competition as any other industry.

We want to hereby give you some advice and arguments to test the possibilities of turning the IT infrastructure into the cloud and at the same time give some practical tips on how to get started in a smaller or larger scale.

Why banks should invest in public cloud solutions

Efficient development

To develop and test services in an IaaS environment is more effective simply because developers get access to the latest technology and tools to develop and test their services, meanwhile the company does not need to invest heavily in updating its own development systems. Today the availability of completely open development standards in the cloud like OpenStack, has created entirely new opportunities when it comes to rapidly test and deploy new services.

Cloud is cost efficient

You have probably heard this argument many times – but whether the project is intended for test and development or simply normal production, you only pay for what capacity you allocate. This, in turn, means that the problem of overinvesting in hardware capacity to secure operations completely disappears. In addition, you are not required to make investments in constantly updating and maintaining security systems.

Security in focus

Discussing cloud internally often causes many skeptical questions about security. All cloud service providers perceive and thus manage security as part of their core business, which means they are always updated and in sync with the latest security developments. A good way moving forward is to ask your supplier what certifications they have. As for example – the latest ISO 27001 certification has a number of requirements for data management related to security.

The advantage of running, for instance, development and testing in the cloud is that these processes get completely separated from the production environment and can therefore continue undisturbed.

Start with a defined project

For many companies, the big question is when and with what to begin. For many businesses it may feel better to start small scale to test IaaS. And many choose to run just a development or test project initially to be able to check the environment, and as next step, scale up with more projects or transfer parts of their production in to the cloud.



What to consider when taking the step to procure a public cloud service solution

Cloud and the law

Common opinions against moving development, testing and production in to the cloud are that it might be illegal to do so as a financial institution. Illegal in the sense that the company wouldn't be able to meet all the existing regulatory requirements. This is actually incorrect but however, a financial institution needs to be a critical purchaser and specifically keep an eye on a few key things:

- Where is your data stored?
- Who has access to your data?
- Who is responsible?

Where is your data stored?

An important criteria that most Financial Supervisory Authorities and Government Data Agencies around the world require, is that data should be protected by the laws and regulations of the country from where it originates. Since the legislation on data storage is tricky and not always synchronized between countries, a rule of thumb is to make sure that your country's laws and regulations always apply to the data you store. It is also important to verify which countries your country has agreements with regarding data protection and to make sure that this chain of agreements is never broken.

About half of the EU countries respect other countries' agreements in relation to data storage, whereas there are countries such as the UK, where domestic laws can overrule other countries legislations with regards to, for example, personal data. The same applies to the US.

But the whole thing is a bit more complicated than just storage location, because it may also be significant in which country your service provider has registered its business.

We have seen examples where governmental institutions have used e-mail services from a domestic supplier, who in turn, is a reseller of said services from a US-based company. In clear text; US regulations might overrule your local agreements with a US based company.

It is not at all impossible to use cloud services from suppliers in other countries, but attention needs to be paid to what laws and regulations apply in the specific country, in order to ensure your own domestic regulations will not be overruled.



Who has access to your data?

In some countries data administration must be managed by a person physically located in the country from where the data originates. So why is this so important? If data would be stolen or compromised by the people assigned to manage it, it is important that national legislation does not change or overrule employment contracts for instance or the other way around. In brief, employment contracts need to be able to comply with national legislation. Note that this may also apply when your company hires staff working from another country. Needless to say, not being able to protect your own and your customers' data according to the legislation in your own country could potentially hurt the business quite hard.

Who is responsible?

Since the provider of IT services is an extended arm of your own operations, it is important that the supplier's staff is assigned with the same personal responsibility as your own staff to improper handling of personal data. In summary, with the right kind of partnership in place with your provider, IaaS is not an obstacle to any industry or business. The advices listed above are based on both legislation and current practices.

Cleura is the European cloud, offering fully automated digital infrastructure services for companies that want to innovate without sacrificing data privacy.

By delivering compliant and secure infrastructure technology built on open-source, Cleura provides organizations with a sustainable foundation for innovation with complete control over their data.

As a part of **Iver**, Cleura is headquartered in Sweden with cloud zones across the world.