www.pwc.ch

Taking Swiss Private Banking to the Cloud

Regulatory situation and consequences in Switzerland and EU

The Swiss Regulator FINMA has amended its circular 2008/7 'Outsourcing – banks' and released the new circular 2018/3 'Outsourcing – banks and insurance companies'.

This new circular applies to banks as well as insurance companies. It introduces important changes in the definition of the materiality of outsourcing, the requirements for intra-group outsourcing, the requirements relating to systemically important banks and the outsourcing of risk and compliance functions. Changes in the requirements for outsourcing abroad are also of particular importance. On the other hand, requirements relating to data protection and client information have been removed from the circular because, according to FINMA, these are regulated by other laws. Therefore, the Swiss Data Protection Act is now the guiding principle, whereby the data protection levels of countries are more important than merely the borders between them.

According to the interpretation of the law, using cloud technology – and, potentially, external cloud providers – is viewed as outsourcing. Consequently, using international cloud providers with data centres located abroad is seen as outsourcing abroad.

The new circular entered into force as of 1 April 2018. There is a transition period of five years for existing outsourcing arrangements to comply with the provisions of the new circular.

At international level, outsourcing options and the use of external cloud providers have been subject to new regulations in recent months. These provide financial institutions with guidance from a regulatory perspective. For example, the regulatory body in Luxembourg (CSSF) and the European Banking Authority (EBA) have issued circulars and guidelines:

- CSSF circular 17/654 'IT outsourcing relying on a cloud computing infrastructure', 17 May 2017
- EBA/REC/2017/03 'Recommendations on outsourcing to cloud providers', 20 December 2017 (will be integrated in the new EBA guidelines mentioned immediately below)
- EBA/CP/2018/11 'Consultation Paper on EBA draft guidelines on outsourcing arrangements', 22 June 2018

Impact

Changes in the requirements promulgated by FINMA and international regulators allow banks and insurance companies to think about new opportunities in the area of outsourcing, such as for example, using cloud services.

In connection with cloud services, the impact of the CLOUD Act is often discussed. The 'Clarifying Lawful Overseas Use of Data' (CLOUD) Act allows US law enforcement to request from US providers of electronic communication services the data stored from US persons. These data have to be provided irrespective of where the stored data is located, whether on US soil or abroad. But providers are given the right to file a motion in front of a US court to modify or quash the legal process if the provider reasonably believes:

1. The person is not a US person and does not reside in the US; and
2. There is a material risk of violating the laws of a foreign government.

The right to file a motion has to be actively pursued by the provider within 14 days.

Thus, the CLOUD Act clarifies the situation under which US providers have to provide data and what the provider's rights are.

We see a clear tendency for banks and insurance companies to use (international) cloud providers to reap the benefits of various cloud business models. PwC is helping banks and insurance companies to change their operating models to comply with regulations governing the use of international cloud providers. Starting with asset management and investment banking, more and more private banking services are going to be discussing and implementing cloud set-ups.

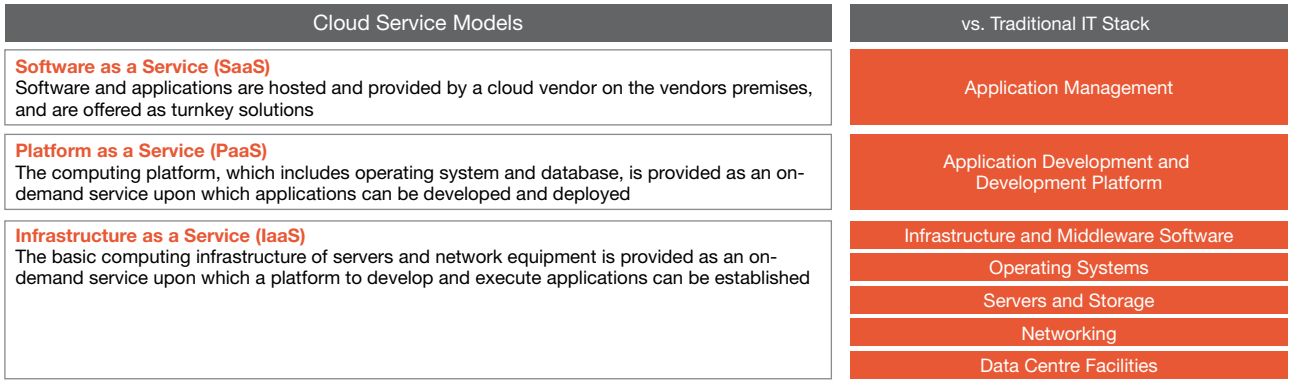
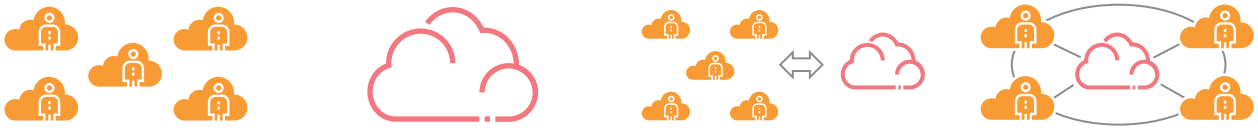


Fig 1: Cloud service models compared with traditional approaches

Technological possibilities



Public cloud

The infrastructure and computational resources are made available to the general public over the internet. It is owned and operated by a cloud provider that is external to the consumer' organisations.

Private cloud

The computing environment is operated exclusively for a single organisation. It may be managed by the organisation or by a third party, and may be hosted within the organisation's data centre or outside of it.

Community cloud

It is similar to a private cloud, but the infrastructure and computational resources are exclusive to two or more organisations that have common privacy, security, and regulatory consider-ations, rather than a single organisation.

Hybrid cloud

This model involves a composi-tion of models (e.g. private and public clouds or on-premises and public cloud). Each model remains a unique entity, but is bound to the others through standardized or proprietary technology that enables identities, application and data portability among them.

Fig 2: Cloud services can be deployed in multiple models

The term 'cloud' is used in combination with various IT business models and solutions. Thus, the exact meaning can differ from situation to situation. Sometimes, it just means (traditional) IT outsourcing to a multitenant-capable solution accessible via the internet.

In the due diligence process, it has to be understood and evaluated what the cloud services comprise exactly and what is provided.

Cloud service providers (CSPs) offer 'as a service' infrastructure (IaaS), platforms (PaaS), functions (FaaS) or software (SaaS). They often have business and operational models in place whereby customers are billed on a pay-per-use basis. Hence, CSPs do not have to know how customers are using the services and what kind of data they are processing ('content agnostic').

With a local or Swiss-based CSP, the data processing is often carried out within Switzerland. Very large CSPs, on the other hand, have data centres located around the world. Nevertheless, even large CSPs may restrict data locations and processing to regions/countries according to the customers' wishes. These CSPs place data sovereignty in the control of the customer. Thus, services can be obtained from specific data locations or regions and processing is set up in line with the customer's own framework ensuring compliance with, for example, the EU's General Data Protection Regulation (GDPR).

Purchasing cloud services from a professional CSP is also an opportunity for organisations for which IT and cyber security is not a core competency. Such organisations may be challenged to keep abreast of developments in IT and cyber security. But they can benefit from the capabilities of a CSP to modernise and transform their security frameworks to adapt to current and future IT and cyber risks. Thanks to their economies of scale, larger CSPs have the capabilities to keep the security bar at the highest levels to thwart attackers. However, security pitfalls are often due to the incorrect integration or insecure use of cloud services by organisations. Furthermore, the data sovereignty principle puts the organisation in the driver's seat to implement appropriate security measures at the data level, such as encryption, anonymisation or pseudonymisation, which may also be sourced as services from the CSP.

Accelerate Time to Market

- Immediate access to computing and storage recourses
- Rapid provisioning of virtual servers to keep pace with changing workloads
- Greater ability to resolve challenges and improve service consistency

Respond Rapidly to Changes in Demand

- Ability to scale services up or down based on group demands
- Automated scaling driven by pre-defined service-level agreements (SLAs)

Innovate with the Business

- IT barriers to innovation lowered
- Alignment of flexible IT infrastructure with changing business demands
- More agile and reliable technology management

Optimise Cost & Usage of Asset

- Resources pooled to create system efficiencies
- Flexible Pay-per-use based on demand cycle
- Improved utilisation: Institutions grew their data centre utilisation

Fig. 3: The potential benefits of cloud operating models

Realising your cloud vision means a shift in your operating model

Operating in a cloud environment will change your current operating model, as it requires deeper integration with the vendor and better management of the vendor relationship.

Figure 4 shows the six dimensions of a cloud-operating model. The first three of these will become more important and they require specific skills in IT if a cloud set-up is to be realised.

In detail, companies need to focus on better management of the relationship with a vendor, the related security aspects and service level agreements. This can be done by closely collaborating with the vendor on its product road map and the possibilities to leverage additional tools and better integrate the cloud stack with the tools offered, so that the company is able to take maximum advantage of the integration (e.g. AI development tools of the cloud provider).

Depending on the goals of your cloud vision, for example harmonising infrastructure to reduce risks or simplifying applications across the globe, different actions will be called for in order to integrate successfully. However, regardless of the chosen vision, the re-skilling of staff and the redesign of processes and SLAs will be key to realise the benefits of a cloud environment.

Shifting workloads to the cloud only does rarely bring expected benefits. In fact a combination of processes and operating model transformation, in combination with adopting new possibilities of the cloud capabilities creates additional value to the organization. This also requires to have engineering, operations and application development involved early in the journey.

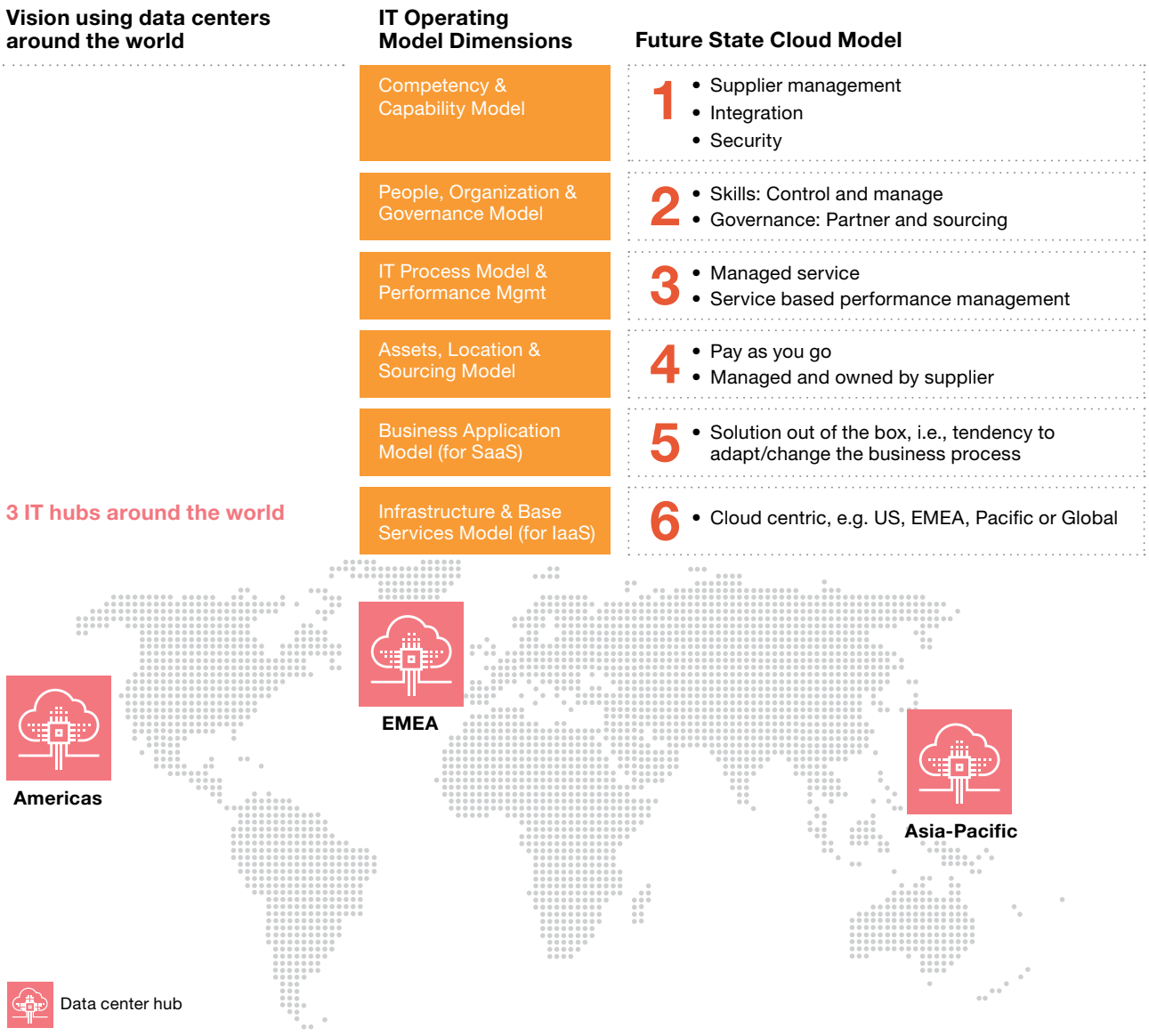


Fig 4: Cloud vision and target IT operating model

Operating in a cloud offers significant opportunities

Banks are looking at cloud solutions to transform traditional IT departments into a business growth engine, revamp operations to achieve scale and enhance speed and collaboration, and spark innovation around new products and services to generate new sources of revenue.

Cloud-based solutions can create remarkable opportunities across the whole institution as they present strategic ways to strike a balance between enabling business growth and innovation and lowering costs while still continuing to provide operating efficiencies.

Gartner's latest forecast for the global public cloud market estimates that the market size in 2021 will be approximately USD 473.1 billion. If we only include IaaS, PaaS and SaaS revenue, the market estimate is USD 228.6 billion. As of 2016, approximately 17% of the total addressable markets for cloud infrastructure, middleware, application and business process services will have shifted to the cloud. By 2021, Gartner predicts that the cloud shift for these markets will increase to 28%.

Every financial service provider is confronted with the increasing disintegration of its current value chain. Universal banks as we know them, servicing customers' needs by designing, creating and deploying services on their own, are coming to an end. Increasingly, Fintech companies are penetrating parts of the value chain by developing and spreading technological and business innovation – often within months if not weeks.

The ability to integrate new services seamlessly and almost immediately becomes a key differentiator in winning customers. Customers get used to downloading new apps and having solu-tions as a service at their fingertips – anywhere and at any time. The main differences compared with traditional IT solutions are:

- 'Order-to-Spec': pre-defined services are made available immediately;
- The provisioning process is highly or fully automated, allowing for rapid availability, i.e. within minutes or hours;
- Options for each service are limited, discrete and predetermined (e.g., 'cookbooks');
- Break/fix is automated.
- Available capacity is mandatory and bursting to external cloud providers is a design option.

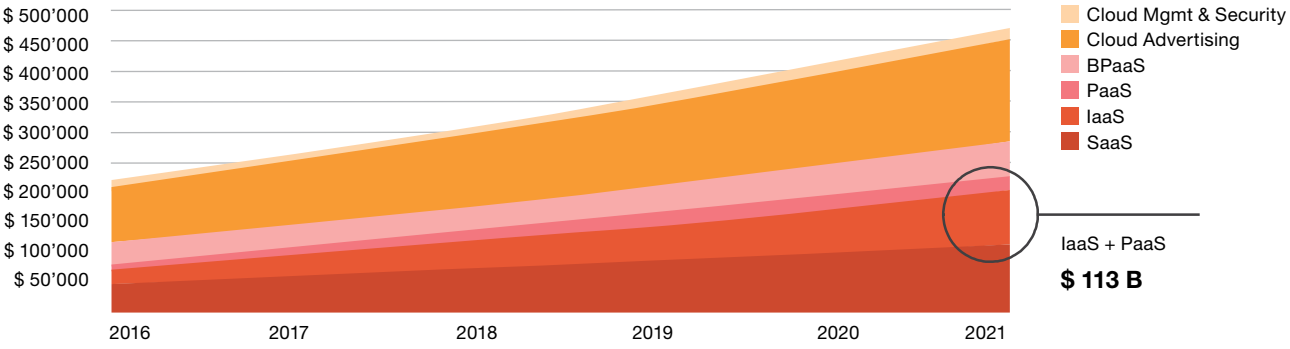


Fig 5: Gartner public cloud market forecast

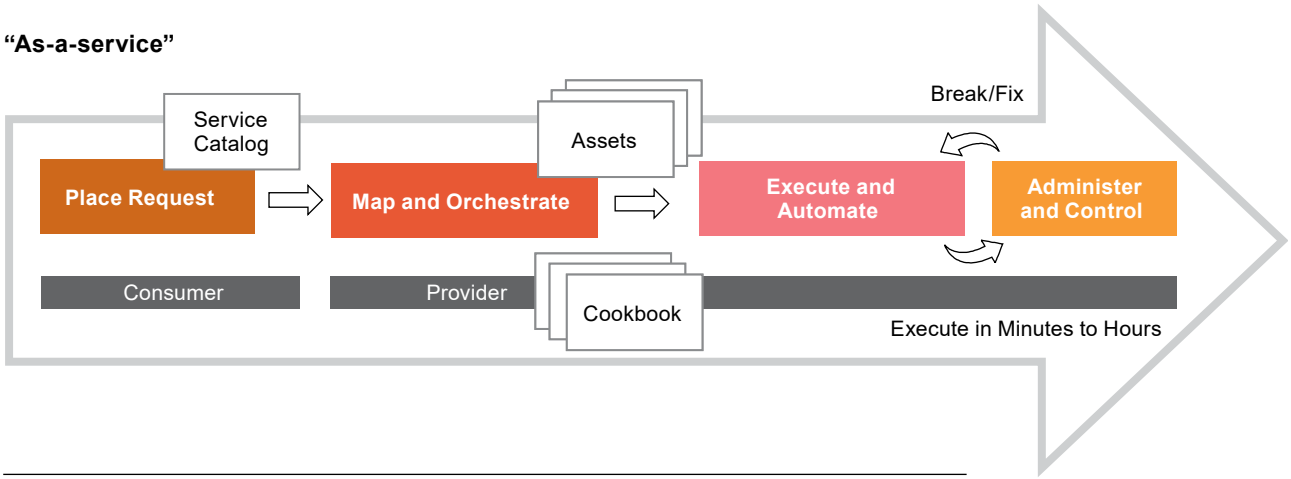


Fig 6: New characteristics of 'as-a-service' (aaS) delivery

Key challenges in bringing Swiss private banking to the cloud

One of the key elements to the success of Swiss private banking in creating decades-long trust in its business model is the protection of customers' assets.

Besides Switzerland's political stability and neutrality in military conflicts for the last 100 years, the industry has also kept banking relationships confidential. Only lately has its reputation started to waver, in part due to regulations that aim to increase tax transparency but also to security breaches perpetrated by individuals. Nevertheless, customer identification and the storage of related client identifying data (CID) is a key element of the current business model and it will be hard to change.

There is a clear difference between Swiss banks and their international counterparts in the use of cloud business models. While many international banks are open to move to the cloud for most of their operations, Swiss banks are particularly reluctant to use similar business models – not least in light of recent regulation.

Nevertheless, the industry in Switzerland is starting to change. Banks are gaining initial experience in using cloud providers. Starting from non-critical processes and environments, increasingly critical business processes will be moved to the cloud. First-movers began with asset management processes and they are now looking into private banking and wealth management processes, including CID. Based on our experience of supporting banks in implementing cloud services relating to CID, we have identified the key aspects that demand the most thought. These aspects include (non-exhaustive list):

- Data protection: It is important to understand the level protection provided by the countries in which data are to be processed, accessed or stored. Depending on this data protection level, additional measures might be necessary to provide adequate protection of personal data.
- Banking secrecy: In general, Swiss banking legislation allows outsourcing and does not distinguish between domestic and foreign outsourcing. However, any transfer of data/breach of banking secrecy must have the (implicit) consent of the client. Furthermore, the appropriate protection of data has to be ensured irrespective of whether the bank is using a service provider or not.
- Security: Security and trust are critical aspects when defining a cloud strategy. Few companies are comfortable allowing sensitive data to reside outside their firewalls and trusting vendors to provide adequate security is equally difficult, especially when there is a chance that the cloud environment may include other organisations' data as well. Most large cloud providers give clients detailed insights into the security of their data centre solutions and provide audit comfort through the use of external security and controls audits. However, thought should also be given to anonymisation, pseudonymisation, encryption,* communication encryption, database encryption, application encryption, key management, etc.
- Anonymisation: Banks need to define whether the anonymisation of CID provides an adequate solution balanced between security and business need. From a data protection perspective, anonymisation might be one of the best solutions, but it may hinder the business from benefitting in full from a cloud provider's services.
- Data accessibility in and from Switzerland: FINMA circular 18/3 and its consultation report specify that data locations can be abroad but access to data must be ensured at all times in or from Switzerland in the event of the restructuring or winding down of the bank.
- Client information: Based on the decisions taken regarding encryption and data anonymisation, information for clients about the bank's outsourcing arrangements and data locations must be considered and evaluated as part of the contractual frameworks, e.g. terms of business. However, in most cases, the explicit consent of clients is not required.
- In defining cloud strategies, it is necessary to document – as part of a diligent and comprehensive risk analysis – the identified risks, the defined measures, the evaluation results and the decisions taken in order to demonstrate legal and regulatory compliance.
- In general, from a legal and regulatory perspective, there is no 'showstopper' regarding the use of cloud business models by banks. However, specific risk considerations and contractual agreements may influence individual bank's cloud strategies.

* Anonymisation, pseudonymisation, encryption – definitions according to FINMA circ. 2008/21, Appendix 3

What else to look out for

As with any technological frontier, the cloud has its pitfalls. Every enterprise that plans to trust applications and other computing services to a cloud computing environment needs to address the following issues before the first service contract is signed. When evaluating a cloud vendor, enterprises should look carefully at:

- Vendor reputation: Don't be the test case for a vendor's competence.
- 'Ironclad' service-level agreements: Make SLAs consistent with your bank's business objectives.
- Business Continuity Management (BCM): Vendors store critical data outside their clients' firewalls, therefore BCM needs to be examined closely.
- Exit path: What happens if the bank decides to terminate a cloud computing agreement?
- Vendor pricing model: CIOs must understand how the cloud service will be used and how frequently the terms of the subscription can be changed.

PwC has significant experience and capabilities in supporting the set-up and integration of cloud environments with all major cloud providers. We are proud to have established partnerships with these providers and we can advise you as a neutral partner both during the selection of a suitable solution and later in the integration phase and in monitoring quality and service delivery.

Global Cloud Capabilities

PwC Cloud Professionals:
2,500+ in over **60** countries.

PwC Thougt Leadership:
published **100+** thought leadership pieces around cloud computing.

PwC Recognition:
Named a **Leader in Worldwide Cloud Professional Services** in the IDC MarketScape report

PwC Cloud Project & Clients:
230+

Contacts

Dr. Marcel Tschanz
Partner
Swiss Head Wealth Management
+41 79 540 60 80
marcel.tschanz@ch.pwc.com

Jens Probst
Partner
Risk Assurance FS
+41 79 372 57 88
jens.probst@ch.pwc.com

Marco Schurtenberger
Senior Manager
Risk Assurance FS
+41 79 674 20 92
marco.schurtenberger@ch.pwc.com

Urs Küderli
Director
Cybersecurity and Privacy
+41 79 912 13 13
urs.kuederli@ch.pwc.com

Chris Fraune
Director
Advisory FS
+41 79 238 64 74
christoph.fraune@ch.pwc.com

Michel Müller
Senior Manager
Advisory FS
+41 79 204 64 91
michel.mueller@ch.pwc.com