Cloud for FINMA-regulated organizations

Tackling the most common challenges

Florian Georg—Developer Audience Lead, Microsoft Switzerland

Michael Siebert—Senior Solution Architect, Red Hat Switzerland

Paul Weinrich—Cloud Strategy—Cloud Regulation and Data Protection, Accenture Switzerland

Florian Schulz—Principal Director Cloud and Infrastructure Advisory, Accenture Switzerland

Executive summary

Swiss financial firms are drawn to cloud computing. But where many advantages and innovative solutions are waiting to be discovered, various difficulties also exist. This whitepaper identifies the most important regulations for Swiss Financial Market Supervisory Authority (FINMA)-regulated organizations, explains the most common myths, and gives practical tips for the journey to a cloud environment.

Introduction

Like many organizations, Swiss financial companies are looking for ways to innovate their business and benefit from digital technology. The awareness of what cloud computing can do in that regard and how it can help banks succeed has grown considerably in recent years. Cloud services open up new opportunities for banks to develop innovative business models and more efficient processes. The competitiveness of the banking sector can be improved with the migration of banking infrastructure from traditional on-premise systems to a cloud environment.

Nonetheless, the use of cloud services is currently associated with legal and regulatory uncertainties. In 2018, FINMA published Circular 2018/3 entitled *Outsourcing–banks and insurers*[1], which defines the requirements that banks, securities dealers, and insurance companies must abide by when they outsource to a service provider any functions that are significant to the company's business activities. Any company that outsources its business activities is accountable to FINMA, just as it would be if it carried out the outsourced functions itself.

This whitepaper aims to give technical decision makers within FINMA-regulated organizations an overview of some of the most common questions to address before moving to a hybrid cloud environment.

One common challenge we see is that the technical leaders responsible for cloud adoption are not experts in IT compliance and data protection laws, while legal and compliance experts know little about the technical implications and practicalities.

There are still widespread misconceptions and emotional (rather than legal) arguments about what exactly is required by the regulators when using a public cloud service. And even when the requirements are properly understood, it is often not obvious how to put them into practice. We hope to dispel these misconceptions by:

- Clearly stating what some of the most misunderstood FINMA compliance requirements mean (and do not mean).
- Discussing some generally good cloud adoption practices that help organizations become—and remain—compliant when adopting a public cloud strategy.
- Giving clear, useful examples of how we have successfully implemented these practices for some of our financial services industry customers in Switzerland, using our products and services.

This whitepaper does not claim complete legal certainty and therefore does not provide any legal or regulatory advice. Rather, our aim is to provide those responsible for information security and compliance in banks with practical advice, tips, and best practices for the move to a cloud environment.

1 FINMA Circ. 18/3 Outsourcing – banks and insurers." finma, 21 Sept. 2017.

Regulations and myths

To begin, we will look at some key regulations for financial institutions that must be observed when using cloud services:

- FINMA's Circular 2018/3 *Outsourcing–banks and insurers* defines the supervisory requirements applicable to outsourcing solutions at banks, securities dealers, and insurance companies in terms of appropriate organization and risk limitation.
- The Swiss Federal Act on Data Protection (FADP) aims to protect the personality and fundamental rights of natural and legal persons about whom data is processed.
- The U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act defines how authorities in the United States can access data stored by U.S. internet companies and IT service providers.

As this overview shows, FINMA-regulated organizations have many rules to consider when migrating to a cloud environment. It is therefore not surprising that there are several myths surrounding adopting a cloud strategy in the financial sector. Three issues in particular require clarification.

"Where security-relevant functions are outsourced (particularly in information technology), the company and the service provider must contractually agree on security requirements. The company must monitor compliance with these requirements." (FINMA Circular 2018/3, margin 24)

Myth 1—Cybersecurity: Cloud computing is less secure than on-premise IT. There are more security breaches in a cloud environment.

Reality: More than 95% of cloud security incidents are due to misconfigurations by end users. Public cloud providers deploy far more resources to monitor and mitigate security breaches and cyberattacks than a local datacenter operator is able to. Their global teams draw their experience in securing workloads and the cloud platform not just from a single organization but from many other critical workloads. In order to mitigate risk, shared responsibility and clear governance for each service used in a cloud environment (from IaaS to SaaS) is necessary. It is critical to understand the shared responsibility model as well as the security tasks handled by the cloud provider and those handled by the organization itself.

"Furthermore, the eventuality of a change of service provider and the possible consequences of such a change must be considered when deciding to outsource and selecting the service provider. […] Provision must be made for insourcing the outsourced function in an orderly manner." (FINMA Circular 2018/3, margin 18)

Myth 2—Exit strategy: Cloud services must be able to be recovered at any time. Two parallel environments must be maintained.

Reality: An exit strategy includes strategic considerations aimed at facilitating the transfer of applications within 3-6 months. The technology exists to enforce this through homogeneous platforms (e.g., same container platform), which makes it possible to build a platform agnostically.

"Outsourcing to another country is admissible if the company can expressly guarantee that it, its audit firm and FINMA can assert and enforce their right to inspect and audit information." (FINMA Circular 2018/3, margin 30)

Myth 3—National data sovereignty: Confidential data in financial organizations, such as personally identifiable information (PII) and bank account details, must always remain within Swiss national borders, and may only be accessed by persons who live in Switzerland and/or fall under Swiss jurisdiction.

Reality: FINMA-regulated institutions must ensure that they are aware of the classification of their data and the protection requirements. With adequate technical and organizational measures such as end-to-end encryption, data segregation, and least privilege access, a transfer of data outside of Switzerland is possible. Remote access such as IT support from foreign experts is allowed provided that processes are in place to restrict such access and monitor privileged rights (e.g., through time-restricted access, clear access protocols and audit trails). The concrete issue is that while these IT governance processes already exist, and organizations have spent years establishing, documenting and approving them, they cannot simply be copied and pasted from an on-premise scenario to a cloud model.

Fortunately, you do not need (and should not even try) to shoehorn on-premise processes into a cloud environment. Cloud services can help to simplify and innovate. New cloud-ready shared responsibility models can help make organizations more agile, efficient, and cost-effective—while ensuring compliance and improving the level of IT security. At present, banks see the guarantee of keeping data in Switzerland as a greater added value for customers than innovative technologies. The question is whether a change will take place in the future, so that out-of-the-box technologies that are not developed and operated on-premise will be seen as offering greater added value.

The regulatory framework in Switzerland permits the use of cloud services, including public cloud services. The transfer of data outside of Switzerland is also allowed, provided that certain requirements are met:

- The financial institution (FI) must be able to expressly guarantee that it, its audit firm, and the regulator can assert and enforce their right to inspect and audit information.
- The possibility of restructuring or resolving the FI in Switzerland must be assured. Access to information required for this purpose must always be possible in Switzerland.
- Personal data may only be transferred to countries with legislation providing for an adequate level of protection of personal data.
- If data is to be transferred to a foreign country that does not have legislation providing an adequate level of data protection, certain conditions must be fulfilled.
- The Federal Data Protection and Information Commissioner (FDPIC) may also need to be notified in certain situations.

FINMA does not require prior approval or notification of outsourcing arrangements. However, FIs should be ready to demonstrate to FINMA and the FDPIC how they are compliant as well as any adverse developments arising from their outsourcing arrangements.

It is recommended that customers validate these prerequisites with legal advisers, for example, by obtaining a legal opinion. As described below, Microsoft contractually commits to provide customers with means of inspecting and reviewing its services. This examination and inspection right has been validated by a range of regulators around the world.

There is no mandatory requirement for FIs to complete defined steps in order to use Microsoft cloud services. However, Microsoft has developed a checklist that maps the relevant requirements against its own contractual terms and conditions (Microsoft Cloud—Checklist for Financial Institutions in Switzerland).

The FDPIC has stated that the U.S. Privacy Shield does not provide an adequate level of data protection according to Swiss regulations. While Microsoft bases its data transfers primarily on standard contractual clauses and not on the Privacy Shield certification, and data transfers outside of the European Union (EU) are still legally possible, European countries in particular are still considered as offering "adequate" protection in relation to Switzerland and do not require specific legal and risk analyses.

On May 6, 2021, Microsoft President and Chief Legal Officer Brad Smith announced the establishment of the EU Data Boundary for the Microsoft Cloud. This will allow its customers to both process and store their data in the EU. This commitment will apply across Microsoft's main cloud services, namely Microsoft Azure, Microsoft 365, and Dynamics 365. Many of those services can already be configured to process data in the EU or Switzerland, but there are some global services that may store or process certain data outside of the specific geographical location. Microsoft is committed to extending these EU Data Boundary Solutions into its main cloud services to further enhance its current offerings. In addition to customers in EU Member States, customers in Switzerland and Liechtenstein will also have access to the EU Data Boundary. These datacenters power cloud services that help regulated customers achieve digital transformation and increase their competitiveness, with the assurance that they can operate in compliance with all applicable laws and regulations.

"The possibility of restructuring or resolving the company in Switzerland must be assured. Access to the information required for this purpose must be possible in Switzerland at all times." (FINMA Circular 2018/3, margin 31)

Major cloud service providers are offering cloud regions in Switzerland (e.g., Microsoft Azure regions, Switzerland North and Switzerland West).

Bearing in mind the above myths, we will now discuss the three core areas you should focus on: Know your data, technical accelerators, and the move to a cloud environment.

Know your data

Handling data the right way is a crucial part of any cloud migration. That said, it is important to know the types of data that exist. Broadly speaking, three kinds of data are relevant:

Synthetic data: This data is artificially generated according to set rules in order to fulfill a specific purpose. It has no relationship to any patterns of client data and can be immediately stored in a public cloud service since its loss would not be critical.

Anonymized data: This is productive data from which the client references have been removed. The client can no longer be identified, but certain patterns can be. For example, if a client trades a certain number of shares every month, you could identify the client by analyzing the trading patterns. This kind of data still requires a certain level of security in a public cloud approach.

Productive/client identifying data (CID): The highest protection level is required for this kind of data.

On the basis of these data types, three questions need to be answered when handling data:

1. Which data can be stored outside the country without any second-guessing?
   NonCID data (i.e., data that is synthetic, anonymized, or by its nature does not contain personal information) does not need to be protected to the same standards as CID. This data can be stored outside of Switzerland without further risk assessments or considerations.
2. Which data needs some protective action?
   Often, use cases do not require data to be personally identifiable, but rather to deliver anonymized or pseudonymized content in bulk, such as for market analysis purposes, data science, and machine learning. By eliminating the factors that make data personally identifiable, this data can then be processed in bulk in a cloud environment and deliver business value—without any risk of noncompliance.
3. How to treat data in a hybrid cloud scenario (front- to back-end)?
   While CID can be processed and stored in a cloud environment (inside and outside of Switzerland), some banks choose to keep their CID on-premise, depending on their risk tolerance and contractual situations. To benefit from a public cloud service, a hybrid cloud scenario is often set up, making it possible to:
   - Run noncritical and nonCID applications.
   - Run development and test environments, while keeping productive environments.

Recommendation for data processing: There are no regulatory restrictions on processing data outside of Switzerland provided the data is adequately protected. Thus, with the right level of data protection, workloads involving CID can be hosted in a cloud environment. Nevertheless, some contracts with end customers (especially in Wealth Management) stipulate data processing and storage in Switzerland. This is an internal rather than a regulatory requirement. In such cases, using hybrid cloud can be the solution: CID is stored and processed on-premise while nonCID can move to the public cloud.

Technical accelerators—preparing the move

Some things are mandatory before moving to a cloud environment such as a thorough analysis of the application landscape and which application uses which data. Other tasks are not mandatory but your cloud migration will suffer if you do not complete them; these are known as accelerators.

Recommendation for service abstraction and APIs: If applications are communicating directly with each other, this can cause deviations in connectivity and data exchange, as there is no single authority controlling the flow. However, even with full end-to-end control, nothing is certain, and there can be surprises. A helpful preparatory step may be to redesign the connectivity layers and route everything via one central application programming interface (API) layer. Within this layer, it is also possible to install a service abstraction. This has two benefits:

- It decouples the different applications from each other, which makes a subsequent wave-based migration to a public cloud service much easier.
- The IT department is aware of what data is exchanged and can install on-the-fly synthetic data parsers for test environments, e.g., to ensure that the correct data is being exchanged.

Recommendation for containerization: The dependencies, documented and undocumented, of an application with the surrounding infrastructure are immense. If the applications are transformed into a container environment by way of preparation, you will benefit from:

- Containers that abstract the infrastructure world completely from the applications.
- Being able to install on-the-fly security controls at the container registry level (e.g., the container registry Red Hat® Quay, which includes the on-the-fly vulnerability scanner, Clair).
- Being able to manage central security monitoring and control as well as policy enforcement with the right tool in place, even across different container platform clusters. In other words, it no longer matters where the containers are running—on-premise, hybrid, or full public—they are all following the same security requirements.

Recommendation for monitoring: The whole setup within a public cloud environment is most probably decoupled from the organization's existing enterprise-level security and compliance monitoring infrastructure. If monitoring into a container transformation preparation phase, you will benefit from:

- Application monitoring that ensures the business activity monitoring needed for compliance will be integrated into existing processes.
- No loss of control over which of your apps run where and in what state.
- Retaining cost control within a much more complex setup from a hosting point of view.

The monitoring needs to include not only the application state but the full infrastructure state, such as virtual networks or firewalls. If a change in this hardened setup happens as a result of an attack or error, the security department needs to be proactively informed so that it can take action.

Recommendation for infrastructure: Hardening a system with automation is often recommended. Automation entails the following benefits:

- Definition and testing the infrastructure with an automation framework in such a way as to automate not only the application but also the whole environment, including the container platform. This means you can define and run the system integration testing (SIT) stage with synthetic data, putting everything in a public cloud environment and then having it pen tested and signed off in a risk-free way, as there is no sensitive data involved. This saves money and provides much more agility because SIT environments are often part of the development team's responsibility, especially in an agile setup.
- Later on, when the infrastructure changes or deployment packages move on to the user acceptance testing (UAT) stage, an organization will know that every firewall rule, network, etc. is exactly the same as in the SIT, as everything is precisely defined in code. This removes a great deal of insecurity and provides many efficiency gains in the areas of defect analysis and security control verification.

Recommendation for operation: Things will change. To take advantage of full cloud potential, a new cloud IT operating model should be defined and implemented before a mass migration starts.

- Review activities, responsibilities, tools, and work processes for the future mode of operation to avoid the perception that a cloud environment is being operated as just another datacenter.

- Knowledge: Help business and IT teams using a cloud service understand what is possible and to focus on value, innovation, and continuous improvements.

The move to a cloud environment

Cloud services have reached maturity in terms of productive use so the question is no longer "why" but "how." To get the cloud adoption journey under way, explore the cloud adoption frameworks of the major public cloud providers to evaluate proven methodology and guidance designed to help cloud architects, IT professionals, and business decision makers succeed in their cloud goals.

In summary, there are a number of points to consider:

- Defining a cloud strategy: Set goals and ambitions and define cloud principles, including cornerstones that will guide the upcoming phases.
- Conducting a cloud assessment: If not already available, start with an exploration of the current on-premise environment, including the server and application landscape. Begin by assessing the migration potential, using a cloud migration checklist. Conduct a high-level walkthrough of the steps to refine your cloud computing plan, prepare your people for cloud computing, create an adoption strategy (roadmap and approach) and put in place cloud governance for transformation and operation.
- Creating a cloud roadmap: Defining an application roadmap helps to shape the volume and boundaries of a cloud transformation project.
- Align migration approach: It is important to select the right migration approach for each application. This is sometimes referred to as the 'xR' approach (Rehost, Replatform, Repurchase, Refactor, Rearchitect, Retire, Retain, Remove, etc.).
- Using a new cloud operating model: Do not simply copy and paste on-premise processes to a cloud environment. On-premise processes and guidelines are often designed for traditional technology and methods. To unlock the benefits of cloud in terms of both security and business value, opt for cloud-native policies, which can also support a faster go-to-market (e.g., through DevSecOps processes and culture, as well as through a higher level of standardization in the customization process—infrastructure as code, enforcing security policies, etc.).
- Designing cloud architecture: Before migrating the first workloads, work on a cloud design following the cloud adoption frameworks or well-architected guidelines. While cloud computing offers scope to change or reconfigure workloads quickly and easily, some basic preliminary design decisions need to be taken and given careful consideration as they may be harder to change once production services are operational. These include, but are not limited to, decisions about regions, account/subscription governance, network connectivity, and identity and access management.
- Building a cloud landing zone: Set up a cloud landing zone or target environment for the on-premise servers or new cloud-native workloads. Follow the best practices of the cloud service provider and consider an architecture that can be scaled out and also allows segregation of duties. Even if you are currently focusing only on the Swiss environment, think about an architecture that can be used globally.
- Starting the migration: Start with a proof of concept (POC) or a small population of workloads to gain experience and feedback regarding the specific environment and situation and adapt the plan and methods accordingly. As soon as the methodology and processes are proven and established, increase the number of workloads to keep the migration efforts as lean as possible. From a

compliance perspective, a foundation built on noncritical applications can help regulated companies ensure they are building a compliant and secure platform and address regulatory requirements adequately. Once cloud maturity is attained, critical applications can follow.

- Optimizing after migration: It is important to monitor the workload after the migration or deployment to verify that the selected cloud sizing fits the actual usage. Getting the architecture right in cloud computing is important as it is directly linked to performance and consumption costs; CPU/RAM are only two parameters in the equation.

At each step, it is encouraged to engage with a system integrator or trusted IT partner and work closely with your preferred cloud service provider to prepare your organization for cloud computing.

Choosing the right path for the cloud journey

Regulatory requirements are no barrier to large-scale cloud migration. However, to fully benefit from cloud computing, financial institutions should approach their cloud transformation from a risk/value-based perspective. It is necessary to clearly analyze and assess all potential risks associated with a cloud environment—from regulatory and financial damage due to noncompliance to reputational risks with customers—and compare these with the value and benefits of modern cloud services, innovation potential and additional revenue streams of new business models.

Often, the risks associated with cloud computing can be mitigated by identifying and addressing the requirements at an early stage through a clear positioning of the financial institution and then implementing them. In addition, setting up a clear governance structure to monitor the shared responsibilities and prove to regulators that the outsourcing management has a clear oversight can ensure that future audits do not interfere with the cloud program.

Adopting cloud computing is not a sprint but a journey. It is an agile approach that starts with noncritical workloads and matures with your experience addressing compliance and using the technology, resulting in an expanded cloud footprint.

With an increased footprint, suitable partners, the right cloud skills, and an awareness of cloud risks and how to mitigate them, FINMA-regulated companies will be well-positioned to move critical workloads away from traditional on-premise environments and benefit from innovative cloud services.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#F30105_1021