eraneos

FOCUS

The cloud in the regulated sector

From left to right: **Christian Mauz**, Partner; **Richard Hess**, Head of Digitalization at the SBA; **Hanspeter Christ**; **Cédric Moullet**; **Adrian Anderegg**, Partner; **Marc Raum**, Senior Manager; **Thomas Vogt**, Senior Manager; **Tom Schons**, Manager

Contents

The journey to the cloud in the regulated sector 4

The cloud in the regulated sector – an ambitious transformation 5

The cloud in the financial sector – a challenge in many ways 11

Interview with Richard Hess, Head of Digitalization at the SBA 15

The cloud in the public sector – an urgent imperative with a lot of potential 20

Pioneer in the Swiss government for the use of public cloud services 24

The journey to the cloud in the regulated sector

There is no longer any debate regarding whether or not the cloud will take off. That decision was taken a long time ago. Cloud providers did their homework and laid the foundation for the secure use of cloud services. But in the regulated sector in particular, there are various different framework conditions that must be taken into account for the compliant implementation of cloud strategies.
Christian Mauz

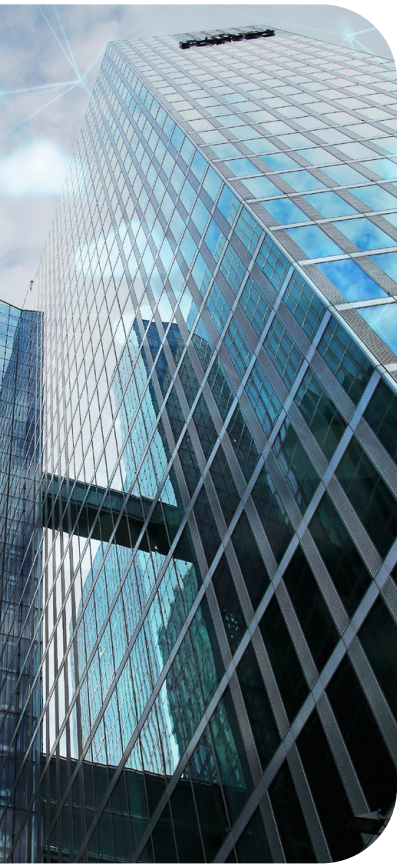
In the regulated sector, the cloud is also widely acknowledged to be an important harbinger of the digital revolution. But a large number of challenges are associated with using the cloud. What does a cloud strategy need to take into consideration? What form should the governance take? What roles, processes and guidelines are required for secure and compliant cloud usage? How should I go about migrating applications to the cloud that had previously been operated on site, and what does that mean for my organization and my operating model? The good news is that many of the early adopters have already successfully overcome a lot of these obstacles. So there is no need to reinvent the wheel. Cloud providers, and the hyperscalers in particular, also offer support. Nevertheless, the transition to the cloud presents IT organizations with a herculean task. In this issue of Focus, we would like to give you some food for thought on your journey to the cloud.

Another exciting development in this context is the major European cloud initiative GAIA-X, which aims to dispel persistent reservations concerning the cloud. GAIA-X was launched by German and French businesses, scientists and government agencies with the goal of working with other European partners to develop standards and rules for a next-generation data infrastructure. GAIA-X repre-sents an open, transparent and secure digital ecosystem in which data and services can be gathered, provided and collectively used in a reliable environment. One key element in this respect is reinforcing digital and data sovereignty in order to guarantee users full control over stored and processed data.

We wish you enjoyable reading.

> "As an enabler of digitalization, the cloud is also key in the regulated sector and essential for modern IT solutions."
>
> **Christian Mauz, Partner**

The cloud in the regulated sector – an ambitious transformation



Besides the legal framework that applies to all organizations, the regulated sector is subject to additional, more extensive or stricter standards and codes of conduct imposed by regulators. These increasingly also apply to digital business processes and set out the commercial and technical conditions for the integration and use of cloud services. The transition to the cloud therefore necessitates changes to governance and requires a conscious cultural shift.
Adrian Anderegg, Marc Raum, Thomas Vogt, Tom Schons

Some of the most important factors underlying the increased use of cloud services – and not just in the regulated sector – include:

- Virtual collaboration within organizations and with external partners, particularly in connection with communication and collaboration processes
- The rapid and automated provision of environments
- "Capacity on demand" in order to flexibly cope with spikes in workload and only pay for actual usage
- Significant, non-functional properties such as granular security functions as well as cyber security and privacy capabilities
- The rapid development and availability of modern technology solution blocks
- Providers only make new solutions available in the form of cloud services
- The focusing of in-house expertise on a higher level of IT value added

What are the challenges, obstacles and risks?

In its report "Clarification of the need for a Swiss cloud[1]," the Swiss government identified the unclear framework conditions for the use of public cloud services as a significant obstacle. While the financial sector has already introduced corresponding guidelines and policies for the use of the cloud, the use of cloud services in the public sector is often prevented by data protection laws as well as the crime of violating official secrecy (Art. 320 StGB).

Existing compliance guidelines, such as the incorporation of audit rights into sourcing contracts, need to be amended since this can often only be implemented in a public cloud context by ensuring compliance with relevant certifications. Cyber security standards and concepts such as the network zoning concept or the integration of existing SIEM[2] processes for cloud-based applications need to be reevaluated and redesigned. The availability of cloud specialists also poses a challenge on account of the "war for talent." The risk of vendor lock-in (i.e., long-term dependence on a single provider) also needs to be taken into consideration. Practice has shown that it takes a lot of knowledge and discipline to take decisions at the technical level that maintain the option of switching providers in a way that is economically sustainable.

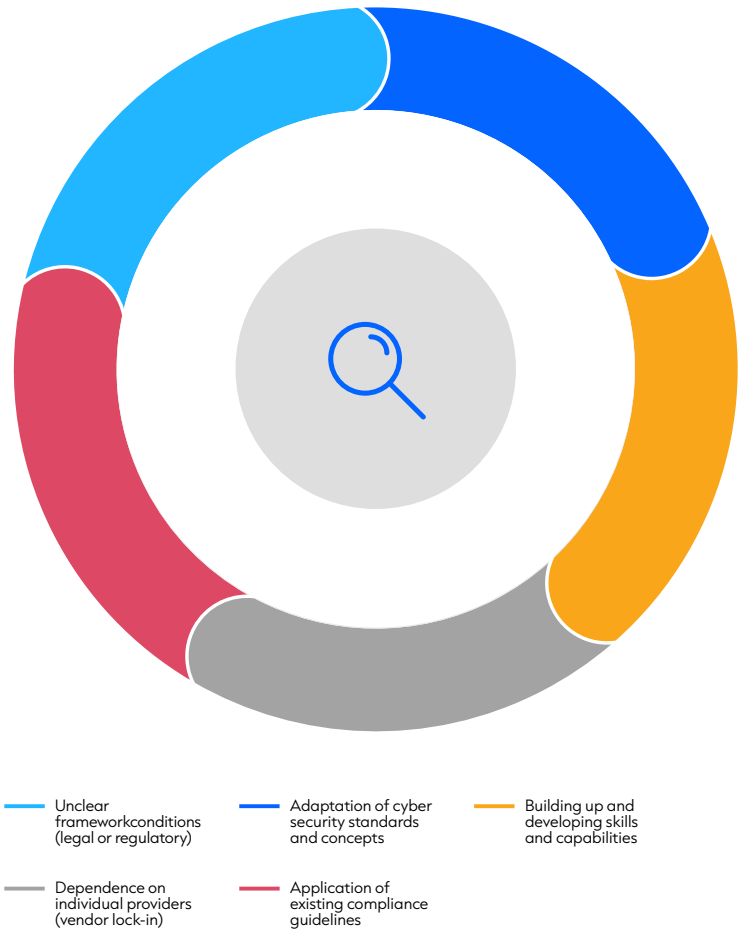


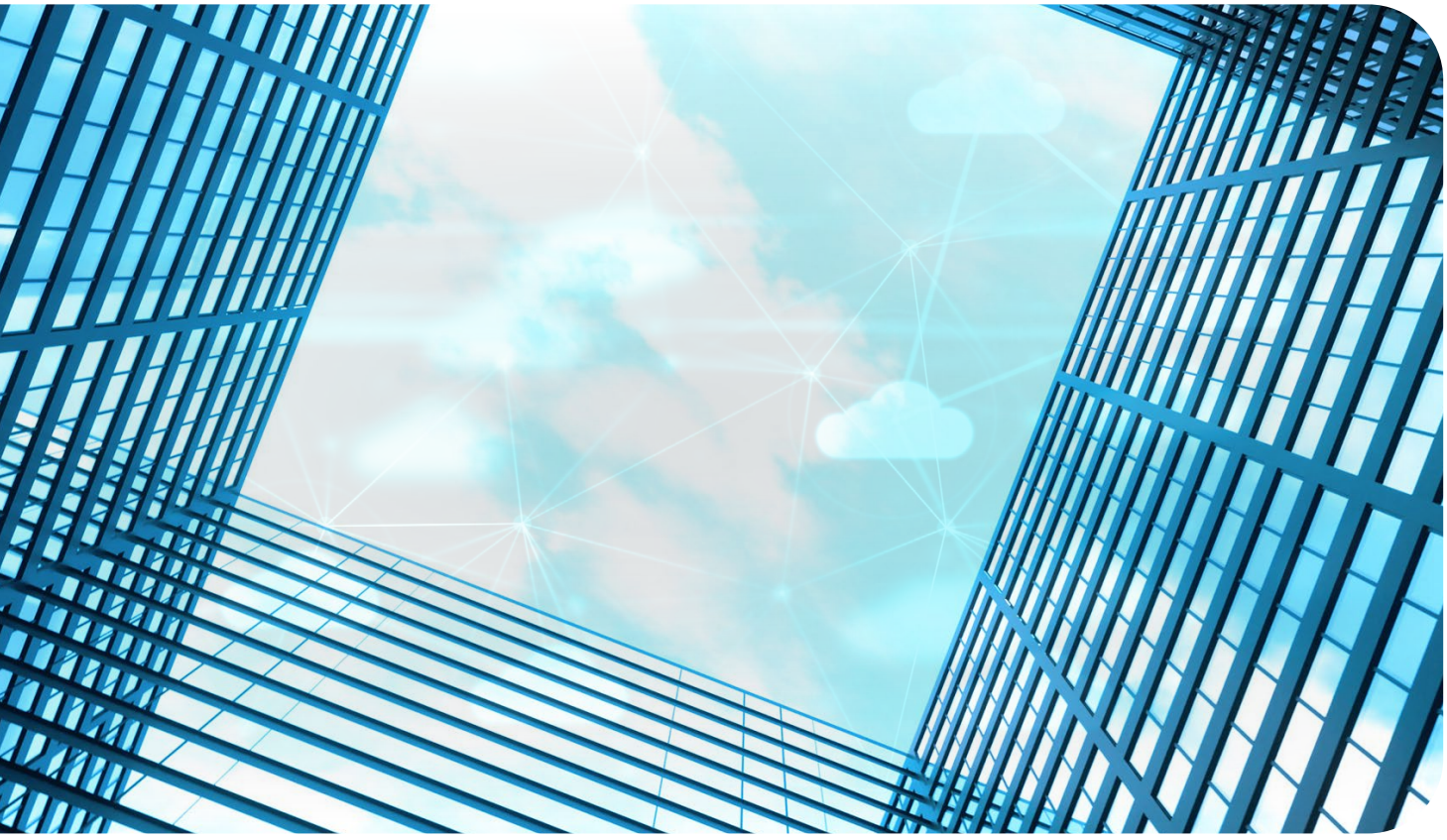
Fig. 1: Critical obstacles to the use of the cloud

1 https://www.newsd.admin.ch/newsd/message/attachments/64462.pdf

2 SIEM: Security Information and Event Management

Recommended elements of a cloud strategy

A cloud strategy provides a clear **vision and mission** as well as an **objective** for the transition to the cloud that primarily addresses the organizational aspects of incorporating the transition into the digital transformation of the entire organization. **Principles for using the cloud** are essential as a foundation that serves as a guide for decision-making. The **risks of using the cloud** also need to be analyzed and evaluated in a way that takes the recommendations applying to the sector into consideration (such as the Swiss Bankers Association's Cloud Guidelines). It goes without saying that it is important to carry out an **economic analysis of cloud use** in order to arrive at a reliable foundation for the anticipated changes from the perspective of the entire IT organization. A definition of the future **governance** and the **target operating model**, including the general organizational framework conditions, the provision of the necessary capabilities and any sourcing models, are also important factors. Using this as a basis, the rough process steps and the functions and decision-making bodies that are to be involved to bring about the **evaluation and procurement of cloud services** also need to be specified. **Business Continuity Management (BCM) measures** and the **guidelines** for a **potential strategy for exiting** the cloud must also be defined. Finally, it is necessary to define the cloud transition initiatives that are to be implemented as part of a longterm **road map**. This is a challenge for the management team since existing principles, working methods and the organization need to be modified.



Implementing the cloud strategy

We recommend breaking down the operationalization and establishment of the defined cloud strategy into multiple phases with different areas of focus that should be planned and implemented on an integral basis. The foundation for this is provided by the cloud governance that deals with the organizational framework conditions and the overarching cloud architecture. The latter should take the existing enterprise architecture and technological dependencies on existing solution components into consideration. Particular attention should be paid to the adjustment of existing ICT security architectures. When it comes to the actual migration of applications to the cloud, it is worth carrying out a cloud readiness assessment first to determine the ideal target state of the application as well as the migration procedure. An agile or iterative approach is usually good for individual cloud migration projects in order to limit the risks involved and gain experience.

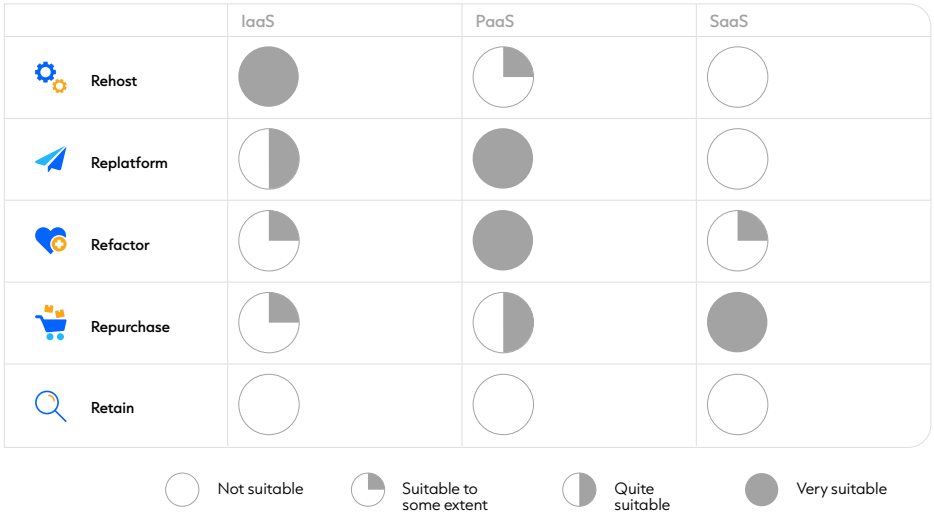


Fig 2: Standard strategies for the migration of applications

Fig. 3: Standard strategies for application migration

Public cloud providers and the regulated sector

In many respects, public cloud providers already offer very good framework conditions for the regulated sector. It often comes down to the geographical or legal location where the data is stored and processed. This is addressed by the data processing centers operated by public cloud providers in Switzerland that are already available or have been announced. These providers also offer a wide range of regulation-specific and industry-specific proofs of certification.

The extremely high levels of availability and the numerous possibilities for the redundant configuration of services on the hyperscaler's platforms are plus points. This is because higher service levels do not require any more substantial or fixed investments since they only affect the service costs.
Today's cloud platforms are increasingly providing cloud services that are specific to particular industries, for example, in the form of configuration blueprints in order to meet compliance requirements. As part of transitions to the cloud, existing cyber security concepts can also be fundamentally updated and their efficacy optimized.

Conclusion: Cloud services have become a permanent fixture in the regulated sector.

Cloud services have become a permanent fixture in the regulated sector. In order for the associated expectations to be met, however, it is important to take a close look at the strategic decisions as well as the planning and implementation in the context of a transition to the cloud and to take the organization's framework conditions into account.

The foundation is provided by the cloud strategy, which lays the strategic groundwork with a clear vision. Potential risks must be addressed at an early stage. It is also important to define clear guidelines regarding the economic and organizational aspects of cloud use.

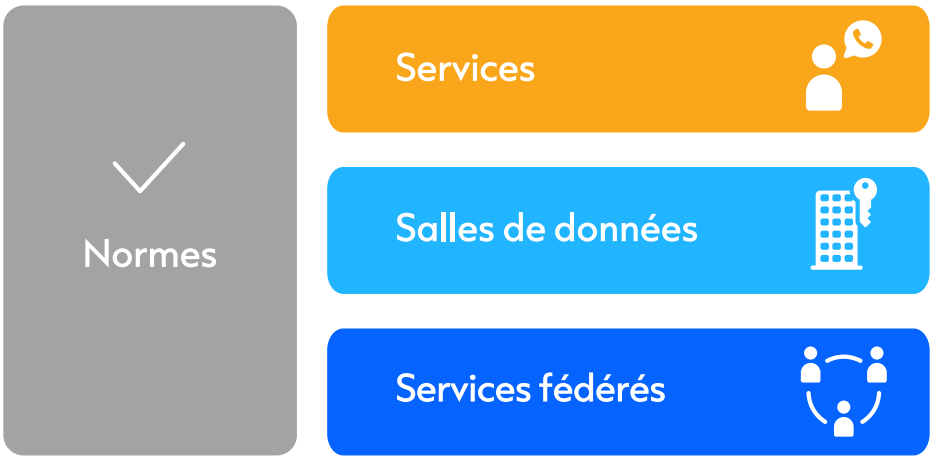
The second step involves defining the cloud governance and target architecture. Migration to the cloud benefits from an iterative approach in order to successively build up the necessary capabilities and manage the risks. The rapid development of cloud services and models means that the defined framework conditions for using the cloud need to be reviewed and updated regularly.

Eraneos is happy to assist organizations in the regulated sector with its expertise and experience, both with respect to both the development of cloud strategies and corresponding concepts and the implementation of transitions to the cloud.

To what extent might GAIA-X become relevant?

GAIA-X[3] is a European project to build up a data infrastructure for Europe that is not only effective and competitive but also secure and reliable. The project is currently being driven mainly by German and French businesses, scientists and government agencies, but is open to any other partners who would like to get involved. For Switzerland, this makes it an interesting project implemented by a political partner with a largely congruent legal framework (e.g., GDPR).

At the highest level of its architecture, the concept for GAIA-X is based on the elements of "federated services," "data spaces" and "services," that are interoperable thanks to jointly defined standards. All participants may offer and use GAIA-X-based services. Thanks to standardization, the technical foundations are clearly defined and the quality categories that are to be complied with (service quality criteria) have been implemented in a uniform manner. This concept largely mitigates dependence on individual (cloud) providers when using cloud services.



Although GAIA-X offers little concrete benefit at present, the initiative could be an important help for regulated organizations in the medium term with these approaches. It is therefore worth following developments in this regard closely and considering getting involved.

Fig. 4: The GAIA-X concept

3 https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

Meeting strict cyber security standards in the cloud

The cloud offers companies an opportunity to enhance their cyber security standards and apply them consistently from the outset of the migration process. For SMEs in particular, the transition to a cloud environment is likely to entail significant improvements in security over their existing, on-premise infrastructure because they benefit more than large companies from standardized security features and the provider's technological progress.

But no matter what size the company, certain key points need to be taken into consideration to make the design and use of cloud solutions secure. Before the migration to the cloud takes place, a detailed (cyber) risk analysis should be carried out involving all relevant stakeholders at the company. This allows mitigating measures that are commensurate to the risk appetite to be defined at an early stage, incorporated into corresponding (security) concepts and then implemented. It is, of course, essential to continue monitoring the identified risks constantly.

The greatest challenges in terms of security include the use of hybrid cloud models, which is set to become widespread in the years ahead. Only a handful of companies will migrate entirely to a single cloud. Most will continue to run some of their applications on-site, or even migrate to a number of different clouds. The security of the overall solution is therefore fundamentally linked to the (security) architecture concepts and their implementation. The shared responsibility model, which forces the providers and users of cloud solutions to clearly delineate their responsibilities, often leads to confusion among newcomers to the cloud, followed by an unclear definition of responsibilities and, therefore, ultimately, (unconscious) gaps in security. Identity and access management (IAM), and the integration of multiple cloud identities and management of their authorizations, are also becoming increasingly complex and require dedicated know-how. This makes IAM and the security architecture a key component in the security of cloud solutions. Finally, a detailed analysis is required of conventional aspects of security such as security event monitoring and threat detection. These face new challenges as a result of the decentralized structures of hybrid cloud models. This makes it all the more important to find clear answers to questions such as: "Where are which logs stored in the near/long term? How do I make sure that my SIEM has a holistic overall picture? How do I protect the large number of (API) interfaces as efficiently as possible?" in advance.

Therefore, we recommend always using established standards, methods and best practices, such as those of the Cloud Security Alliance (CSA).

The cloud in the financial sector – a challenge in many ways

Strict regulatory, compliance and risk standards governing the implementation of technical and organizational projects are in place in the financial sector. Due to Switzerland's requirement of bank-client confidentiality, data has mostly been kept at a single location in Switzerland thus far, while outsourcing data storage to another country has been deemed unfeasible. In the absence of public cloud providers based in Switzerland, the only remaining option has been traditional hosting using Swiss providers. This trend has, however, been broken by the establishment of cloud computing centers in Switzerland that has changed the market in favor of non-Swiss public cloud providers. This has been reinforced by the commitment on the part of those providers to keep data in Switzerland.

Adrian Anderegg, Tom Schons

As the lead regulatory authority, FINMA published the circular "2018/3 Outsourcing" in 2017 already, and updated it in the winter of 2020. Not only does the circular stipulate a suitable framework for the conventional outsourcing of IT services, it also has significant consequences for the use of public clouds. Since it is often not easy to correctly interpret individual paragraphs with respect to cloud computing, the Swiss Bankers Association published Cloud Guidelines containing best practices in summer 2020. But these guidelines lack specific details regarding individual cloud solutions as well as recommended technical and organizational courses of action. The banks and their service providers have to fill in these gaps themselves.

Key issues and stumbling blocks for the implementation of public cloud solutions

The list of which functions and data a bank outsources to the cloud has significant ramifications for the applicability of "significant" or "non-significant" outsourcing. Correct classification in accordance with Circular 2018/3 is essential in this regard. In practice, there are mainly risks associated with classification as "non-significant outsourcing" that gradually evolves into "significant outsourcing" over time as a result of the continuous expansion of cloud solutions. Institutions that initially put their cloud projects on hold should be particularly wary of the increased risk of "shadow IT" that is fueled, for example, by the relatively easy provision and use of SaaS solutions that bypass central IT structures.

By setting up Swiss cloud computing centers, the major providers are taking on those who cast doubt on the (data) sovereignty of foreign cloud providers as a result of the US CLOUD Act and subsequent "Schrems" rulings. Caution is still advisable in practice, however, since individual services and features are still provided by global data centers. In cases of doubt, data is "at rest" in a Swiss data processing center but is temporarily "in transit" in the EU or even in the US. New functionalities and services are also often introduced at a later date in Swiss data processing centers. Particular attention should also be paid to business continuity and the disaster recovery failback because the big hyperscalers secure their clouds using multiple layers of redundancy,

usually across national borders. It is therefore advisable to check thoroughly in advance which countries the services and functionalities used are provided from, both in normal operation and in emergencies. This information must be taken into account accordingly in the risk analysis. The issue of "unlawful access" also plays a pivotal role in the context of the US CLOUD Act. According to publicly available data sources and the providers (who are aware of the seriousness of such access), however, the risk of this occurring is low and can be reduced to a reasonable level by technical, organizational and contractual means.

It is critical that a strategic decision to outsource personal, customer or business data to a cloud provider is made on the basis of a solid foundation. The following procedure is recommended in this regard:

1 Prepare a thorough risk analysis that covers both the institution and the provider, as well as the services and features used

2 Model the risks based on the management's risk appetite

3 Identify and implement the necessary technical, organizational and contractual measures

4 Continuously monitor the identified risks and define effective countermeasures

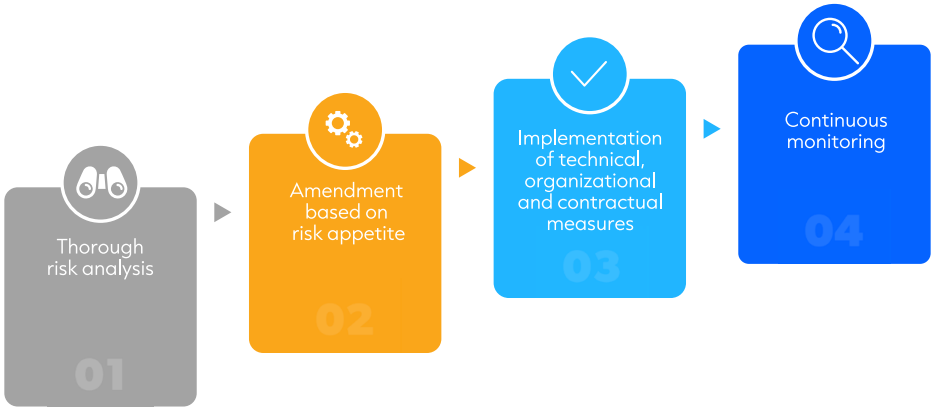


Fig. 1: Implementation of public cloud solutions

For financial institutions, the existing IT infrastructure landscape also plays an important role. In many cases, banks' and insurance companies' core systems run on very specific hardware such as mainframes. Since these kinds of systems are particularly hard to virtualize, migrating these servers to the cloud can be ruled out for now. The stability and availability of these systems are also top priorities. Modern concepts such as continuous deployment have not yet been used in connection with core systems because even minor bugs in the software can have enormous consequences. Maturity already needs to be very advanced at the time of the rollout. In this context, a minimum viable product (MVP) is often not mature enough for real-life operation.

As a result, financial institutions are still operating on the basis of two-speed IT, with mainframes and rather slow, quarterly release cycles. This, therefore, makes it difficult to take advantage of the typical benefits of a SaaS solution. The architecture of the core applications needs to be redefined prior to a migration to the cloud. Many banks and insurance companies, and also their software providers, are still in the early days of this process. The other aspect of two-speed IT are portals, apps and analytics applications. This is where the benefits of the cloud are particularly apparent, including in a financial context. It provides access to new technologies such as artificial intelligence with- out requiring substantial investment in hardware or software. The ability to analyze large volumes of data in real time using cloud computing power makes it possible to offer customers innovative advisory services or to automate complex compliance and risk processes. The development and testing of new applications can also be made faster and more efficient. Load and performance tests can also be carried out cost effectively using cloud resources. Flexibility and agility reduce the time-to-market.

In a financial context, the cloud is primarily suited to areas in which agile and short-lived development is feasible, while the core systems operated by the institution itself are kept on its own infrastructure. In the case of complex back-office applications that give an institution little opportunity to differentiate itself from the competition, how-ever, there is a discernible trend toward outsourcing and the use of SaaS applications. These applications include CRM, accounting and office applications. This requires modular systems on which individual components can be developed rapidly without jeopardizing the stability of the entire system. Cloud-compatible interfaces are also crucial in order to connect peripheral systems.

Conclusion: More use can be made of public clouds in a financial context

From a regulatory perspective, a corresponding framework is in place and countermeasures can be defined on the basis of risk considerations to make the associated risks manageable. The important thing is to give a suitable amount of consideration to the decision for or against a particular cloud outsourcing solution, to document it using an appropriate risk decision and to consciously implement it using adequate measures. This is mostly likely to succeed if the representatives of the institution's business, IT, risk, compliance and legal functions share a common vision for the cloud-based future.

The "early adopters" among Switzerland's financial institutions are already at the operational stage, while many others are in the process of strategic decision-making or assessing conceptual considerations. This shows that Swiss financial institutions are increasingly realizing and taking advantage of the benefits of public cloud environments. Institutions that do not manage to make this technological and innovative leap will lose out in the long run.

The cloud in the regulated sector An interview with Richard Hess

→

> "There is no such thing as a world without risk. That is why objectifying the cloud discussion is of central importance to me."
>
> **Richard Hess, Head of Digitalization at the SBA**

How would you describe your role at the Swiss Bankers Association (SBA)?
Richard Hess: I have had the privilege of being in charge of the digitalization function since July 2020. I would certainly describe my role as varied, multidisciplinary and enriching. Hardly a day goes by when I don't come to some realization or learn something new. Our work focuses on the issues and challenges that arise in the context of digitalization for the financial sector, at the interface between technology and regulation. To this end, we work with our members to develop the necessary frameworks and solutions by asking the right questions, bringing the right experts together and coordinating the relevant work in committees. In this context, we also act as an intermediary between the financial industry, the authorities and other important stakeholders, such as large technology companies.

In my experience, however, many of the issues that arise cannot always be addressed by following a conventional "problem-solving" approach. It's often also a matter of recognizing the opportunities provided by individual trends for the financial center at an early stage and actively working on those opportunities from the perspective of the industry without always working toward a concrete solution for a specific problem. Examples of this include open finance and the tokenization of assets. The common goal of all these activities is to put the best possible framework conditions in place in Switzerland for our members by providing entrepreneurial freedom and facilitating innovation.

We are currently mainly dealing with the opportunities and challenges presented by open finance, responsible artificial intelligence, electronic identity, digital currencies (CBDC), digital assets and DLT. We are also focusing on the various regulatory aspects of banks using public cloud services. The SBA already published a corresponding set of guidelines for our members back in 2019.

What trends do you see for the use of cloud services?
RH: The SBA's recently published "Perspectives on the Future of Swiss Banking" study clearly showed that cloud computing will be one of the key resources of the future. Banks want to make use of cloud services and recognize the benefits they bring.

According to the study's findings, the journey to the cloud in the financial sector still places a strong emphasis on infrastructure (Infrastructure-as-a-Service, IaaS), while legal capacity, applications, middleware, databases and development platforms are often kept at the bank. Looking ahead, however, Platform as a Service (PaaS) and Software as a Service (SaaS) are set to become much more important. Banking-as-a-Service is also already being offered. The Swiss government's Swiss cloud needs analysis study is very helpful in this context because it was able to quantify this trend.

Banks already have several points of contact with the public cloud in their office settings, such as due to the increased use of collaboration tools like Microsoft Teams. But it's going to get really interesting when banks migrate entire workloads from their internal divisions to the public cloud.
Last but not least, the actions of global hyperscalers such as Microsoft and Google, who have also had their own data processing centers in Switzerland since 2018, have also caused banks to look more closely at the cloud.

What are the driving forces behind the increased use of cloud services?
RH: I see the conditions on the market and customers' changing needs as the main driving forces. We can no longer imagine a life without smartphones. At the same time, new competitors and challenger banks are changing what customers expect of financial services. The key words here are fast, simple and secure. A short time-to-market is crucial to be able to keep up with this competition. For many banks with aging legacy systems, this poses a challenge. Against this backdrop, the cloud can enable banks to meet customers' changing needs better, making it an enabler for innovative business models. Many new technologies can also only be used effectively via a cloud. Finally, the coronavirus pandemic has further accelerated banks' demand for cloud services since most virtual collaboration tools, for example, can only be accessed via the cloud as an SaaS.

What are the legal situation and regulatory framework like with regard to the use of the cloud?
RH: That is certainly a crucial question for us. Switzerland's principle of regulation that is neutral with respect to particular technologies and based on a set of principles essentially offers enough flexibility for cloud services to be used within the existing framework. But this requires a concrete interpretation of the applicable legal and regulatory requirements in the context of the cloud. We have drawn up a number of recommendations in this regard in the form of our Cloud Guidelines. We therefore consider the current legal situation to be reasonable and sufficiently practicable. However, there are still some points that have not yet been fully resolved. The handling of cloud providers' obligation to release data to third parties in accordance with the US CLOUD Act, for example, is still a disputed issue with no conclusive answer – even among experts. The Schrems II ruling is another important factor with respect to risk management. It means that banks not only need to know who their cloud providers are (including their subcontractors), they also need to know exactly where their data goes, where it is being stored, and who can access and potentially process it and for what purpose.

What feedback have your members given regarding the Cloud Guidelines?
RH: As far as we know, many of our members consider the guidelines helpful and use them to help implement their own cloud strategies. Our members also tell us that the guidelines help to immediately focus discussions within institutions and with cloud providers on the key topics. We are glad to hear it, because that is exactly why we created them. I believe that they also helped to overcome, or at least relativize, resistance to the public cloud and make the discussion surrounding the use of could services more objective.

The guidelines consist of recommendations that can be consulted by banks and cloud providers when procuring and using cloud services. They deal with four areas: data processing, collaboration with subcontractors, audits and the handling of subpoenas issued by international authorities. They also recommend technical, organizational and contractual measures relating to data protection and compliance with bank-client confidentiality in the cloud.

What do you consider to be the greatest challenges in terms of cyber security and privacy when it comes to adapting to the cloud?
RH: It is clear that cyber security is becoming more and more important, including in the context of open banking and the associated increase in the sharing of data with third parties. We are addressing the issue at the sector level by working with the Swiss national government to set up a cyber security center of excellence.

In the context of cloud services, the location of data storage and data sovereignty are also particularly central, so the question is how do I retain control over my data and what means do I have at my disposal to assert my rights in this regard. Transparency is important in this context.

What is your assessment of the availability and development of the necessary skills among your members with respect to the implementation of cloud projects?
RH: That depends which institutions we are talking about. As we know, banks are increasingly turning into technology companies. Based on current trends, many experts believe that bank employees will need better technology skills and IT employees will need to understand more of the business in the future. The "war for talent" over specific IT skills, particularly in the field of cloud services, is therefore certainly having an impact in the financial sector. In this, the banks are competing directly with technology companies and need to position themselves accordingly in order to appeal to prospective employees. Small and medium-sized banks in particular could struggle to maintain their own IT organizations with the ability to keep on top of all of the legal, risk-related and technical issues. One potential approach would be to enter into partnerships with third-party providers and break up the value added chain. We are endeavoring to provide our members with the best possible support when it comes to training their employees, for example through partnerships with selected training platforms.

Where do you see additional potential in adapting to the cloud?
RH: The subject of artificial intelligence (AI) and machine learning (ML) presents a strong argument for using the cloud. Using AI and ML offers banks entirely new possibilities for processing and providing large volumes of high-quality data. There is also on-demand computing power, which can be obtained directly from the hyperscalers – such as for transaction monitoring or fraud detection. Last but not least, security-related aspects are another key factor in banks' decisions to get involved with the cloud.

In your experience, what are the relevant elements of a cloud strategy in your organization/industry?
RH: A distinction should be made in this context between banks with a domestic focus and global banks. These two groups have different situations and needs. Banks that focus on the domestic market are more interested in local providers based in Switzerland and have less complex strategies. Global banks, on the other hand, are taking a much more comprehensive approach to the topic. The cloud strategies of these banks are often defined by the parent company and rolled out to the individual countries.

No matter what size the bank, the question that often arises is whether the cloud is an IT or business issue. I am of the opinion that the transition to the cloud needs to be viewed as a strategic project and discussed at senior management level. This is the level at which decisions need to be made for or against the cloud, as well as regarding the appetite for risk.

With respect to implementation, discussions with representatives of the banks have indicated the importance of the transformation process, which generally takes several years along the IT life cycle, being based on the "cloud-first" principle. A clear vision and principles are required, as is critical investigation in the event of deviations from this principle. The organizational consequences of migrating to the cloud must also be taken into consideration and not overlooked.

In my opinion, regulatory aspects are an essential part of any cloud strategy – in the financial sector in particular. As previously mentioned, it is important to already answer all questions regarding the cloud provider and its subcontractors during strategy development. A clear answer to the question "Who is allowed to access what data, when, how and for what purpose?" is also crucial from a risk perspective. A decision in favor of a provider should only be made once all the points referred to have been clarified.

Is there anything else that you would like to say to our readers?
RH: There is no such thing as a world without risk. That is why we believe it is important to have an objective discussion of the cloud. Because this step by no means represents a transition from a world of zero risk into a high-risk environment. There are also many risks for applications that run locally in an institution's own data processing center. What we need is a risk-based approach to the relevant issues surrounding the cloud. For banks that carefully weigh up all the potential risks, the cloud offers a huge opportunity to enhance their capacity for innovation and their ability to compete.

Our goal is to ensure that all banks wanting to venture into the public cloud are able to do so. We cannot wait to see where the journey will take us in the next few years. After all, this is a highly dynamic and rapidly evolving environment that not only raises technical and regulatory questions but ultimately also geopolitical ones, all of which need to be taken into consideration and discussed.

The cloud in the public sector – an urgent imperative with a lot of potential

The public sector includes organizations at all levels of federal government, including those in the fields of public administration, education and research, security organizations and public utility, transportation and logistics companies. This sector's size means that it could be a significant factor in the transition to the cloud. But usage levels are still low at present.

Marc Raum, Thomas Vogt

The public sector is governed by the principle of legality set out in the Swiss Constitution that requires a formal foundation for the government's actions (Art. 5 (1)). The parliaments and, within the set executive framework, the administration primarily assume the role of regulator on their own responsibility. There are a lot of requirements based on laws and ordinances. However, their exact interpretation with respect to the possibilities of and restrictions on cloud usage is rarely unambiguous. While public regulators, such as in the field of data protection, point out the risks, they do not offer any solutions themselves.

The use of cloud services is also a political issue for the public sector, particularly with respect to the matter of data sovereignty in an international context. Among other things, the Swiss government dealt with this issue in its Swiss Cloud feasibility study in 2020. This indicated that there was no or very little need for a cloud infrastructure operated by the federal government, but a significant need for clear framework conditions governing the use of commercial cloud services. The survey of demand considers public institutions and, above all, the trade organizations and corresponding regulators to be responsible for putting these framework conditions in place.

The public authorities have thus far failed to provide regulatory clarity regarding the use of public cloud services. Practical resources and services could easily be developed in partnership with the trade organizations.

Trends and driving forces behind the use of the cloud in the public sector

For the public sector, cloud usage is of particular interest in fields where the possibilities offered by the cloud provide direct added value and the framework conditions with respect to the storage and processing of data for cloud usage can be clearly defined. These include:

- Portals and applications (or mobile apps) for the direct provision of services for the general public and private companies
- Applications where the need for resources fluctuates and that need to be scalable at short notice
- Services that include or are intended to facilitate the sharing of data with external stakeholders (such as open government data services)
- Specific applications providing capabilities that are subject to constant technological development, such as services in the fields of data analytics, machine learning or artificial intelligence

Specific examples for the use of public cloud services in the public sector include the management and provision of topographic maps of Switzerland by swisstopo, the Federal Office of Public Health's COVID contact tracing app, the testing and development solutions in the field of agile development and the use of cloud solutions in the internal and interorganizational communication and collaboration of many government services.

"Death by a thousand cuts"

The journey toward the use of cloud solutions by government services is generally a very difficult one. In addition to the framework conditions for the use of cloud services in the public sector that are also yet to be clarified at a political level, particularly with regard to information security and data protection, there is a significant obstacle that must be overcome in this regard. This is that government procurement processes frequently require an invitation to tender with new contracts for the services, which therefore also makes it necessary to already have a very precise concept for the future operating model, compliance requirements and needs. This in turn requires well-devel-oped architectural foundations, particularly in the field of inte-gration, networks and security systems, to ensure that public cloud services can also be used effectively. A lot of smaller organizations fail to meet these requirements.

This highly fragmented approach makes it difficult for individual organiza-tions to meet the cost-effectiveness threshold to secure the necessary inter-nal financing. But the situation is improving. Swiss Federal Railways (SBB), Swiss Post and the Federal Administration are three large organizations that have decided to procure public cloud services. Their experiences will prove valuable since they provide models on how it is done. Nevertheless, a stra-tegically coordinated approach is required in order to exploit the benefits of cloud services.

A possible vision for the use of the cloud in the public sector

In order to have a foundation for the secure, compliant and efficient use of cloud services, organizations in the public sector need politically robust and broadly supported organizational development with strategic principles that serve as guidelines for the integration and use of the cloud. From an organizational perspective, it is advisable to not view the subject of the cloud in isolation but as an essential component of or enabler for the digital transformation.

We mainly consider the following elements to be crucial for an active and lasting transition to the cloud in the public sector:

- Making the experience gained visible
- Putting application-oriented foundations in place in the fields of architecture, information security and data protection
- Bundling requirements by means of a formalized collaboration between different organizations and flex-ible procurement principles, such as by tapping into potential synergies via IT service providers
- Initiating a political process and ratifying a vision with application scenarios as well as an ambitious time line
- Switching to agile and iterative methods such as Scrum and SAFe to establish a culture of learning that is tolerant of errors – constantly monitoring and adapting the organization
- Training employees in the necessary cloud skills, models and technologies
- Establishing and collaborating in national and international cloud initiatives to bundle and focus expertise and decision-making frameworks in the context of transitions to the cloud in the public sector

One possible way to give the necessary boost to cloud usage in Switzerland's public sector would be to implement a targeted and coordinated initiative on the subject. Examples of government cloud initiatives include the UK Government G-Cloud, the US government's FedRamp, cloud.gov.au in Australia and the Government Commercial Cloud (GCC) in Singapore. The UK Government G-Cloud mainly comprises clearly defined framework conditions to facilitate the procurement of cloud services. The US government's FedRamp goes one step further and provides a certification process that ensures a standardized appraisal of the risks and security of cloud services. This makes it possible to quickly and logically decide whether and, if so, which cloud services may be used for a particular use case. With its cloud.gov.au initiative, the Australian government made a strategic decision that the administration's ICT services must generally be compatible with the cloud. The Singaporean government's GCC allows the use of innovative cloud services in sensitive areas of the administration.

GAIA-X is a major cloud initiative launched in Europe that addresses similar topics to the those mentioned above, and that the Swiss public sector should also keep a close eye on. The ability of GAIA-X to offer or list cloud services in different service classes in particular could be very helpful for cloud usage in the public sector. The Swiss Federal Council's Swiss Cloud1 needs analysis report also addressed this angle with the recommendation to consider the possibility of a certification system for cloud services.

In the full range of topics surrounding the transition to the cloud, the public sector still has valuable potential to free up additional synergies through partnerships between the various different organizations and across different levels of federal government. Open and intensive cooperation is beneficial since many of the issues that public sector organizations face with respect to the cloud are similar. It is also just as important to work together to develop robust decision-making frameworks that significantly advance the transition to the cloud and, therefore, the individual organizations' general digital transformations.

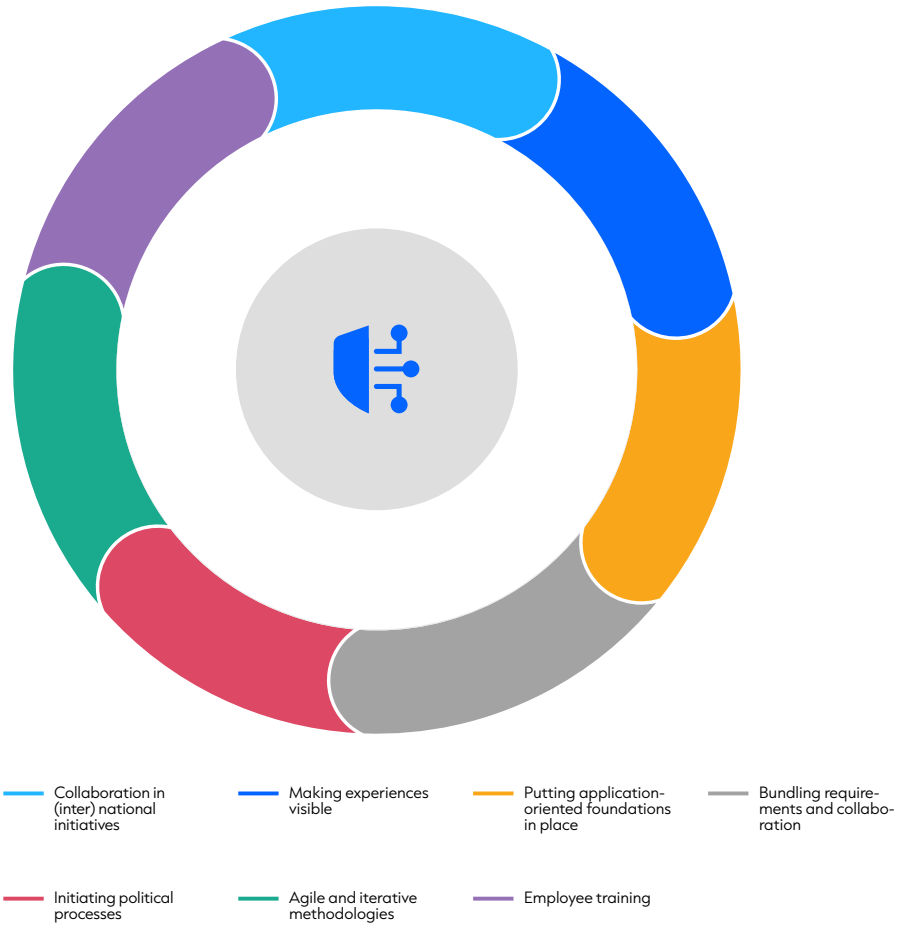


Fig. 1: Recommended elements for successful transitions to the cloud

1 https://www.newsd.admin.ch/newsd/message/attachments/64462.pdf

Pioneer in the Swiss government for the use of public cloud services

Hanspeter Christ graduated in Environmental Engineer-ing at ETH Zurich and has been working for swisstopo, the Swiss Federal Office of Topology, since the year 2000. He has been working on the planning, setup and operation of geodata infrastructures consisting primarily of open source components since 2004. He already gained some experience of using public cloud services in 2008, and he spent the next few years working on the front line of the cloud concept and migration of the entire Swiss geodata infrastructure to the public cloud.

"In 2008, we received an urgent request from a customer to use swisstopo's digital map data. If we had done this in the conventional way by procuring and integrating our own infrastructure, the necessary hardware wouldn't even have been available in time for the requested go-live deadline."

"Our journey to the cloud took us from an infrastructure that was operated on-premises to a hybrid architecture and then what is now a largely cloud-based implementation of the geoportal."

The factors driving the use of the cloud at swisstopo were the need for a flexible infrastructure that could be tailored as much as possible to the various requirements of geoportal usage and highly scalable map services. The associated transition to the cloud at swisstopo initially involved migrating to a hybrid architecture that made use of both internal infrastructure and public cloud resources. The geoportal architecture was then developed to become what is now a largely cloud-based infrastructure.

This procedure also influences our new approach:

"Rather than defining proposed new infrastructures and architectures on the drawing board, we follow the market. In the process, we focus on 'low-hanging fruit' with significant potential benefits."

Recommendations for public organizations with respect to migrations to the public cloud

- Simply migrating virtual machines to the public cloud (lift and shift) does not take full advantage of the benefits offered by cloud capabilities. Using optimized cloud solution models (for example, using microservice architectures) opens up much greater potential to tap into. Many user organizations are limited by provider-specific services that make subsequent migration more difficult. Standardized architectural principles help to ensure effective decision making.

- A culture of productive experimentation with new technologies makes it possible to achieve significant improvements in efficiency when it comes to the development and operation of IT solutions. Agile work methods, such as SAFe, are well suited to this because innovation and planning sprints help make investigating new approaches a part of everyday life.

"One critical success factor for the efficient, secure and lasting adaptation of public cloud services is giving employees throughout the organization the requisite cloud-related skills."

Cédric Moullet studied at EPFL and has an MBA from the Haute Ecole de Gestion in Fribourg and a CAS in Artificial Intelligence from Bern University of Applied Sciences. He started his professional career at ETH Zurich before moving on to the US-based software developer Autodesk and the open-source software company Camptocamp, which led him to swisstopo and then the Swiss Federal Office of Information Technology, Systems and Telecommunication (FOITT). There, he most recently led the development of the SwissCovid app and the Covid Certificate. Since September 1, 2021, he has been in charge of the Digitalization & IT division at the Swiss Alpine Club (SAC).

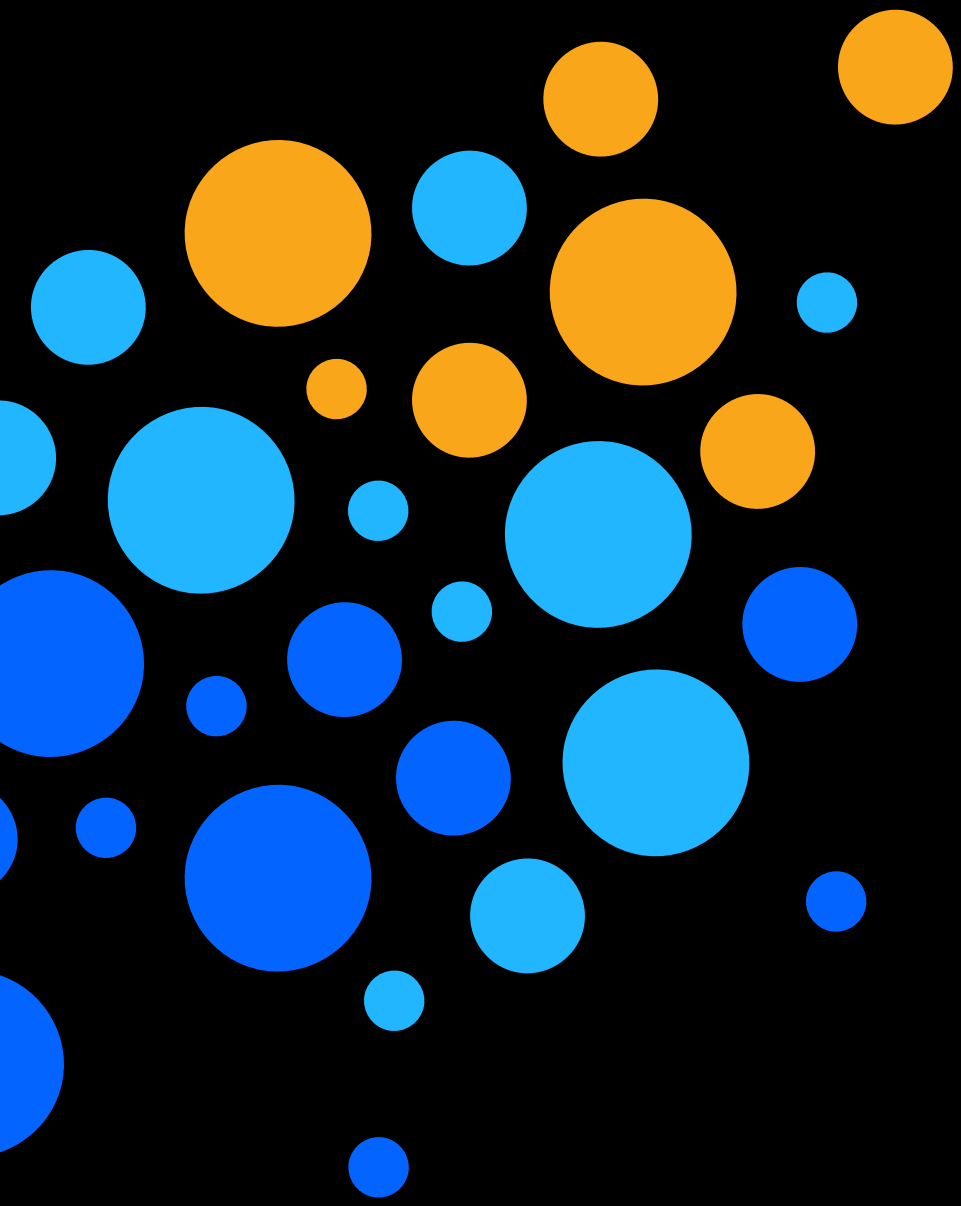
During the coronavirus crisis, Cédric was able to apply the relevant experience with the cloud that he gained by leading the creation of the geoportal at swisstopo to the development of the SwissCovid tracing app and Covid Certificate app. The very large volume of traffic that was expected was too much for the organization's own data processing centers to handle. At the same time, it was absolutely essential for citizens to have faith in the solution. These challenges were overcome using a hybrid model. A Content Delivery Network (CDN) provides flexible traffic management. Basic backend functions were provided using the organization's own data processing centers. The code was also made open source and subjected to a public security test to allow any-one to satisfy themselves that it worked. Another benefit of the CDN service was that it was very easy to integrate, which meant that the solution could be delivered sooner. The transfer of knowledge between the specialists themselves did not take much time. There was a discussion regarding whether users' IP addresses constitute personal data, since these could, for example, be combined with the CovidCode to determine whether someone was ill.

But in Cédric's experience, technology is only one aspect of security:

"People are often the weakest link in the chain. Venturing into the cloud only increases those risks."

Recommendations for public organizations with respect to migrations to the public cloud

- Access to a pool of experts helps organizations plan cloud solutions properly and implement them quickly. The goal should be to empower internal employees by transferring knowledge and responsibility.
- Security and trust need to be actively cultivated. Secure architectures and a high level of transparency (for example, by means of open source and audits) are important factors in this respect.



eraneos

Experienced in a wide range of industries

Eraneos Group is an international management & technology consulting group that provides services from strategy to implementation. It has emerged from the alliance of Ginkgo Management Consulting, Quint Group, and AWK Group, as announced in 2021. The Group serves clients across three continents where some 1,000 dedicated and highly skilled professionals work jointly to unleash the full potential of digital. Services range from the development of digital business models and data analytics to cyber security, and from sourcing and IT advisory to the management of complex transformation projects. Eraneos Group has offices in Switzerland, Germany, Luxembourg, Spain, the Netherlands, China, Singapore, and the USA. In 2021, Eraneos Group realized a turnover of close to 200m EUR.

Contact us >

Our offices >

Visit our website >