SwissBanking

June 2020, 2nd edition

Cloud Guidelines

A guide to secure cloud banking

Contents

Foreword

Cloud services give banks and securities dealers new scope for innovative business models and more efficient processes. Targeted migration of bank infrastructure from on-premises systems (on site or local) to a cloud environment will lead to a lasting improvement in the banking sector's competitiveness. However, the use of cloud services is currently subject to legal and regulatory uncertainty which is holding back the migration of bank infrastructure to the cloud.

Under the aegis of the Swiss Bankers Association (SBA), a working group has drawn up a set of legal and regulatory guidelines (hereinafter referred to as the guidelines) for the use of cloud services by banks and securities dealers. These guidelines contain recommendations for institutions and cloud providers on the procurement and use of cloud services.

The guidelines are divided into two parts. The first contains a general introduction to the topic of the cloud. It identifies the benefits and advantages of cloud technology for banks and sheds light on what the SBA sees as the key regulatory issues and the responses to them formulated by the SBA in the guidelines. The second part contains detailed legal and regulatory recommendations from the SBA.

This document does not claim to cover all eventualities. It will be updated and revised regularly to take account of future developments in technology and the law. The current version will be published.

Management summary

- The **cloud** is a **critical success factor** for Switzerland and its financial centre. However, a number of legal and regulatory uncertainties have had to be resolved before it can be properly used by the banks.
- The SBA has set up a **working group** tasked with finding swift answers to these uncertainties. The group focused on drawing up a set of legally **non-binding guidelines** as an aid to interpretation in practice. They cover four main areas where the uncertainties are viewed as substantial or an obstacle to migration to the cloud:
  - **Governance**: choosing the cloud provider and its subcontractors, consent to a change of subcontractor
  - **Data processing**: processing data on bank clients and bank-client confidentiality
  - **Authorities and proceedings**: transparency and collaboration between institutions and cloud providers with regard to measures ordered by the authorities and the courts
  - **Audit**: auditing the cloud services and the cloud infrastructure used to deliver them
- The clarification of regulatory issues contained in the guidelines **will enable banks to act quickly and flexibly** and offers pragmatic, reliable solutions. This approach is preferable to specific regulations covering the cloud, which would be slow and not technology-neutral and would soon be overtaken by advances in technology.
- Even when using the guidelines, the task of assessing the **risks** of migrating to the cloud remains **with the individual banking institutions**. Each bank should decide for itself how widely it wishes to use cloud solutions.

Fundamentals of cloud banking

Benefits and advantages of cloud banking

Digital innovations and agility in responding to new developments are vital to the Swiss financial centre's competitiveness. This includes the use of cloud services, which allow for innovative products and cost savings, while specialised cloud providers offer enhanced security for banking infrastructure. As such, cloud services and cloud banking are a critical success factor for the Swiss financial centre.

Many bank clients use cloud services in their everyday lives without knowing that they are doing so, for example when they send e-mails, stream music and films or save their holiday photos in the cloud. What works in the private sphere should also be possible for highly specialised banks and their complex business. As things stand, however, a range of legal and regulatory uncertainties mean that this is not the case.

Migrating infrastructure and processes to a cloud can drastically reduce the time it takes for banks to bring innovative products and services to the market and thus significantly increase their competitiveness. The cloud enables banks to exploit new technologies such as artificial intelligence without making substantial investments in their own hardware and software. Access to a large pool of data and the corresponding computing power allows large data volumes to be analysed in real time, enabling banks to offer innovative, tailor-made advisory services to individual clients or automate complex compliance and risk processes. The cloud also permits substantial efficiency gains in the development and testing of new applications and systems: innovative ideas can be piloted simply and flexibly, explored in more depth or abandoned, and therefore realised more easily. Finally, the cloud allows for full cost transparency and more effective corporate governance. Companies only pay for the services they directly use, and so can react flexibly to fluctuations in demand by switching IT resources on or off. The functionality on offer can be used on a self-service basis, with the cost varying accordingly.

There is no longer a need to build up or buy in the skills and resources needed to operate an in-house IT infrastructure, making migration to the cloud a particularly attractive proposition for small banks. Certain technologies that used to be restricted to large companies will also become accessible to small banks (democratisation of technology access) and enable significant economies of scale[1]. Moreover, the growing demands placed on IT operations (IT security, keeping up to date with patches[2] managing the IT infrastructure lifecycle) are increasingly difficult for smaller banks in particular to meet.

Swiss banks are becoming increasingly aware of the advantages of cloud computing and keen to switch to the cloud. At the same time, a welcome degree of competition has opened up between national and international cloud providers. Owing to their specific needs, however, banks cannot yet make full use of these services for client data. The increasing exploitation of cloud services will nevertheless further strengthen Switzerland's financial centre and financial ecosystem in the future.

1 A marginal cost equation indicates that many banks cannot set up a cloud of their own at the same costs as specialised cloud providers. The cloud allows IT resources to be turned on or off as required and thus matched precisely to the fluctuating demands of business activity.
2 A small piece of code that repairs errors in (mostly large) application programs.

Definitions

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud can be used in three models – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) – and supplied in four different ways – private cloud, community cloud, public cloud and hybrid cloud.[3]

Cloud banking in this context is the provision and delivery of banking and financial services using cloud technology.

Regulatory issues related to cloud banking

Given the huge potential of cloud banking, the SBA is heavily involved in improving the environment for it to operate in. The authorities, providers and the sector are liaising closely in this area.

At present, legal and regulatory uncertainties entailing risks that cannot be fully assessed constitute a major hurdle to the wider use of cloud services. They include:

- **Governance**: choosing the cloud provider and its subcontractors, consent to a change of subcontractor
- **Data processing**: processing data on bank clients and bank-client confidentiality
- **Authorities and proceedings**: transparency and collaboration between institutions and cloud providers with regard to measures ordered by the authorities and the courts
- **Audit**: auditing the cloud services and the cloud infrastructure used to deliver them

3 Definition according to NIST (2011) https://csrc.nist.gov/publications/detail/sp/800-145/final.

In particular, there has until now been no interpretation of the current legal framework or understanding of the technical, organisational and contractual measures most appropriate to reducing risks in those areas.

These guidelines are an attempt by the SBA working group to create the basis for facilitating the procurement and use of cloud services by banks and securities dealers. The SBA is performing an important task in clarifying the legal context for cloud banking. This approach is efficient and means that banks do not all have to conduct the same inquiries themselves. The working group can also pool valuable expertise. Ultimately, all institutions and clients benefit from legal certainty leading to the widespread use of cloud technology and, with it, innovative products and cost benefits.

These SBA guidelines are a collection of non-legally binding recommendations for banks and cloud providers on the procurement and use of cloud services. They also contain interpretations designed to remove legal uncertainty or close gaps in the case law concerning the sometimes novel challenges of using cloud services. They offer pragmatic solutions that allow users to act quickly and flexibly. This approach is preferable to specific regulations covering the cloud, which are slow and not technology-neutral and would swiftly become outdated. When applying the guidelines, however, institutions should adopt a risk-based and proportionate approach that reflects their size and the complexity of their business model.

Key approaches from the SBA in the guidelines

A) Choosing and changing cloud providers and subcontractors

Purpose of the recommendations set out in the guidelines:
The banking institution should, **at all times, have the information it needs to carry out a risk-based assessment of a cloud provider**, taking account of its significant subcontractors.

Cloud providers take advantage of the opportunity to define and change the operating models, the technologies used, service providers within and outside the group, and other essential factors, with a view to efficient and competitive service delivery (design authority).

When choosing a cloud provider, a number of points therefore need to be considered, including:

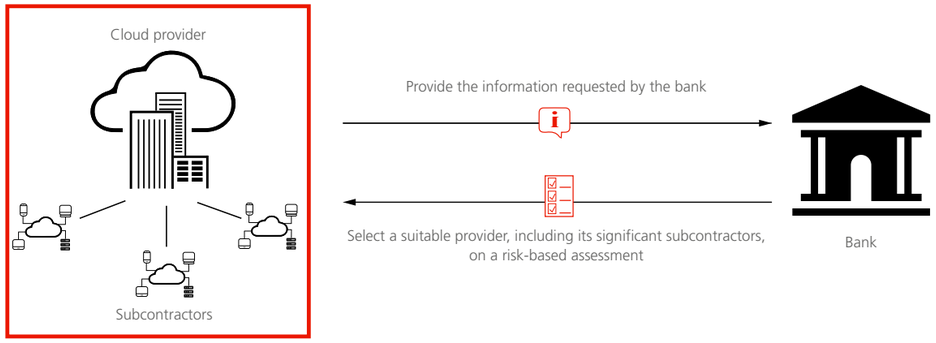
- ability to fulfil contractual obligations;
- financial stability;
- jurisdiction to which the provider is subject.

The bank should also establish whether, in addition to these performance-related criteria, the cloud provider is prepared to assume the essential duties arising out of financial market and data protection legislation.

Fig. 1

Choosing and changing providers and subcontractors

Providers' duties towards the bank



The cloud provider should provide the bank with the information it requests and notify it of any change of a significant subcontractor. If the bank does not agree to this, it may terminate its contract with the cloud provider and recover the functions, services and any protected information that have been outsourced, or transfer them to new cloud providers.

Source: Swiss Bankers Association (SBA) 2019

When choosing a cloud provider and its subcontractors, high priority must be attached to the confidentiality and security of the data as an integral part of the underlying due diligence.

The bank should be informed in advance of a change of significant subcontractor (see Figure 1). It should also take suitable precautions to ensure that the outsourced functions, services and protected information can be brought back in-house or transferred to new cloud providers. These include an appropriate termination period or the option to extend the existing operating model.

B) Maintaining banking secrecy in the cloud

Purpose of the recommendations set out in the guidelines:
Banking secrecy and data protection should also **be ensured at all times in the cloud**.

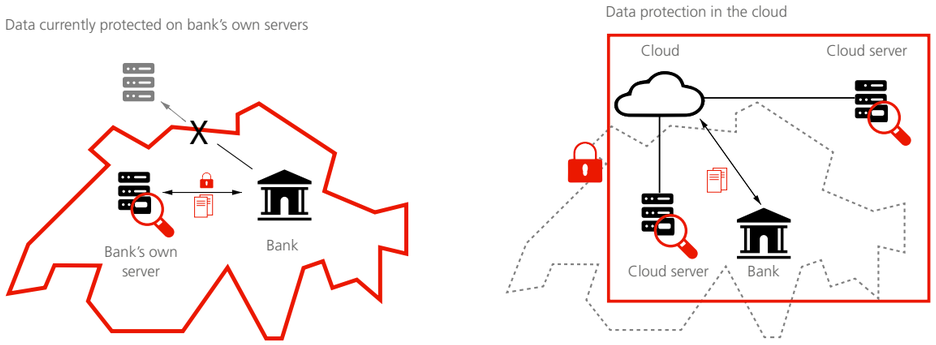
Whenever client data (CID) or personal data are being processed in the cloud, banking secrecy and data protection legislation need to be taken into account.

Until now, banks have applied the "over the border out of control" principle: as soon as data are stored outside Switzerland they are beyond the control of the Swiss courts. Consequently, CID and personal data are not stored outside Switzerland and cannot be accessed from abroad. If this principle were to be maintained absolutely, it would render use of the cloud impossible.

The guidelines focus on processing CID that are covered by banking secrecy under Art. 47 BA. They define technical, contractual and organisational measures to appropriately limit the risk of CID being accessed by the cloud provider and its subcontractors (see Figure 2).

Fig. 2

Banking secrecy in the cloud



Data protected in accordance with banking secrecy. "Over the border out of control": in practice, jurisdiction marked the border in relation to control of data.

Data protected in accordance with banking secrecy by means of technical, organisational and contractual measures.

Source: Swiss Bankers Association (SBA) 2019

Protecting client data in the cloud

Technical measures

- **Anonymisation**: Anonymisation involves irreversibly or irrevocably changing personal attributes (e.g. a person's name or other identifiers) so that it can no longer be linked to the person concerned. As a result, data that have been anonymised no longer constitute CID or personal data.
- **Pseudonymisation**: In pseudonymisation, personal attributes are replaced by an artificial identifier or pseudonym. The assignment rule used should remain under the bank's control in Switzerland and be adequately protected. Access should be restricted on a need-to-know basis and documented in a verifiable manner.

- **Encryption**: Encryption uses a key to convert cleartext[4] into an encoded text so that the original information can only be made readable again by using the correct key. Access to the key should be controlled by the bank and protected against unauthorised persons; however, the key may be made available to or held by the cloud provider. The encryption procedure and the strength of the encryption key must meet current security standards, so that the encryption can be regarded as cryptographically secure. CID should always be transferred in encrypted form.

Organisational measures

- Appropriate monitoring by the bank of the operational measures implemented by the cloud provider and its subcontractors;
- Auditing of the cloud provider's security and confidentiality standards with reference to independent reports and on the basis of recognised reporting standards.

Contractual measures

- Technical and organisational measures appropriately specified in the contract;
- Where the subcontractors process CID, duty for the cloud provider to bind those subcontractors to comply with the essential organisational and technical measures;
- Agreement by the cloud provider to maintain confidentiality;
- Consideration of the sensitivity of the data and imposition of a responsibility in this respect on the provider;
- Monitoring of the implementation of and compliance with the technical, organisational and contractual measures by the cloud provider and auditing by a recognised audit firm;
- Agreements on how the bank or cloud provider are to proceed in response to requests from the authorities or proceedings relating to the handover or transfer of protected information that is processed in the cloud.

4 Text in a readily understandable form, unencrypted information.

C) Transparency and collaboration between institutions and cloud providers with regard to measures ordered by the authorities and the courts

Purpose of the recommendations set out in the guidelines:
A **coordinated procedure agreed by the cloud provider and institution** should be adopted in response to requests from foreign authorities involving the handover of protected information.

Requests from the authorities or proceedings may relate to the handover or transfer of protected information that is processed in the cloud. Foreign laws can also provide for the handing over of data by cloud providers.

The guidelines recommend that the cloud provider and institution put in place a coordinated approach to dealing with requests from the authorities relating to the handover or transfer of protected information.

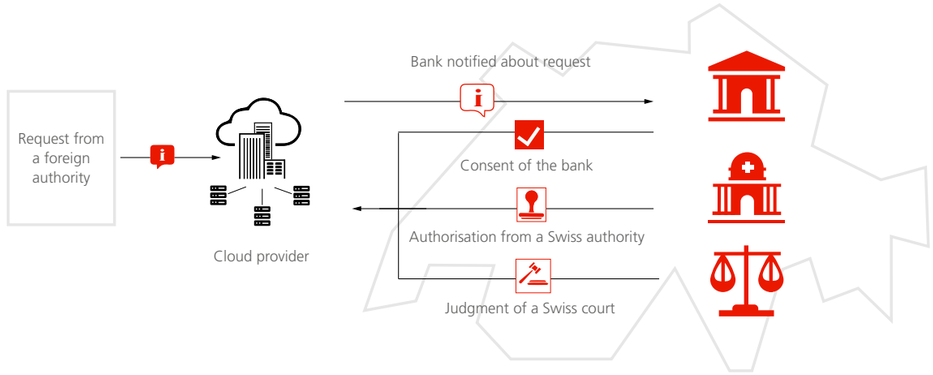
To the extent the law allows, protected information should only be transferred to foreign authorities subject to the written consent of the institution, or on the basis of a judgment of the competent Swiss court or authorisation from a Swiss authority (see Figure 3).

Where the law permits, the cloud provider should inform the institution in good time if approached by a foreign authority with a request to transfer or disclose protected information in the cloud. It should also give the institution the rights to conduct the proceedings and support it in dealing with requests from foreign authorities.

Fig. 3

Requests from foreign authorities

Protected information is handed over only under certain conditions



When the cloud provider receives a request from a foreign authority to hand over protected information that is being processed in the cloud, the cloud provider must agree with the bank on how to proceed. Protected information may only be transferred in accordance with the applicable legal provisions and with the written consent of the bank, on the basis of a judgment of the competent Swiss court or on the basis of authorisation from the competent Swiss authority.

Source: Swiss Bankers Association (SBA) 2019

D) Audit of the cloud services and means used

Purpose of the recommendations set out in the guidelines:
Third-party **access to data in the cloud for the purposes of auditing** should be guaranteed at all times.

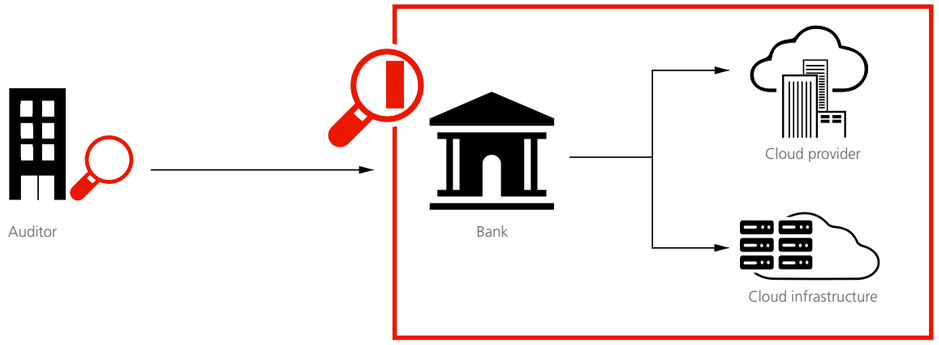
Cloud services are normally delivered by providers from highly secure computer centres to a large number of customers. Auditing the infrastructures used requires a high degree of specialisation.

Cloud providers' compliance with the applicable legal, regulatory and contractual requirements should be audited at regular intervals. These include in particular requirements concerning outsourcing, data protection and information security. There should be provision for the audits to be carried out and ordered by the institution, its internal and external auditors or FINMA. Pool audits by a number of institutions or their auditors as well as indirect or accompanied audits are permitted.

Fig. 4

Auditing in the cloud

Auditing the cloud infrastructure requires a high degree of specialisation



The auditor should have at least logical access to the cloud infrastructure in order to audit the bank.

Source: Swiss Bankers Association (SBA) 2019

An on-site audit of the IT infrastructures actually used to deliver the cloud services is not absolutely necessary, except for inspecting the physical security measures. Logical access[5] will suffice. The institution's audit of the significant subcontractors can be carried out indirectly by auditing the cloud provider (see Figure 4).

5 Technical access control or interaction with the hardware via remote access as opposed to physical access involving interactions with the hardware in the physical environment.

Legal and regulatory guidelines

for the

use of cloud services by banks and securities dealers in the context of FINMA-regulated outsourcing

Content

Chapter I: General provisions

1 Subject matter and purpose, scope of application, non-binding nature

1 These guidelines contain recommendations for institutions and providers on the procurement and deployment of cloud services. They are intended to be an aid to the interpretation of the legal and regulatory requirements in practice, with particular reference to the following four key areas:

- **Governance**: selection of the provider and its subcontractors, consent to a change of subcontractors (chapter II)
- **Data processing**: processing of data on bank clients and banking secrecy (chapter III)
- **Authorities and procedures**: transparency and collaboration between institutions and providers with regard to measures ordered by the authorities and the courts (chapter IV)
- **Audit**: auditing the cloud services and the cloud infrastructure used to deliver them (chapter V)

These guidelines also include interpretations designed to remove legal uncertainty or close gaps in the case law regarding the sometimes novel challenges related to the deployment of cloud services. Consequently, they have not been confirmed with all competent bodies. When applying the guidelines, however, institutions may adopt a proportionate and risk-based approach based on their size and the complexity of their business model.

2 These guidelines have been developed with a view to cloud services that are delivered by providers to institutions and constitute outsourcing of significant functions as covered by FINMA Circ. 18/3.

3 These guidelines are non-binding and do not constitute a self-regulation within the meaning of FINMA Circ. 08/10.

2 Terms

4 For the purposes of these guidelines, certain terms are defined as follows:

a) "**Annex 3 to FINMA Circ. 08/21**" Annex 3 "Handling of electronic client data" to FINMA Circ. 08/21.
b) "**BA**": the Federal Act on Banks and Savings Banks (Banking Act, BA), SR 952.0.
c) "**bank secrecy**": the secrecy protected under Art. 47 BA.
d) "**BO**": the Ordinance on Banks and Savings Banks (Banking Ordinance, BO), SR 952.02.
e) "**CID**": client identifying data as defined in margin no. 52 of Annex 3 to FINMA Circ. 08/21.
f) "**clients**": the clients of an institution.
g) "**cloud**" or "**cloud computing**": as defined by the National Institute of Standards and Technology (NIST)[1] or the European Union Agency for Network and Information Security (ENISA)[2]; cloud or cloud computing includes the Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) models, and can be supplied as public cloud, private cloud or hybrid cloud.
h) "**cloud services**": the cloud computing service models supplied by the provider on order of the institution.
i) "**FADP**": the Federal Act on Data Protection, SR 235.1.
j) "**FINMA Circ. 18/3**": Circular 2018/3 of the Swiss Financial Market Supervisory Authority, "Outsourcing – Banks and Insurers, Outsourcing by banks and insurance companies", date of issue: 21 September 2017, in the currently valid version.
k) "**FINMA Circ. 08/21**": Circular 2008/21 of the Swiss Financial Market Supervisory Authority, "Operational Risks – Banks, Capital adequacy requirements and qualitative requirements for operational risks at banks", date of issue: 20 November 2008, in the currently valid version.
l) "**FINMA Circ. 08/10**": Circular 2008/10, "Self-regulation as a minimum standard", date of issue: 20 November 2008, in the currently valid version.
m) "**guidelines**": the principles and recommendations set out in this document.

1 https://csrc.nist.gov/publications/detail/sp/800-145/final.
2 https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

n) "**institution**": banks and securities dealers as defined in margin no. 5 of FINMA Circ. 18/3.
o) "**mass CID**": mass CID as defined in margin no. 53 of Annex 3 to FINMA Circ. 08/21.
p) "**personal data**": as defined in the applicable data protection legislation. It also includes equivalent terms used in the applicable data protection legislation.
q) "**processing**": as defined in the Federal Act on Data Protection. It also includes equivalent terms used in the applicable data protection legislation.
r) "**protected information**" is CID, personal data and other information and data designated by the institution as requiring to be treated confidentially.
s) "**provider**": the provider of the cloud services outside the institution or the institution's company group.
t) "**SESTA**": the Federal Act on Stock Exchanges and Securities Trading (Stock Exchange Act, SESTA), SR 954.1.
u) "**SESTO**": the Ordinance on Stock Exchanges and Securities Trading (Stock Exchange Ordinance, SESTO), SR 954.11.
v) "**significant subcontractors**": subcontractors that, as part of the delivery of cloud services by the provider, (i) perform significant functions within the meaning of FINMA Circ. 18/3 or (ii) in the institution's view are to be regarded as significant subcontractors.

Chapter II: Governance

Legal basis

- Arts 3 and 47 BA, Art. 12 BO
- Arts 10 and 43 SESTA and Art. 19f. SESTO.
- FADP
- FINMA Circ. 08/21 and in particular Annex 3 to FINMA Circ. 08/21
- FINMA Circ. 18/3

3 Decision to procure cloud services

5 Cloud computing covers a wide variety of available services, ranging from highly standardised cloud infrastructures and services to bespoke solutions. The decision to procure cloud services should therefore be taken on the basis of a structured process.

6 If the decision to procure cloud services is taken on the basis of a risk analysis[3] carried out in advance, this should take account not just of the opportunities and risks associated with using cloud services but also of the significance of the cloud services for the purposes of FINMA Circ. 18/3 and the categorisation of the protected information, in particular CID, processed as part of the cloud services.

7 When assessing the risks, the institution should also take into account those that may be associated with the inadequate delivery of the cloud services or the total or partial failure of those services or of the provider.

3 For example, this would include assessing the risks associated with data security or the applicable legislation.

8 If there are risks associated with the procurement, deployment or termination of the use of the cloud services, appropriate mitigating measures should be defined and implemented, further developed and monitored as part of risk management for as long as the cloud services are being used.

4 Responsibilities and roles

9 In view of the regulation the institution is subject to, account must be taken of financial market legislation as well as – where CID or personal data are processed as part of the cloud services – banking secrecy and data protection legislation.

10 When allocating responsibilities and defining roles, the service and delivery models must be considered. The provider should cooperate as appropriate and necessary, making relevant information available to the institution. Ideally this cooperation should begin during the tender process.

11 If the provider uses subcontractors to deliver the cloud services, due account should be taken of this when defining the roles and responsibilities with regard to the significant subcontractors.

12 The contract between the institution and the provider should set out the corresponding rights and duties of the parties and others involved, and should also cover their implementation.

5 Selecting and changing the provider and significant subcontractors

13 Providers (especially providers of highly standardised cloud services) routinely reserve the right to define and change the operating models, the technologies used, service providers within and outside the group, and other essential factors (design authority), with a view to efficient and competitive service delivery.

14 When selecting the appropriate provider it is in the institution's interest to take account of the provider's ability to fulfil the contractual obligations, its financial stability and the jurisdiction to which it is subject, as well as other essential points. Significant subcontractors should be included in the assessment. The provider should assist as appropriate in gathering the information on this matter requested by the institution.

15 The risk assessment should in particular include defining the mitigating measures and the responsibilities for implementing them.

16 When selecting a provider, its willingness to assume responsibility for the essential duties arising out of financial market[4] and data protection legislation and the design of its operating model should be considered in addition to performance-related criteria. When selecting a provider and its subcontractors to process CID from the institution or other personal data, the confidentiality and security of the data should be a decisive criterion and an integral part of the underlying due diligence. This applies in particular to all activities involving access to mass CID[5].

17 A change of provider should be subject to the prior consent of the institution, which may be given in writing or another verifiable manner. A restructuring that is purely internal to the group and within the same jurisdiction that does not have a material impact on the existing circumstances, criteria and risks may be exempted from this consent requirement. The provider should, at the institution's request, agree to put in place arrangements governing a change of the company controlling the provider or a significant subcontractor.

18 The involvement of new significant subcontractors or a change of subcontractors must be conducted in accordance with the principles set out in FINMA Circ. 03/18.[6] A contractual agreement on criteria for the involvement of significant subcontractors, with the provider required to ensure compliance and demonstrate fulfilment to the institution in advance, can give the institution additional security. In any event the institution must be notified before the provider involves a new significant subcontractor and given the opportunity to terminate the contract with the provider by a specific deadline, for good or justified reason where appropriate. In such cases the institution should take suitable precautions – in particular allowing itself an appropriate termination period and requiring appropriate cooperation on termination from the provider, as well as, if necessary, options to extend while maintaining the existing operating model – so that the outsourced functions and services and protected information can be returned or transferred to a new provider. Lock-in effects and the amount, number and criticality of the outsourced functions and protected information should be taken into account.

4 Including banking secrecy.
5 See the requirements set out in FINMA Circular 08/21 "Operational risk-banks", in particular Annex 3
6 FINMA Circ. 03/18, margin no. 33.

6 Data centres and operating centres

19 Concerns are sometimes expressed that the use of cloud services entails a loss of control over the data processed and that it is no longer possible to identify where the data is being stored and processed (data ubiquity). From the institutions' perspective, their clients' trust in the way their data are handled is of central concern.

20 The provider should disclose the locations where the cloud infrastructures (data centres) that the institution deploys (or can deploy) are situated and from which the cloud is operated (operating centres), as well as changes of location during the period of deployment. This disclosure should include information on the (legal) entities, specifically the provider and significant subcontractors, that operate, own or otherwise control the data centres and operating centres.

21 Where protected information is involved, a change of location to another jurisdiction during the term of the contract should be subject to a contractually defined change procedure and, depending on the individual need for protection, require the prior consent of the institution. The provider should detail the risks associated with the change of location and supply the institution with all the relevant information, in particular regarding the security measures applied, to enable it to take a decision.

22 It should be permissible to refuse prior consent without giving reasons. Otherwise the institution should take suitable precautions – in particular allowing itself an appropriate termination period and requiring appropriate cooperation on termination from the provider, as well as, if necessary, options to extend while maintaining the existing operating model – so that the outsourced functions and services and the protected information can be returned or transferred to a new provider. Lock-in effects and the amount, number and criticality of the outsourced functions and services and protected information should be taken into account. Further requirements arising out of data access by third parties are described in the following chapters.

Chapter III: Data and data security

Legal basis

- Art. 47 BA
- Art. 43 SESTA
- Annex 3 FINMA Circ. 08/21
- FINMA Circ. 18/3
- FADP

7 Classification of data and information

23 To enable proper implementation of the requirements under data protection legislation and ensure the banking secrecy is maintained, the institution should classify the protected information processed by means of the cloud services.

24 This classification should allow the institution, and where relevant the provider, to assess and define the applicable legal and regulatory requirements with regard to data processing and data flows, access concepts and the appropriateness of further controls.

25 Consideration should be given to whether, and to what extent, clients have been informed that processing of CID has been outsourced to a provider of cloud services in Switzerland or abroad or, if and to the extent necessary, they have agreed to such outsourcing.[7]

26 Material changes to the classification of the outsourced protected information during the term of the contract should be recorded and necessary measures taken before such outsourcing.

7 See Chapter III:10 below.

8 Storage locations and data flows, access concept

27 The provider should allow the institution to review the acceptability of the locations where the CID and, where relevant, other protected information are processed and inspect those locations. The institution should also be in a position to comply with its duties of transparency to clients and therefore know where processing is carried out (in particular the locations where protected information is stored) to the level of detail required for this purpose.

28 Likewise, data flows involving protected information, which take place in the sphere of the provider and, where relevant, its subcontractors, should be disclosed to the institution in advance and the architecture underlying the data flows should, where required, be specified as precisely as necessary in the contract.

29 The latter also includes the definition and implementation of an access concept[8] by the provider. The provider should disclose access authorisations granted[9] on request and access to protected information, in particular CID, should be monitored and recorded in an appropriate manner by the provider.

30 The access concept should also define the purpose of access in sufficiently narrow terms and indicate the precisely defined cases in which access to systems used to process protected information can be granted or is unblocked. Such cases may include emergencies or other critical failures of the cloud infrastructure that cannot be remedied in any other way.

8 With regard to access to protected information.
9 See footnote 8.

9 General technical and organisational measures on data security

31 In general, the provider should offer and, in accordance with the agreement, implement appropriate technical and organisational measures to protect the institution's protected information that it is processing. International and local standards should be taken into account. The subcontractors and the members of staff deployed by the provider and the subcontractors should also, where applicable[10], be bound to comply with such measures.

32 The provider should ensure that its staff and those of the subcontractors that have access to protected information, including CID, verifiably undertake to maintain confidentiality and treat the data accordingly, and receive information and training to this effect. This undertaking is deemed to be sufficient if it is made by the staff to the provider or its subcontractors as part of the employment relationship, or if it corresponds to the confidentiality required by data protection legislation, even if no explicit undertaking is given with regard to banking secrecy. However, providers are recommended to expressly advise their staff working in Switzerland of banking secrecy and the fact that breaching it is a criminal offence. The same applies with regard to breaches of business confidentiality, as well as the criminal sanctions attached to them.[11]

10 Banking secrecy and security measures

10.1 Introductory remarks

33 Before deploying cloud services, the institution must clarify whether it is necessary to obtain a waiver of banking secrecy (Art. 47 BA) from the client. This would apply if the institution were to intentionally or negligently breach banking secrecy through the use of cloud services.

34 This document argues that a waiver of banking secrecy by the client is not necessary, provided the institution has put in place adequate security measures covering the CID processed using the cloud services.

10 Account should be taken of the significance of a subcontractor.
11 Art. 162 Criminal Code.

This chapter contains an overview of the arguments supporting this interpretation and the security measures to be taken.

10.2 Technical, organisational and contractual security measures

35 An actual disclosure of CID to unauthorised persons caused intentionally or negligently by the institution constitutes a breach of banking secrecy.[12] Art. 47 para. 1 BA is a result crime: the mere possibility that unauthorised persons may obtain knowledge of CID does not in itself constitute a breach of banking secrecy.

36 Therefore, if the provider and its subcontractors do not actually obtain knowledge of the CID being processed in the cloud as part of the cloud services, there is no disclosure within the meaning of Art. 47 para. 1 BA. However, the institution must have put in place appropriate technical, organisational and contractual measures to limit the risk of the provider and its subcontractors accessing the CID.

37 The measures to be considered are set out in Annex 3 to FINMA Circ. 08/21 and the applicable provisions of data protection legislation. An assessment of the appropriateness of these measures should take account of the state of the art, the costs of implementation and the nature, scope, circumstances and purposes of processing the CID, as well as the differing probabilities of occurrence and gravity of the risk for the rights of the clients affected.

Some examples of measures are listed below.

38 Technical measures to protect CID:

Technical measures may have the effect that the data processed in the cloud no longer constitute CID. The definition of CID[13] is based on the concept of personal data under data protection legislation. This means that in accordance with Swiss legal practice, anonymised data or pseudonymised or encrypted data that the recipient cannot attribute to a specific person because they do not have a concordance or encryption key are not to be regarded as personal data or CID.

12 See judgment of the Federal Supreme Court 6B_1403/2017 of 8 August 2017.
13 Annex 3 to FINMA Circ. 08/21,margin no. 52.

The following security measures are particularly suitable technical processes for appropriately protecting CID.[14]

39 **Anonymisation**. Anonymised data (irreversible method) no longer constitute CID or personal data.[15] The requirements set out in this section therefore do not apply to anonymised data.

40 **Pseudonymisation**. Where the data constitute CID, the assignment rule should be appropriately protected under the institution's control in Switzerland. In particular, the rights to use the reference table should be restricted on a need-to-know basis and access documented in a verifiable manner.

41 **Encryption**. When encrypting CID, care should be taken to ensure that the encryption key is protected against unauthorised access and access remains under the institution's control, even if the encryption key is also available to the provider or kept by it and used for the automated encryption and decryption of the CID as part of the cloud service. With regard to the classification of CID in particular, the institution should, on the basis of a risk assessment, consider which procedures are appropriate to define the control of the encryption key.

The encryption procedure and the strength of the encryption key must meet current security standards, so that the encryption can be regarded as cryptographically secure.

CID should always be transferred in encrypted form. The encryption procedure and the strength of the encryption key must meet current security standards, so that the transfer can be regarded as cryptographically secure.

14 See FINMA Circ. 08/21, Annex 3, margin no. 20 and the definitions in margin nos 61 to 65.
15 See FINMA Circ. 08/21, Annex 3, margin no. 64.

42 Organisational measures to protect CID:

The operational measures implemented by the provider and its subcontractors should be subject to appropriate supervision by the institution.

The required[16] audit of the provider's security and confidentiality standards should be conducted with reference to independent reports and on the basis of recognised reporting standards.[17]

43 Contractual measures to protect CID:

Contractual measures include in particular:

- appropriate stipulations in the contract between the provider and the institution regarding the technical and organisational measures and a requirement for the provider to bind its subcontractors to comply with the essential organisational and technical measures, to the extent that they process CID;
- an agreement by the provider to maintain confidentiality;
- taking account of the sensitivity of the data and imposing a responsibility in this respect on the provider;
- monitoring the implementation of and compliance with the technical, organisational and contractual measures;
- agreements as per chapter IV (Authorities and proceedings in court and by authorities).

10.3 Persons subject to the duty of confidentiality

44 Depending on the cloud service model, it may be necessary for staff of the provider and its subcontractors to process the CID in the cloud in cleartext, i.e. neither encrypted nor pseudonymised, and therefore actually obtain knowledge of them. In this event, the question arises as to whether the provider and its subcontractors constitute unauthorised persons for the purposes of Art. 47 para. 1 BA. For the sake of clarity, fully automated encryption and decryption as part of the cloud service is not to be viewed as cleartext data processing for the purposes of this section.

16 The audit must comply with the requirements of FINMA Circ. 08/21, Annex 3, Principle 9.
17 For example, the auditing standards of the reporting options under ISAE 3000 or SOC2.

45 These guidelines are based on the view that the provider and its subcontractors do not constitute unauthorised persons within the meaning of Art. 47 para. 1 BA. The deployment of cloud services of a provider in principle reflects the institution's sincere interest in optimising service quality, costs and data security. The dispatch on the revision of the BA explicitly refers to the status of IT service providers as representatives (representative in the meaning of Art. 47 para. 1 BA; "Beauftragte").[18] Additionally, the institution normally has the right to issue instructions[19] to the provider and its subcontractors. They are therefore to be regarded as representatives for the purposes of Art. 47 para. 1 BA and can be categorised as persons subject to the duty of confidentiality.

46 Providers and subcontractors based outside Switzerland are also representatives and, as such, authorized persons subject to the duty of confidentiality. This corresponds to the meaning and purpose of Art. 47 para. 1 BA and is not excluded by the wording.[20] Moreover, the legal and regulatory provisions applying in other countries may also provide for effective protection mechanisms.

47 However, the increased risk resulting from processing of data in cleartext outside Switzerland must be taken into account as part of the applicable security measures. The key criteria for assessing appropriateness include country-specific risks, in particular (but not limited to) the issue of whether the respective legislation ensures adequate data protection.

48 The relevant technical, organisational and contractual measures are also set out in Annex 3 to FINMA Circ. 08/21 and the applicable provisions of data protection legislation.

49 The additional measures listed below can be regarded as appropriate in relation to an increased risk outside Switzerland.

18 Dispatch on the revision of the BA dated 13 May 1970, BBL 1970, 1182: "The extension [of the duty of banking secrecy] to representatives is also to include in particular computer centres entrusted by banks with electronic data processing."
19 FINMA Circ. 03/18, margin no. 21.
20 The need for an explicit exclusion follows from the legality principle of Art. 1 of the Swiss Criminal Code.

- Processing of data in cleartext by staff of the provider or its subcontractors outside Switzerland should only take place to the extent necessary for the secure and reliable operation of the cloud, and subject to narrowly defined conditions with respect to time and subject matter.
- Processing activities must be monitored and recorded by the provider and the institution should have the option to retain control over the timing, duration and scope of processing. The provider must be in a position to terminate processing without delay where there is a suspicion of unauthorised processing activity.
- The institution must be informed about the processing by the provider or must have the opportunity to obtain information itself.
- The institution must attach particular importance to the agreements under chapter IV (Authorities and proceedings).

50 As indicated above, cleartext processing of CID by staff of the provider and its subcontractors does not in principle constitute a breach of banking secrecy by the institution.

51 CID could be assumed to have been disclosed to unauthorised persons if third parties outside the sphere of the provider, such as foreign authorities, obtain knowledge of CID due to the use of cloud services by the institution. If the appropriate technical, organisational and contractual measures to protect the CID have been taken, the question nevertheless arises as to whether in such a case the institution can be held in any way responsible for a causal and intentional or negligent action or failure to act[21].

10.4 Duties to inform under data protection legislation

52 Under data protection legislation, there is a duty to inform if personal data is processed within the scope of cloud services. This duty can be fulfilled by means of the institution's general data protection policy. In accordance with the principle of transparency, the information is to be provided in a simple and comprehensible manner. For the purposes of clarity, data protection legislation does not in principle require the disclosure of the individual providers and their subcontractors.

21 This means that in a case where there is a mere possibility of accessing CID, the assumption of a criminal attempt at disclosure to unauthorised parties does not arise, because the offence requires intent.

10.5 Additional duties to inform

53 Additional duties to inform that may arise for reasons outside the scope of data protection legislation must be assessed on a case-by-case basis. For example, the customer's expectations, contractual agreements, provisions under mandate law and the principle of good faith should be considered. Points of reference could be the institution's market presence and any communication of the institute regarding its prior commissioning of service providers.

10.6 Measures to secure the availability and return of information

54 The institution should be able to access any protected information that is stored or processed abroad or in Switzerland at any time from Switzerland. The provider should undertake to continue to deliver the cloud services to the institution, a successor company or rescue company and, where applicable, FINMA if the institution is in recovery or resolution, to the extent that such access from Switzerland to information abroad or in Switzerland is assured as a result.

55 The provider should undertake to return the protected information to the institution, a successor company or rescue company at any time as part of assistance with termination, if the institution is in recovery or resolution and on the instructions of the institution or FINMA, provided the provider has the means[22] and knowledge[23] to do so. In this case, the provider should transfer the protected information back in a standardised, machine-readable format.

56 If the provider uses proprietary solutions that result in lock-in effects, the provider should declare its willingness to support the institution with a migration to other solutions or with licensing such solutions.

22 Such as encryption keys.
23 Especially where cloud services as part of IaaS or PaaS are concerned, the provider may have no knowledge of the architecture chosen by the institution and/or the components used by the institution.

Chapter IV: Authorities and Proceedings

Legal basis

- Art. 271 Criminal Code
- Art. 273 Criminal Code
- Art. 47 BA
- Art. 6 FADP
- International treaties on international legal assistance
- FINMA Circ. 08/21 Annex 3, margin no. 20

57 The provider must agree with the institution a procedure for both parties to adopt in response to requests from the authorities relating to the handover or transfer of protected information that is processed in the cloud. To the extent that there is no conflict with mandatory law, the provider must supply the institution with a contractual undertaking covering the points set out in margin nos 57–60.

58 In the context of foreign proceedings the provider, its subcontractors and group companies may only transfer or disclose protected information processed in the cloud to foreign authorities or other parties abroad in accordance with the applicable legal and regulatory provisions and (i) with the prior written consent of the institution, (ii) on the basis of a judgment of the competent Swiss court, or (iii) on the basis of an authorisation from the competent Swiss authority.

59 The provider should notify the institution in due time prior to handing over the protected information, give the institution the rights to conduct the proceedings, and support the institution in handling requests from foreign authorities.

60 If, on account of mandatory law, the provider is unable to notify the institution in advance of the transfer or disclosure of protected information to foreign authorities or other parties abroad, the provider should implement the appropriate legal or protective measures within the scope of the agreement made and in the interest of the institution and its clients.[24]

61 In addition, the provider should inform the institution in a general way of the number (per year), subject matter and conduct of proceedings that involve or could involve the transfer or disclosure of protected information under applicable foreign law or regulations and that are applicable to the provider and the subcontractors[25] or group companies of the provider.[26]

62 The institution should, with appropriate cooperation from the provider where necessary, assess the risks of foreign authorities being able to override the effectiveness of the technical, organisational and contractual measures listed in section 10.

24 See chapters II and III, in particular the comments on bank-client confidentiality and transparency under data protection law.
25 Subcontractors that have access to protected information, in particular CID.
26 See footnote 25.

Chapter V: Audit of the cloud services and means used

Legal basis

- Arts 18 and 23ff. BA and the implementing provisions of the BO
- Art. 17 SESTA
- FINMA Circ. 08/21
- FINMA Circ. 18/3

63 Cloud services are normally delivered by providers from highly secure computer centres to a large number of customers.[27] Auditing the infrastructures used by the providers requires a high degree of specialisation; account should be taken of the provider's duties of confidentiality to its other customers.

64 Compliance with the requirements applicable to or contractually imposed on the provider arising out of the legal and regulatory requirements (in particular with regard to outsourcing, data protection and information security) should be audited regularly, taking account of the fact that the effectiveness of measures results from a combination of controls at the provider and at the institution. The provider should assist in this process to an appropriate extent. Performance of the contractually agreed services may also form part of the audit.

65 There should be provision for the audits to be carried out and ordered by the institution, its internal and external auditors or FINMA. Pool audits by a number of institutions or their audit firms, as well as indirect or accompanied audits in which auditing and reporting are conducted by the provider's audit firm or an audit firm designated by the provider are permitted, provided the audit firm has the necessary independence and specialist expertise. This also applies to audits ordered by FINMA.

27 Public cloud.

66 An on-site audit of the IT infrastructures actually used to deliver the cloud services is not absolutely necessary, except for inspecting the physical security measures. Granting the institution, its audit firm or the competent authority logical access can be regarded as sufficient. The provider can agree the arrangements for this right of access directly with the supervisory authority.

67 In the case of cloud services with links outside Switzerland, a contractual agreement covering the right for the institution, its audit firm, the provider's audit firm and FINMA to audit the provider directly or indirectly satisfies the requirement for appropriate clarification of audit rights.

68 The principles set out above should also be prescribed in relation to significant subcontractors. In the absence of an agreement between the institution and the subcontractors, this should be done by binding the subcontractors to comply with the provider's contractual obligations.

69 The audit of the significant subcontractors can be carried out indirectly by auditing the provider, though a direct audit of the significant subcontractors may become necessary.

SwissBanking

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
P.O. Box 4182
CH-4002 Basel

office@sba.ch
www.swissbanking.org