SwissBanking

December 2020

Appendix I to the SBA Cloud Guidelines

Guide to interpreting Chapter V, margin nos 63 – 69:
Audit of the cloud services and means used

Content

List of abbreviations

AICPA	American Institute of Certified Public Accountants
AT	Attestation Standards
BSI	Bundesamt für Sicherheit und Informationstechnik (German Federal Office for Information Security)
CSA STAR	Cloud Security Alliance Security Trust Assurance and Risk
CIA protection goals	Confidentiality, Integrity, Availability
CID	Client identifying data
COBIT	Control Objectives for Information and Related Technology framework
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
MTCS	Multi-Tier Cloud Security
NIST	National Institute of Standards and Technology
PII	Personally identifiable information
PS	Swiss Auditing Standards
Circ.	Circular of the Swiss Financial Market Supervisory Authority FINMA
SSAE	Statement on Standards for Attestation Engagements
SOC	Service Organization Controls

1 Introduction

The Swiss Bankers Association (SBA) published its Cloud Guidelines in March 2019. The guidelines contain recommendations intended to help banks migrate their data to the cloud more easily and securely and outsource critical functions reliably to the cloud. They address, among other things, the auditing of cloud services and the means required for this purpose. This document supplements Chapter V of the SBA Cloud Guidelines and serves as a non-binding guide to interpreting the statements made therein. It outlines the general requirements for the audit[1] and the typical contents of an audit report,[2] and it also provides an overview of the main international certifications and attestations.

In general, cloud providers' compliance with the applicable legal, regulatory and contractual requirements should be audited. This includes in particular the topics of 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. A more detailed examination as part of a pool audit can also be considered (see margin no. 65, Cloud Guidelines). It is permitted to rely on reports, certifications and attestations from the cloud provider.

The requirements outlined below can be taken as a guide with regard to basing the audit on reporting by the provider's audit firm or an audit firm designated by the provider. As a rule, the cloud provider makes the audit report or reports available, although not all audit reports are intended for forwarding. Past audit reports are to be taken into account to the extent that is relevant and reasonable. Attention must also be paid to organisational aspects and aspects specific to the nature and scope of the cloud services to be provided (e. g. SaaS, PaaS or IaaS).

The content of the audit must be selected via an institution-specific and risk-based

1 Unless otherwise stated, the term "audit" is used in the broader sense in this document and corresponds to a what audit firms refer to as a "non-audit assurance". Non-audit assurance services supply verifiable information in the form of reports produced by trusted third parties confirming to institutions that the cloud providers they use can be relied on to perform the tasks entrusted to them.

2 The term "audit report" hereinafter refers to a report on the organisation and processes underlying the service (e. g. according to the SOC 2 standard) rather than a financial audit report.

approach. To avoid duplication, the use of reports, certifications and attestations from the cloud provider is permitted if these are deemed sufficient by the institution. If the audit does not cover any banking services per se, it is not subject to regulatory requirements. The same applies if it is not relevant for the purposes of the financial or regulatory auditing. Legal requirements (e. g. in terms of data protection) must always be taken into account.

In this respect, it is advisable to adapt the requirements for the audit or relax certain rules. The following criteria may optionally be used to select the key audit points:

- Type of service (e. g. core application, software development or translation)
- Systemic importance
- Relevance of the service for the institution
- Scope of service (e. g. hosting versus cloud services)
- CIA protection goals
  - Protection of involved data, e. g. CID (Confidentiality)
  - Protection against unauthorised changes, or immutability (Integrity)
  - Protection against outages/catastrophes (Availability); includes all aspects integral to the service, e. g. guaranteed processing time, data processing capacity, data availability
- Data storage location and access by the institution and third parties (in particular from abroad or if encryption is not under the control of the institution)
- Context risk, i.e. third-party and fourth-party risk (subcontractors/suppliers)
- Threat landscape (global context)
- Indicators to be taken into account in connection with an exit strategy (e. g. documentation of the procedure, contractual agreements)
- Indicators of controls explicitly expected from cloud providers by the institution (cloud user) (e. g. contractually agreed additional services that are not part of the cloud provider's standard offering)

This document does not cover provider management on the part of individual institutions.

2 General requirements for the audit

- The audit programme should be based on tried-and-tested international standards such as the NIST Cloud Computing Security Reference Architecture, the Singapore Standard for Multi-Tier Cloud Security (MTCS, SS 584), ISO/IEC 27001 and 27017, COBIT, AICPA SOC 2, CSA STAR or the BSI Cloud Computing Compliance Controls Catalogue (C5).
- The auditing and reporting process should conform to a tried-and-tested international standard such as ISAE 3000, ISAE 3402/SSAE 18 or SOC 2 and, if relevant for the audit of the annual financial statements or the regulatory audit, should be at least equivalent to ISAE 3402.
- The qualifications and independence of the auditor and the audit firm must satisfy the requirements of the competent regulators under financial market law. In Switzerland, for example, this means Article 11a of the Ordinance on the Authorisation and Supervision of Auditors and FINMA Circ. 2013/3 "Auditing".
- Depending on the quality of the data (e. g. mass CID) and/or the quantity of data stored in the cloud and especially in view of the requirements of banking secrecy, the requirements set out in Annex 3 of FINMA Circ. 2008/21 "Operational risks – banks" and in FINMA Circ. 2018/3 "Outsourcing – banks and insurers" must also be taken into account.
- Where cloud services are used to process personal data, the above standards must be assessed with regard to data protection in particular.

3 Typical content of an audit

The following are typical audit points that may be relevant for a bank, depending on the cloud services it uses. They should be audited in accordance with the international standards listed in section 2 above.

- Organisation and governance
- Risk management
- Cybersecurity
- Data protection and banking secrecy
- Design, implementation and execution of controls
- Monitoring of controls
- Logical and physical access controls
- Data management and data transfer
- Development, maintenance and change management
- System and infrastructure operations
- Availability and recovery
- Accounting (licence management, invoices, billing)
- Content of standard contracts

4 Possible evaluation criteria for reports and attestations

The following statements apply to the audit firm's report:

- It contains general information on the scope and time frame of the audit. Any liability restrictions (e. g. restriction to a specific jurisdiction, areas not covered) must be borne in mind when evaluating the report.
- It contains at least a confirmation by the audit firm that the scope and depth of the audit satisfy the requirements of at least one of the jurisdictions to be specified.[3] As a rule, this will be the jurisdiction of the headquarters of the commissioning cloud provider.
- It contains a list of all significant laws and regulations taken into account in the audit.
- It contains a detailed description of the system used for the cloud service in line with the associated risk, including geographical and legal setup as well as system elements attributable to subcontractors (suppliers).
- It makes clear which services with relevance for the institutions are covered by the audit and which are not covered ("out of scope"). Ideally, customer billing processes should also be included.
- It conforms to Type 2 (design and effectiveness).
- It contains information on relevant cyber incidents and data security violations, i.e. unauthorised data access by third parties (including authorities), as well as significant system outages.
- It includes the cloud provider's significant subcontractors (suppliers). The significance of subcontractors is determined by their relevance with regard to the confidentiality and integrity of the data and the availability of the service (CIA protection goals, see section 1 above). The provider's audit firm or an audit firm designated by the provider confirms the completeness of the assurance or states its limitations.

3 The institution must determine the scope of the audit based on the applicable criteria (see section 2 above).

- It contains an audit depth and an audit scope that are proportionate to the CIA protection goals and the expected risks.
- It covers a sufficient period of time (e. g. 12 months for the audit of annual financial statements and the regulatory audit).
- It provides details of existing or newly discovered deviations from the requirements as well as measures and deadlines agreed in connection with such deviations. This makes it clear which deviations are affecting and have affected the institution. The disclosure is not institution-specific, but general.
- It takes account of any further known security certifications (e. g. ISO 27001) or attestations by trusted third parties (e. g. SOC 2).[4] The institution should also request these and take them into consideration in its assessment.
- It shows in detail the security controls and their adequacy with regard to potential crossborder access to sensitive data. This also applies to any access rights granted to the provider's parent or group companies outside Switzerland under local laws.
- It should not be more than one year old in order to serve as a reliable reference.
- It confirms correctness, integrity, validity and functionality insofar as the cloud provider offers data, tools or information on the (security) monitoring of its services (e. g. as part of Full Cloud Assurance and Transparency).

Procedure in the event of gaps in the audit report

- If there are gaps in the audit firm's report (e. g. topics, scope, relevant jurisdictions or liability restrictions are omitted), these must be addressed in the next audit at the latest and ideally in the wording of the contract. There are essentially three ways to close such gaps:
  - ensure through the wording of the contract that the gap in the report is closed;
  - add the omitted audit points to the internal audit;
  - explicitly state the risk resulting from gaps in the report.

4 If available in addition to the reporting by the provider's audit firm or an audit firm designated by the provider.

5 Overview of international certifications and attestations

Figure 1: Overview of existing certifications and attestations[5]

Designation	ISAE 3402	ISAE 3000	SSAE 18	SOC 2	PS 870
Title	International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization	International Standard on Assurance Engagements (ISAE) No. 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information	Statement on Standards for Attestation Engagements (SSAE) No. 18	Service Organization Controls Report 2 • Type 1 (control design) • Type 2 (also checks effectiveness of the controls)	Swiss Auditing Standard on auditing software products
Type	Auditing standard	Auditing standard	Auditing standard	Reporting option	Auditing standard
Main region	Global	Global	USA	Global	Switzerland
Report coverage	Any criteria with relevance for financial reporting: • Transactions • Transaction processing procedures • Reporting • Handling of significant business events	Any criteria of a business audit that is neither an audit nor a review of historical financial information	Any criteria with relevance for financial reporting (analogous to ISAE 3402) or topics such as: • Infrastructure • Software • Processes • People • Data	Primarily topics such as: • Infrastructure • Software • Processes • People • Data	Software product
Typical content	Controls on transaction processing with relevance for financial reporting and controls on supporting IT processes	Any controls or facts requiring confirmation	Controls on transaction processing with relevance for financial reporting and controls on supporting IT processes or any controls related to the "Trust Service Principles" or matters to be confirmed.	One or more of the Trust Services Criteria: • Confidentiality • Availability • Security • Processing integrity • Privacy	Software functionality, e. g.: • Multiclient capability • Auditability • Compliance
Addressees	Reports under ISAE 3402 have a restricted group of addressees (customers and their auditors).	Reports under ISAE 3000 may have a restricted group of addressees (e. g. SOC 2) or no such restriction (e. g. SOC 3).	Reports under SSAE 18 may have a restricted group of addressees (e. g. SOC 2) or no such restriction (e. g. SOC 3).	SOC 2 reports have a restricted group of addressees (customers and their stakeholders).	PS 870 reports may have a restricted group of addressees.
Certification possible	No	No	No	No	Yes
Time span of reports / certificates	Punctual or periodic	Punctual or periodic	Punctual or periodic	Punctual or periodic	Punctual
Audit standard largely equivalent to	SSAE 18	SSAE 18 (AT-C 320)	ISAE 3402, ISAE 3000	ISAE 3000	n / a
Remarks	Reports conforming to the ISAE 3402 standard are also produced for controls on service providers with no direct relevance for the service recipient's financial reporting.	ISAE 3000 is an overarching standard. This means that reports conforming to the ISAE 3402 standard implicitly conform to the ISAE 3000 standard as well. However, the opposite is not true.	SSAE 18 reports are also known as SOC reports.	SOC 2 is a reporting option. The underlying standard is either ISAE 3000 or SSAE 18.	The certificate refers only to the audited version of the software and is only valid in full for that version.

Sources: EXPERTsuisse, SBA

5 The reporting options SOC 1 and 3 are not discussed here as they are less relevant or insufficiently detailed in the context of auditing cloud services.

Figure 2: Overview of existing certifications and attestations (continued)

Designation	PS 920	PS 950	ISO/IEC 27001	ISO/IEC 27002	ISO/IEC 27017	ISO/IEC 27018
Title	Swiss Auditing Standard, agreed audit actions regarding financial information	Swiss Auditing Standard, business audits that are neither audits nor reviews of historical financial information	Information technology • Security techniques • Information security management systems • Requirements	Information technology • Security techniques • Code of practice for information security controls	Information technology • Security techniques • Code of practice for information security controls based on ISO/IEC 27002 for cloud services	Information technology • Security techniques • Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
Type	Audit standard	Audit standard	Control standard	Guideline	Guideline	Guideline
Main region	Switzerland	Switzerland	Global	Global	Global	Global
Report coverage	Audit actions agreed between the auditor and audited company regarding financial information	Any criteria of a business audit that is neither an audit nor a review of historical financial information	Scope of the defined information security management system in combination with non-excluded controls from the Annex or ISO 27002, i.e. a clearly defined part of the organisation, processes or products	n/a	Security of cloud services	Security of cloud services
Typical content	Statements on the agreed audit actions	Any controls or facts requiring confirmation	Existence of an information security management system (ISMS)	n/a	Implementation of information security controls for cloud service customers	Data protection law requirements for processing personal data in the cloud
Addressees	The report is only intended for parties who know the terms of the engagement.	PS 950 reports may have a restricted group of addressees or no such restriction, depending on the underlying criteria (publicly known or not).	ISO 27001 certificates do not have a restricted group of addressees.	n/a	ISO 27017 certificates do not have a restricted group of addressees.	ISO 27018 certificates do not have a restricted group of addressees.
Certification possible	No	No	Yes	No	Yes	Yes
Time span of reports/certificates	Punctual or periodic	Punctual or periodic	Periodic (3 years)	n/a	Punctual or periodic	Punctual or periodic
Audit standard largely equivalent to	AT 201 (US)	ISAE 3000	n/a	n/a	n/a	n/a
Remarks	Where expedient, the standard may also be used for engagements that are not financially relevant.	Implementation of ISAE 3000 in Switzerland	The scope of an ISO 27001 certificate's applicability is clearly defined (Statement of Applicability/SoA). It may, for example, apply to an individual department or the entire company.	Contrary to popular belief, certification under ISO/IEC 27002 is not possible.		

Sources: EXPERTsuisse, SBA

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