SwissBanking

Dezember 2020

Anhang I zum Cloud-Leitfaden der SBVg

Orientierungshilfe zu Kapitel V Rz 63 – 69: Prüfung der Cloud-Dienstleistungen und der eingesetzten Mittel

Inhaltsverzeichnis

1	**Einleitung**	**4**
2	**Allgemeine Anforderungen an die Prüfung**	**6**
3	**Typische Inhalte einer Prüfung**	**7**
4	**Mögliche Beurteilungskriterien von Berichten und Attestierungen**	**8**
5	**Übersicht internationaler Zertifizierungen und Attestierungen**	**11**

Abkürzungsverzeichnis

AICPA	American Institute of Certified Public Accountants
AT	Attestation Standards
BSI	Bundesamt für Sicherheit und Informationstechnik
CSA STAR	Cloud Security Alliance Security Trust Assurance and Risk
CIA-Schutzziele	*Confidentiality, Integrity, Availability* (Vertraulichkeit, Integrität, Verfügbarkeit)
CID	*Client Identifying Data* (Kundenidentifikationsdaten)
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-Tiered Cloud Security
NIST	National Institute of Standards and Technology
PII	*Personally Identifiable Information* (Persönlich identifizierbare Informationen)
PS	Schweizer Prüfungsstandards
RS	Rundschreiben der Finanzmarktaufsicht FINMA
SSAE	Statement on Standards for Attestation Engagements
SOC	Service Organization Controls

1 Einleitung

Die Schweizerische Bankiervereinigung (SBVg) hat im März 2019 einen Cloud-Leitfaden veröffentlicht. Dieser beinhaltet Empfehlungen, damit Banken ihre Daten sicher und einfacher in die Cloud migrieren, respektive kritische Funktionen zuverlässig daraus beziehen können. Im Leitfaden wird unter anderem auf die Prüfung der Cloud-Dienstleistungen und der dafür notwendigen Mittel eingegangen. Dieses Dokument ergänzt die bestehenden Ausführungen in Kapitel V des Cloud-Leitfadens der SBVg und dient dem Leser als unverbindliche Orientierungshilfe. Es zeigt die allgemeinen Anforderungen an die Prüfung[1], und die typischen Inhalte eines Prüfberichts[2] auf und gibt eine Übersicht der gängigen internationalen Zertifizierungen und Attestierungen.

Generell sollte die Einhaltung der auf den Cloud-Anbieter anwendbaren gesetzlichen, regulatorischen und vertraglichen Anforderungen geprüft werden. Zu diesen gehören insbesondere die Themen Outsourcing, Datenschutz und Informationssicherheit. Die Prüfungen sollten vom Institut, dessen internen oder externen Prüfgesellschaft oder von der FINMA durchgeführt und veranlasst werden können. Auch eine weitergehende Prüfung im Rahmen eines Pool-Audits kommt in Betracht (vgl. RZ 65, Cloud-Leitfaden). Dabei ist es zulässig, sich auf Berichterstattungen, Zertifizierungen und Attestierungen des Cloud-Anbieters abzustützen.

Um sich im Rahmen einer Prüfung auf die Berichterstattung der Prüfgesellschaft des Anbieters oder durch eine vom Anbieter bezeichnete Prüfgesellschaft abstützen zu können, können untenstehende Anforderungen als Orientierungshilfe herangezogen werden. Der Cloud-Anbieter stellt in der Regel den Prüfbericht bzw. die Prüfberichte zur Verfügung, wobei nicht alle Prüfberichte für die Weiterleitung vorgesehen sind. Prüfberichte der Vergangenheit sind, soweit massgeblich und sinnvoll, zu

1 Im Rahmen dieses Dokumentes wird unter dem Begriff «Prüfung» die Prüfung im Sinne der Non-Audit Assurance verstanden, sofern nicht anderweitig ausgeführt. Non-Audit-Assurance-Dienstleistungen liefern überprüfbare Informationen in Form von durch vertrauenswürdige Drittparteien erstellte Berichte und bestätigen den Instituten die Zuverlässigkeit betreffend Zielerfüllung durch die beauftragten Cloud-Dienstleister.

2 Mit Prüfbericht ist nachfolgend ein Prüfbericht gemeint, der die Organisation und Prozesse der Dienstleistung (z. B. SOC 2) zum Gegenstand hat. Nicht gemeint ist die Rechnungsprüfung.

berücksichtigen. Organisatorische, sowie spezifische auf den Umfang und die Art der zu beziehenden Cloud-Dienstleistung (z. B. SaaS, PaaS, IaaS) anwendbare Gesichtspunkte sind gleichermassen zu berücksichtigen.

Die Auswahl der zu prüfenden Inhalte hat institutsspezifisch und risikobasiert zu erfolgen. Zur Vermeidung von Duplikationen ist die Abstützung auf Berichterstattungen, Zertifizierungen und Attestierungen des Cloud-Anbieters zulässig, wenn diese vom Institut als ausreichend beurteilt werden. Deckt die Prüfung keine Bankdienstleistung im eigentlichen Sinne ab, bestehen keine regulatorischen Anforderungen an ebendiese. Dasselbe gilt, wenn sie weder für die Rechnungsprüfung, noch die Aufsichtsprüfung relevant ist. Rechtliche Anforderungen (z. B. Datenschutz) sind in jedem Fall zu berücksichtigen.

Folglich empfiehlt es sich, die Anforderungen an die Prüfung anzupassen oder Erleichterungen zu gewähren. Für die Auswahl der wesentlichen Punkte für die Prüfung können folgende Kriterien optional herangezogen werden:

- Art der Dienstleistung (z. B. Core Applikation, Software Entwicklung, Übersetzungsservice)
- Systemrelevanz
- Relevanz der Dienstleistung für das Institut
- Umfang der Dienstleistung (z. B. Hosting vs. Cloud-Dienstleistungen)
- CIA-Schutzziele
  - Schutz der involvierten Daten, z. B. CID (Confidentiality)
  - Schutz vor nicht autorisierten Veränderungen, respektive Unabänderbarkeit (Integrity)
  - Ausfallschutz / Katastrophenschutz (Availability). Dazu gehören alle Gesichtspunkte, die für die konkrete Dienstleistung im Fokus stehen, z. B. zugesicherte Verarbeitungszeit, Datenverarbeitungskapazität, Datenverfügbarkeit
- Speicherort der Daten und Zugriff durch Institut sowie Dritte (insbesondere aus dem Ausland oder wenn Verschlüsslung nicht unter Kontrolle des Institutes ist)
- Kontextrisiko, d.h. Drittparteien- sowie Viertparteien-Risiko (Unterakkordanten bzw. Zulieferer)

- Bedrohungslandschaft (globaler Kontext)
- Hinweise, die es im Zusammenhang mit einer Exit-Strategie zu berücksichtigen gilt (z. B. Dokumentation des Vorgehens, vertragliche Vereinbarungen)
- Hinweise zu Kontrollen, die seitens Cloud-Anbieter explizit vom Institut (Cloud Nutzer) erwartet werden (z. B. vertraglich vereinbarte Zusatzleistungen, die nicht zum Standardangebot des Cloud-Anbieters gehören)

Das Provider Management seitens der einzelnen Institute liegt nicht im Geltungsbereich dieser Ausführungen.

2 Allgemeine Anforderungen an die Prüfung

- Das Prüfprogramm sollte sich an international verwendeten und erprobten Standards (z. B. NIST Cloud Computing Security, Multi-Tiered Cloud Security (MTCS) Singapore Standard (SS 584), ISO/IEC 27001 und 27017, COBIT, AICPA SOC 2, CSA STAR, BSI Anforderungskatalog Cloud Computing C5) orientieren.
- Der Prozess der Prüfung und Berichterstattung erfolgt nach einem international verwendeten und erprobten Standard (z. B. ISAE 3000, ISAE 3402/SSAE 18, SOC 2) und ist, falls relevant für die Jahresabschlussprüfung oder die aufsichtsrechtliche Prüfung, mindestens gleichwertig zu ISAE 3402.
- Qualifikation und Unabhängigkeit des Prüfers und der Prüfgesellschaft müssen die Anforderungen der zuständigen Regulatoren nach den Finanzmarktgesetzen erfüllen. In der Schweiz sind dies zum Beispiel Artikel 11a der «Verordnung über die Zulassung und Beaufsichtigung der Revisorinnen und Revisoren» (Revisionsaufsichtsverordnung) sowie FINMA RS 2013/3 «Prüfwesen».
- Je nach Qualität der Daten (z. B. Massen-CID) bzw. Ausmass der Daten-Auslagerung in die Cloud ist ausserdem, insbesondere unter Berücksichtigung der Anforderungen des Bankkundengeheimnisses, der Anforderungskatalog gemäss FINMA RS 2008/21 Operationelle Risiken – Banken, Anhang 3, bzw. die Anforderungen gemäss FINMA RS 2018/3 Outsourcing Banken und Versicherer, ergänzend zu berücksichtigen.

- Sollten im Rahmen der Cloud-Dienstleistungen Personendaten bearbeitet werden, sind die vorgenannten Standards insbesondere im Hinblick auf den Datenschutz zu bewerten.

3 Typische Inhalte einer Prüfung

Die folgenden Punkte sind Kategorien typischer Prüfinhalte, die je nach Dienstleistungsangebot durch einen Cloud-Anbieter für die Bank relevant sein können. Sie werden anhand der unter Kapitel 2 aufgeführten internationalen Standards geprüft.

- Organization and Governance
- Risk Management
- Cybersecurity
- Datenschutz und Bankkundengeheimnis
- 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 (License Management, Invoices, Billing)
- Inhalt der Standardverträge

4 Mögliche Beurteilungskriterien von Berichten und Attestierungen

Der Bericht der Prüfgesellschaft:

- enthält generelle Angaben zu Prüfumfang und Zeitraum. Allfällige Haftungsbeschränkungen (z. B. Beschränkung auf eine bestimmte Jurisdiktion, nicht abgedeckte Bereiche) sind für die Bewertung des Berichts miteinzubeziehen.
- enthält mindestens eine Bestätigung des Revisionsunternehmens, dass der Prüfumfang und die Prüftiefe den Anforderungen mindestens einer zu spezifizierenden Jurisdiktion genügt[3]. In aller Regel wird dies die Jurisdiktion am Sitz des Auftrag gebenden Cloud-Anbieters sein.
- enthält eine Aufstellung aller für die Prüfung wesentlichen und berücksichtigten Gesetze und Regularien.
- enthält eine dem verbundenen Risiko angemessen detaillierte Systembeschreibung der Cloud-Dienstleistung, inkl. des geografischen und juristischen Setups sowie Systemelemente involvierter Unterakkordanten (Zulieferer).
- macht nachvollziehbar, welche für das Institut relevanten Dienstleistungen durch die Prüfung abgedeckt sind und welche nicht («Out of Scope»). Im Idealfall sind auch die Prozesse rund um die Rechnungsstellung an den Kunden mitberücksichtigt.
- ist vom Typ-2 (Design und Wirksamkeit).
- gibt Auskunft über relevante Cybervorfälle und Verletzungen der Datensicherheit, d. h. unautorisierte Zugriffe auf Daten durch Dritte (inkl. Behörden), sowie über signifikante Systemausfälle.

3 Wobei der Prüfumfang vom Institut anhand der anwendbaren Kriterien (siehe Ziff. 2 vorstehend) bestimmt werden muss.

- schliesst wesentliche Unterakkordanten (Zulieferer) des Cloud-Anbieters ein. Für die Beurteilung der Wesentlichkeit ist die Relevanz im Hinblick auf Vertraulichkeit und Integrität der Daten und Verfügbarkeit der Dienstleistung (CIA-Schutzziele, vgl. Ziff. 1) massgebend. Die Prüfgesellschaft des Anbieters oder eine vom Anbieter bezeichnete Prüfgesellschaft bestätigt die Durchgängigkeit des Testats oder weist Einschränkungen aus.
- enthält eine Prüftiefe und einen Prüfumfang, welcher im Verhältnis zu CIA-Schutzzielen und den erwarteten Risiken steht.
- deckt eine ausreichende Zeitperiode ab (z. B. 12 Monate für die Jahresabschlussprüfung und die aufsichtsrechtliche Prüfung).
- weist bestehende bzw. festgestellte Abweichungen von den Anforderungen sowie darüber vereinbarte Massnahmen und Termine aus. Es wird hierbei für das Institut offengelegt, von welchen Abweichungen es betroffen war und ist. Die Offenlegung ist dabei nicht institutsspezifisch, sondern allgemein.
- berücksichtigt allfällige weitere anerkannte Zertifizierungen zur Sicherheit (z. B. ISO 27001) oder Attestierungen durch vertrauenswürdige Drittparteien (z. B. SOC 2)[4]. Diese sollten ebenfalls vom Institut eingefordert und im Rahmen der Beurteilung beachtet werden.
- zeigt detailliert die Sicherheitskontrollen sowie deren Adäquanz hinsichtlich des möglichen grenzüberschreitenden Zugangs auf besonders schützenswerte Daten. Dies gilt auch für solche Zugangsrechte von Mutter- oder Gruppengesellschaften des Anbieters im Ausland, sofern diese nach lokalem Recht hierzu befähigt sind.
- sollte, um als verlässliche Abstützungsgrundlage dienen zu können, nicht älter als ein Jahr sein.
- bestätigt Korrektheit, Integrität, Aktualität und Funktionstüchtigkeit sofern der Cloud-Anbieter Daten, Tools oder Informationen zur (Sicherheits-)Überwachung seiner Dienstleistungen zur Verfügung stellt (z. B. im Rahmen von «Full Cloud Assurance and Transparency»).

4 Falls ergänzend zur Berichtserstattung der Prüfgesellschaft des Anbieters oder durch eine vom Anbieter bezeichnete Prüfgesellschaft verfügbar.

Vorgehen bei Lücken im Prüfbericht

- Weist der Bericht der Prüfgesellschaft Lücken auf (z. B. Themen, Umfang, betroffene Jurisdiktionen, Haftungsbeschränkung), sind diese spätestens im Rahmen einer nachfolgenden Prüfung, idealerweise aber bereits bei der Vertragsausgestaltung, entsprechend zu berücksichtigen und zu adressieren. Zur Schliessung der Lücken stehen grundsätzlich drei Optionen zur Verfügung:
  - den Vertrag so ausgestalten, dass die Lücke im Bericht geschlossen wird;
  - die eigene Prüfung um die fehlenden Prüfpunkte ergänzen;
  - die Risiken der Lücken im Bericht entsprechend ausweisen.

5 Übersicht internationaler Zertifizierungen und Attestierungen

Abbildung 1: Übersicht bestehender Zertifizierungen und Attestierungen[5]

Bezeichnung	ISAE 3402	ISAE 3000	SSAE 18	SOC 2	PS 870
Titel	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 • Typ 1 (Kontrolldesign) • Typ 2 (prüft darüber hinaus die Wirksamkeit der Kontrollen)	Schweizer Prüfungsstandard, Prüfung von Softwareprodukten
Typ	Prüfungsstandard	Prüfungsstandard	Prüfungsstandard	Berichterstattungsoption	Prüfungsstandard
Primäre Verbreitung	Weltweit	Weltweit	Vereinigte Staaten von Amerika	Weltweit	Schweiz
Abdeckung Bericht	Beliebige Kriterien mit Relevanz für die finanzielle Berichterstattung: • Transaktionen • Prozesse für Transaktionsabwicklung • Berichterstattung • Umgang mit wichtigen Geschäftsereignissen	Beliebige Kriterien einer betriebswirtschaftlichen Prüfung, die weder eine Prüfung noch ein Review von vergangenheitsorientierten Finanzinformationen darstellt	Beliebige Kriterien mit Relevanz für die finanzielle Berichterstattung (analog ISAE 3402) oder zu Themen wie: • Infrastruktur • Software • Prozesse • Personen • Daten	Primär Themen wie: • Infrastruktur • Software • Prozesse • Personen • Daten	Software-Produkt
Typische Inhalte	Kontrollen über die Transaktionsverarbeitung mit Relevanz für finanzielle Berichterstattung sowie Kontrollen über die unterstützenden IT-Prozesse	Beliebige Kontrollen oder zu bestätigende Sachverhalte	Kontrollen über die Transaktions-verarbeitung mit Relevanz für finanzielle Berichterstattung sowie Kontrollen über die unterstützenden IT-Prozesse oder auch beliebige Kontrollen rund um die «Trust Service Principles» oder zu bestätigende Sachverhalte.	Eines oder mehrere der Trust Service Principles: • Vertraulichkeit • Verfügbarkeit • Sicherheit • Integrität in der Verarbeitung • Datenschutz	Funktionalität der Software, wie z. B.: • Mandantenfähigkeit • Revisionsfähigkeit • Ordnungsmässigkeit
Empfängerkreis	Der Empfängerkreis eines Berichts nach ISAE 3402 ist eingeschränkt (Kunden und deren Prüfer).	Der Empfängerkreis eines Berichts nach ISAE 3000 kann, je nach Berichterstattungsoption eingeschränkt (bspw. SOC 2) oder nicht eingeschränkt (bspw. SOC 3) sein.	Der Empfängerkreis eines Berichts nach SSAE 18 kann je nach Berichterstattungsoption eingeschränkt (bspw. SOC 2) oder nicht eingeschränkt (bspw. SOC 3) sein.	Der Empfängerkreis eines SOC 2-Berichts ist eingeschränkt (Kunden und deren Stakeholder).	Der Empfängerkreis eines PS-870-Berichts kann eingeschränkt werden.
Zertifizierung mögl.	Nein	Nein	Nein	Nein	Ja
Ausprägung von Berichten/Zertifikaten	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Zeitpunkt
Prüfungsstandard weitgehend entsprechend mit	SSAE 18	SSAE 18 (AT-C 320)	ISAE 3402, ISAE 3000	ISAE 3000	n/a
Kommentar	Berichte nach ISAE 3402 Standard werden auch für Kontrollen von Dienstleistungserbringern erstellt, die keine direkte Relevanz für die Finanzberichterstattung des Dienstleistungsbezügers haben.	ISAE 3000 hat übergreifende Gültigkeit. Deswegen halten Berichte nach ISAE 3402 Standard implizit auch den ISAE 3000 Standard ein. Umgekehrt ist dies nicht der Fall.	SSAE 18 Berichte werden auch SOC Berichte genannt.	SOC 2 ist eine Berichterstattungsoption. Als zugrundeliegender Standard wird ISAE 3000 oder SSAE 18 angewendet.	Das Zertifikat bezieht sich nur auf die geprüfte Version der Software und ist auch nur für diese vollumfänglich gültig.

Quelle: EXPERTsuisse, SBVg

5 Auf die Aufführung der Berichterstattungsoption SOC 1 und 3 wird bewusst verzichtet, da im Kontext Prüfung Cloud-Dienstleistung weniger relevant bzw. zu wenig detailliert.

Abbildung 2: Übersicht bestehender Zertifizierungen und Attestierungen (Fortsetzung)

Bezeichnung	PS 920	PS 950	ISO / IEC 27001	ISO / IEC 27002	ISO / IEC 27017	ISO / IEC 27018
Titel	Schweizer Prüfungsstandard, Vereinbarte Prüfungshandlungen bezüglich Finanzinformationen	Schweizer Prüfungsstandard, Betriebswirtschaftliche Prüfungen, die weder Prüfungen noch Reviews von vergangenheitsorientierten Finanzinformationen darstellen	Information technology • Security techniques • Information security management systems • Requirements	Information technology • Security techniques • Code of practice for information security management	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
Typ	Prüfungsstandard	Prüfungsstandard	Kontrollstandard	Leitfaden	Leitfaden	Leitfaden
Primäre Verbreitung	Schweiz	Schweiz	Weltweit	Weltweit	Weltweit	Weltweit
Abdeckung Bericht	Zwischen Prüfer und Unternehmen definierte Prüfungshandlungen bezüglich Finanzinformationen	Beliebige Kriterien einer betriebswirtschaftlichen Prüfung, die weder eine Prüfung noch ein Review von vergangenheitsorientierten Finanzinformationen darstellt	Scope des definierten Informations-Sicherheits-Management-Systems in Kombination mit nicht ausgeschlossenen Kontrollen aus Anhang resp. ISO 27002; d. h. klar gekennzeichneter Teil der Organisation resp. Prozesse oder Produkte	n/a	Absicherung von Cloud-Dienstleistungen	Absicherung von Cloud-Dienstleistungen
Typische Inhalte	Aussage zu den vereinbarungsgemäss vorgenommen Prüfungshandlungen	Beliebige Kontrollen oder zu bestätigende Sachverhalte	Vorhandensein eines Informations-Sicherheits- Management-Systems (ISMS)	n/a	Implementierung von Informations-sicherheitskontrollen für Kunden von Cloud-Dienstleistungen	Datenschutzrechtliche Anforderungen zur Verarbeitung von personenbezogenen Daten in der Cloud
Empfängerkreis	Der Bericht ist nur für die Parteien bestimmt, welche die Auftragsbedingungen kennen.	Der Empfängerkreis eines PS-950-Berichts kann – je nach den zugrunde liegenden Kriterien (öffentlich bekannt oder nicht) – eingeschränkt oder nicht eingeschränkt sein.	Der Empfängerkreis eines ISO-27001-Zertifikats ist nicht eingeschränkt.	n/a	Der Empfängerkreis eines ISO-27017-Zertifikats ist nicht eingeschränkt.	Der Empfängerkreis eines ISO-27018-Zertifikats ist nicht eingeschränkt.
Zertifizierung mögl.	Nein	Nein	Ja	Nein	Ja	Ja
Ausprägung von Berichten/Zertifikaten	Zeitpunkt oder Periode	Zeitpunkt oder Periode	Periode (3 Jahre)	n/a	Zeitpunkt oder Periode	Zeitpunkt oder Periode
Prüfungsstandard weitgehend entsprechend mit	AT201 (US)	ISAE 3000		n/a	n/a	n/a
Kommentar	Der Standard kann, soweit sinnvoll, auch für nicht finanzrelevante Aufträge verwendet werden.	Umsetzung von ISAE 3000 in der Schweiz	Ein ISO-27001-Zertifikat ist gültig für einen klar beschriebenen Geltungsbereich (**Statement of Applicability SoA**). Der Geltungsbereich kann bspw. eine Abteilung oder die gesamte Unternehmung sein.	Entgegen der allgemeinen Auffassung ist eine Zertifizierung nach ISO/IEC 27002 nicht möglich.		

Quelle: EXPERTsuisse, SBVg

•SwissBanking

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

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

office@sba.ch
www.swissbanking.org