SwissBanking

Décembre 2020

Annexe I au Guide «Cloud» de l'ASB

Complément au chapitre V, Cm 63 à 69: contrôle (audit) des prestations de cloud computing et des moyens mis en œuvre

Table des matières

Liste des abréviations

AICPA	American Institute of Certified Public Accountants
AT	Attestation Standards
BSI	Bundesamt für Sicherheit und Informationstechnik (office fédéral allemand de la sécurité des technologies de l'information)
CSA STAR	Cloud Security Alliance Security Trust Assurance and Risk
Objectifs de protection «CIA»	*Confidentiality, integrity, availability* (confidentialité, intégrité, disponibilité)
CID	*Client Identifying Data* (données d'identification de clients)
COBIT	Control Objectives for Information and Related Technology Framework
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization / Organisation internationale de normalisation
IEC	International Electrotechnical Commission / Commission électrotechnique internationale
MTCS	Multi-Tiered Cloud Security
NIST	National Institute of Standards and Technology
PII	*Personally Identifiable Information* (informations personnelles identifiables)
NAS	Normes d'audit suisses
Circ.	Circulaires de l'Autorité fédérale de surveillance des marchés financiers (FINMA)
SSAE	Statement on Standards for Attestation Engagements
SOC	Service Organization Controls

1 Introduction

L'Association suisse des banquiers (ASB) a publié un Guide «Cloud» en mars 2019. Ce dernier fournit aux banques des recommandations pour une migration sûre et aisée de leurs données vers le cloud, autrement dit pour une utilisation en toute confiance des fonctions clés. Le guide aborde notamment le contrôle des prestations de cloud computing et des moyens mis en œuvre. Le présent document complète les explications du chapitre V du guide susmentionné et constitue une aide non contraignante à l'intention du lecteur. Il présente les exigences générales applicables à l'audit[1], le contenu typique d'un rapport d'audit[2] ainsi qu'un aperçu des certifications et attestations internationales courantes.

En règle générale, le respect des prescriptions légales, réglementaires et contractuelles applicables au prestataire de services de cloud computing doit faire l'objet de contrôles, en particulier pour ce qui concerne les aspects d'externalisation, de protection des données et de sécurité des informations. Ces contrôles doivent pouvoir être demandés et réalisés par l'établissement, par sa société d'audit interne et/ou externe, ou par la FINMA. Un contrôle approfondi dans le cadre d'un audit groupé (pool audit) est également possible (voir Cm 65, Guide «Cloud»). Il est permis de s'appuyer sur des rapports, des certifications et des attestations du prestataire de services de cloud computing.

Lors d'un audit, afin de pouvoir se fonder sur le rapport de la société d'audit du prestataire ou d'une société d'audit désignée par ce dernier, les critères mentionnés cidessous peuvent être utilisés à titre d'aide. Le prestataire de services de cloud computing fournit en général le ou les rapports d'audit, qui ne sont pas tous destinés à être communiqués. Les rapports d'audit antérieurs doivent être pris en compte dans la mesure où cela paraît déterminant et pertinent. Les aspects organisationnels, de même que les aspects spécifiques applicables à l'étendue et au type

1 Aux fins du présent document, le terme «audit» désigne, sauf indication contraire, l'audit au sens d'une *non-audit assurance*. Ce type de services livre des informations vérifiables sous la forme de rapports établis par des tiers dignes de confiance et fournit aux établissements une confirmation quant à l'atteinte en bonne et due forme des objectifs par les fournisseurs de prestations de cloud computing.

2 «Rapport d'audit» désigne ci-après un rapport d'audit qui traite de l'organisation et des processus en lien avec la prestation (audit SOC 2 par exemple). Il ne désigne pas ici la vérification des comptes.

de prestations de cloud computing utilisées (p. ex. SaaS, PaaS, IaaS), sont à considérer de la même manière.

Le choix des aspects à contrôler doit être propre à chaque établissement et basé sur le risque. Afin d'éviter les doublons, l'utilisation de rapports, de certifications et d'attestations du prestataire de services de cloud computing est autorisée si l'établissement juge ces documents suffisants. Si l'audit ne porte pas sur des prestations bancaires au sens strict, aucune exigence réglementaire ne lui est applicable. Il en va de même si l'audit n'est pertinent ni pour la vérification des comptes ni pour l'audit prudentiel. Toutefois, il convient de respecter dans tous les cas les obligations légales, notamment en matière de protection des données.

Il est donc conseillé d'adapter les exigences de l'audit au cas concerné et de prévoir des assouplissements le cas échéant. Les critères optionnels suivants peuvent être utilisés pour sélectionner les éléments clés de l'audit:

- Type de prestation (p. ex. application centrale, développement de logiciels, service de traduction)
- Pertinence systémique
- Pertinence de la prestation pour l'établissement
- Etendue de la prestation (p. ex. service d'hébergement ou de cloud)
- Objectifs de protection CIA
  - Protection des données concernées (p. ex. CID) (Confidentiality)
  - Protection contre des modifications non autorisées, autrement dit inaltérabilité (Integrity)
  - Protection contre les défaillances/les catastrophes (Availability). Font partie de cette catégorie de critères tous les aspects essentiels pour la prestation de service concrète, par exemple le temps de traitement garanti, la capacité de traitement des données ou la disponibilité de ces dernières
- Lieu de stockage des données et accès par l'établissement et par des tiers (notamment depuis l'étranger ou si le cryptage n'est pas sous le contrôle de l'établissement)
- Environnement de risque, c'est-à-dire le risque de tiers et de quatrième partie (sous-traitants)

- Menaces (contexte mondial)
- Eléments à considérer en lien avec une stratégie de sortie (p. ex. documentation de la procédure, accords contractuels)
- Indications concernant les contrôles que l'établissement (utilisateur du cloud) attend explicitement du prestataire de services de cloud computing (p. ex. prestations supplémentaires convenues contractuellement et qui ne font pas partie de l'offre standard du prestataire de services de cloud computing)

Les présentes explications ne portent pas sur la gestion des prestataires par chacun des établissements.

2 Exigences générales applicables à l'audit

- Le programme d'audit doit se fonder sur des normes utilisées et éprouvées au niveau international, comme les standards NIST Cloud Computing Security, Multi-Tiered Cloud Security (MTCS)/Singapore Standard (SS 584), ISO/IEC 27001 et 27017, COBIT, AICPA SOC 2, CSA STAR, ou encore le catalogue allemand BSI Anforderungskatalog Cloud Computing C5.
- La procédure d'audit et de reporting se conforme à une norme utilisée et éprouvée au niveau international (p. ex. ISAE 3000, ISAE 3402/SSAE 18, SOC 2) et à une norme au moins équivalente à l'ISAE 3402, dans la mesure où cela est pertinent pour l'audit des états financiers ou l'audit prudentiel. Si des données personnelles sont traitées dans le cadre de prestations de cloud computing, les normes susmentionnées doivent être évaluées, notamment en ce qui concerne la sécurité des données.
- La qualification et l'indépendance de l'auditeur et de la société d'audit doivent être conformes aux exigences des régulateurs compétents en vertu de la législation sur les marchés financiers. En Suisse, sont notamment applicables les dispositions de l'article 11a de l'ordonnance sur l'agrément et la surveillance des réviseurs (ordonnance sur la surveillance de la révision) et celles de la Circ.-FINMA 2013/3 «Activités d'audit».

- Selon la qualité des données (p. ex. «grandes quantités de CID») ou selon l'étendue de l'externalisation des données dans le cloud, il faut également satisfaire – en tenant particulièrement compte du secret bancaire – au catalogue des exigences figurant à l'annexe 3 de la Circ.-FINMA 2008/21 «Risques opérationnels – banques», c.-à-d. également à celles de la Circ.-FINMA 2018/3 «Outsourcing – banques et assureurs».
- Si des données personnelles sont traitées dans le cadre des prestations de cloud computing, il convient d'évaluer les normes susmentionnées en tenant particulièrement compte de la protection des données.

3 Contenus typiques d'un audit

Voici ci-après différentes catégories de thématiques figurant généralement dans un audit. Leur pertinence dépend de l'offre de services de cloud computing proposée par un prestataire à une banque. Leur contrôle se fonde sur les normes internationales énumérées au chapitre 2.

- Organisation et gouvernance
- Gestion des risques
- Cybersécurité
- Protection des données et secret bancaire
- Concept, mise en œuvre et exécution des contrôles
- Surveillance des contrôles
- Contrôles des accès logiques et physiques
- Gestion et transferts des données
- Développement, maintenance et gestion du changement
- Exploitation des systèmes et des infrastructures
- Disponibilité et récupération
- Comptabilité (gestion des licences, factures/facturation)
- Contenu des contrats standard

4 Critères d'évaluation possibles des rapports et des attestations

Le rapport de la société d'audit:

- contient des informations générales sur le périmètre et la durée de l'audit. Les éventuelles limites de responsabilité (p. ex. limitation à une juridiction spécifique, domaines non couverts) doivent être prises en compte lors de l'évaluation du rapport;
- contient au moins une confirmation de la société d'audit selon laquelle l'étendue et le périmètre de l'audit satisfont aux exigences d'au moins une juridiction à préciser[3]. En règle générale, ce sera la juridiction du siège du prestataire de services de cloud computing qui a mandaté la société d'audit;
- énumère toutes les lois et réglementations importantes pour l'audit et prises en compte pour ce dernier;
- doit décrire le système utilisé pour la prestation de cloud computing d'une manière détaillée en tenant compte du risque encouru. Cette description indique également la configuration géographique et juridique ainsi que les éléments du système des soustraitants concernés;
- indique clairement quelles sont les prestations pertinentes pour l'établissement couvertes par l'audit et quelles prestations ne sont pas abordées dans ce dernier (out of scope); idéalement, le rapport tient également compte des processus liés à la facturation aux clients;
- est de type 2 (concept et efficacité);
- renseigne sur les cyberincidents et les violations pertinents concernant la sécurité des données, autrement dit sur l'accès non autorisé aux données par des tiers (y c. des autorités) et sur les défaillances importantes du système;
- intègre les principaux sous-traitants du prestataire de services de cloud computing. Les critères déterminants pour évaluer l'importance d'un sous-traitant sont la pertinence en matière de confidentialité des données, d'intégrité des

3 Ici, l'établissement doit définir le périmètre de l'audit en se fondant sur les critères applicables (cf. le chiffre 2).

données et de disponibilité du service (objectifs de protection CIA, cf. chiffre 1). La société d'audit du prestataire ou une société d'audit désignée par ce dernier confirme le caractère continu de l'attestation ou signale les restrictions;

- a une étendue et un périmètre adéquats compte tenu des objectifs de protection CIA et des risques attendus;
- couvre une période suffisante (p. ex. douze mois pour l'audit des états financiers et l'audit prudentiel);
- indique les divergences existantes (ou identifiées) avec les exigences ainsi que les mesures prises pour y remédier (avec mention des délais). A cet égard, le rapport indique à l'intention de l'établissement les divergences passées et présentes. Ces indications ne sont pas propres à l'établissement, mais générales;
- tient compte de toute autre certification de sécurité reconnue (p. ex. ISO 27001) ou toute autre attestation de tiers jugée fiable (p. ex. SOC 2)[4]. L'établissement doit aussi exiger ces documents et en tenir compte pour l'évaluation;
- montre en détail les contrôles de sécurité réalisés ainsi que leur adéquation en ce qui concerne un éventuel accès transfrontalier à des données particulièrement sensibles. Ce qui précède vaut également pour les droits d'accès des sociétés mères ou des groupes de sociétés du prestataire à l'étranger, pour autant que le droit local leur confère de tels droits;
- ne devrait pas avoir plus d'un an afin de pouvoir servir de référence fiable;
- peut livrer une confirmation quant à l'exactitude, l'intégrité, le caractère actuel et le bon fonctionnement pour autant que le prestataire de services de cloud computing mette à disposition les données, outils ou informations utilisés pour contrôler (la sécurité de) ses prestations (p. ex. dans le cadre de la certification de niveau Full Cloud Assurance and Transparency).

4 Si un tel document est disponible en complément du rapport établi soit par la société d'audit du prestataire, soit par une société d'audit désignée par ce dernier.

Procédure en cas de lacunes dans le rapport d'audit

- Si le rapport de la société d'audit comporte des lacunes (concernant par exemple les thèmes examinés, le périmètre, les juridictions concernées ou la limitation de la responsabilité), celles-ci doivent être prises en compte et traitées au plus tard lors d'un audit ultérieur, mais idéalement déjà lors de l'établissement du contrat. Ces lacunes peuvent être comblées de trois manières:
  - rédiger le contrat de sorte à combler les lacunes du rapport;
  - intégrer les points manquants dans son propre audit;
  - présenter de manière adéquate les risques que font encourir les lacunes du rapport.

5 Aperçu des certifications et attestations internationales

Illustration 1: Aperçu des certifications et attestations existantes[5]

Désignation	ISAE 3402	ISAE 3000	SSAE 18	SOC 2	NAS 870
Titre	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 (conception du contrôle) • Type 2 (vérifie également l'efficacité des contrôles)	Norme d'audit suisse, Audit de progiciels
Type	Norme d'audit	Norme d'audit	Norme d'audit	Option de reporting	Norme d'audit
Diffusion primaire	A l'échelle mondiale	A l'échelle mondiale	Aux Etats-Unis	A l'échelle mondiale	En Suisse
Thèmes couverts	Tout critère pertinent pour le reporting financier: • Transactions • Processus pour le traitement des transactions • Reporting • Gestion des événements importants pour la marche des affaires	Tout critère pertinent d'un audit d'entreprise qui n'est pas un audit ou une revue axés sur les données financières passées d'une entité	Tout critère pertinent pour le reporting financier (idem ISAE 3402) ou des thèmes tels que: • L'infrastructure • Les logiciels • Les processus • Les personnes • Les données	Principalement des thèmes tels que: • L'infrastructure • Les logiciels • Les processus • Les personnes • Les données	Les produits logiciel
Contenus typiques	Contrôles du traitement des transactions pertinents pour le reporting financier ainsi que contrôles des processus IT sousjacents	Tout contrôle jugé pertinent ou tout élément à confirmer	Contrôles du traitement des transactions pertinents pour le reporting financier ainsi que contrôles des processus IT sous-jacents ou encore tout contrôle concernant les «principes pour un service de confiance» ou des éléments à confirmer.	Un ou plusieurs des principes pour un service de confiance définis par la norme (Trust Service Principles): • Confidentialité • Disponibilité • Sécurité • Intégrité du traitement • Protection des données	Fonctionnalités du logiciel, p. ex.: • Capacité multientité (ou multilocataire) • Capacité d'audit • Conformité
Cercle des destinataires	Le cercle des destinataires d'un rapport selon la norme ISAE 3402 est restreint (clients et leurs auditeurs).	Selon l'option de reporting concernée, le cercle des destinataires d'un rapport selon la norme ISAE 3000 peut être restreint (option SOC 2) ou non (option SOC 3).	Selon l'option de reporting concernée, le cercle des destinataires d'un rapport selon la norme SSAE 18 peut être restreint (option SOC 2) ou non (option SOC 3).	Le cercle de destinataires d'un rapport SOC 2 est restreint (clients et leurs parties prenantes).	Il est possible de restreindre le cercle des destinataires d'un rapport selon la norme PS 870.
Certification possible	Non	Non	Non	Non	Oui
Orientation des rapports / certificats	Moment ou période	Moment ou période	Moment ou période	Moment ou période	Moment
Norme d'audit correspondant en grande partie à la norme	SSAE 18	SSAE 18 (AT-C 320)	ISAE 3402, ISAE 3000	ISAE 3000	s/o
Commentaire	Les rapports selon la norme ISAE 3402 sont également établis pour contrôler des prestataires de services qui ne sont pas directement pertinents pour le reporting financier du bénéficiaire du service.	La norme ISAE 3000 a une validité globale. Par conséquent, les rapports selon la norme ISAE 3402 sont implicitement conformes à la norme ISAE 3000. L'inverse n'est pas vrai.	Les rapports selon la norme SSAE 18 sont également appelés rapports selon la norme SOC 1.	La norme SOC 2 correspond à une option de reporting. Elle est basée sur les normes ISAE 3000 ou SSAE 18.	Le certificat se réfère uniquement à la version du logiciel qui a été contrôlée. Il n'est donc pleinement valable que pour cette version.

Sources: EXPERTsuisse, ASB

5 Nous avons délibérément renoncé à mentionner les options SOC 1 et 3 pour le reporting, car elles sont moins pertinentes, c.-à-d. pas assez détail-lées, pour les audits de prestations de cloud computing.

Illustration 2: Aperçu des certifications et attestations existantes (suite)

Désignation	NAS 920	NAS 950	ISO / IEC 27001	ISO / IEC 27002	ISO / IEC 27017	ISO / IEC 27018
Titre	Norme d'audit suisse, Examen d'informations financières sur la base de procédures convenues	Norme d'audit suisse, Missions d'assurance autres que les missions d'audit ou de review (examen succinct) d'informations financières historiques	Technologies de l'information • Techniques de sécurité • Systèmes de management de la sécurité de l'information • Exigences	Technologies de l'information • Techniques de sécurité • Code de bonne pratique pour le management de la sécurité de l'information	Technologies de l'information • Techniques de sécurité • Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO / IEC 27002 pour les services du nuage	Technologies de l'information • Techniques de sécurité • Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII
Type	Norme d'audit	Norme d'audit	Norme de contrôle	Guide	Guide	Guide
Diffusion primaire	Suisse	Suisse	A l'échelle mondiale	A l'échelle mondiale	A l'échelle mondiale	A l'échelle mondiale
Thèmes couverts	Mesures d'audit telles que décidées par l'auditeur et l'entreprise. Ces mesures concernent les informations financières	Tout critère pertinent pour un audit d'entreprise qui n'est pas un audit ou une review axés sur les données financières passées d'une entité	Champ d'application (scope) du système choisi pour la gestion de la sécurité de l'information, ainsi que contrôles non exclus de son annexe (autrement dit de la norme ISO 27002); c.-à-d. éléments clairement identifiés de l'organisation (processus ou produits)	s/o	Techniques assurant la sécurité des prestations de cloud computing	Techniques assurant la sécurité des prestations de cloud computing
Contenus typiques	Déclaration concernant les mesures d'audit réalisées selon accord	Tout contrôle jugé pertinent ou tout élément à confirmer	Existence d'un système de gestion de la sécurité de l'information (SGSI)	s/o	Déploiement de contrôles relatifs à la sécurité de l'information pour les clients des prestations de cloud computing	Exigences liées à la législation sur la protection des données concernant le traitement des données personnelles enregistrées dans le cloud
Cercle des destinataires	Le rapport est destiné uniquement aux parties qui connaissent les termes du contrat.	Le cercle des destinataires d'un rapport selon la norme PS 950 peut être restreint ou non, en fonction des critères sous-jacents (rendus publics ou non).	Le cercle des destinataires d'un certificat selon la norme ISO 27001 n'est pas restreint.	s/o	Le cercle des destinataires d'un certificat selon la norme ISO 27017 n'est pas restreint.	Le cercle des destinataires d'un certificat selon la norme ISO 27018 n'est pas restreint.
Certification possible	Non	Non	Oui	Non	Oui	Oui
Orientation des rapports / certificats	Moment ou période	Moment ou période	Période (trois ans)	s/o	Moment ou période	Moment ou période
Norme d'audit correspondant en grande partie à la norme	AT201 US	ISAE 3000	s/o	s/o	s/o	s/o
Commentaire	Pour autant que cela soit judicieux, la norme est également applicable à des fins non pertinentes sur le plan financier.	Mise en œuvre de la norme ISAE 3000 en Suisse	Un certificat ISO 27001 est valable pour un champ d'application clairement décrit (déclaration d'applicabilité / DdA). Le champ d'application peut, par exemple, être un département ou l'entreprise dans son ensemble.	Contrairement à une opinion répandue, une certification selon la norme ISO / IEC 27002 n'est pas possible.		

Sources: EXPERTsuisse, ASB

•SwissBanking

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

Aeschenplatz 7
Case postale 4182
CH-4002 Bâle

office@sba.ch
www.swissbanking.org