CHRISTOPHER OEHRI

EXAMEN D'UN ENVIRONNEMENT INFORMATIQUE HÉBERGÉ SUR LE CLOUD

La numérisation croissante a conduit les entreprises à externaliser leurs applications vers le cloud ou à se procurer des services sur celui-ci. L'audit de l'externalisation vers le cloud est une tâche spécialisée qui nécessite des connaissances techniques et de l'expérience. Aussi est-il recommandé, pour une question de risques, de faire appel à un expert pour l'audit informatique.

Introduction. Pour les auditeurs, il est très important de comprendre les aspects et les défis spécifiques de l'audit d'un environnement informatique hébergé sur le cloud. Le présent article fournit un aperçu des principaux points que l'auditeur doit prendre en compte lors de l'audit d'un environnement informatique hébergé sur le cloud dans le cadre de l'audit des états financiers (pour plus d'informations, cf. PP 20 [1]). L'externalisation vers le cloud comporte des risques importants, il est donc nécessaire de procéder à des clarifications lors de la définition de la stratégie d'audit. En raison de la complexité du sujet, l'auditeur ne peut souvent pas traiter de manière appropriée les points suivants sans recourir à un expert, lorsqu'il s'agit d'auditer un établissement qui traite ou stocke des données dans un environnement cloud. Les questions complexes qui constituent la base de la compréhension de l'externalisation vers le cloud ne peuvent généralement pas être traitées par des collaborateurs du département financier de l'entreprise auditée, mais seulement par des experts au sein de cette entreprise ou par ses prestataires de services. Il convient d'en tenir compte dans la stratégie d'audit.

Définition du cloud. Dans le contexte du présent article, le terme *cloud* désigne l'externalisation de ressources et de services informatiques vers une infrastructure externe accessible via Internet. Il existe différents types d'externalisation ou de services cloud, qui sont détaillés à la fois dans la PP 20 [2] et dans les questions-réponses sur le thème du cloud computing [3]. Pour des raisons de protection des données ou de loi spéciale, il peut être important de comprendre dans quel pays les données sont stockées. Les auditeurs peuvent s'appuyer sur des rapports d'audit externes pour vérifier les externalisations vers le cloud. Ainsi, non seulement la qualité des résultats est efficacement assurée, mais l'auditeur et les entreprises auditées réalisent des économies de temps et d'argent (cf. Q&A «attestations ISAE» des prestataires de services IT [4]).

CHRISTOPHER OEHRI, CISA, MEMBRE EXPERT-SUISSE COMMISSION TECHNIQUE AUDIT INFORMATIQUE, PARTNER, HEAD OF ADVISORY IT & DIGITALISATION GRANT THORNTON

Externalisation de services vers le cloud

→ Prescriptions juridiques et réglementaires: En cas d'externalisation vers le cloud, il convient de respecter les prescriptions juridiques et réglementaires en vigueur. Celles-ci dépendent de la situation spécifique de l'environnement cloud. L'externalisation vers le cloud est soumise à des lois et prescriptions particulières qui peuvent varier d'un pays à l'autre.

→ Risques liés à l'accès au site et aux données: En cas d'externalisation vers le cloud, le contrôle de l'infrastructure et des systèmes est du ressort du fournisseur de services cloud. L'externalisation vers le cloud comporte divers risques, tels que la gestion des accès. Selon le fournisseur de services cloud, il peut être difficile de connaître le lieu de stockage des données et des activités externalisées. Il faut notamment tenir compte du site et des droits d'accès du fournisseur de services cloud, ainsi que de son organisme d'assistance. S'il existe des données sensibles, il convient d'accorder une attention particulière au contenu des contrats de prestations de services.

→ Droit de contrôle et transparence: En cas d'infrastructure informatique interne ou d'externalisation vers un fournisseur en Suisse, les auditeurs ont souvent un accès direct à l'infrastructure et peuvent effectuer des contrôles techniques approfondis. Dans le cas d'une externalisation vers le cloud, les auditeurs ne peuvent généralement s'appuyer que sur les rapports d'audit fournis par les fournisseurs de cloud. Les auditeurs doivent examiner que le fournisseur de services cloud a mis en œuvre des normes et des contrôles de sécurité appropriés pour la période d'audit donnée et que ces normes et contrôles ont été vérifiés par des auditeurs indépendants. Les environnements cloud ne peuvent généralement pas faire l'objet d'un audit autonome en raison de leur grande complexité technologique et des capacités techniques étendues requises. ■

Notes: 1) Expertsuisse, Prise de position suisse relative à la présentation des comptes 20: Principes de régularité de la comptabilité lors de l'utilisation de services pertinents pour la présentation des comptes, y compris le cloud computing, applicable depuis le 1er juillet 2019. **2)** Cf. Expertsuisse, Prise de position suisse relative à la présentation des comptes 20, p. 1. **3)** Expertsuisse, Sélection de questions et réponses sur le thème du cloud computing / centre de calcul virtualisé, 4 septembre 2019. **4)** Expertsuisse, Sélection de questions et réponses concernant les attestations ISAE 3000 et ISAE 3402 des prestataires de services IT (Provider), 22 mars 2023