AWS publie un rapport d'attestation FINMA ISAE 3000 de type 2 pour le secteur financier suisse

Gagner et conserver la confiance des clients est un engagement permanent chez Amazon Web Services (AWS). Les exigences de sécurité des secteurs d'activité de nos clients déterminent la portée et le portefeuille des rapports de conformité, des attestations et des certifications que nous recherchons. À la suite à notre annonce en novembre 2020 de la nouvelle région EU (Zurich), AWS est heureux d'annoncer l'émission du rapport d'attestation ISAE 3000 de type 2 de l'Autorité suisse de surveillance des marchés financiers (FINMA).

Le rapport FINMA ISAE 3000 de type 2, réalisé par un cabinet d'audit indépendant, fournit aux clients du secteur financier suisse l'assurance que l'environnement de contrôle AWS est conçu et mis en œuvre de manière appropriée pour faire face aux principaux risques opérationnels, ainsi qu'aux risques liés à la sous-traitance et à la gestion de la continuité des activités. En outre, le rapport fournit aux clients des conseils importants sur les contrôles complémentaires des entités utilisatrices (CUEC), que les clients devraient envisager de mettre en œuvre dans le cadre du modèle de responsabilité partagée pour les aider à se conformer aux objectifs de contrôle de la FINMA. Le rapport couvre la période allant du 4/1/2020 au 30/9/2020, avec un total de 124 services AWS et 22 Régions mondiales incluses dans le champ d'application. Une liste complète des services et des Régions certifiés est présentée dans le rapport publié par la FINMA.

Le rapport couvre les cinq circulaires principales de la FINMA qui sont applicables aux banques et aux assureurs suisses dans le cadre des accords de sous-traitance dans le cloud. Ces circulaires de la FINMA sont destinées à aider les institutions financières réglementées à comprendre les approches en matière de diligence raisonnable, de gestion des tiers et de contrôles techniques et organisationnels clés qui devraient être mis en œuvre dans les accords de sous-traitance dans le cloud, en particulier pour les charges de travail importantes. Le champ d'application du rapport couvre en détail les exigences des circulaires suivantes de la FINMA :

- 2018/03 « Sous-traitance – banques et assureurs » (31/10/2019) ;
- 2008/21 « Risques opérationnels – banques » – Principe 4 Infrastructure technologique (31/10/2019) ;
- 2008/21 « Risques opérationnels – banques » – Annexe 3 Traitement des données électroniques d'identification des clients (31/10/2019) ;
- 2013/03 « Audit » (04/11/2020) – Technologies de l'information (21/04/2020) ;
- Les normes minimales de gestion de la continuité des activités (BCM) proposées par l'Association suisse d'assurances (01/06/2015) et l'Association suisse des banquiers (29/08/2013) ;

L'alignement d'AWS sur les exigences de la FINMA démontre notre engagement continu à répondre aux attentes des prestataires de services cloud définies par les régulateurs des services financiers et les clients suisses. Les clients peuvent utiliser le rapport FINMA pour effectuer leur

diligence raisonnable, ce qui peut minimiser les efforts et les coûts requis pour la conformité. Le rapport FINMA pour AWS est désormais disponible gratuitement pour les clients AWS dans le cadre d'AWS Artifact. Vous trouverez plus d'informations sur la façon de télécharger le rapport FINMA ici.

Quelques ressources utiles liées à la FINMA :

- Centre de conformité AWS Suisse – https://aws.amazon.com/financial-services/security-compliance/compliance-center/ch/
- Autorité suisse de surveillance des marchés financiers FINMA – https://www.finma.ch/en/
- Programme de conformité AWS – FINMA ISAE3000 – https://aws.amazon.com/compliance/finma/

Comme toujours, AWS s'engage à intégrer de nouveaux services dans le cadre de son programme FINMA à l'avenir, en fonction des besoins architecturaux et réglementaires des clients. Veuillez contacter votre équipe chargée des comptes AWS si vous avez des questions sur le rapport FINMA.

Si vous avez des commentaires sur cet article, soumettez-les dans la section **Commentaires** ci-dessous.

Vous souhaitez davantage de contenu, d'actualités et d'annonces sur les fonctionnalités AWS Security ? Suivez-nous sur Twitter.