Kiteworks

NOTE DE CONFORMITÉ

Kiteworks garantit la conformité avec la Circulaire 2023/1 de la FINMA “Risques et résilience opérationnels - banques”.

La centralisation de la protection des données critiques et les contrôles intégrés simplifient la conformité avec les exigences suisses.

La FINMA est l’autorité suisse qui supervise et régule les établissements financiers en Suisse. Son nom complet en allemand est “Eidgenössische Finanzmarktaufsicht”, qui se traduit par Autorité fédérale de surveillance des marchés financiers. Les banques, les courtiers, les groupes et conglomérats financiers sont tenus de respecter la circulaire 2023/1de la FINMA “Risques opérationnels et résilience - banques” pour éviter des répercussions réglementaires, financières et d’atteinte à l’image de marque. Les problèmes de non-conformité créent des risques prudentiels susceptibles de menacer la stabilité et la pérennité d’une organisation. Les infractions peuvent entraîner des poursuites, des restrictions d’activités, des amendes, voire la perte du droit d’exploitation. Étant donné la complexité des interconnexions, tout problème interne à une institution peut rapidement perturber le marché financier. Ainsi, les autorités privilégient des mesures de protection comme les mesures de résilience et de continuité opérationnelles décrites dans la Circulaire. Bien que les petites entreprises bénéficient de certains allègements, les risques opérationnels concernent toutes les tailles d’entreprise. Toutes les banques et tous les courtiers doivent appliquer les principes fondamentaux. Quant aux institutions et aux grands groupes, ils devront être exemplaires et se soumettre à des audits réguliers. L’enjeu est de taille pour les banques avec des prêts aux particuliers et aux entreprises, car toute défaillance opérationnelle pourrait impacter immédiatement les clients et les contreparties. Mais la portée de cette Circulaire va au-delà du secteur bancaire, du trading et des compagnies d’assurance. Kiteworks accompagne les organisations à conformer à cette circulaire :

Maîtriser les risques opérationnels grâce à une sécurité multicouche

Les établissements bancaires sont tenus de classer les risques opérationnels, d’évaluer les risques inhérents et résiduels et de mettre en place des contrôles clés et des mesures d’atténuation. Outre des audits réguliers, ils ont l’obligation de surveiller les pertes et les indicateurs liés à la tolérance aux risques définie par le Conseil, et de fournir des rapports de risque à leur direction. L’appliance virtuelle durcie de Kiteworks et son modèle de sécurité multicouche minimisent les surfaces d’attaque pour éviter les perturbations opérationnelles. Son architecture zéro trust prévoit le cloisonnement des composants et le double chiffrement pour protéger les données non structurées. Des journaux d’activité

Avantages de la solution

Contrôles d’accès granulaires

Journaux d’activité détaillés

Architecture zero-trust

Restrictions géo/IP personnalisables

Intégration de tiers

permettent d'enregistrer toutes les actions administratives, les tentatives d'intrusion, les anomalies et activités des utilisateurs pour chaque fichier et composant du système. Les journaux alimentent les systèmes SIEM pour faciliter la conduite des audits de conformité, les enquêtes de sécurité et la détection des menaces. Des politiques granulaires contrôlent l'accès aux IP et aux données. L'authentification multifactorielle et le SSO permettent de contrôler les accès et sont conçus selon le principe du moindre privilège.

Ainsi, les établissements financiers suisses sont en mesure de satisfaire aux principales exigences de la FINMA en matière de résilience, de continuité, de sécurité et de conformité dans les systèmes et les opérations bancaires.*

Déployer et faire respecter les politiques de gestion des risques TIC

Les institutions doivent mettre en place un système de gouvernance IT, de conduite du changement, tenir des inventaires et définir des plans de continuité pour les actifs et les opérations TIC. Sans compter qu'elles doivent restreindre les environnements de développement/test, valider les exigences des systèmes, et prévoir un mécanisme de réponse aux incidents en cas de défaillance informatique majeure ou de cyberincident. Kiteworks enregistre toutes les activités du système et des utilisateurs pour la surveillance de la sécurité, la réponse aux incidents et les audits. L'appliance virtuelle durcie minimise les surfaces d'attaque avec des pare-feux intégrés, des pare-feux pour applications web et un système de détection d'intrusion. Les tests d'intrusion automatisés et les programmes de récompenses pour la découverte de bugs assurent que les vulnérabilités sont détectées et corrigées rapidement. Les mises à jour de cluster apportent des correctifs en un seul clic. Tous ces éléments contribuent à répondre aux attentes de la FINMA en matière de gouvernance des TIC et de résilience opérationnelle.

Obtenir un reporting rapide des risques cybernétiques

Les établissements bancaires ont besoin de pouvoir évaluer les menaces, de protéger les données et les systèmes, de détecter les incidents et de réagir conformément aux normes internationales de cybersécurité. Ils ont 72 heures pour signaler toute attaque significative à la FINMA. En outre, des tests de vulnérabilité et des exercices d'entrainement doivent être effectués régulièrement, dans le but d'analyser et de corriger les éventuelles lacunes détectées.. La structure de Kiteworks prévoit des couches de sécurité supplémentaires via des pare-feux intégrés, des pare-feux pour applications web, le blocage d'IP et un système de détection d'intrusion. Le sandboxing isole les composants logiciels tandis que le chiffrement et les contrôles d'accès limitent l'accès aux données et aux systèmes. L'intelligence cybernétique configurable s'intègre à la surveillance SIEM. Ensemble, ces éléments contribuent à satisfaire aux attentes de la FINMA en matière d'identification, de protection, de détection, de réponse et de récupération face aux risques cybernétiques.

Définir et appliquer les bonnes pratiques en matière d'hygiène informatique

L'ISO a reconnu que Kiteworks protégeait efficacement tous les contenus sensibles contre les risques informatiques (ISO 27001), y compris lorsqu'il était déployé en tant que service en cloud (ISO 27017), et qu'il protégeait votre organisation contre les fuites préjudiciables d'informations personnelles identifiables (ISO 27018). En outre, Kiteworks dispose d'une bibliothèque de certifications de conformité, y compris la conformité SOC 2 et la certification SOC 2. Ces certifications, ainsi que l'architecture à locataire unique et le renforcement multicouche, valident la capacité de Kiteworks à atténuer les risques liés au contenu avec le système de gestion du contenu et à maintenir les bonnes pratiques d'hygiène informatique conformément à NIS 2.

Protections efficaces pour la gestion des risques des données sensibles

Les établissements financiers doivent adopter une logique de classement des données sensibles selon leur degré de criticité. Restreindre l'accès par des systèmes d'autorisation et de surveillance et sélectionner des fournisseurs de services de confiance. En s'armant de protections renforcées pour assurer la disponibilité/l'intégrité/confidentialité des données partagées en externe, ils seront en mesure de signaler tout incident compromettant l'intégrité des données critiques. L'intégration Enterprise Connect de Kiteworks permet de gérer les données non structurées via une gouvernance centralisée des données. Les règles de classification déterminent le degré de sensibilité, le chiffrement sécurise les données et les

autorisations granulaires contrôlent l'accès à des référentiels intégrés tels que SharePoint et Dropbox. Des logs de suivi enregistrent les activités des utilisateurs dans cet écosystème unifié et génèrent un historique qui sert de preuve lors des audits de conformité. La plateforme Kiteworks assure la protection des données critiques et la surveillance des systèmes bancaires suisses, tout en réduisant les risques liés à la fragmentation des modèles de sécurité. La restriction des accès, la détection des anomalies et les contrôles d'accès aux systèmes tiers sont conformes aux exigences de la FINMA en matière de sécurisation des données financières sensibles et de détection des tentatives d'accès indésirables.

Gestion Centralisée des Risques Transfrontaliers

Les institutions doivent être en mesure d'évaluer avec précision les risques inhérents aux transactions internationales et de les maitriser, pour éviter toute poursuite juridique ou réglementaire avec les autorités étrangères. Elles doivent également veiller à respecter les spécificités de chaque pays et à faire preuve de diligence en engageant des entreprises qui interviennent à l'étranger. Kiteworks centralise la gouvernance des données bancaires suisses partagées à l'étranger. Avec des restrictions d'autorisations basées sur les IP, le pays et la zone géographique, les flux de données internationaux sont contrôlés en fonction du rôle utilisateur et de la sensibilité du contenu. Des mesures de sécurité légales appliquent le chiffrement sur site, dans les référentiels en cloud et en transit. Des journaux d'activité exhaustifs assurent la traçabilité des systèmes globaux intégrés en vue de justifier le respect de la conformité. Ces mesures de contrôles sont conformes aux exigences de la FINMA concernant l'évaluation des risques, l'application des clauses de confidentialité suisses à l'étranger, le respect de la conformité propre à chaque juridiction.

Kiteworks assure la sécurité, la gouvernance et la surveillance des données non structurées intégrées, conformément aux exigences de la FINMA. Son architecture (résilience, chiffrement, contrôles d'accès et suivi des activités) répond aux exigences en matière de risques opérationnels, de TIC, de cybersécurité et de sécurité des données. La plateforme fait le lien entre des environnements différents et centralise les politiques, intègre la traçabilité et apporte des correctifs rapides et clés en main. Il est possible de limiter des accès par IP, par pays et par système, ce qui permet de respecter les règles de confidentialité suisses même à l'étranger. Au global, la solution réduit les coûts de mise en conformité réglementaire en consolidant la sécurité et en remplaçant tous les outils fragmentés. Enfin, elle améliore la protection du système bancaire et la souveraineté des données des consommateurs.