Risque technologique et cyberhygiène

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland and Germany),
Solicitor (England & Wales and Hong Kong)
Of Counsel, KGP Legal LLC
alexander.ressos@kgplegal.com.sg
www.ressos.com.sg

Les contrôles LBC/FT d'un titulaire de licence DPT reposent sur la technologie, et la MAS (Monetary Authority of Singapore, l'autorité monétaire et de surveillance financière) encadre cette technologie par deux notices et un ensemble de lignes directrices qui sont en pratique indissociables du programme LBC.

La MAS Notice PSN05 on Technology Risk Management impose aux prestataires de services de paiement des exigences juridiquement contraignantes. L'établissement doit disposer d'un cadre permettant d'identifier ses systèmes critiques. Chaque système critique ne peut subir plus de quatre heures d'indisponibilité non planifiée sur toute période glissante de douze mois et doit avoir un objectif de délai de rétablissement de quatre heures. La MAS doit être informée dans l'heure suivant la découverte d'un incident pertinent, un rapport sur la cause première devant suivre dans les quatorze jours.[1] La MAS Notice PSN06 on Cyber Hygiene impose six mesures de base. Il s'agit de sécuriser les comptes d'administration, d'appliquer rapidement les correctifs de sécurité, d'établir un ensemble écrit de normes de sécurité, de mettre en place des défenses du périmètre réseau, de déployer une protection contre les logiciels malveillants et d'utiliser l'authentification multifacteur pour l'accès administratif et l'accès aux informations des clients.[2] Les Technology

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Risk Management Guidelines de janvier 2021 fixent pour tout le reste un standard non contraignant mais contrôlé lors des inspections. Elles couvrent la gouvernance, le développement logiciel, la gestion des tiers, la réponse aux incidents, le contrôle des accès, la gestion des clés cryptographiques et les tests d'intrusion.[3]

Pour un établissement DPT, la section des TRM Guidelines consacrée à la gestion des clés revêt un poids particulier, car les clés privées de l'établissement sont les actifs de ses clients. La MAS attend des cérémonies de génération de clés documentées et des modules matériels de sécurité (HSM) ou un équivalent. Elle attend une séparation des tâches telle qu'aucune personne ne puisse à elle seule déplacer les fonds des clients, une conservation à froid pour l'essentiel des actifs et des procédures de récupération testées. Ce sont aussi des exigences de conservation au titre de la partie K, chapitre II, et la MAS les inspecte comme un seul et même sujet. Un piratage est aussi un événement LBC. Les jetons volés sortent par les portefeuilles de l'établissement. Celui-ci doit pouvoir les tracer, les déclarer au titre de la PSN03 et de la section 45 du CDSA, et coopérer avec la police et avec d'autres plateformes d'échange pour les faire geler. Un plan de réponse aux incidents qui ne couvre que la reprise technique, sans la déclaration réglementaire ni le traçage on-chain, est incomplet. La partie Q, chapitre II contient une liste de contrôle pour les soixante-douze premières heures suivant un piratage.

Notes

1. MAS Notice PSN05, Technology Risk Management, émise en vertu du Payment Services Act 2019, paragraphes relatifs à l'identification des systèmes critiques, à l'indisponibilité non planifiée maximale de 4 heures, à la notification des incidents dans un délai d'une heure et au rapport sur la cause première dans les 14 jours. ↩
2. MAS Notice PSN06, Cyber Hygiene, émise en vertu du Payment Services Act 2019, paras 4–9, sur les six exigences de cyberhygiène. ↩
3. MAS, Technology Risk Management Guidelines, 18 janvier 2021, en particulier la section 10 sur la gestion des clés cryptographiques et la section 12 sur le contrôle des accès. ↩

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Disclaimer

This article is provided for general information only. It is based on publicly available sources as at its date of publication. These sources have not been independently verified against licences, regulatory registers or the records of the entities concerned. It is not legal, tax, financial or investment advice. Nor is it a recommendation to invest in, transact with or use the services of any entity mentioned. Law and regulation change frequently, so the content may be incomplete or outdated. To the fullest extent permitted by law, Dr Alexander Ressos and the publisher of SingaporeIQ exclude all liability for loss or damage arising from the use of or reliance on this article. Readers should obtain advice on their specific circumstances before acting or refraining from action.

Names and trademarks of the entities discussed belong to their owners and are used for identification only. Their mention implies no endorsement, affiliation or allegation of wrongdoing. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. Corrections and updates: contact@ressos.com.

© 2026 Dr Alexander Ressos. This article may be quoted with attribution to SingaporeIQ (SingaporeIQ.com). Reproduction in full and any commercial use require prior written consent. The Legal Terms at https://singaporeiq.com/legal-terms apply.

Author contact: Dr Alexander Ressos, TEP · contact@ressos.com