テクノロジー・リスクとサイバー衛生

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

DPTライセンス保有者のAML/CFT統制はテクノロジーの上で稼働しており、シンガポール金融管理局（MAS）はそのテクノロジーを2つの通達と1つのガイドラインによって規制しています。これらは実務上、AMLプログラムと切り離せないものです。

テクノロジー・リスク管理に関するMAS Notice PSN05は、決済サービス事業者に法的拘束力のある要件を課しています。企業は、重要システムを特定するための枠組みを備えなければなりません。各重要システムの予定外の停止時間は、直近12か月の期間内で4時間を超えてはならず、目標復旧時間は4時間としなければなりません。該当するインシデントを発見した場合は1時間以内にMASに通知し、14日以内に根本原因に関する報告書を提出しなければなりません。[1] サイバー衛生に関するMAS Notice PSN06は、6つの基本的措置を課しています。管理者アカウントの保護、セキュリティ・パッチの速やかな適用、書面によるセキュリティ基準の策定、ネットワーク境界防御の実装、マルウェア対策の導入、そして管理者アクセスおよび顧客情報へのアクセスにおける多要素認証の使用です。[2] 2021

© 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.

年1月のテクノロジー・リスク管理ガイドライン（Technology Risk Management Guidelines）は、それ以外のすべてについて、拘束力はないものの検査の対象となる基準を定めています。対象は、ガバナンス、ソフトウェア開発、第三者管理、インシデント対応、アクセス管理、暗号鍵管理、ペネトレーション・テストに及びます。[3]

DPT企業にとって、TRMガイドラインの鍵管理に関する節は特に重要です。企業の秘密鍵は顧客の資産そのものだからです。MASは、文書化された鍵生成セレモニーと、ハードウェア・セキュリティ・モジュール（HSM）またはそれと同等のものを期待しています。また、一人の人物が顧客資金を移動できないようにするための職務分掌、資産の大部分を対象とするコールドストレージの体制、検証済みの復旧手続も期待しています。これらは第K部第II章に基づくカストディ要件でもあり、MASはこれらを一つのテーマとして検査します。ハッキングはAML上の事象でもあります。窃取されたトークンは企業のウォレットを通じて流出します。企業はそれを追跡し、PSN03およびCDSA第45条に基づいて報告し、警察や他の取引所と協力して凍結しなければなりません。技術的な復旧のみを対象とし、規制当局への報告とオンチェーンの追跡を含まないインシデント対応計画は不完全です。第Q部第II章には、ハッキング後の最初の72時間のためのチェックリストを掲載しています。

注

1. MAS Notice PSN05, Technology Risk Management。Payment Services Act 2019に基づき発出。重要システムの特定、予定外停止時間の上限4時間、1時間以内のインシデント通知、14日以内の根本原因報告に関する各項。 ↩

2. MAS Notice PSN06, Cyber Hygiene。Payment Services Act 2019に基づき発出。6つのサイバー衛生要件に関する第4項〜第9項。 ↩

© 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.

3. MAS, Technology Risk Management Guidelines, 18 January 2021、特に暗号鍵管理に関する第10節およびアクセス管理に関する第12節。 ↩

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