Risco tecnológico e higiene cibernética

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

Os controles de AML/CFT de um licenciado de DPT funcionam sobre tecnologia, e a MAS regula essa tecnologia por meio de duas notices e de um conjunto de guidelines que, na prática, são inseparáveis do programa de AML.

A MAS Notice PSN05 on Technology Risk Management impõe exigências juridicamente vinculantes aos prestadores de serviços de pagamento. A empresa deve ter um modelo para identificar sistemas críticos. Cada sistema crítico não pode sofrer mais de quatro horas de indisponibilidade não programada em qualquer período móvel de doze meses e deve ter um objetivo de tempo de recuperação (recovery time objective) de quatro horas. A MAS deve ser notificada em até uma hora após a descoberta de um incidente relevante, seguindo-se um relatório de causa-raiz em até catorze dias.[1] A MAS Notice PSN06 on Cyber Hygiene impõe seis medidas básicas. São elas: proteger as contas administrativas, aplicar prontamente as atualizações de segurança, estabelecer um conjunto escrito de padrões de segurança, implementar defesas de perímetro de rede, instalar proteção contra malware e usar autenticação multifator para o acesso administrativo e o acesso a informações de clientes.[2] As Technology Risk Management Guidelines de janeiro de 2021 fixam o

© 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.

padrão não vinculante, mas objeto de inspeção, para todo o resto. Abrangem governança, desenvolvimento de software, gestão de terceiros, resposta a incidentes, controle de acesso, gestão de chaves criptográficas e testes de invasão.[3]

Para uma empresa de DPT, a seção das TRM Guidelines sobre gestão de chaves tem peso especial, porque as chaves privadas da empresa são os ativos de seus clientes. A MAS espera cerimônias documentadas de geração de chaves e módulos de segurança de hardware (HSM) ou equivalentes. Espera segregação de funções, de modo que nenhuma pessoa sozinha possa movimentar recursos de clientes, arranjos de armazenamento a frio (cold storage) para a maior parte dos ativos e procedimentos de recuperação testados. Essas são também exigências de custódia nos termos da Parte K, Capítulo II, e a MAS as inspeciona como um único tema. Um ataque hacker também é um evento de AML. Os tokens furtados saem pelas carteiras da empresa. A empresa deve ser capaz de rastreá-los, comunicá-los nos termos da PSN03 e da seção 45 do CDSA e cooperar com a polícia e com outras exchanges para bloqueá-los. Um plano de resposta a incidentes que abranja apenas a recuperação técnica, sem a comunicação regulatória e o rastreamento on-chain, é incompleto. Parte Q, Capítulo II contém um checklist para as primeiras setenta e duas horas após um ataque hacker.

Notas

1. MAS Notice PSN05, Technology Risk Management, emitida com base no Payment Services Act 2019, parágrafos sobre a identificação de sistemas críticos, o limite máximo de 4 horas de indisponibilidade não programada, a notificação de incidentes em 1 hora e o relatório de causa-raiz em 14 dias. ↩
2. MAS Notice PSN06, Cyber Hygiene, emitida com base no Payment Services Act 2019, pars. 4–9, sobre as seis exigências de higiene cibernética. ↩
3. MAS, Technology Risk Management Guidelines, 18 de janeiro de 2021, em particular a seção 10, sobre gestão de chaves criptográficas, e a seção 12, sobre controle de acesso. ↩

© 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