Technology risk and cyber hygiene

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

A DPT licensee's AML/CFT controls run on technology, and MAS regulates that technology through two notices and one set of guidelines that are in practice inseparable from the AML programme.

MAS Notice PSN05 on Technology Risk Management imposes legally binding requirements on payment service providers. The firm must have a framework for identifying critical systems. Each critical system may suffer no more than four hours of unscheduled downtime within any rolling twelve-month period and must have a recovery time objective of four hours. MAS must be notified within one hour of the discovery of a relevant incident, with a root-cause report to follow within fourteen days.[1] MAS Notice PSN06 on Cyber Hygiene imposes six baseline measures. They are securing administrative accounts, applying security patches promptly, establishing a written set of security standards, implementing network perimeter defences, deploying malware protection and using multi-factor authentication for administrative access and access to customer information.[2] The Technology Risk Management Guidelines of January 2021 set the non-binding but inspected standard

© 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.

for everything else. They cover governance, software development, third-party management, incident response, access control, cryptographic key management and penetration testing.[3]

For a DPT firm the key-management section of the TRM Guidelines has particular weight because the firm's private keys are its customers' assets. MAS expects documented key-generation ceremonies and hardware security modules or equivalent. It expects segregation of duties so that no single person can move customer funds, cold-storage arrangements for the bulk of assets and tested recovery procedures. These are custody requirements under Part K, Chapter II as well, and MAS inspects them as a single topic. A hack is an AML event too. Stolen tokens leave through the firm's wallets. The firm must be able to trace them, report them under PSN03 and s. 45 CDSA and cooperate with the police and with other exchanges to freeze them. An incident-response plan that covers only the technical recovery and not the regulatory reporting and the on-chain tracing is incomplete. Part Q, Chapter II contains a checklist for the first seventy-two hours after a hack.

Notes

1. MAS Notice PSN05, Technology Risk Management, issued under the Payment Services Act 2019, paras on critical system identification, the 4-hour maximum unscheduled downtime, the 1-hour incident notification and the 14-day root-cause report. ↩
2. MAS Notice PSN06, Cyber Hygiene, issued under the Payment Services Act 2019, paras 4–9 on the six cyber-hygiene requirements. ↩
3. MAS, Technology Risk Management Guidelines, 18 January 2021, in particular section 10 on cryptographic key management and section 12 on access control. ↩

© 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