Technology risk management

Dr Alexander Ressos, TEP
Of Counsel, KGP Legal LLC
Attorney-at-Law (Switzerland and Germany), Solicitor (England & Wales and Hong Kong)

The MAS Technology Risk Management Guidelines of January 2021 are guidelines, whereas the Notice on Technology Risk Management is binding. Both apply to DPT licensees, the Notice since the Part 2 consultation response of 23 November 2023 extended it to them with a transition period.[1] The Notice requires that critical systems have a maximum unscheduled downtime of four hours within any twelve-month period. MAS must be notified within one hour of discovering a relevant incident, with a root cause and impact analysis to follow within fourteen days.[2] The Guidelines go into detail on access control, cryptographic key management, change management, penetration testing and third-party risk, and MAS treats non-compliance with the Guidelines as a factor in licensing and enforcement even though they are not themselves binding.

For a crypto business the central technology question is the wallet architecture. MAS expects an applicant to explain the key generation ceremony, the storage of key material in hardware security modules or equivalent, and the signing workflow with its approval thresholds. It also expects an account of the separation between hot and cold environments, the recovery procedure for lost key shards and the controls that prevent a single individual from moving customer tokens. The outline of the 90 per cent cold storage rule described above has made this a regulatory requirement as well as a security practice. Applicants that rely on a third-party custody technology provider must still show that they control the keys or that the provider is itself an appropriately regulated custodian. The arrangement must also meet the MAS Guidelines on Outsourcing.

Notes

1. Morgan Lewis, "MAS introduces further investor protection measures for digital payment token service providers", November 2023, recording that MAS Notice PSN05 on technology risk management will apply to DPT service providers.
2. MAS Notice PSN05 on Technology Risk Management, paras on critical system availability (four hours in twelve months), incident notification (one hour) and root cause reporting (fourteen days); the same architecture appears in FSM-N30 for digital token service providers.

Copyright © 2026 Dr Alexander Ressos, TEP – Of Counsel, KGP Legal LLC. SingaporeIQ is an information website and gives no legal advice. For Singapore law advice through KGP Legal LLC, please write to alexander.ressos@kgplegal.com.sg