Technologierisiko und 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

Die AML/CFT-Kontrollen eines DPT-Lizenznehmers laufen auf Technologie, und die MAS reguliert diese Technologie durch zwei Notices und eine Reihe von Guidelines, die sich in der Praxis nicht vom AML-Programm trennen lassen.

MAS Notice PSN05 zum Technology Risk Management stellt rechtsverbindliche Anforderungen an Zahlungsdienstleister. Das Unternehmen braucht einen Rahmen zur Bestimmung kritischer Systeme. Jedes kritische System darf innerhalb eines rollierenden Zwölfmonatszeitraums höchstens vier Stunden ungeplant ausfallen und muss ein Wiederherstellungszeitziel von vier Stunden haben. Die MAS ist innerhalb einer Stunde nach Entdeckung eines relevanten Vorfalls zu benachrichtigen. Ein Bericht zur Ursache muss innerhalb von vierzehn Tagen folgen.[1] MAS Notice PSN06 zur Cyber-Hygiene schreibt sechs Grundmaßnahmen vor. Dazu gehören die Absicherung von Administratorkonten, das zügige Einspielen von Sicherheitspatches, ein schriftliches Regelwerk von Sicherheitsstandards, Schutzmaßnahmen am Netzwerkperimeter, Schutz vor Schadsoftware und Multi-Faktor-Authentifizierung für administrativen Zugang und für den Zugriff auf Kundeninformationen.[2] Die Technology Risk Management Guidelines vom Januar 2021 setzen für alles Übrige den unverbindlichen, aber geprüften Standard. Sie

© 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.

erfassen Governance, Softwareentwicklung, Management von Drittanbietern, Reaktion auf Vorfälle, Zugriffskontrolle, Verwaltung kryptografischer Schlüssel und Penetrationstests.[3]

Für ein DPT-Unternehmen hat der Abschnitt der TRM Guidelines zur Schlüsselverwaltung besonderes Gewicht, weil die privaten Schlüssel des Unternehmens die Vermögenswerte seiner Kunden sind. Die MAS erwartet dokumentierte Zeremonien zur Schlüsselerzeugung und Hardware-Sicherheitsmodule oder Gleichwertiges. Sie erwartet eine Funktionstrennung, sodass keine Einzelperson Kundengelder bewegen kann, Cold-Storage-Lösungen für den Großteil der Vermögenswerte und getestete Wiederherstellungsverfahren. Das sind zugleich Verwahrungsanforderungen nach Teil K, Kapitel II, und die MAS prüft sie als ein einziges Thema. Ein Hackerangriff ist auch ein AML-Ereignis. Gestohlene Token verlassen das Unternehmen über dessen Wallets. Das Unternehmen muss sie nachverfolgen, nach PSN03 und s. 45 CDSA melden und mit der Polizei und anderen Börsen zusammenarbeiten, um sie einzufrieren. Ein Notfallplan, der nur die technische Wiederherstellung abdeckt und weder die regulatorische Meldung noch die On-Chain-Nachverfolgung, ist unvollständig. Teil Q, Kapitel II enthält eine Checkliste für die ersten zweiundsiebzig Stunden nach einem Hackerangriff.

Anmerkungen

1. MAS Notice PSN05, Technology Risk Management, erlassen auf Grundlage des Payment Services Act 2019, Ziffern zur Bestimmung kritischer Systeme, zur maximalen ungeplanten Ausfallzeit von 4 Stunden, zur Meldung von Vorfällen binnen 1 Stunde und zum Ursachenbericht binnen 14 Tagen. ↩
2. MAS Notice PSN06, Cyber Hygiene, erlassen auf Grundlage des Payment Services Act 2019, Ziff. 4–9 zu den sechs Anforderungen an die Cyber-Hygiene. ↩
3. MAS, Technology Risk Management Guidelines, 18. Januar 2021, insbesondere Abschnitt 10 zur Verwaltung kryptografischer Schlüssel und Abschnitt 12 zur Zugriffskontrolle. ↩

© 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