Continuum

DIGITAL ASSET RISK AND REGULATION IN ASIA

MARKET OVERVIEW

FEBRUARY 2026

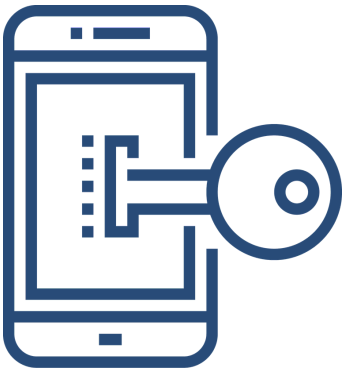
Contents

Introduction

The rapid expansion of digital asset markets has been accompanied by repeated incidents of exchange failures, custody breaches, and cyber thefts. Loss events stemming from compromised wallets, private key failures, and inadequate internal controls have resulted in significant client losses and periods of market disruption.[1] These incidents highlighted structural weaknesses in how digital assets are safeguarded and underscored that operational and governance failures often pose a greater risk to users than market volatility.[2]

In response, regulators have increasingly shifted their focus toward formalising accountability through licensing regimes, supervisory oversight, and client protection measures. While regulatory frameworks differ in structure and emphasis, there is a growing convergence around safeguards related to custody governance, asset segregation, technology risk management, and conduct standards.[3] In this review we examine these developments across Hong Kong, Singapore, Japan, South Korea, Taiwan, Thailand, and Dubai. All of which represent active and evolving regulatory environments for digital asset activities.

These regulatory approaches have material implications for market participants. As rules governing custody, conduct, and oversight become more explicit, responsibility for safeguarding client assets is increasingly placed on licensed entities, custodians, and senior management. Cyber incidents, operational outages, misappropriation, and regulatory enforcement actions therefore become foreseeable risk scenarios rather than exceptional events.[4]



Drawing on jurisdictional and topic-specific analysis, this short report considers how regulatory design choices shape operational exposure for digital asset service providers, particularly those operating across multiple markets. It also highlights the trade-offs inherent in different regulatory models and the implications for firms seeking to align with evolving supervisory expectations while maintaining resilience in a complex risk environment.[5]

We also include a breakdown of the different insurance types and how they help mitigate exposures for digital assets firms together with a short note on captive insurance and how could be utilised as a more efficient risk transfer mechanism.

Background

Why Regulation Shifted Toward Client Asset Protection

Early regulatory responses to digital assets were fragmented and cautious. In many markets, regulators focused on anti money laundering, market integrity, and retail participation limits, while largely leaving custody and asset protection to industry practice.

That posture changed following a series of high-profile failures. Exchange insolvencies revealed that client assets were often commingled or inadequately safeguarded. Custody breaches demonstrated weaknesses in operational controls. Governance failures showed that responsibility was frequently unclear or dispersed.

These events exposed a fundamental issue. Users assumed their assets were protected in a manner similar to traditional financial institutions, while legally those protections often did not exist. Regulators responded by reframing the problem. Rather than asking whether digital assets should exist, they began asking who is responsible for client assets when something goes wrong.

Across Asia, this reframing led to a common direction of travel. Regulators began to formalise accountability by defining who may hold client assets, how those assets must be held, and what standards apply when failures occur. The result is a set of regulatory regimes that differ in form but converge in intent.

Jurisdiction	Regulatory Intent	Client asset protection method	Who holds responsibility	Insurance relevance
Hong Kong	Enforce accountability	Mandatory segregation and safe custody standards	Exchanges may custody under strict SFC rules	Insurance is explicitly referenced or strongly expected
Singapore	Prevent misuse of client funds	Safeguarding and segregation under PSA	Licensed entity remains responsible for custody	Insurance is not mandated but expected in practice
Dubai	Build institutional trust	Safeguarding, governance, and resilience controls	Exchange and custody functions are encouraged to be separate	Insurance is explicitly expected by the regulator
Japan	Prevent repeat exchange failures	Strict legal separation of client and company assets	Custody is tightly regulated with low tolerance for error	Insurance is effectively required due to strict liability
South Korea	Protect retail users	Compensation mechanisms and reserve requirements	Exchanges bear primary responsibility for user losses	Insurance supports compensation and consumer claims
Taiwan	Control financial crime risk	AML registration and transaction monitoring	Custody governed through compliance discipline	Insurance is not mandated but increasingly expected
Thailand	Control market participation	Licensing plus security and custody requirements	Custody treated as a distinct and scrutinised function	Insurance depends on licensing and compliance status

The table above compares how major jurisdictions across Asia and the Middle East protect client assets — and how those regulatory choices shape risk and insurance expectations for digital asset firms operating across borders.

How Regulation Reshapes Risk and Insurance

Why Regulation Shifted Toward Client Asset Protection

From a regulatory perspective, client asset protection is achieved through control and accountability. From a risk and insurance perspective, these same controls reshape how liability and loss are defined.

Three regulatory mechanisms are particularly influential.

Custody and segregation requirements

Rules governing custody and asset segregation clarify ownership and responsibility. When client assets must be held under defined standards, asset loss becomes traceable to a specific control failure rather than an indeterminate market event.

Licensing and governance frameworks

Licensing regimes concentrate responsibility within identifiable legal entities. This allows regulators to attribute failures to firms and, where applicable, to directors and senior management. Enforcement actions, investigations, and civil claims therefore become more direct and predictable consequences of control breakdowns

Operational and conduct standards

Technology risk management, internal controls, and conduct obligations expand the scope of recognised loss scenarios. Cyber incidents, internal fraud, process failures, and third-party breaches become relevant not only operationally, but legally.

Insurance operates alongside these mechanisms. It does not replace regulatory controls. It addresses the financial impact when controls fail. As regulatory frameworks mature, insurers increasingly assess digital asset firms based on governance quality, custody architecture, and regulatory alignment, rather than technical security measures alone.[11]

Capital and compensation mechanisms

Regulatory frameworks increasingly embed financial safeguards alongside operational controls. Compensation arrangements, reserve requirements, capital thresholds, and, in some jurisdictions, insurance mandates formalise how losses must be absorbed when failures occur. These mechanisms shift risk from theoretical exposure to defined financial responsibility, requiring firms to align capital structure and insurance limits with regulatory expectations.

Jurisdictional Analysis

Hong Kong SAR, China

Regulatory approach

Hong Kong has adopted a structured and increasingly prescriptive approach to the regulation of virtual asset activities, centred on licensing, supervision, and client asset protection. Regulatory oversight is led by the Securities and Futures Commission, with policy direction set by the Financial Services and the Treasury Bureau. The current framework is designed to bring virtual asset trading platforms and related activities within a clearly defined regulatory perimeter.[12]

The licensing regime for virtual asset trading platforms was introduced under amendments to the Anti Money Laundering and Counter Terrorist Financing Ordinance. Under this framework, the operation of a virtual asset trading platform in Hong Kong requires authorisation from the SFC, subject to ongoing supervisory oversight and compliance with detailed regulatory requirements.[13]

Client asset protection and custody

Client asset protection is a core component of Hong Kong's regulatory model. The SFC's Guidelines for Virtual Asset Trading Platform Operators set out explicit requirements relating to custody, segregation, and safekeeping of client assets. Licensed platforms are required to segregate client assets from proprietary assets and implement robust custody arrangements designed to mitigate the risk of loss arising from cyber incidents, internal misconduct, or operational failure.[14]

Custody is treated as a regulated function rather than a purely operational consideration. The guidelines impose requirements on wallet management, access controls, reconciliation processes, and oversight of third-party service providers where applicable. These measures are intended to ensure that responsibility for client assets is clearly defined and enforceable.

Governance and accountability

The Hong Kong framework places significant emphasis on governance and senior management accountability. Licensed virtual asset trading platforms are required to maintain appropriate governance structures, risk management systems, and internal controls proportionate to the scale and nature of their activities. Directors and senior management are subject to fitness and propriety assessments and are expected to exercise effective oversight of custody, technology risk, and compliance functions.[15]

This approach reflects a broader regulatory objective of ensuring that responsibility for client asset protection rests with identifiable legal entities and accountable individuals.
Regulatory breaches, including custody failures or control. breakdowns, may result in enforcement action, licence conditions, or suspension.

Implications for risk and insurance

Hong Kong's regulatory framework creates clear lines of responsibility for client asset safeguarding. Custody failures, cyber incidents, and governance breakdowns are attributable to the licensed platform and its management, rather than being treated as external or market-driven events. This has implications for how operational risk, liability exposure, and financial resilience are assessed within regulated virtual asset businesses.[16]

Singapore

Regulatory approach

Singapore's regulatory framework for digital assets is grounded in payments and financial services regulation rather than a standalone digital asset regime. Oversight is led by the Monetary Authority of Singapore, with digital asset activities regulated primarily under the Payment Services Act and, where applicable, the Securities and Futures Act. The framework applies to digital payment token service providers, including exchanges, custodians, and related intermediaries.[17]

Under this approach, digital payment token service providers are required to be licensed to operate in Singapore and are subject to ongoing supervisory oversight. Regulatory focus is placed on operational resilience, consumer protection, and financial stability rather than the promotion of speculative activity. The framework has evolved through successive amendments and guidance, reflecting supervisory responses to market developments and observed risk exposures.[18]
\

Client asset protection and safeguarding

Client asset protection is addressed through mandatory safeguarding requirements. Licensed digital payment token service providers are required to implement arrangements that protect customer assets and ensure that responsibility remains with the licensed entity, even where custody or operational functions are outsourced to third parties.[19]

These safeguarding requirements are supported by detailed regulatory guidance on segregation, record-keeping, and control of customer assets. The framework is designed to prevent the commingling of customer and proprietary assets and to ensure that client assets remain identifiable and protected in the event of insolvency or operational failure.

Governance and accountability

Singapore's framework places significant emphasis on governance, risk management, and senior management accountability. License holders are required to maintain appropriate internal controls, compliance arrangements, and oversight of outsourced service providers. Directors and key officers are subject to fitness and propriety requirements and are expected to ensure compliance with regulatory obligations across custody, technology risk, and consumer protection.[20]

In addition, MAS has imposed restrictions on certain activities, including the offering of incentives to retail customers and the facilitation of lending and staking by retail users. These measures reflect a supervisory view that consumer harm in digital asset markets often arises from operational complexity and risk misalignment rather than information asymmetry alone.[21]

Implications for risk and insurance

Singapore's regulatory model concentrates responsibility for client asset protection within the licensed entity. Losses arising from custody failures, cyber incidents, internal fraud, or operational breakdowns are therefore attributable to the service provider rather than being treated as external or market-driven events. This has direct implications for how firms assess operational risk, liability exposure, and financial resilience.[22]

While insurance is not formally mandated under the regulatory framework, it is commonly expected by banking partners, institutional counterparties, and other regulated participants. Coverage relating to cyber incidents, crime, and professional liability increasingly functions as part of the baseline risk architecture for licensed digital payment token service providers operating at scale.

Japan

Regulatory approach

In addition to statutory regulation, industry self-regulatory organisations play a formal role in rule-setting and supervision. The Japan Virtual and Crypto Assets Exchange Association operates as a certified self-regulatory organisation, issuing detailed rules on custody, security management, and operational practices that apply to licensed exchanges.[24]

Client asset protection and custody

Client asset protection is a central pillar of Japan's regulatory model. Licensed crypto-asset exchange service providers are required to segregate client assets from proprietary holdings and maintain custody arrangements that meet strict regulatory and self-regulatory standards. These requirements are designed to reduce the risk of client losses arising from insolvency, misappropriation, or operational failure.[25]

Custody controls extend to wallet management, internal access restrictions, reconciliation processes, and oversight of third-party service providers. The framework reflects lessons learned from early exchange failures and security breaches, which highlighted the consequences of inadequate segregation and weak internal controls.[26]

Governance and accountability

Japan's framework places strong mphasis on governance and accountability.

Registration under the Payment Services Act subjects exchanges to ongoing supervisory oversight by the FSA, including inspections, reporting obligations, and enforcement powers. Senior management and directors are expected to ensure that custody, security, and compliance functions operate effectively and in line with regulatory expectations.[27]

Failures relating to custody, internal controls, or governance are treated as serious regulatory breaches. The supervisory approach prioritises prevention of loss events through conservative controls rather than remediation after the fact.

Implications for risk and insurance

Japan's regulatory framework concentrates responsibility for client asset protection within licensed entities and their management. Custody failures, cyber incidents, and control breakdowns are attributable to the exchange rather than external market factors. As a result, liability exposure following loss events is clear and enforcement action is typically swift.[28]

While insurance is not explicitly mandated, the regulatory environment creates strong expectations around financial resilience. Coverage relating to cyber incidents, crime, and management liability is therefore commonly treated as a necessary component of operating within Japan's tightly supervised digital asset market.

"Client asset protection is a central pillar of Japan's regulatory model"

South Korea

Regulatory approach

South Korea's regulatory framework for digital assets places strong emphasis on retail user protection and market integrity. Oversight is led by the Financial Services Commission and the Financial Supervisory Service, with enforcement support from other authorities where applicable. The framework is anchored in amendments to the Act on Reporting and Use of Certain Financial Transaction Information, which brought virtual asset service providers within a formal regulatory perimeter.[29]

Rather than adopting a custody-centric model alone. South Korea has prioritised consumer protection through licensing requirements, conduct standards, and financial safeguards. Exchanges and other virtual asset service providers are required to register, meet operational and governance standards, and maintain ongoing compliance with supervisory expectations.[30]

Client asset protection and custody

Client asset protection in South Korea is addressed through a combination of segregation, reserve requirements, and compensation-related mechanisms. Licensed exchanges are required to separate customer assets from proprietary holdings and maintain sufficient reserves to address potential losses. These measures are designed to ensure that customer claims can be met in the event of operational failure, security breaches, or misconduct.[31]

Custody standards are complemented by requirements relating to information security management systems and internal controls. Regulatory focus is placed on outcomes for retail users, particularly the ability of platforms to compensate customers when losses occur.

Directors and senior management are responsible for ensuring compliance with regulatory obligations, including customer protection measures, internal controls, and risk management systems. Governance failures, including inadequate preparation for loss events, may result in enforcement action, sanctions, or business restrictions.[32]
\

Supervisory scrutiny is closely tied to consumer outcomes. Regulatory intervention is more likely where failures result in customer harm, even where technical compliance with certain operational standards may have been met.

Implications for risk and insurance

Under the Act on the Protection of Virtual Asset Users (VAUPA), virtual asset service providers (VASPs) must safeguard user assets and are required to maintain liability insurance or set aside reserve funds to cover losses arising from hacking, network malfunction, or operational accidents.[29] [30]

Subordinate rules establish that VASPs must maintain coverage or reserves equal to at least 5 percent of customers' virtual assets held in hot wallets, subject to minimum thresholds (for example, KRW 3 billion for KRW-market exchanges and KRW 500 million for other VASPs).[29] In addition, customers' deposits and virtual assets must be segregated from proprietary assets, and at least 80 percent of customer virtual assets must be held in cold storage.[31] [32] These requirements formalise compensation responsibility at the platform level. Custody failures and cyber incidents are treated as compliance events with defined financial consequences, reinforcing the need for insurance or reserve structures aligned with statutory thresholds.

Taiwan

Regulatory approach

Taiwan's regulatory framework for digital assets is anchored in financial crime prevention and market integrity. Oversight is led by the Financial Supervisory Commission, with digital asset activities addressed primarily through anti money laundering regulation rather than a comprehensive digital asset licensing regime. Virtual asset service providers are required to comply with registration, reporting, and ongoing monitoring obligations under Taiwan's anti money laundering framework.[34]

This approach reflects a policy choice to prioritise systemic and reputational risk management over prescriptive regulation of business models. Rather than defining detailed operational requirements for custody and trading infrastructure, regulators have focused on ensuring transparency, traceability, and accountability through financial crime controls.[35]

Client asset protection and custody

Client asset protection in Taiwan is addressed indirectly through compliance and monitoring obligations rather than detailed custody prescriptions. Virtual asset service providers are required to implement customer due diligence, transaction monitoring, and suspicious activity reporting, with custody practices assessed as part of broader compliance reviews.[36]

While explicit segregation and custody standards are less detailed than in some other jurisdictions, the regulatory framework seeks to reduce the risk of misuse or misappropriation of client assets by strengthening oversight of transaction flows and counterparty behaviour.

Governance and accountability

Governance expectations in Taiwan are closely linked to compliance discipline. Registered virtual asset service providers are expected to maintain internal controls, compliance functions, and record-keeping systems sufficient to meet regulatory expectations. Directors and senior management are responsible for ensuring adherence to anti money laundering obligations and may be subject to regulatory action in cases of non-compliance.[37]

As supervisory scrutiny increases, accountability for failures relating to transaction monitoring, reporting, or internal controls has become clearer. Enforcement activity has focused on compliance breaches rather than technical design failures.

Implications for risk and insurance

Taiwan's regulatory model places less emphasis on prescriptive custody rules and greater emphasis on compliance outcomes. As a result, regulatory risk is closely tied to enforcement exposure rather than operational design alone. Loss events may arise not only from cyber incidents or internal misconduct, but from regulatory action following compliance failures.[38]

Insurance is not mandated under the current framework. However, as accountability becomes more explicit and enforcement activity increases, coverage is increasingly expected by institutional counterparties. Director and officer liability exposure is particularly relevant where regulatory breaches translate into personal responsibility for governance and compliance failures.

Thailand

Regulatory approach

Thailand's regulatory framework for digital assets is centred on licensing, market access control, and supervisory oversight. Regulation is led by the Securities and Exchange Commission of Thailand, with authority derived from the Emergency Decree on Digital Asset Businesses. This framework brings digital asset exchanges, brokers, and dealers within a formal regulatory perimeter and subjects them to approval, supervision, and enforcement.[39]

Under this approach, participation in the digital asset market is conditional on regulatory approval. Firms that do not meet licensing, operational, or conduct requirements are excluded from operating in the market. The framework reflects a policy objective of maintaining market order and investor protection through controlled participation rather than open access.[40]

Client asset protection and custody

Client asset protection in Thailand is enforced through licensing conditions, custody requirements, and security standards prescribed by the SEC. Licensed digital asset operators are required to segregate client assets from proprietary assets and implement custody arrangements designed to safeguard client holdings against loss arising from cyber incidents, internal misconduct, or operational failure.[41]

Custody is increasingly treated as a distinct and closely scrutinised function. Regulatory requirements address wallet management, internal controls, and the use of service providers, with compliance assessed as part of ongoing supervisory reviews. Failure to meet custody standards may result in licence suspension or revocation.

Governance and accountability

Thailand's framework places accountability on licensed entities and their management. Directors and senior management are responsible for ensuring compliance with regulatory obligations, including custody safeguards, information security, and operational controls. The SEC has the authority to impose sanctions, revoke licences, or restrict activities where governance or control failures are identified.[42]

This supervisory approach reinforces the link between regulatory compliance and the right to operate. Firms are expected to maintain regulatory alignment on an ongoing basis rather than relying on remediation after incidents occur.

Implications for risk and insurance

Thailand's framework places accountability on licensed entities and their management. Directors and senior management are responsible for ensuring compliance with regulatory obligations, including custody safeguards, information security, and operational controls. The SEC has the authority to impose sanctions, revoke licences, or restrict activities where governance or control failures are identified.[42]

Insurance is not formally mandated, but coverage is often conditional on regulatory compliance and licensing status. From a risk perspective, firms must consider not only whether coverage exists, but whether it will respond in the event of a loss where regulatory obligations have not been met. This creates a close relationship between regulatory alignment, operational resilience, and financial risk management.

Dubai

Regulatory approach

While not part of the Asia Pacific region, Dubai provides a useful comparator due to its explicit and structured approach to digital asset regulation. Oversight of virtual asset activities in Dubai is led by the Virtual Assets Regulatory Authority, established to regulate virtual asset activities in the Emirate outside the Dubai International Financial Centre. Within the DIFC, oversight is exercised by the Dubai Financial Services Authority. The regulatory framework is designed to support institutional participation by providing clear mandates around governance, safeguarding, and operational resilience.[44]

Dubai's approach differs from many APAC jurisdictions in that it was developed with the objective of positioning the Emirate as a regulated digital asset hub. Regulation is structured to provide clarity for market participants while setting high entry thresholds through licensing, supervision, and ongoing compliance requirements.[45]

Client asset protection and custody

Client asset protection is a central feature of Dubai's regulatory model. VARA's rulebooks set out explicit requirements relating to custody, safeguarding, and the handling of client assets. Exchange and custody functions are encouraged to be clearly delineated, either through internal segregation or the use of licensed custodians, in order to reduce conflicts of interest and operational concentration risk.[46]

Custody arrangements are subject to detailed scrutiny, including requirements around wallet controls, asset segregation, reconciliation, and oversight of third-party service providers. These measures are intended to provide institutional-grade assurances regarding the safekeeping of client assets.

Governance and accountability

Dubai's framework places strong emphasis on governance and senior management accountability. Licensed entities are required to maintain robust governance structures, risk management systems, and compliance functions. Directors and senior management are expected to demonstrate fitness and propriety and to exercise effective oversight over custody, technology risk, and operational resilience.[47]

Regulatory expectations are enforced through licensing conditions and ongoing supervision. Failure to meet governance or safeguarding requirements may result in licence restrictions, suspension, or revocation.

Implications for risk and insurance

Dubai's regulatory framework explicitly recognises insurance as a component of market stability rather than a discretionary risk transfer tool. Insurance is not treated as a substitute for controls, but as a mechanism to absorb financial losses when operational or custody failures occur.[48]

For APAC operators, Dubai illustrates the implications of a regulatory model designed with insurance expectations embedded from the outset. Explicit treatment of insurance within the regulatory framework can accelerate institutional participation, while simultaneously raising the bar for governance, operational discipline, and financial resilience.

Cross-Jurisdictional Observations

Across the jurisdictions analysed, several consistent themes emerge despite differences in regulatory design and market maturity.

First, client asset protection has become the central organising principle of digital asset regulation. Whether through segregation requirements, safeguarding rules, reserve mechanisms, or compensation obligations, regulators are focused on clarifying responsibility for client assets and defining acceptable custody arrangements.[49] [50]

Second, accountability is becoming more concentrated. Licensing regimes and governance requirements increasingly assign responsibility to identifiable legal entities and their governing bodies. This reduces ambiguity when failures occur and strengthens the link between regulatory compliance, operational design, and legal exposure.[51]

Third, financial resilience has become a practical consideration even where insurance is not explicitly mandated. As regulatory expectations mature and enforcement activity increases, loss scenarios related to custody failures, cyber incidents, internal misconduct, and governance breakdowns are no longer treated as exceptional events. In several jurisdictions, financial protection mechanisms, including insurance, are increasingly referenced as part of sound risk management expectations.[52] [53]

These patterns reflect a broader regulatory shift away from abstract market oversight toward defined responsibility for asset protection and operational outcomes.

Implications for Digital Asset Firms

For digital asset firms operating across Asia Pacific, regulation now directly shapes operational architecture, counterparty expectations, and exposure to loss.

Understanding regulatory requirements at a jurisdictional level is necessary but insufficient. Firms must also understand how those requirements allocate responsibility, how liability arises when failures occur, and how financial protection responds in practice. Regulatory reviews and enforcement actions across multiple jurisdictions demonstrate that misalignment between regulatory obligations, operational design, and risk management can materially increase exposure when incidents occur.[54]

As regulatory regimes mature, firms that integrate compliance, governance, and financial resilience into their operating model are better positioned to engage with institutional counterparties and operate sustainably in regulated markets.

Insurance in Regulated Digital Asset Markets

Regulation defines accountability. Insurance addresses financial consequence.

Across Asia, digital asset regulation now assigns clear responsibility for client asset safeguarding, operational integrity, and governance. When those obligations fail, financial exposure follows. Insurance does not replace regulatory controls. It responds when loss occurs within defined terms.

The relevance and structure of insurance depend on the regulatory environment. In jurisdictions such as Hong Kong, Dubai, and South Korea, compensation arrangements or insurance are embedded within the licensing framework. In others, including Singapore, Japan, Thailand, and Taiwan, insurance is not mandated but is frequently required by institutional counterparties, banking partners, and investors.

The following categories of insurance are typically relevant for regulated digital asset firms.

Digital Asset Insurance and Custody Protection

Digital asset insurance is designed to address the loss of client digital assets arising from:

- External hacking and network intrusion
- Insider theft or employee dishonesty
- Key compromise or wallet security failure
- Operational errors affecting asset transfers

In regulated environments, custody structures are prescribed. Segregation rules, cold storage thresholds, and compensation requirements create defined exposure points. Insurance may be used to support regulatory compensation arrangements or reserve requirements where permitted.

Coverage scope varies materially. Policies may distinguish between hot and cold storage, impose sublimits, or require adherence to specific security controls. The structure of custody architecture directly affects insurability.

Cyber Insurance

Cyber insurance addresses liability and response costs arising from:

- Data breaches
- Ransomware and network compromise
- Regulatory investigations following cyber incidents
- Incident response, forensic, and legal costs

For digital asset firms, cyber risk intersects with custody but remains distinct. A cyber event may trigger regulatory scrutiny even if no digital assets are lost. Cyber policies typically cover liability, investigation costs, and business interruption, but may not automatically cover direct asset loss unless specifically structured to do so.

Directors and Officers Liability Insurance

As regulatory regimes formalise accountability, exposure extends to directors and senior management.

D&O insurance responds to:

- Regulatory investigations and enforcement actions
- Allegations of governance failure
- Claims arising from inadequate supervision or internal control
- Shareholder or investor actions following material loss events

In regulated digital asset markets, enforcement focus increasingly examines governance oversight. D&O coverage addresses defence costs and potential settlement exposure.

Technology Professional Indemnity

Where firms provide custody, brokerage, execution, or technology services, professional indemnity coverage may respond to:

- Alleged negligence
- Service errors
- Failure to execute instructions
- Technology system failures affecting clients

This is particularly relevant for custodians, infrastructure providers, and platforms offering technology-enabled services.

Crime Insurance

Commercial crime insurance addresses:

- Internal fraud
- Employee dishonesty
- Third-party theft
- Social engineering losses

In digital asset environments, crime coverage may form part of the broader custody protection strategy, particularly where internal access controls and key management present exposure.

Commercial General Liability

While not digital-asset-specific, CGL coverage addresses bodily injury and property damage claims that may arise from physical operations, office premises, or events. It remains part of a baseline risk architecture for regulated entities.

Specie Insurance

Specie insurance is relevant where firms hold physical assets linked to digital structures, such as tokenised commodities or bullion. It provides protection for physical asset storage and transit risk.

Structuring Insurance in Regulated Markets

Insurance must align with regulatory design.

Where regulators mandate compensation arrangements, coverage limits and structure must correspond to required thresholds. Where segregation and cold storage rules apply, policies must reflect actual custody architecture. Where governance accountability is formalised, D&O limits must reflect enforcement exposure.

Insurance operates as a financial backstop within regulatory frameworks. Its effectiveness depends on policy structure, limit adequacy, and alignment with licensing conditions.

In regulated digital asset markets, risk transfer is no longer discretionary positioning. It forms part of the broader financial resilience of licensed operators.

The Role of Captive Insurance

A captive insurance company is a wholly-owned subsidiary established to insure the risks of its parent and affiliated companies. Rather than just buying coverage on the commercial market, the parent organization retains a selection of those risks, ideally the profitable ones, and partially funds potential losses through the captive. This concept is not new but may have an increasingly important role of the digital asset sector as regulators mandate cover that the commercial insurance market is either not set up to absorb or is simply too expensive.

Summary

Across the jurisdictions analysed, several consistent themes emerge despite differences in regulatory design and market maturity.

Digital asset regulation across Asia has entered a more settled phase. The period of regulatory ambiguity, where asset protection relied largely on industry practice and user assumption, is giving way to frameworks that explicitly assign responsibility for client assets, operational integrity, and governance outcomes.[55]

Across jurisdictions, regulators are no longer debating whether digital asset activity should exist. The focus has shifted to defining who bears responsibility when failures occur and how those failures are addressed. Licensing regimes, custody requirements, governance standards, and supervisory enforcement are increasingly structured to ensure that accountability can be traced to identifiable entities and decision makers.[56]

This shift has practical consequences. Operational failures, custody breaches, and governance breakdowns are no longer treated as market risks absorbed by volatility. They are treated as compliance and control failures with legal, financial, and personal implications.[57] As a result, regulatory alignment, operational design, and financial resilience are becoming inseparable considerations for firms operating in regulated digital asset markets.

For regulators, this convergence reflects a move toward durable frameworks that prioritise asset protection without relying on speculative enforcement after loss events. For firms, it establishes a higher threshold for credibility. Operating in regulated markets now requires not only compliance with formal rules, but a clear understanding of how responsibility is allocated and how loss is absorbed when safeguards do not perform as intended.[58]

As regulatory frameworks continue to mature, firms and jurisdictions that recognise this alignment between regulation, accountability, and financial resilience will be better positioned to support institutional participation and maintain confidence in digital asset markets.

References

1. Reuters, “Crypto’s biggest hacks and heists after $1.5 billion theft from Bybit.” https://www.reuters.com/technology/cybersecurity/cryptos-biggest-hacks-heists-after-15-billion-theft-bybit-2025-02-24/

2. Reuters, “Japan raps Coincheck, orders broader checks after $530 million cryptocurrency theft.” https://www.reuters.com/article/world/japan-raps-coincheck-orders-broader-checks-after-530-mln-cryptocurrency-theft-idUSKBN1FI073/

3. Monetary Authority of Singapore, “Guidelines on Consumer Protection Measures by Digital Payment Token Service Providers (PS-G03).” https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/pso/ps-g03-guidelines-on-consumer-protection-measures-by-digital-payment-token-service-providers/ps-g03_guidelines-on-consumer-protection-safeguards-by-dpt-service-providers_vf.pdf

4. Financial Stability Board, “Assessment of Risks to Financial Stability from Crypto-assets.” https://www.fsb.org/uploads/P160222.pdf

5. Hong Kong Securities and Futures Commission, “Guidelines for Virtual Asset Trading Platform Operators.” https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/Guidelines-for-Virtual-Asset-Trading-Platform-Operators/Guidelines-for-Virtual-Asset-Trading-Platform-Operators.pdf

6. Bank for International Settlements, “Regulating crypto: policy considerations,” BIS Quarterly Review. https://www.bis.org/publ/qtrpdf/r_qt2112b.htm

7. Reuters, “Crypto’s biggest hacks and heists after $1.5 billion theft from Bybit.” https://www.reuters.com/technology/cybersecurity/cryptos-biggest-hacks-heists-after-15-billion-theft-bybit-2025-02-24/

8. Reuters, “Japan raps Coincheck, orders broader checks after $530 million cryptocurrency theft.” https://www.reuters.com/article/world/japan-raps-coincheck-orders-broader-checks-after-530-mln-cryptocurrency-theft-idUSKBN1FI073/

9. Financial Stability Board, “Assessment of Risks to Financial Stability from Crypto-assets.” https://www.fsb.org/uploads/P160222.pdf

10. Monetary Authority of Singapore, “Guidelines on Consumer Protection Measures by Digital Payment Token Service Providers (PS-G03).” https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/pso/ps-g03-guidelines-on-consumer-protection-measures-by-digital-payment-token-service-providers/ps-g03_guidelines-on-consumer-protection-safeguards-by-dpt-service-providers_vf.pdf

11. Hong Kong Securities and Futures Commission, “Guidelines for Virtual Asset Trading Platform Operators.”
Reuters, “Crypto’s biggest hacks and heists after $1.5 billion theft from Bybit.” https://www.reuters.com/technology/cybersecurity/cryptos-biggest-hacks-heists-after-15-billion-theft-bybit-2025-02-24/

12. Financial Services and the Treasury Bureau, “Policy Statement on Development of Virtual Assets in Hong Kong.” https://www.fstb.gov.hk/fsb/en/publication/policy_statement/virtual_assets_policy_statement_en.pdf

13. Hong Kong Government, Anti Money Laundering and Counter Terrorist Financing (Amendment) Ordinance 2022. https://www.elegislation.gov.hk/hk/cap615

14. Securities and Futures Commission, “Guidelines for Virtual Asset Trading Platform Operators.” https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/Guidelines-for-Virtual-Asset-Trading-Platform-Operators/Guidelines-for-Virtual-Asset-Trading-Platform-Operators.pdf

15. Securities and Futures Commission, “Fit and Proper Guidelines.” https://www.sfc.hk/en/Rules-and-standards/Rules-and-standards/Fit-and-proper

16. Securities and Futures Commission, “Licensing Handbook for Virtual Asset Trading Platform Operators.” https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/licensing/licensing-handbook/VA_Trading_Platform_Operators.pdf

17. Monetary Authority of Singapore, Payment Services Act 2019. https://sso.agc.gov.sg/Act/PSA2019

18. Monetary Authority of Singapore, “Regulation of Digital Payment Token Services.” https://www.mas.gov.sg/regulation/payments/digital-payment-token-services

19. Monetary Authority of Singapore, “Guidelines on Consumer Protection Measures by Digital Payment Token Service Providers (PS-G03).” https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/pso/ps-g03-guidelines-on-consumer-protection-measures-by-digital-payment-token-service-providers/ps-g03_guidelines-on-consumer-protection-safeguards-by-dpt-service-providers_vf.pdf

20. Monetary Authority of Singapore, “Guidelines on Fit and Proper Criteria.” https://www.mas.gov.sg/regulation/guidelines/fit-and-proper-criteria

21. Monetary Authority of Singapore, “Prohibition on Provision of DPT Services to Retail Customers.” https://www.mas.gov.sg/news/media-releases/2022/mas-issues-consultation-paper-on-regulatory-measures-for-digital-payment-token-services

22. Monetary Authority of Singapore, “Technology Risk Management Guidelines.” https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines

23. Financial Services Agency of Japan, Payment Services Act (as amended). https://www.japaneselawtranslation.go.jp/en/laws/view/3625

24. Japan Virtual and Crypto Assets Exchange Association, Self-Regulatory Rules and Guidelines. https://jvcea.or.jp/en/

25. Financial Services Agency of Japan, Cabinet Office Order on Crypto-Asset Exchange Service Providers. https://www.japaneselawtranslation.go.jp/ja/laws/download/3353/09/h29Aa000070104en12.0.pdf

26. Reuters, "Japan raps Coincheck, orders broader checks after $530 million cryptocurrency theft." https://www.reuters.com/article/world/japan-raps-coincheck-orders-broader-checks-after-530-mln-cryptocurrency-theft-idUSKBN1FI073/

27. Financial Services Agency of Japan, "Supervisory Guidelines for Crypto-Asset Exchange Service Providers." https://www.fsa.go.jp/en/policy/virtual_currency.html

28. Bank for International Settlements, "Regulating crypto: policy considerations." https://www.bis.org/publ/qtrpdf/r_qt2112b.htm

29. Financial Services Commission, Republic of Korea, Act on Reporting and Use of Certain Financial Transaction Information (as amended). https://elaw.klri.re.kr/eng_service/lawView.do?hseq=55958

30. Financial Supervisory Service, "Guidelines on Virtual Asset Service Providers." https://www.fss.or.kr/fss/eng/main.jsp

31. Reuters, "South Korea to require crypto exchanges to hold reserves to compensate users." https://www.reuters.com/technology/south-korea-require-crypto-exchanges-hold-reserves-compensate-users-2023-02-07/

32. Financial Services Commission, "Measures to Strengthen Consumer Protection in Virtual Asset Markets." https://www.fsc.go.kr/eng/pr010101/79547

33. Bank for International Settlements, "Policy responses to crypto-asset risks." https://www.bis.org/publ/bppdf/bispap122.pdf

34. Financial Supervisory Commission, Taiwan, "Regulations Governing Anti Money Laundering of Virtual Currency Platforms and Trading Businesses." https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380266

35. Financial Supervisory Commission, Taiwan, "Statement on the Regulation of Virtual Asset Service Providers." https://www.fsc.gov.tw/en/home.jsp?id=96

36. Financial Supervisory Commission, Taiwan, "Guidance on AML and CFT Obligations for Virtual Currency Platforms." https://www.banking.gov.tw/en/home.jsp?id=582

37. Reuters, “Taiwan tightens oversight of crypto firms to curb money laundering risks.” https://www.reuters.com/world/asia-pacific/taiwan-tightens-oversight-crypto-firms-curb-money-laundering-risks-2021-07-01/

38. Bank for International Settlements, “Global regulatory responses to cryptoasset risks.” https://www.bis.org/publ/bppdf/bispap122.pdf

39. Securities and Exchange Commission Thailand, Emergency Decree on Digital Asset Businesses B.E. 2561 (2018). https://www.sec.or.th/EN/Pages/LawandRegulations/DigitalAsset.aspx

40. Securities and Exchange Commission Thailand, “Licensing of Digital Asset Businesses.” https://www.sec.or.th/EN/Pages/Business/DigitalAssetBusiness.aspx

41. Securities and Exchange Commission Thailand, “Rules on Safekeeping of Customer Assets for Digital Asset Businesses.” https://www.sec.or.th/EN/Pages/Regulations/DigitalAsset/DigitalAssetCustodian.aspx

42. Securities and Exchange Commission Thailand, “Supervisory and Enforcement Powers.” https://www.sec.or.th/EN/Pages/AboutSEC/Enforcement.aspx

43. Reuters, “Thailand tightens oversight of crypto exchanges amid investor protection push.” https://www.reuters.com/world/asia-pacific/thailand-tightens-oversight-crypto-exchanges-2022-11-22/

44. Dubai Government, Law No. 4 of 2022 Establishing the Virtual Assets Regulatory Authority. https://dlp.dubai.gov.ae/Legislation%20Reference/2022/Law%20No.%204%20of%202022.pdf

45. Virtual Assets Regulatory Authority, “Virtual Assets and Related Activities Regulations.” https://www.vara.ae/en/regulations

46. Virtual Assets Regulatory Authority, “Custody Services Rulebook.” https://www.vara.ae/en/rulebooks

47. Dubai Financial Services Authority, “Regulatory Framework for Crypto Tokens.” https://www.dfsa.ae/publications/consultation-papers/dfsa-regulatory-framework-crypto-tokens

48. Reuters, “Dubai’s VARA sets strict rules for crypto firms as it builds global hub.” https://www.reuters.com/world/middle-east/dubais-vara-sets-strict-rules-crypto-firms-builds-global-hub-2023-02-09/

49. International Organization of Securities Commissions, Policy Recommendations for Crypto and Digital Asset Markets, 2023. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf

50. Financial Stability Board, Global Regulatory Framework for Crypto-asset Activities, 2023. https://www.fsb.org/2023/07/global-regulatory-framework-for-crypto-asset-activities/

51. Bank for International Settlements, Cryptoassets and Decentralised Finance: Functions and Financial Stability Implications, BIS Quarterly Review. https://www.bis.org/publ/qtrpdf/r_qt2112b.htm

52. Financial Action Task Force, Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs, 2021. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html

53. International Association of Insurance Supervisors, Issues Paper on the Prudential Treatment of Crypto-assets, 2023. https://www.iaisweb.org/uploads/2023/06/Issues-Paper-on-the-Prudential-Treatment-of-Crypto-assets.pdf

54. International Organization of Securities Commissions, Policy Recommendations for Crypto and Digital Asset Markets, 2023. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf

55. Financial Stability Board, Global Regulatory Framework for Crypto-asset Activities, 2023. https://www.fsb.org/2023/07/global-regulatory-framework-for-crypto-asset-activities

56. International Organization of Securities Commissions, Policy Recommendations for Crypto and Digital Asset Markets, 2023. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf

57. Bank for International Settlements, Supervisory Challenges Associated with Cryptoasset Activities, BIS Papers No. 122. https://www.bis.org/publ/bppdf/bispap122.pdf

58. International Association of Insurance Supervisors, Issues Paper on the Prudential Treatment of Crypto-assets, 2023. https://www.iaisweb.org/uploads/2023/06/Issues-Paper-on-the-Prudential-Treatment-of-Crypto-assets.pdf

Continuum

Risk. Insurance. Technology.

hello@continuuminsure.com

www.continuuminsure.com