CoinCover

COINCOVER.COM

CoinCover digital asset recovery regulatory review

FEBRUARY 2026

INDEPENDENT REGULATORY RESEARCH UNDERTAKEN BY LHI CONSULTING, ON BEHALF OF COINCOVER.

OVERVIEW

Across jurisdictions, regulators consistently expect firms to demonstrate:

i. Robust private key security and access controls;
ii. Segregation and redundancy to avoid single points of failure;
iii. Tested recovery and continuity capabilities; and
iv. Audit-ready recordkeeping and evidence production.

The Digital Asset Recovery Regulatory Review shows how CoinCover's wallet disaster recovery solutions can help support compliance with regulatory expectations in key jurisdictions:

- CoinCover Recover: a non-custodial recovery solution designed to support retail end-users in regaining access to self-custodied wallets in the event of lost keys/seed phrases.
- CoinCover Recover for Institutions: a recovery solution designed to support institutions by strengthening wallet access recoverability with independently verifiable recovery infrastructure.

For each jurisdiction, we look at the main regulatory themes (security, operational resilience, governance, and evidence), and the specific regulations that CoinCover's products may assist firms in aligning with.

Please note that CoinCover does not provide legal or regulatory compliance services. Responsibility for regulatory compliance remains with the regulated entity. CoinCover products support firms in implementing technical and operational controls that may assist in meeting regulatory expectations.

JURISDICTIONS COVERED

AUSTRALIA

Australian Securities & Investments Commission (ASIC)

Regulatory focus

ASIC's guidance and regulatory expectations emphasise custody characterisation, technology-neutral custody obligations, and effective controls over private-key security, segregation, recordkeeping, and operational resilience.

ASIC's principles-based approach focuses on whether a service involves key control and on whether the firm can evidence adequate safeguards to protect client interests in the event of disruption, compromise, or failure.

Private key material and hot storage limitations (ASIC PART E)

ASIC states:

"Private key material should not be held on internet-connected systems or networked hardware (hot storage) beyond what is strictly necessary for the operation of the product."

CoinCover Recover helps firms support alignment with ASIC's expectations for strong security controls by enabling customers to back up and retain their own key phrases using wallet-provider-branded recovery flows, while applying configurable security requirements and onboarding controls to manage the risk of unauthorised access.

CoinCover Recover supports a risk-based compliance posture by allowing wallet providers to select security levels aligned to their operating model and customer risk profile, and to integrate verification through existing customer credentials, CoinCover's ID-less approach, or an ID verification flow controlled by the provider.

CoinCover Recover for Institutions helps firms support alignment with ASIC's expectation that private key material should not be held on internet-connected systems or networked hardware (hot storage) beyond what is strictly necessary for the operation of the product.

Principles-based custody obligations (ASIC PART E)

ASIC states:

"The obligations on custodial or depository service providers are principles-based and apply to custody of any financial product, regardless of its form."

CoinCover Recover for Institutions helps firms support alignment with this expectation through encryption standards and multi-party authentication, designed to reduce single points of failure and support secure, controlled access to client assets.

Custody characterisation and private key control (ASIC INFO 225)

ASIC states:

"Where an entity holds financial products or a beneficial interest in the financial product on trust for, or on behalf of, their clients" and that "Where a person controls the private keys related to an address on a public blockchain, they will likely be providing a custodial or depository service."

CoinCover Recover helps support self-custody models in which the customer retains control of their own wallet and private keys. CoinCover does not hold client assets or act as a custodian. Instead, CoinCover Recover provides a security and recovery layer that supports wallet providers and their customers by enabling user-managed key phrase backup and recovery flows, configurable onboarding, and risk-based verification controls.

This helps firms reduce their customers' risk of loss of access, and strengthen access governance - while maintaining a structure that is consistent with ASIC's framing of custody risk indicators (i.e., key control as the relevant custody trigger), and without CoinCover assuming control of private keys or holding assets on behalf of clients.

CoinCover Recover for Institutions helps support institutional custody and custody-adjacent operating models by strengthening key access governance and recoverability. CoinCover provides independently auditable recovery infrastructure and continuity controls (without holding client assets) that help institutions evidence robust operational resilience and security measures consistent with ASIC's custody risk indicators, including mitigation of key loss, compromise, and operational disruption risks.

Funds management and custodial services (ASIC Regulatory Guide 133, RG 133.141)

ASIC states that:

"Effective systems and processes for key backup and recovery should be maintained, with geographically distributed backup sites preferred.... (iii) Signing approaches that minimise 'single point of failure risk' should be adopted (d)"

RG 133.143 in the same document states:

"Asset holders should adopt a transaction-signing approach that minimises single point of failure risk. For example, a multi-signature or sharding-based signing approach is preferred to a single private key to sign transactions."

CoinCover Recover helps firms support alignment with ASIC's expectations regarding the maintenance of effective systems and processes for private key backup and recovery. CoinCover Recover provides resilient key backup and recovery processes that eliminate reliance on a single private key, individual or storage location. Backup and recovery components are structured to avoid a single point of failure. This approach helps support firms' alignment with ASIC's guidance that signing arrangements should minimise single-point-of-failure risk, and RG 133.143's preference for multi-component or sharding-based signing approaches over single private key models.

CoinCover Recover for Institutions helps support distributed recovery and transaction-signing processes, governed by formal access controls and approval workflows.

Private key recovery material is fragmented and protected across geographically distributed infrastructure, with recovery requiring multiple independent authorisations in accordance with defined governance policies. No individual, system, or location is capable of independently reconstructing signing authority. This design helps firms support alignment with ASIC's expectation that asset holders adopt transaction-signing approaches that minimise single-point-of-failure risk, including the use of multi-signature or sharding-based mechanisms.

CANADA

CSA and FINTRAC

Regulatory focus Canadian requirements centre on investor protection and market integrity for crypto-asset trading platforms, including the adequacy of custody-related controls (especially where platforms control private keys), system resiliency, security governance, and expectations for independent assurance over control design and operating effectiveness.

CSA (Crypto Asset Trading Platforms)

CSA Staff Notice 21-332 outlines enhanced investor protection provisions required in the Pre-Registration Undertaking (PRU) for unregistered CTPs.

Investor protection provisions (CSA 21-329, Appendix A – Key Risks)

CSA requires sufficient risk of mitigation regarding the custody of securities tokens or crypto assets underlying crypto contracts.

The CSA states that crypto asset trading platforms must:

> "Obtain an independent report from a reputable accounting firm providing assurance on the suitability of the design of, and operating effectiveness of, the custodian's controls around the systems and processes in place to safeguard the Crypto Assets. These controls should address risks such as theft, loss, or misuse of Crypto Assets and the adequacy of insurance coverage maintained by the custodian."

CoinCover Recover for Institutions can help support firms in demonstrating these controls through secure key management, continuous asset availability, and auditable access procedures that mitigate key custody risks.

System resiliency, reliability and security controls (CSA/IIROC Staff Notice 21-329)

> “System resiliency, reliability and security controls are important for investor protection and market integrity, especially when CTP maintains custody of participants’ assets, including through holding the private keys.... marketplaces are required by Part 12 of NI 21-101 to have adequate internal and information technology controls over their trading, surveillance and clearing systems and information security controls over these systems.”

CoinCover Recover’s configurable security requirements, onboarding and verification options, and documented recovery flows reduce the operational and customer-impact risks associated with permanent access loss. This can contribute to overall system reliability and client protection outcomes within a platform’s broader operational resilience framework and help support firms’ alignment with the principles reflected in Appendix A(c).

CoinCover Recover for Institutions helps firms support alignment with the CSA/IIROC expectation for resiliency and security controls by strengthening institutional governance and continuity over digital asset access and private-key recovery. Where a CTP or custody provider holds or controls private keys, the solution provides independently verifiable recovery processes and operational resilience measures designed to mitigate loss-of-access and disruption events that could impair platform operations or customer asset accessibility. This helps support firms’ alignment with the establishment of robust ICT controls and continuity capability that underpin investor protection and market integrity outcomes contemplated by Appendix A(c).

FINTRAC Registration

FINTRAC Registration: Crypto platforms must register as Money Services Businesses (MSBs) under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA).

Money laundering and terrorist financing (Section 7 & 7.1)

Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), FINTRAC requires that:

"STRs must be filed for any transaction (attempted or completed) with reasonable grounds to suspect links to money laundering or terrorist financing."

CoinCover Recover for retail customer wallets helps firms support alignment with this requirement by maintaining detailed logs for STR preparation including: customer identity verification results, wallet addresses and blockchain transaction IDs, verification of ownership or loss claims. These records help compliance teams in identifying irregular or high-risk recovery attempts (e.g., repeat claims, compromised wallets, or recoveries linked to sanctioned entities).

CoinCover Recover for Institutions helps firms support alignment with AML/CTF governance by enabling auditable access controls and verifiable recovery workflows in institutional contexts where wallet access events may be operationally and reputationally material. The solution generates structured logs and evidence relating to access governance and recovery execution (e.g., initiation, authentication, approvals, and completion), which can help support compliance and investigations teams in documenting activity, validating authorisation, and responding to supervisory or internal AML/CTF inquiries. Where recovery or access events intersect with a firm's transaction monitoring and suspicious activity workflows, these records can help in evidencing decision-making, and help supporting STR preparation and escalation processes under the PCMLTFA framework.

EUROPEAN UNION

The Market in Crypto Assets (MiCA) & the Digital Operational Resilience Act (DORA)

Regulatory focus

MiCA imposes obligations on CASPs relating to ICT security, safekeeping of clients' crypto-assets, and protection of clients' private keys, supported by resilient systems and defined access protocols.

DORA focuses on digital operational resilience, requiring comprehensive ICT risk management, business continuity and recovery planning, incident classification and reporting, resilience testing programmes, and governance of ICT third-party risk (including contractual controls and exit planning).

Markets in Crypto Assets (MiCA)

ICT security requirements (Article 62)

"Crypto-asset service providers shall have in place and maintain resilient ICT systems, protocols and tools that are appropriate and proportionate to the nature, scale and complexity of their business, and that ensure a high level of security, integrity and confidentiality of data and information."

CoinCover Recover for Institutions helps firms support alignment with ICT-security obligations through a resilient recovery infrastructure designed to maintain data integrity, availability, and confidentiality. Backup and recovery events are cryptographically verified, access-controlled, and logged, helping ensure that recovery operations can occur only under validated and authorised conditions.

Safekeeping of client's cryptoassets (Article 70)

> “Such providers shall have in-place systems and security access protocols to ensure the safekeeping of crypto-assets and the protection of clients’ private keys.”

CoinCover Recover’s recovery and access-governance controls help support firms’ obligations without taking custody of private keys. Its architecture is designed to support segregation and prevent unauthorised reconstruction, helping firms align with MiCA’s mandate to “safeguard the ownership rights of clients” and prevent unauthorised use.

Digital Operational Resilience Act (DORA)

ICT risk management and business continuity (Chapter II), Article 6(1) and Article 11(1)

> Article 6(1): “Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework … to ensure a high level of digital operational resilience.”

And

> Article 11(1): Financial entities must put in place a “comprehensive ICT business continuity policy” and ICT response and recovery plans as part of that framework.

CoinCover Recover helps firm support DORA-aligned ICT continuity objectives in retail-facing self-custody contexts by enabling structured, controlled recovery workflows that reduce the risk and impact of customer access-loss events, which may otherwise generate operational disruption.

CoinCover Recover for Institutions helps firms support alignment with DORA Chapter II by providing a documented and auditable recovery capability designed to strengthen ICT resilience for digital asset access continuity. The solution can be incorporated into a firm’s ICT risk management framework as a control supporting continuity and recovery planning, including evidence-based recovery governed by access procedures, recovery testing outputs, and recovery event logs.

This assists firms in evidencing that response and recovery plans are operationalised, tested, and supported by appropriate controls consistent with Articles 6(1) and 11(1), particularly for key-loss and disruption scenarios that could impact client access and service continuity.

Incident classification and reporting (Chapter III)

Article 18(1): “Financial entities must classify ICT incidents by impact criteria (clients affected, duration, geographic spread, data loss on availability/integrity/confidentiality, criticality, economic impact).”

And

Article 19 and Commission Delegated Reg. (EU) 2024/1772: Financial entities must “report major ICT-related incidents to the competent authority; templates, timelines and content are harmonised via RTS/ITS.”

CoinCover Recover helps firms support incident classification and reporting readiness in retail-facing self-custody contexts by maintaining structured, time-stamped recovery case records (e.g., initiation, verification outcomes, resolution timing, and affected wallet identifiers where applicable).

These records can assist firms in assessing the scope, duration and client impact of access-loss or recovery-related disruption events and in evidencing incident handling and escalation decisions, supporting the firm’s broader incident governance and reporting processes under Articles 18 and 19 where relevant.

CoinCover Recover for Institutions helps firms support alignment with these obligations by generating audit–ready evidence (including what occurred, when, and which wallets/users were affected).

This helps firms classify ICT-related incidents against Article 18 criteria and provides structured evidentiary inputs for major-incident reporting under Article 19 and related RTS/ITS requirements, supporting consistent escalation, investigation, and regulatory reporting workflows.

Digital operational resilience testing (Article 24)

Financial entities shall "establish, maintain and review a sound and comprehensive digital operational resilience testing programme" as part of the ICT RM framework; tests must be risk-based, independent, with prioritisation and remediation, and at least yearly on critical systems.

CoinCover Recover helps support digital operational resilience testing in retail-facing self-custody contexts by providing defined, repeatable recovery workflows that can be incorporated into a firm's broader testing programme. Recovery scenarios (e.g., key loss, credential compromise, customer account takeover attempts) can be tested through controlled exercises, with outcomes evidenced through time-stamped case records and verification logs.

CoinCover Recover for Institutions helps firms support alignment with Article 24 by enabling structured resilience testing for digital asset access continuity, including table-top exercises through to live-switch recovery drills. The solution can generate RTO/RPO evidence, pass/fail outputs, and remediation tracking, supporting the testing programme and audit trail required for critical systems.

Third-party risk management (Article 28, General principles)

Article 28(1)(a): "Financial entities shall manage ICT third-party risk within the ICT RM framework and remain fully responsible for compliance."

And

Article 28(3): "As part of their ICT risk management framework, financial entities shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers."

CoinCover Recover helps firms support alignment with Article 28 in retail-facing deployments where it is integrated as a third-party service within a wallet provider's customer access and recovery journey. CoinCover Recover can be documented within the firm's ICT third-party register and assessed through due diligence, contractual controls, and operational oversight consistent with the firm's ICT risk management framework.

CoinCover Recover for Institutions operates as a governed ICT third-party recovery service with contractual controls (security standards, audit/inspection support, termination/exit, data portability), helping firms with their alignment with Article 28 requirements on due diligence, registers, and tested exit strategies.

HONG KONG

Security & Futures Commission (SFC)

Regulatory focus

Hong Kong's regime places strong emphasis on custody arrangements, including cold storage requirements, protection of client assets, and robust security for seed phrases and private keys.

Key expectations include security aligned to international standards, appropriate segregation and redundancy, avoidance of single points of failure, and strong governance over access and storage practices in a manner consistent with investor protection outcomes.

Cold storage requirement (Securities and Futures Commission (SFC) 10.6(c))

"Platform Operators are required to store 98% of the client virtual assets in cold storage (referred to as the '98/2 Requirement') as required under paragraph 10.6(c) of the VATP Guidelines."

CoinCover Recover helps firms support alignment with the operational and client-protection intent of paragraph 10.6(c) in retail-facing contexts by enabling secure customer recovery workflows that reduce loss-of-access risk while maintaining a self-custody model.

CoinCover Recover for Institutions helps firms support alignment with paragraph 10.6(c) by enabling platforms to implement robust, independently verifiable recovery and continuity controls for cold-storage environments.

The solution provides institutional-grade recovery governance and disaster recovery testing capability designed to support resilience and continuity of access to cold-held keys, thereby assisting platforms in evidencing that cold storage arrangements are supported by appropriate recoverability measures consistent with the "98/2 Requirement."

Key generation storage, segregation and redundancy (Section 10.8(a))

"Platform Operators should ensure that clients' seeds and private keys are generated and stored in accordance with applicable international security standards, and with appropriate segregation and redundancy to prevent single points of failure."

CoinCover Recover helps support alignment with Section 10.8(a) in self-custody and retail wallet contexts by enabling customers to back up and retain their own key phrases through secure, wallet-provider–branded flows, supported by configurable security requirements and verification options designed to mitigate unauthorised recovery attempts.

CoinCover Recover for Institutions helps support alignment with Section 10.8(a) by being designed to align with industry standards for cryptographic key generation, backup and storage, including adherence to ISO 27001, FIPS 140-3, and NIST SP 800-57 principles.

Key shares and recovery credentials are distributed across multiple controlled locations and entities, helping ensure that no single custodian, employee, or system can reconstruct a client key alone. This helps compliance with the SFC's single-point-of-failure avoidance requirement.

Every key event (generation, validation, rotation, recovery) is logged and timestamped in immutable records, helping provide the verifiable evidence the regulator expects under Section 10.8(a).

SINGAPORE

MAS and FSMA (Money Authority of Singapore & Financial Services Market Act, 2022)

Regulatory focus

Singapore's framework emphasises robust operational risk management, technology risk controls (as reflected in MAS TRM guidance), and regulator-driven requirements for reporting and returns, incident readiness, and strong governance.

FSMA requirements also emphasise AML/CFT responsiveness and the need for firms to maintain reliable records and demonstrate control effectiveness when responding to supervisory requests and customer/user complaints.

Reports and returns (FSMA, section 146 - Reports and Returns)

"A licensee must submit to the Authority such reports or returns … in such form, manner and frequency as the Authority may specify."

CoinCover Recover helps firms support alignment with FSMA section 146 in retail-facing deployments by maintaining structured recovery case records and verification evidence that can be used to support supervisory reporting requirements where requested (e.g., recovery events, customer access disruptions, and operational risk management).

CoinCover Recover for Institutions helps firms support alignment with FSMA section 146 by strengthening firms' operational resilience, access governance and incident readiness, and by generating audit-ready evidence that can support regulatory reporting and supervisory requests.

The solution maintains structured records of recovery governance and execution (including approvals, authentication and event logs), supporting the firm's ability to produce consistent documentation and demonstrate control effectiveness where reporting obligations require disclosure of operational disruptions, access incidents or continuity measures.

AML/CFT query responsiveness (FSMA, section 143)

"A licensee must appoint at least one person … to respond to any queries related to anti-money laundering or countering the financing of terrorism, or complaints from any digital-token service user."

CoinCover Recover centralises customer identity verification, correspondence, and evidence within each recovery case, helping enable the AML/CFT officer to resolve queries or complaints quickly with documented proof.

CoinCover Recover for Institutions helps firms support alignment with FSMA section 143 by providing structured, auditable records of access governance and recovery events that can assist an appointed AML/CFT officer or compliance function in responding to user queries.

The solution's documented workflows and event evidence help support timely, evidence-based responses and facilitate consistent handling and escalation of cases where AML/CFT concerns arise in connection with wallet access or recovery processes.

UNITED ARAB EMIRATES

VARA and ADGM FSRA

Regulatory focus

UAE frameworks emphasise operational resilience, continuity of access, and strong controls over custody arrangements. Expectations commonly include independence and segregation of safeguards, geographically distributed redundancy, and scenario-based recovery planning aligned with appropriate recovery objectives (e.g., RTO/RPO).

ADGM guidance additionally emphasises ongoing confidence-building through testing and, where practicable, operating from recovery arrangements to validate recoverability and continuity.

VARA

Custody continuity planning and independent custody controls (VARA Rule 2.4 and Rule 2.6)

"VASPs must ensure that custody arrangements are independently managed and segregated to prevent conflicts of interest and ensure asset protection."

CoinCover Recover helps firms support alignment with the underlying continuity and protection intent of VARA's custody resilience expectations in retail-facing and self-custody contexts by enabling a structured, controlled recovery mechanism that reduces loss-of-access risk while maintaining a non-custodial model.

CoinCover Recover's configurable security levels, verification options, and auditable recovery case records can be integrated into a VASP or platform's broader continuity planning and client protection framework, helping support demonstrable customer access resilience and recovery readiness consistent with VARA's focus on secure and resilient access to digital assets.

CoinCover Recover for Institutions helps firms support alignment with VARA Rules 2.4 and 2.6 by providing independently managed recovery and continuity controls designed to maintain secure access to wallet keys in the event of a disaster, operational disruption, or service failure.

The solution helps support segregation of recovery infrastructure and authorisation processes from the VASP's day-to-day operational environment, reducing conflicts of interest and strengthening resilience and access governance consistent with VARA's expectations for independent custody controls and continuity planning.

ADGM FSRA

Redundant key management and scenario-based recovery planning (Section 9.3.3)

Under ADGM FSRA's Guidance digital asset custodians must implement redundant, independently verifiable key management systems to mitigate the risk of key loss or compromise.

"In developing a recovery plan, a financial institution should study a range of scenarios and identify what disruptions would result from each scenario. For example, a faulty hardware could result in system failure thereby disrupting business operations or services to customer."

CoinCover Recover helps firms support alignment with the underlying resilience intent of ADGM's scenario-based recovery guidance in retail-facing self-custody contexts by enabling structured recovery workflows and configurable verification mechanisms designed to reduce the risk and impact of access-loss events.

CoinCover Recover for Institutions helps firms support alignment with ADGM FSRA Guidance Section 9.3.3 by enabling redundant, independently verifiable recovery and continuity controls intended to mitigate the risk of key loss, compromise, or operational disruption.

The solution is designed to support multi-region resilience and secure recovery execution through distributed recovery authorisation, strong authentication, and auditable recovery procedures. This assists custodians and regulated firms in evidencing scenario-based recovery planning and business continuity for digital asset access, consistent with the guidance's expectation that firms anticipate disruptions (including hardware failure) and implement robust recovery arrangements that protect customer service continuity.

Recovery objectives (ADGM Section 9.3.3)

> "Recovery plans should be aligned with RTOs and RPOs … and approved by the appropriate level of management."

CoinCover Recover helps firms support alignment with the underlying intent of RTO/RPO-aligned recovery planning in retail-facing deployments by providing standardised recovery workflows that can be designed, monitored, and governed as part of a firm's customer service continuity objectives.

CoinCover Recover for Institutions' processes are customisable to institutional Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Each recovery execution is cryptographically logged and timestamped for audit purposes.

Live operations (ADGM Section 9.3.7)

> "Where possible, a financial institution should regularly operate fully from its recovery or alternative arrangements to build confidence…"

CoinCover Recover helps firms support alignment with the underlying intent of Section 9.3.7 in retail-facing contexts by providing repeatable, operationally executable recovery workflows that can be periodically exercised to validate readiness and helping customer access continuity processes to remain effective.

Providers can conduct controlled recovery drills (e.g., simulated access-loss events and fraud attempts), with outcomes evidenced through time-stamped case records and verification logs, supporting confidence-building, governance oversight and continual improvement consistent with the principles reflected in ADGM's guidance.

CoinCover Recover for Institutions' infrastructure helps firms support live switch testing, temporarily routing operations through recovery systems without impacting performance. Recovery scenarios are tailored to institutional scale, system architecture, and custody type (MPC, HSM, or hot wallet).

UK

The FCA perspective

Regulatory focus

UK requirements are principles-led, focusing on the adequacy of systems and controls (SYSC), effective governance and oversight, and firms' ability to maintain continuity and regularity of regulated activity. Consumer protection is reinforced through the Consumer Duty (outcomes-based expectations) and PRIN obligations relating to the protection of client assets where a firm is responsible for them.

The FCA's approach places emphasis on "reasonable steps," supervisory defensibility, and effective operational resilience.

Systems and controls; continuity of regulated activities (SYSC 4.1 and SYSC 13)

SYSC 4.1: "A firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business."

SYSC 13: "A firm must take reasonable steps to ensure continuity and regularity in the performance of its regulated activities."

CoinCover Recover helps firms support alignment with the underlying intent of SYSC 4.1 and SYSC 13 in retail-facing self-custody contexts by helping enable structured, controlled recovery workflows that reduce the risk of customer access-loss events escalating into broader service disruption and consumer harm.

CoinCover Recover for Institutions' segregated recovery architecture helps firms maintain client-asset access and operational uptime even in the event of a catastrophic technology failure or custodian compromise, demonstrating that reasonable steps have been taken to provide uninterrupted activity.

Consumer Duty (Principle 12 and associated cross-cutting rules)

"Firms must act in good faith towards retail customers, avoid causing foreseeable harm, and enable and support retail customers to pursue their financial objectives."

CoinCover Recover helps firms support alignment with Consumer Duty by enabling customers to retain continuous, secure access to their digital assets, even in the event of lost keys, custodian failure, or operational disruption. Its independent recovery framework, verified identity process, and insured asset continuity reduce *foreseeable harm* in digital-asset ownership.

Clients' assets — adequate protection (Principle 10: Clients' Assets)

"A firm must arrange adequate protection for clients' assets when it is responsible for them." Therefore, strengthening obligations to ensure adequate protection of client assets by applying robust security, authentication and continuity controls that reduce the risk of unauthorised access, loss of access, misuse, or theft.

CoinCover Recover helps firms support alignment with Principle 10 in retail-facing self-custody contexts by providing structured, controlled recovery mechanisms that reduce the risk of permanent loss of access and unauthorised recovery attempts.

CoinCover Recover for Institutions helps firms support alignment with Principle 10 by helping strengthen the security and continuity controls that regulated firms rely on to protect client assets, particularly where loss of access or key compromise could impair client-asset availability.

USA

The SEC perspective

Regulatory focus

SEC expectations relevant to digital assets emphasise the need for robust safeguards around private key security, clear governance over access and authorisation, and measures to ensure the continued safekeeping and accessibility of crypto asset securities in disruption scenarios.

Related requirements also emphasise market integrity and system resiliency (e.g., Reg SCI where applicable), as well as cybersecurity risk governance and disclosure frameworks that require timely, accurate incident documentation, escalation, and reporting capability.

Statement on the Custody of Crypto Asset Securities by Broker-Dealers, Division of Trading and Markets, 2025

"A broker-dealer establishes, maintains, and enforces reasonably designed written policies, procedures, and controls that are consistent with industry best practices to protect against the theft, loss, or unauthorized or accidental use of the private keys necessary used to access and transfer the crypto asset security."

CoinCover Recover and CoinCover Recover for Institutions helps firms support alignment with these principles by providing non-custodial security and recovery mechanisms—such as encryption and multi-party authentication—that reduce single points of failure and strengthen controlled access and recoverability of private keys.

This helps institutions and custody providers reinforce authorisation controls and operational resilience, consistent with the SEC's focus on preventing unauthorised transfers and maintaining secure client access even under adverse events (including technology failures and blockchain-specific disruptions).

Systems compliance and integrity (Reg SCI)

"Each SCI entity shall... have levels of capacity, integrity, resiliency, availability, and security adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets." and [R]registrants [must] describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats..."

CoinCover Recover helps firms support alignment with Reg SCI resilience expectations in retail-facing self-custody contexts, by helping enable structured, controlled recovery workflows designed to reduce the operational impact of customer access-loss events.

CoinCover Recover's configurable security requirements, onboarding and verification options, and auditable recovery case records provide evidence of controlled recovery execution and service continuity processes, supporting a firm's broader availability and resiliency controls where customer access continuity is operationally material.

CoinCover Recover for Institutions provides a recovery and continuity framework that helps enhance firms' system availability and resiliency by enabling digital-asset access restoration through an independent, auditable process.

This assists institutions in evidencing operational capability and resilience in the face of disruption scenarios that could otherwise impair access to client assets or undermine market confidence, helping firms support alignment with the operational resilience outcomes contemplated by Regulation SCI.

Cybersecurity incidents (SEC Item 1.05)

"Item 1.05 requires disclosure of ... the nature, scope, and timing of the incident; and the material impact or reasonably likely material impact on the registrant's financial condition and results of operations."

CoinCover Recover helps firms support alignment with disclosure readiness in retail-facing contexts by maintaining structured, time-stamped recovery case records and verification outcomes that can assist in documenting incidents affecting customer access and service continuity.

Where access-loss events or attempted recovery fraud are assessed as cybersecurity incidents, CoinCover Recover's case logs help provide evidentiary inputs to support internal investigation, impact assessment and reporting decision-making, including documenting incident timing, affected users and operational impact as relevant to SEC disclosure requirements.

CoinCover Recover for Institutions records recovery-related events — including initiation, authentication, key reconstruction, and completion — in a cryptographically sealed audit log. These logs capture precise details about the *nature* (e.g., access-loss, hardware failure, compromise), *scope* (affected wallets, users, or assets), and *timing* (exact initiation and resolution timestamps) of any recovery or disruption event.

Regulatory overview

Please note that CoinCover does not provide legal or regulatory compliance services. Responsibility for regulatory compliance remains with the regulated entity. CoinCover's products support firms in implementing technical and operational controls that may assist in meeting regulatory expectations.

Jurisdiction	Regulations	Themes	How CoinCover assists
Australia	**ASIC INFO 225; ASIC RG 133 (incl. RG 133.141–143); ASIC custody guidance (Part E); ASIC Report 705**	Private key control as custody trigger; minimise hot storage; key backup & recovery with geographic distribution; minimise single point of failure (multi-sig/sharding); operational resilience & recordkeeping.	**CoinCover Recover** helps support self-custody by enabling user-managed backup/recovery via wallet-branded flows with configurable verification, without CoinCover holding keys/assets. **CoinCover Recover for Institutions** helps support institutional custody and custody-adjacent operating models by strengthening key access governance and recoverability.
Canada	**CSA Staff Notices (e.g., 21-329, 21-332) and PRU expectations; FINTRAC Registration (Section 7 and 7.1)**	Custody/control safeguards; system resiliency & security controls; cold storage & independent assurance; AML/CTF recordkeeping to support STR preparation.	**CoinCover Recover** helps structure recovery case records (verification outcomes, timestamps, wallet identifiers) to support compliance documentation aligned to AML/CTF workflows. **CoinCover Recover for Institutions** helps strengthen key access governance and recoverability where platforms/custodians control keys; helps support independent audit readiness with documented procedures and logs.
EU	**MiCA (Articles 62, 70); DORA (Chapter II and III: Articles 6, 11, 24, 28)**	MiCA: safeguarding client cryptoassets and protecting private keys via systems and access protocols DORA: ICT risk management framework + business continuity and recovery plans	**CoinCover Recover** helps support retail-facing continuity objectives by providing structured recovery workflows and recovery case records that reduce the operational impact of customer access-loss events. **CoinCover Recover for Institutions** helps support MiCA safeguarding and DORA Chapter II alignment by providing a documented and auditable recovery capability that can be incorporated into ICT risk management and business continuity frameworks.
Hong Kong	**SFC VATP Guidelines (2022) (incl. 98/2 requirement; 10.6(c) 10.8(a); related SFC/HKMA security governance guidance**	Client assets in cold storage; seed/private key generation & storage to international standards; segregation/redundancy to avoid single points of failure.	**CoinCover Recover** helps secure retail/self-custody recovery flows with configurable security checks to reduce permanent loss-of-access risk. **CoinCover Recover for Institutions** helps support independently verifiable recovery governance for keys (multi-actor approvals, distributed recovery components), helping support resilience while maintaining storage intent, and with audit-ready logs.

Jurisdiction	Regulations	Themes	How CoinCover assists
Singapore	**Payment Services Act; MAS TRM Guidelines (s.8–10); FSMA section 143 and 146**	Technology risk management; disaster recovery & business continuity; external validation/testing; ability to produce records for supervisory requests	**CoinCover Recover** helps firms define recovery workflows to support operational risk management. **CoinCover Recover for Institutions** helps provide independently verifiable recovery infrastructure, documented procedures, and evidence of outputs supporting externally validated resilience.
UAE	**VARA Regulations 2023 (Rule 2.4 and 2.6); ADGM FSRA 2022 Guidance (Section 9.3.3 and 9.3.7)**	Operational resilience, risk management and disaster recovery; segregation/ geographic separation to reduce concentration risk; governance & evidence	**CoinCover Recover for Institutions** helps support distributed recovery design with multi-party governance, geographic separation options, and auditable evidence trails supporting disaster recovery and supervisory oversight, without holding client assets.
UK	**FCA SYSC 4.1 and 13; Principles for Businesses (Principle 10 and 12)**	Sound systems & controls; continuity planning; protection of client assets by reducing key-loss and access governance failures	**CoinCover Recover** helps firms support alignment with the underlying intent of SYSC 4.1 and SYSC 13 in retail-facing self-custody contexts. **CoinCover Recover for Institutions** helps provide governed recovery execution and evidence of production (logs/approvals), helping support continuity and client asset protection outcomes.
USA	**SEC custody expectations; SEC Item 1.05; Reg SCI; cybersecurity disclosure expectations**	Systems integrity/availability and monitoring; incident readiness; audit evidence production	**CoinCover Recover** helps firms support alignment with disclosure readiness in retail-facing contexts by maintaining structured, time-stamped recovery case records. **CoinCover Recover for Institutions** helps provide controlled recovery governance, monitored recovery operations, and time-stamped event logs, helping support audit readiness and incident documentation.

HELLO@COINCOVER.COM

CoinCover