CoinCover

COINCOVER.COM →

The recovery playbook

AN INSTITUTIONAL TOOLKIT FOR CRYPTO RECOVERY & OPERATIONAL RESILIENCE

COINCOVER.COM →

Table of contents

01 What is crypto recovery?

Crypto recovery underpins business continuity, responsibility to customers, & regulatory readiness.

COINCOVER.COM →

What is crypto wallet recovery?

Crypto wallet recovery is the controlled process of restoring a firm's access to their crypto assets, by securely re-establishing the required keys, permissions, and approvals after a loss, compromise, or failure event.

• CRYPTO WALLET RECOVERY GLOSSARY •

C

Custodian:
A provider that holds and safeguards crypto assets (or manages the systems that control them) on behalf of customers.

K

Key material:
The cryptographic secret(s) needed to sign transactions or prove material. This could be a private key, seed phrase, shard, or device-held credential.

M

MPC (Multi-Party Computation):
A signing approach where multiple parties hold “shares” of a key and collaborate to produce a signature without ever assembling the full private key in one place.

Multi-sig (Multi-signature):
A wallet structure where multiple independent signatures are required to approve a transaction.

P

Private key:
A secret cryptographic key used to sign blockchain transactions. Whoever has the private key can move assets.

R

Recoverability:
How feasible recovery is given wallet architecture, custody models and signer distribution.

S

Seed phrase:
A set of words (usually 12-24) that can regenerate a private key.

Signing authority:
The ability to approve blockchain actions. This is usually distributed across signers or key shares.

W

Wallet:
A system that manages keys and creates signatures to perform blockchain actions. Wallets can be software-based (hot storage), hardware-based (cold storage), multi-sig or MPC-based.

02 Why you need to act now

Having recovery processes in place reduces long-term costs, avoids disruption, and helps institutions scale confidently.

COINCOVER.COM →

The crypto loss problem

20% of all Bitcoin (BTC) is permanently lost and unrecoverable.

• NO RESET BUTTON •

No “forgot password” process exists for assets on blockchains.

When signing authority is lost, fragmented, mismanaged, or simply unavailable when you need it, there is no central authority who can reverse the outcome.

If your organisation cannot assemble the right authority to sign transactions, the assets may remain visible on-chain but be operationally unusable.

For digital asset institutions, there’s a very simple practical question to answer: can you 100% reliably control, and restore access to client and treasury assets under real operating conditions?

Most access failures come down to practical realities you may not have planned for or tested.

This playbook provides a structured institutional framework for recovery under pressure.

It is designed to support rapid yet controlled execution, preserve stakeholder trust through disciplined communication, and satisfy regulatory expectations through audit-ready documentation.

03 Key issues

Digital assets introduce a fundamentally different risk profile from traditional financial instruments, where loss of access often equates to permanent loss of value.

COINCOVER.COM →

The risks shaping institutional recovery

If you are an exchange, custodian, asset manager, or corporate treasury, your scale and sophistication do not automatically make your digital assets recoverable in a disaster.

• THE TEST IS SIMPLE •

Can your organisation reliably, rapidly reassemble authorised signing power when something goes wrong?

The most common causes of loss of access are operational and governance failures:

- ✕ Recovery key shares, seed backups, or access credentials are missing, outdated, or stored somewhere no one can access quickly.
- ✕ The people, devices, or systems needed to approve transactions are unavailable.
- ✕ The organisation doesn't have a clear, reliable way to reach decision-makers and get approvals fast.

A defining characteristic of institutional key loss is gradual degradation.

- ✕ Recovery material is generated, copied, and relocated.
- ✕ Signers change roles, leave organisations, or become unavailable due to jurisdictional or compliance constraints.
- ✕ Documentation lags operational reality.

Over time, you accumulate what auditors refer to as *latent access risk.*

Seed phrases written on paper, screenshots stored in cloud drives, or recovery instructions known only to specific individuals are fundamentally incompatible with the principles of institutional governance. These practices introduce single points of failure that stay invisible until it is too late.

• INDUSTRY EXAMPLES •

01 — EXCHANGE

Exchange unable to restore access

QuadrigaCX is the clearest real-world illustration of what happens when operational access cannot be reconstituted.

The exchange's CEO was believed to be the only person with access to the firm's cold wallet credentials. After his death, access to the firm's crypto wallet was lost permanently. This demonstrates the principle of "quorum is not achievable in practice."

02 — SINGLE LOSS EVENT

Dependency on a single device or location

Image credit: CBC News / CBC Radio (15 Jan 2021)

Wired reported on the long-running case of Stefan Thomas, who has been unable to access 7,002 BTC because the credentials are locked behind a specific encrypted USB device (an IronKey) and a forgotten password.

If access depends on a single device and a single secret, recovery is no longer a normal operational process but has become a technical and governance problem.

• PREPARING FOR AN INCIDENT •

1 **Who can officially declare a recovery incident for your firm's wallets?**
(Name the role or person)

2 **Where is the recovery material for your firm's wallets stored?**
(e.g., MPC provider process, secure vault, HSM backup, sealed escrow, external disaster recovery solution provider, etc.)

3 **If one signer is unavailable right now, how do you reach quorum?**
(e.g., alternate signers, replacement process, threshold still achievable)

COINCOVER.COM →

• YOU'VE GOT TROUBLE IF: •

- → answers are unclear or "someone else probably knows"
- → there's a dependency on one specific person
- → teams give different answers for the same wallet

Simple rule:

If you can't answer these basics quickly and consistently, your recovery readiness is not reliable.

04 Wallet recovery

Wallet recovery is the mechanisms and controls that enable a firm to securely restore their access to a digital asset wallet.

COINCOVER.COM →

Why wallet recovery matters

Wallet access loss is a different beast to the failures more normally encountered in traditional finance or enterprise IT. It is visible, and it is final.

Unlike an outage, you cannot reroute a missing private key. On-chain, the assets remain publicly observable even when you cannot access them. That combination makes wallet inaccessibility uniquely damaging for institutions.

Billions of dollars in digital assets are estimated to become inaccessible each year due to key loss and access failures, and these losses are often irreversible.

Visibility creates immediate consequences for you.

- Clients can see balances but cannot see movement, which raises questions about control.
- Counterparties reassess settlement reliability and may adjust terms or require additional assurances.
- Liquidity providers tighten risk limits when operational uncertainty appears.
- Regulators and auditors can also detect service disruption quickly, particularly if client withdrawals or settlement activity is affected.
- Even when the underlying issue is administrative or procedural, the market reads inaccessibility as a control issue.

The implication for your organisation is straightforward.

- ✓ If you **can** restore access quickly, safely, and with evidence, you reinforce trust under pressure.
- ✗ If you **cannot,** confidence erodes rapidly and the impact can exceed direct financial exposure.

• IS YOUR RECOVERY PLAN FAST ENOUGH TO MEET YOUR BUSINESS NEEDS? •

1

List the activities that rely on wallet access

List the most important activities that rely on wallet access.

Examples might include:

- Customer withdrawal
- Settlement and transfers to counterparties
- Treasury rebalancing / liquidity moves
- Funding margin accounts or clearing obligations
- Moving assets for operational security (e.g., rotating wallets)

2

Set the longest downtime you can tolerate

For each service, define the maximum time it can be disrupted without causing serious harm.

Examples of harm	Maximum disruption time
Missed settlement deadlines	
Client complaints and churn	
Liquidity shortfalls	
Regulatory escalation	
Contractual breaches	

3

Estimate recovery time

Estimate (honestly) how long recovery would take today to restore signing access for that service:

Examples of harm	**Best case**	**Realistic case**	**Worst case** *(weekend / travel / unavailable signers)*
Missed settlement deadlines			
Client complaints and churn			
Liquidity shortfalls			
Regulatory escalation			
Contractual breaches			

If your expected recovery time is longer than the tolerated downtime for any critical service, then recovery risk is not just a custody problem, it is an operational resilience issue and it requires a remediation plan (people, process, and controls), not “we’ll handle it if it happens.”

Simple rule:

If your business needs access in hours, but recovery takes days, you don’t have recovery readiness.

05 The five pillars

Effective crypto recovery rests on five pillars, working together to keep assets recoverable under defined conditions without weakening control or resilience.

COINCOVER.COM →

The five pillars of institutional recovery

Institutional recovery is the ability to restore access to digital assets in a way that is secure, controlled, tested, and audited. Our five pillars of institutional recovery define what “good” looks like.

PILLAR 01

Clear ownership and governance

Effective recovery starts with clearly defined ownership, decision-making authority, and accountability. Institutions must establish who can initiate recovery, under what conditions, and with which approvals, ensuring actions are aligned with internal risk frameworks and regulatory expectations.

PILLAR 02

Prepare for real-life situations

Recovery frameworks must be designed for real operational stress. This includes preparing for human error, personnel changes, market volatility, and infrastructure outages, with procedures that can be executed reliably under time pressure and uncertainty.

PILLAR 03

Technical repeatability

Recovery processes should be technically repeatable, predictable, and resilient across environments. Standardised mechanisms, documented workflows, and regular testing ensure recovery can be executed consistently without relying on ad-hoc actions or institutional memory.

COINCOVER.COM →

PILLAR

04

Providing an audit trail

All recovery-related actions must be traceable, verifiable, and reviewable. Comprehensive logging, evidence capture, and reporting enable institutions to demonstrate control effectiveness, support audits and meet regulatory requirements.

PILLAR

05

Crisis communications

Clear communication plans are essential during recovery events to manage internal coordination and external stakeholder expectations. Defined messaging, escalation paths, and disclosure protocols help maintain trust with regulators, clients, partners, and the market.

COINCOVER.COM →

01 Clear ownership and governance

COINCOVER.COM →

Clear roles, tested steps, & ready materials

Recovery is fastest and safest when there is no confusion about who is allowed to start the recovery process and approve actions. Every institution therefore needs clear answers to three questions:

01

Who can declare a recovery incident?

02

Who can approve recovery actions?

03

How are decisions made when normal operating procedures don't apply?

• BUILDING RECOVERY GOVERNANCE •

Recovery governance is the decision structure that lets wallet access recovery start fast and stay controlled. The goal is to remove ambiguity about who can declare an incident, who can approve actions, and what restrictions apply while access is being restored.

1 **Appoint a Recovery Incident Owner (RIO)**

Name one accountable owner and a deputy. This is a person who can declare an incident, activate recovery mode, coordinate teams and vendors, and ensure the timeline, approvals and evidence are recorded.

Owner

Deputy

2 **Define a Recovery Approval Matrix (RAM)**

Document, in one place, who can authorise recovery actions (by role, with backups), which actions require dual control (so that no single person can initiate and approve), and what evidence must be recorded for each action (such as approvals, logs, and reconciliation).

Recovery actions	Who can authorise them?	Do they require dual control?	Evidence

3

Agree recovery actions

Agree in advance what measures will automatically apply during recovery, so they can be activated immediately, including limits (such as transaction caps), allowlists (approved destination addresses only), staged approvals (extra sign-offs for high-risk actions), and enhanced monitoring with escalation triggers.

- [ ] Allowlists
  (approved destination addresses only)
- [ ] Limits (transaction caps)
- [ ] Staged approvals
  (extra signoffs for high-risk actions)
- [ ] Enhanced monitoring & escalation triggers

Simple rule:

If you cannot activate recovery mode and approvals in minutes, governance is not ready.

02 Prepare for real-life situations

• BUILDING SCENARIO RUNBOOKS •

A runbook is a step-by-step playbook for a specific recovery situation. It removes guesswork when things go wrong and ensures everyone follows the same process under pressure.

Every runbook must include the following:

1 Trigger conditions:

- [ ] A key, key share, signing device, or recovery material is missing, locked, damaged, or cannot be verified.
- [ ] The custodian, MPC service, policy engine, or signing infrastructure is down and cannot be restored quickly.
- [ ] You don't have enough authorised signers available to approve transactions.
- [ ] Approvals cannot be obtained or verified (e.g., required approvers unavailable, disputed authority, missing approval evidence).
- [ ] There is a credible risk that a key, signer device, or signing system has been exposed or misused.

If the quorum is unavailable beyond the agreed time window or compromise is suspected, declare a recovery incident and activate this runbook.

2 What happens immediately

List the first actions taken to reduce risk while recovery is underway. Examples include temporarily restricting withdrawals, applying transaction limits, and enabling heightened monitoring.

Why: Stops the situation from getting worse while recovery is organised.

3 **Define the Access Control List (ACL) for recovery actions**

Set clear ownership of duties for recovery actions so approvals, thresholds and execution responsibilities are unambiguous.

Actions	Responsibility/role
Identify ACL members	
Define approval threshold (how many individuals are required	
Recovery execution (who executes the recovery)	

Why: Ensures recovery actions are authorised and responsibilities are clearly defined.

4 **Define checks**

Define the checks that must be passed before proceeding to the next step in recovery, such as verifying the approver's identity, confirming the destination address, completing a successful test transaction, and reconciling balances.

Why: Stops progression if something is wrong

5

Post recovery actions

Set clear ownership of duties for recovery actions so approvals, thresholds and execution responsibilities are unambiguous.

- [ ] **Check it's safe to operate**
  Confirm the right people can sign, and the wallet rules (limits, allowlists, monitoring) are working.

- [ ] **Replace anything that might be exposed**
  Rotate keys/shares and reset any logins, MFA, or access used during recovery (especially if compromise is suspected).

- [ ] **Create new backups if needed**
  If recovery material was used or touched, create a fresh backup, test it works, and store it securely.

- [ ] **Bring services back slowly**
  Do a small test first, then gradually lift limits and re-enable withdrawals/services.

- [ ] **Wrap up and improve**
  Record follow-ups, update the runbook and signer lists, and schedule a review and a new recovery test.

Simple rule:

If **any one of these elements is missing,** the runbook is incomplete and cannot be relied on in a live recovery.

03 Technical repeatability

Recovery must be repeatable

Recovery is a controlled reconstruction of signing authority.

The standard to aim for is simple. If you cannot run wallet access recovery as a repeatable procedure, you are relying on individual expertise and memory at the highest-pressure moment your custody model may face.

Recovery should instead be treated as an operational workflow with controlled steps and constant monitoring. It must also produce an audit trail that can be independently reviewed.

• TEST-PROOFING RECOVERY •

1. Double-check where funds are being sent

If you move funds during recovery, the destination wallet address must be checked by someone who didn't create the transfer.

Why: Sending to the wrong address is irreversible. Recovery is when mistakes happen most.

Simple rule:

Treat any failed check as a red flag. Pause recovery, escalate, and only proceed once the cause is confirmed, and controls are restored.

2. Do a small test transfer first

Before moving large amounts or turning withdrawals back on, do a small test transaction to prove everything works end-to-end.

Why: During recovery, teams are under pressure and normal controls may change. A small test transaction is the safest way to verify control, confirm the destination address, and ensure the signing process works end-to-end.

How:

- Send a small amount first,
- Confirm it lands where expected,
- Confirm your internal records match the blockchain,
- Only then increase size or resume service gradually.

04 Providing an audit trail

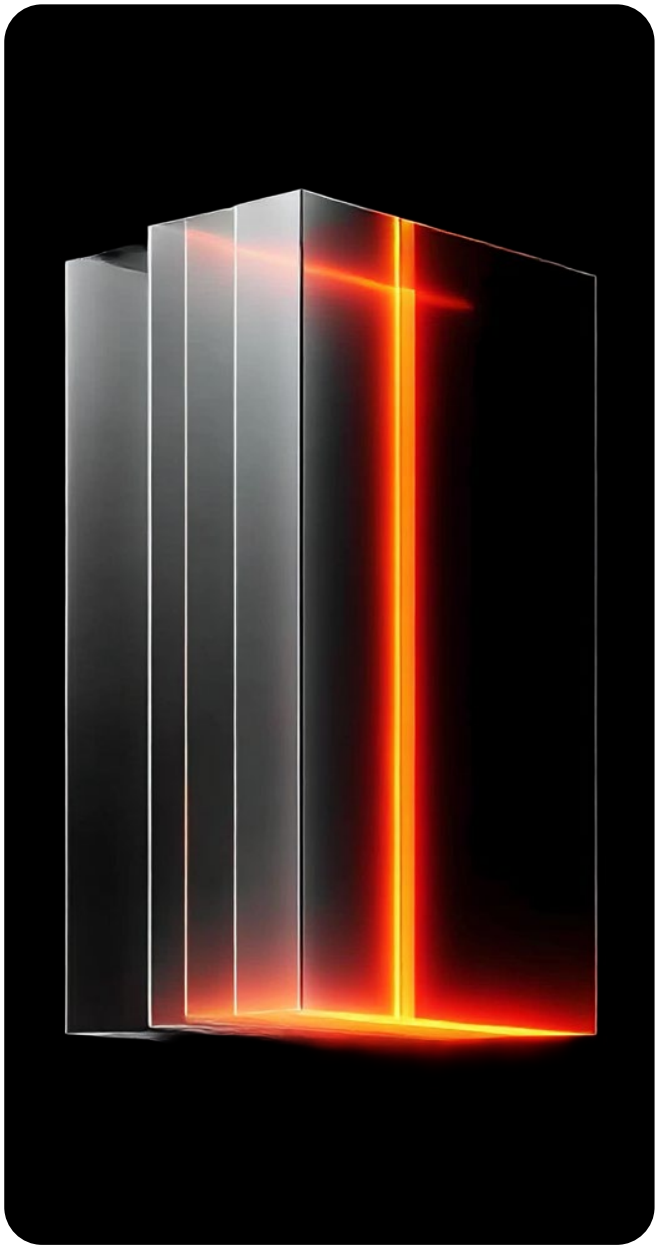
COINCOVER.COM →

Auditable proof of control

Recovery is not complete when access is restored. It is complete when you can prove, to auditors and supervisors, that control was maintained, decisions were authorised, and client protection obligations were met throughout the event.

Regulators expect recovery systems to be auditable, tested, and resilient, and they view informal or self-managed backup approaches as a common source of control failure.

In practice, institutions that treat evidence recording as a component of infrastructure recover faster, report more confidently, and withstand scrutiny with less disruption.



• RECOVERY EVIDENCE PACKS •

A recovery evidence pack is the file you can hand to auditors, regulators, and internal leadership that proves what happened, who authorised actions, what was done, and that funds and records match.

Simple rule:

If you can't produce this evidence pack within **24–72 hours**, your compliance risk increases. This is because you may not be able to prove the recovery was properly authorised and controlled.

• MINIMUM CONTENTS •

01

Incident declaration record

A clear starting point: when the incident was declared, who declared it, what wallets/services were affected, and what immediate constraints were applied.

02

Approval and decision logs

A record of key decisions and approvals: who approved what, when, and why (especially for fund movements, signer changes, key reconstruction, or enabling/disabling withdrawals).

03

Technical execution logs

A factual record of the recovery steps taken, what actions were executed, by whom, on what systems/tools, and the results (including timestamps).

04

Reconciliation reports

You need proof that balances and transactions match both the on-chain reality and your internal ledger or client records. This is what demonstrates control and correctness after recovery.

05

Communications log

A record of what was communicated, to whom, when, and through which channels (clients, counterparties, regulators, internal teams).

06

Remediation actions

A documented list of what will change so it doesn't happen again: root cause summary, fixes, owners, deadlines, and when you'll retest.

COINCOVER.COM →

05 Crisis communications

COINCOVER.COM →

Communicate to maintain control

Communication during a recovery event helps you maintain order while you reconstitute access.

In digital asset markets, stakeholders respond to uncertainty faster than in traditional finance because on-chain activity is observable; rumours travel quickly, and counterparties price operational risk immediately.

When your wallet activity slows or stops, clients, liquidity partners, and supervisors will notice. If you do not communicate with structure and discipline, the gap will be filled by speculation.

The objective is to provide enough information to demonstrate governance, progress, and client protection, while avoiding operational detail that increases risk or creates inconsistencies you later must correct.

Done properly, communication buys decision time, supports regulatory engagement, and preserves confidence while technical recovery is underway.

• COMMUNICATION STEPS •

1. Pre-approved messages

Prepare short, approved statements you can use immediately when a recovery incident starts.

Why this matters:

The first hour is when uncertainty spreads fastest. If you delay, people assume the worst. If you rush, you risk making irreversible mistakes.

What to prepare in advance:

- **Initial acknowledgement**
  A short statement that confirms you are aware and responding.

  Example: "We are aware of an issue and are investigating. Some services may be temporarily limited."

- **Update template**
  A standard format for ongoing updates: what's changed, what's restricted, and when the next update will be.

- **Resolution template**
  A standard message for when services are restored: what is back, what controls remain, and what happens next.

Simple rule:

If you can't send a first message quickly, you lose control of the narrative.

2. Update schedule

Set a fixed schedule for updates, even if the update is "no change."

Why this matters:

Predictable updates reduce panic, reduce speculation, and reduce inbound noise from clients, partners, and internal teams.

What to prepare in advance:

- How often you update each audience (internal, clients, partners, regulators).
- What triggers an additional update (e.g., service restored, transaction activity resumed, key rotation complete).
- A single place where updates are logged and time-stamped for the evidence pack.

Example cadence (adjust to your institution):

- Internal leadership: every 1–2 hours in the early phase.
- External clients and counterparties: every 4–6 hours or at key milestones.
- Regulators: as required, plus material confirmed updates.

Simple rule:

Always include the next update time even if you don't yet have answers.you lose control of the narrative.

3. Assign a comms owner

Assign one person responsible for crisis communications.

Why this matters:

Multiple teams may contribute, but one person must control the final message to prevent contradictions.

Responsibilities of the comms owner:

- Collect verified facts from technical, operations, and compliance leads.
- Run the approval process for every external statement.
- Publish updates on schedule.
- Keep a record of exactly what was shared, when, and with whom.
- Coordinate client support messaging so front-line teams stay aligned.

Simple rule:

No external messages go out without one accountable owner managing the release.

4. Define the messaging

Define what you will and won't share and stick to it.

Why this matters:

During recovery, details change quickly. Sharing too much creates security risk and sets you up for later corrections.

Share externally:

- ✓ Service impact (what is affected).
- ✓ What is temporarily restricted.
- ✓ What clients should expect next.
- ✓ Timing of the next update.
- ✓ Where clients can get support.

Do not share externally:

- ✗ Exact wallet addresses involved (unless legally required).
- ✗ Internal recovery steps.
- ✗ Security controls and technical details.
- ✗ Identities of recovery participants.
- ✗ Anything not yet verified.

Simple rule:

Only share facts you can prove.
If you are unsure, say what you are doing next and when you will update.

5. Approval process

Define what you will and won't share and stick to it.

Why this matters:

Crisis communications often stall because drafting sits with Comms, while approval sits with senior leadership and Legal/Compliance. If roles and timelines aren't agreed in advance, messaging becomes a bottleneck.

Define the approval chain in advance:

- → **Who drafts:**
  Marketing/Comms (with input from technical and compliance leads).
- → **Who approves:**
  Typically, the CEO and Legal/Compliance team(s) (plus named backups).
- → **Who must be informed:**
  Client support, risk, and operations.

Define what requires approval:

- Any public statement.
- Client updates.
- Partner/counterparty messages.
- Press queries.
- Regulatory communications.

Agree response time targets (SLAs):

- Initial holding statement approved within X minutes.
- Routine update approvals within X minutes.
- Material incident updates (e.g., withdrawal restrictions, key rotation, suspected compromise) within X minutes.

Set an escalation path:

Define how approvals happen when approvers are unavailable, including named deputies and emergency delegation rules.

Simple rule:

If public statements require approval, the approval chain and response times must be defined and rehearsed before an incident.

06 Recovery testing

Regular testing proves recovery works under real conditions.

COINCOVER.COM →

Recovery testing process

Recovery is only real if it has been tested. Institutions should be able to show regulators, auditors, insurers, and clients that recovery is proven, repeatable, and governed.

• WHAT IS RECOVERY TESTING? •

A recovery test is a structured simulation that proves your organisation can restore wallet access and signing authority safely, under controlled conditions, using the same governance and runbooks you would use in a real incident.

It is designed to prove:

- ✓ Your recoverability architecture works as intended (secure, robust, geo-redundant).
- ✓ Backup materials exist and are validated.
- ✓ Roles and approvals are governed & clear.
- ✓ Runbooks exist and are understood.
- ✓ Recovery has been tested and evidenced.
- ✓ Governance is reviewed regularly.

• HOW OFTEN SHOULD YOU TEST? •

Run a full recovery simulation at least once per year and produce evidence that it was completed successfully.

- → **Quarterly reviews**
  Hold evidenced quarterly review sessions to keep governance, signers, and runbooks up to date.
- → **Annual recovery test**
  Run a full recovery simulation at least once per year and produce evidence that it was completed successfully.

• THE ANNUAL RECOVERY TEST •

1. Choose the scenario to test

Pick one realistic recovery scenario (examples):

- → Quorum cannot be reached (signer unavailable).
- → Key share / signing device lost.
- → Suspected compromise requiring key rotation.
- → Custody/signing service outage.

Goal:

Test a scenario that would force real decision-making.

2. Confirm governance and roles

Before the simulation begins, confirm:

- ✓ Recovery Incident Owner (RIO) and deputy are assigned.
- ✓ Approval matrix is up to date.
- ✓ Required participants are available.
- ✓ Comms approval process is defined.
- ✓ Recovery mode constraints are ready to apply (limits, allowlists, monitoring).

Goal:

Prove that recovery can be activated quickly and safely.

3. Validate backups

Before “executing recovery”, confirm:

- ✓ Backup materials exist.
- ✓ Backups can be validated.
- ✓ Storage locations and access controls are correct.
- ✓ Recovery materials are accounted for and current.

This supports the certification requirement that backup materials exist and are validated, with verified backup evidence.

4. Run the recovery simulation

Execute the runbook end-to-end in the correct order, including:

- ● Approvals and ACL checks.
- ○ Recovery actions (restore access, re-establish signing authority).
- ○ Required participants are available.
- ○ Validation gates (identity checks, destination checks, test transaction if appropriate).

Goal:

To prove that recovery is repeatable.

5. Validate success

A test is only successful if you can demonstrate that:

- ✓ Signing authority is restored correctly.
- ✓ Policy controls are active and enforced.
- ✓ Balances and records reconcile.
- ✓ Audit trail is complete and time-stamped.
- ✓ The organisation is safe to return to normal operations.

Goal:

Show you are back in control, with proof.

6. Produce evidence and certification outputs

Capture the required documentation so the test is defensible and reviewable.

CoinCover | Certified

CoinCover certification includes:

- ✓ A signed Business Certification Document proving readiness.
- ✓ An audit-ready Recovery Policy Document documenting workflows.
- ✓ Verified Backup Evidence.
- ✓ An Annual Recovery Test Certificate following the simulation.
- ✓ Evidenced quarterly review sessions.

Third-party & vendor readiness

Recovery depends on third-party ICT and custody providers that support wallet access, signing, monitoring, and operational controls. If a critical provider fails, recovery can stall — even if your internal teams are ready.

To reduce this risk, institutions should treat vendor readiness as part of recovery governance and maintain an ongoing view of supplier criticality, contractual rights, performance, and exit options.

• KEY CONTROLS •

1. Maintain a vendor registry, ranked by criticality

- → Keep an up-to-date registry of all ICT and custody-related suppliers.
- → Classify each provider by how critical they are to wallet operations and recovery (e.g., “critical”, “important”, “non-critical”).
- → This ensures recovery planning reflects real dependencies.

2. Contract for recovery-relevant rights

Ensure supplier contracts include the right to:

- → Access audit reports and relevant assurance (e.g., SOC reports or equivalent).
- → Receive timely incident notifications (with defined reporting timelines).
- → Access documented exit & transition plans.
- → Enforce service continuity requirements during incidents.

3. Monitor performance against defined metrics

Track provider performance on clear operational and security metrics, such as uptime, incident response times, recovery time objectives (RTOs), and support SLAs.

4. Maintain robust offboarding and transition plans

Have a clear strategy for switching providers without losing access, signing capability, or recovery pathways.

Offboarding plans should include:

- ✓ How keys/signers/policies are migrated or rotated.
- ✓ How access and authorisations are transferred.
- ✓ How recovery materials remain valid and available throughout the transition.

Goal:

Change providers without creating a new recovery risk.

5. Require independent security testing for critical providers

Critical third-party ICT providers should undergo independent, deep penetration testing on a scheduled basis (e.g., every three years) to uncover hidden weaknesses that standard controls can miss.

This helps ensure that recovery dependencies are resilient even under advanced attack conditions.

08 Practical recovery checklist

A clear, step-by-step guide for executing recovery under pressure.

• RECOVERY CHECKLIST •

This checklist reflects common failure points observed in institutional key loss and access unavailability events. Treat each unchecked item as a specific, remediable control gap.

When multiple gaps exist, access loss should be treated as a material operational resilience risk.

Contracts must assign clear roles during recovery events, mandate timely information, and include vendor obligations for access to system/infrastructure, personnel, and documentation needed for recovery validation.

1 Wallet inventory and custody architecture

- [ ] We maintain a complete, current inventory of all wallets, including chain, address, owner, and value or exposure.
- [ ] Each wallet has a documented purpose and criticality rating (treasury, settlement, client funds, operations).
- [ ] The signing model is documented and current for each wallet (MPC, multisig, HSM, custodian), including threshold rules.
- [ ] Dependencies are recorded per wallet (vendors, jurisdictions, signer locations, devices, systems).
- [ ] Documentation has a named owner, version control, and a defined review cycle.

2 Access resilience and authority

- [ ] We can meet quorum today if one signer or one signing device becomes unavailable.
- [ ] There is a documented signer replacement process, including who approves replacement and how it is executed.
- [ ] Recovery incident declaration authority is clearly defined (who can trigger recovery and under what criteria).
- [ ] Recovery approvals are clearly defined (who can approve migrations, key reconstruction, signer changes, constraints).
- [ ] No wallet is dependent on a single individual, single device, or single physical location without an approved exception and mitigation.

3 Recovery material and key governance

- [ ] Recovery material locations are known, access-controlled, and auditable (who can access, how, and when).
- [ ] Recovery material handling is classified as sensitive, with clear rules for storage, access, and transfer.
- [ ] Recoverability has been tested within the last 12 months for critical wallets, with evidence retained.
- [ ] Rotation and deprecation rules exist when wallets, signers, or vendors change.
- [ ] Obsolete recovery material is securely retired and disposal is documented.

4 Execution controls and validation

- [ ] Recovery actions require identity verification of participants and dual control for high-risk steps.
- [ ] Destination address verification is independent and enforced for any recovery fund movement.
- [ ] Canary transactions are used before moving material value or resuming normal service levels.
- [ ] On-chain balances are reconciled to internal ledgers before returning to normal operations.
- [ ] We can meet quorum today if one signer or one signing device becomes unavailable.

5 Evidence, compliance, and reporting readiness

- [ ] Recovery actions and authorities are explicitly authorised in policy and mapped to applicable regulations.
- [ ] We can produce an audit-ready evidence pack within 24 to 72 hours (timeline, approvals, logs, reconciliation, comms).
- [ ] Regulatory notification obligations are mapped to scenarios and have owners, templates, and timelines.
- [ ] Recovery exercises are conducted regularly (tabletop at least quarterly for critical scenarios).
- [ ] Issues found during testing are tracked to closure and re-tested.

Interpretation

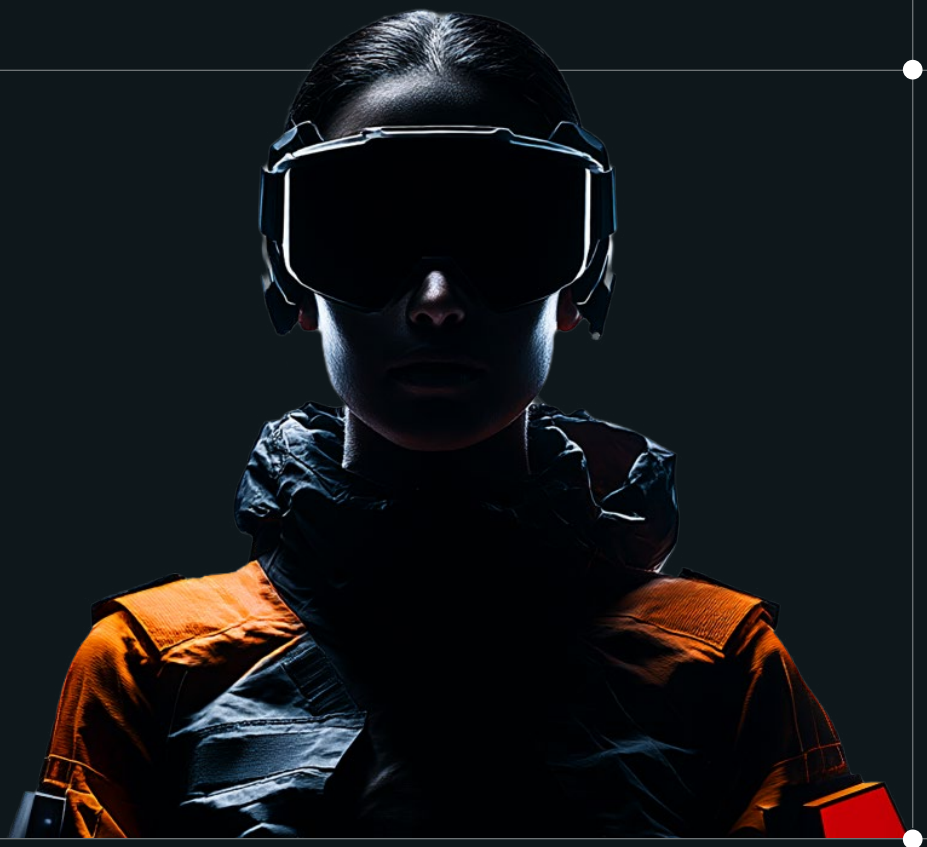
If more than a few boxes are unchecked, recovery risk is already material. If any unchecked box relates to high-value or client-asset wallets, treat it as an urgent remediation item.

COINCOVER.COM →

09 Get started

This playbook is a starting point, not the finish line. The real work is turning it into a repeatable routine: assign ownership, test it, capture evidence, and communicate with discipline.

COINCOVER.COM →



Recovery is a test of institutional control

Crypto wallet recovery is no longer a specialist concern reserved for security teams. It is a fundamental test of whether an institution truly controls the digital assets it holds, manages, or safeguards on behalf of clients.

In markets governed by cryptographic authority, ownership is exercised through access. When access fails, legal entitlement alone does not restore operational control.

The industry has reached a more mature understanding of what drives real loss. Recovery material that cannot be located, signers who cannot be assembled, thresholds that cannot be met in practice, and governance pathways that break under pressure remain the most common causes of irreversible inaccessibility.

Recovery is what keeps an institution in control when wallet access fails. In digital assets, you don't get second chances. The organisations that can execute recovery quickly and safely reduce disruption, protect clients, and preserve trust under pressure.

CoinCover

HELLO@COINCOVER.COM

CoinCover partners with leading exchanges and custodians worldwide to strengthen resilience and protect access to digital assets. CoinCover Recover for Institutions is designed to help organisations maintain and restore cryptographic access with governance, speed, and auditability. We support institutions in building recovery capability as an operational standard.

If you are already a customer, use your dedicated recovery channel for priority support aligned to your agreed recovery operating model. If you are assessing CoinCover for the first time, our team can walk you through a readiness assessment, identify recoverability gaps across wallets, people, and processes, and define a practical roadmap to reach an institutional standard of recovery.

Recovery starts with a conversation.
The objective is simple. Ensure access can be restored quickly, safely, and with proof.

GET IN TOUCH →