# Stablecoin unavailable, wallet blocked, network interrupted:

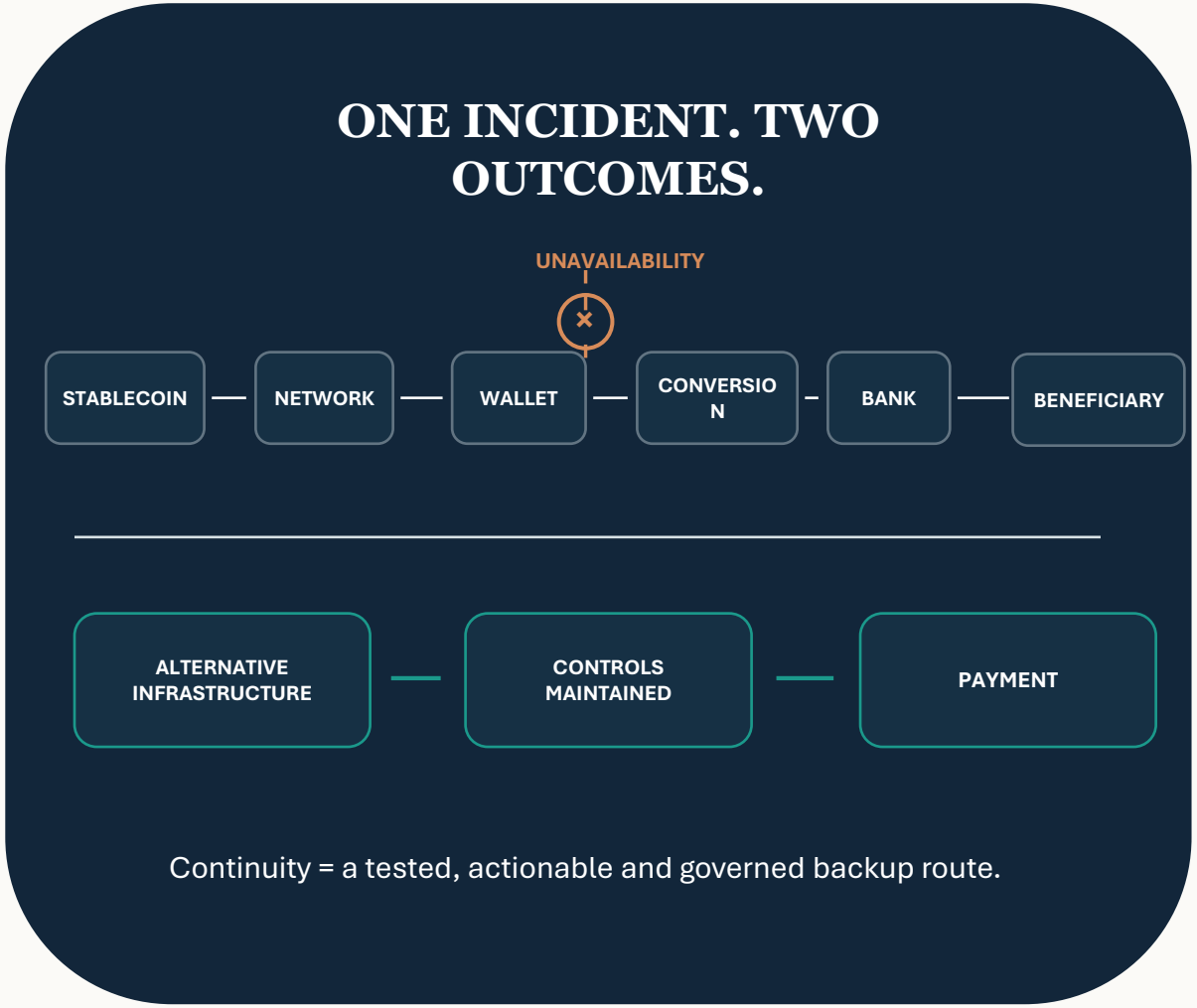
## Can your company keep paying?

Building a continuity plan for stablecoin payments

An incident can affect the stablecoin, the network, the wallet, the custodian, the conversion platform, the bank or internal access rights. The real question is not whether the infrastructure works today, but how long your company can keep paying if it stops working tomorrow morning.

**Objective**

Identify critical dependencies, single points of failure and trigger conditions in order to build a truly actionable plan B.

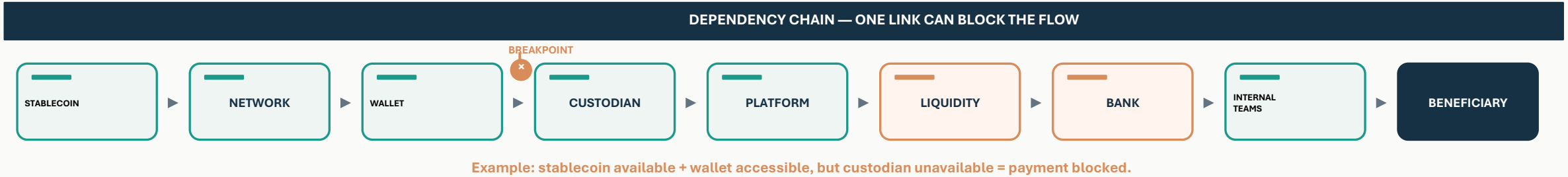


PAGE 02 • DECISION SUMMARY

# Your continuity depends on several links

## A payment can become impossible even if the stablecoin itself still works.

The failure point may sit in the infrastructure, liquidity, the bank or the internal organization.




Example: stablecoin available + wallet accessible, but custodian unavailable = payment blocked.

### THE GUIDE FOLLOWS 6 ACTIONS

1. **IDENTIFY** dependencies
2. **PRIORITIZE** critical flows
3. **PREPARE** backup routes
4. **TEST** the real switchover
5. **SWITCH** based on thresholds
6. **RECONCILE** after the incident

**WHAT EXECUTIVES SHOULD REMEMBER**

**Do not count your providers: count the routes that are truly independent, tested and actionable end to end.**

SOURCES

1. CPMI / Bank for International Settlements — Considerations for the use of stablecoin arrangements in cross-border payments, 31 October 2023. Link

2. Financial Stability Board — High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 17 July 2023. Link

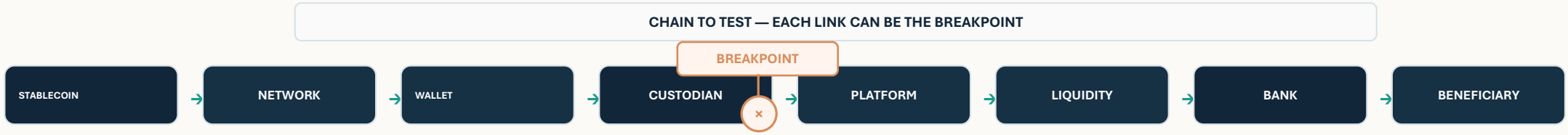
Qualification: the diagram is a resilience and internal-control good practice. The cited FSB recommendations are addressed to authorities and do not, by themselves, create a general obligation for every company.

PAGE 03 • DEPENDENCY MAPPING

# Where can your company actually fail?

## A payment can be blocked by an invisible link — even if the stablecoin still works.

Continuity starts with an honest map: asset, network, access, custody, conversion, liquidity, bank, teams and beneficiary. The critical risk is the single point of failure: one blockage is enough to stop the payment.




### 1 ASSET & NETWORK

Stablecoin unavailable or mint/redeem suspended · network unusable · severe congestion or exceptional fees.

### 2 ACCESS & CUSTODY

Wallet blocked · custodian unavailable · API outage · loss or absence of an authorized employee.

### 3 CONVERSION, LIQUIDITY & BANK

Platform unavailable · insufficient liquidity · fiat withdrawal impossible · bank account or traditional rail unavailable.

### 4 COMPLIANCE & BENEFICIARY

New regulatory restriction · KYT/sanctions alert · beneficiary unable to receive via the planned route.

**WHAT EXECUTIVES SHOULD REMEMBER**

**Your “plan B” only truly exists if its route does not share the same breakpoint as the main route.**

SOURCES

1. CPMI / Bank for International Settlements — Considerations for the use of stablecoin arrangements in cross-border payments, 31 October 2023. Link
2. Financial Stability Board — High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 17 July 2023. Link
3. EUR-Lex — Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, 14 December 2022. Link
4. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010. Link

PAGE 04 • CRITICAL FLOWS

# Which payments must continue first?

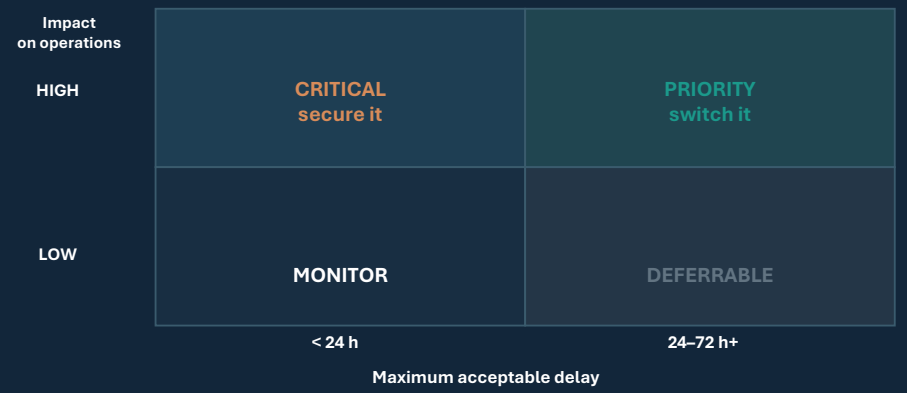
## Plan B first protects the flows whose delay blocks operations.

Before choosing a backup route, classify each payment by maximum acceptable delay, financial or legal impact, deferral options and the existence of a substitute route.

### CLASSIFY FLOWS BEFORE THE INCIDENT

| | | |
|---|---|---|
| 1 | **MUST CONTINUE**<br>**Max delay: immediate to 24h** | Essential supplier · payroll/critical contractor · contractual deadline with penalty. |
| 2 | **SWITCH UNDER THRESHOLD**<br>**Max delay: 24 to 72h** | Sensitive customer refund · intragroup transfer · urgent international payment. |
| 3 | **DEFER / MONITOR**<br>**Max delay: beyond 72h** | Non-operational payment · non-critical supplier · transaction with no immediate penalty. |

### PRIORITY MATRIX




Amount alone is not enough: a small payment can be critical if it blocks a delivery or a contractual obligation.

### THE 6 QUESTIONS TO DOCUMENT FOR EACH FLOW

- Criticality
- Max delay
- Amount
- Deferrable?
- Substitute?
- Legal impact

**WHAT EXECUTIVES SHOULD REMEMBER**

**The priority payment is not always the largest amount: it is the one whose delay blocks operations, creates a penalty or prevents the company from meeting an essential commitment.**

SOURCES

1. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010. Link
2. ISO — ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements. Link
3. EUR-Lex — Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, 14 December 2022. Link

These references support a continuity good practice; DORA is sector-specific and does not apply universally.

# Where are your hidden concentrations?

## Several providers do not necessarily create several independent routes.

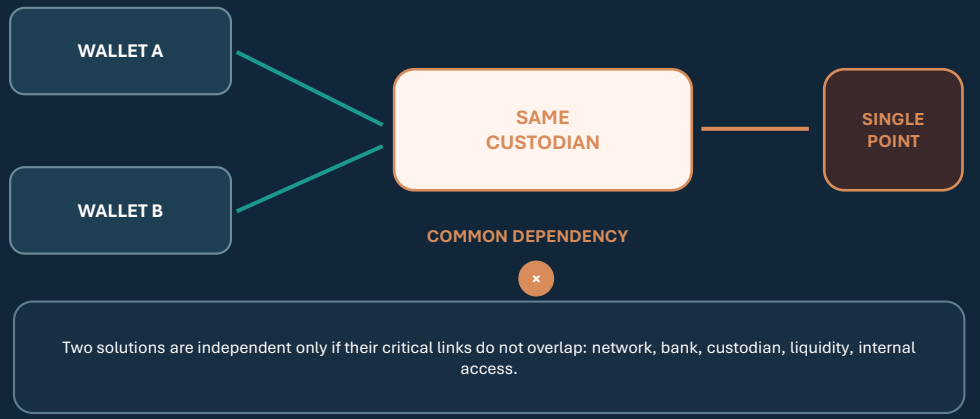
Two wallets, two platforms or two banks can depend on the same stablecoin, the same network, the same custodian, the same bank account or the same authorized person.

### MAP CONCENTRATIONS

| LINK | CONCENTRATION | COMMON DEPENDENCY TO CHECK |
|---|---|---|
| Stablecoin | One asset used | Same issuer, same reserve, same redemption right |
| Network | One on-chain rail | Congestion, outage, extreme fees or unsupported network |
| Custody | Multiple wallets in appearance | Same custodian, technology provider or access rights |
| Conversion | One off-ramp | Same platform, liquidity or exit bank |
| Bank | One critical account | Withdrawal impossible if banking incident or local restriction |
| Team | One key person | Rights, approvals, 2FA, process knowledge |

### DIVERSIFICATION IS NOT CONTINUITY

Plan B must break common dependencies.




### TEST BEFORE APPROVING PLAN B

Same stablecoin? | Same network? | Same custodian? | Same bank? | Same key person?

**WHAT EXECUTIVES SHOULD REMEMBER**

**Having several providers is not enough: continuity exists only if the alternative route can operate without the same critical link as the main route.**

SOURCES

1. CPMI-IOSCO — Application of the Principles for Financial Market Infrastructures to stablecoin arrangements, July 2022. Link
2. CPMI — Considerations for the Use of Stablecoin Arrangements in Cross-border Payments, October 2023. Link
3. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010. Link
4. ISO — ISO 22301:2019, Business continuity management systems — Requirements. Link

# Build a backup solution that is actually usable

## Your plan B exists only if it can execute a real payment while keeping controls in place.

An alternative opened “just in case” is not enough. It must be actionable within the deadline, have liquidity, be compliant, be authorized by the right people and not depend on the same breakpoint as the main route.

### CHOOSE A BACKUP ROUTE — NOT A THEORETICAL OPTION

| OPTION | WHAT IT COVERS | CHECK BEFORE APPROVAL |
|---|---|---|
| Alternative stablecoin or network | Asset or rail incident | Real liquidity, fees, network supported by the beneficiary |
| Second wallet | Access and execution | Rights, 2FA, thresholds and tested payment procedure |
| Second custodian or platform | Custody, off-ramp, conversion | Common dependencies, transaction limits and SLA |
| Traditional banking route | Backup fiat payment | Active account, registered beneficiaries, cut-off and delays |
| Bank liquidity reserve | Payment without conversion | Buffer amount, usage rules and replenishment |

**TO VALIDATE: the backup solution must not bypass essential controls or recreate the same single point of failure.**

### PROOF OF ACTIVATION

A backup route is valid only if it meets 4 conditions.

1. **OPEN** — Accounts, wallets and access ready
2. **FUNDED** — Available liquidity or confirmed credit
3. **AUTHORIZED** — Roles, thresholds and approvals known
4. **TESTED** — Real payment or documented test

**Untested = unavailable on incident day**

**WHAT EXECUTIVES SHOULD REMEMBER** — **A backup solution is not the one that exists on paper: it is the one that can pay, convert and document the transaction within the acceptable deadline.**

SOURCES

1. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010.
2. ISO — ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements.
3. CPMI — Considerations for the Use of Stablecoin Arrangements in Cross-border Payments, 31 October 2023.
4. FSB — High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 17 July 2023.

# When should plan B be triggered?

## Plan B is triggered based on written thresholds.

The objective is neither to switch too early nor to wait for a critical payment to fail. Each level must specify the event, possible decision, authorized people and controls maintained.

### TRIGGER MATRIX — FROM SIGNAL TO SUSPENSION

| LEVEL | EVENT | DECISION | AUTHORITY |
|---|---|---|---|
| MONITORING | Weak signals: slowness, abnormal fees, liquidity or networl | Strengthen monitoring; prepare evidence and alte | Treasury + IT |
| DEGRADED MODE | Unavailability beyond the short threshold or slower convers | Prioritize flows; reserve liquidity; prepare the swit | CFO / treasurer |
| PARTIAL SWITCHOVER | Critical transaction impossible or main route unstable. | Use the backup route for priority flows. | CFO + compliance |
| FULL SWITCHOVER | Wallet, custodian, network, platform or bank unavailable. | Switch authorized payments to the validated infra | Authorized management |
| SUSPEND | Uncontrolled sanctions, security or compliance alert. | Block affected payments until formal decision. | Management + compliance |

**DEFINE BEFORE THE INCIDENT: duration, critical amount, minimum liquidity, compliance and authorized decision-maker.**

## WHO CAN DECIDE?

The switchover must be governed: detecting is not deciding, and deciding is not executing alone.

1. **DETECTION**
   Treasury, IT or provider reports the incident.
2. **QUALIFY**
   Impacted flows, liquidity, compliance and beneficiaries.
3. **DECISION**
   Level activated according to thresholds and written delegation.
4. **EXECUTION**
   Alternative payment with controls maintained.

**No urgency without checking beneficiary, network, address, authorization and retained evidence.**

**WHAT EXECUTIVES SHOULD REMEMBER** — **The right time to switch is the one planned before the incident: thresholds, roles and controls must already be written.**

SOURCES

1. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010.
2. ISO — ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements.
3. ISO — ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance.
4. CPMI — Considerations for the Use of Stablecoin Arrangements in Cross-border Payments, 31 October 2023.

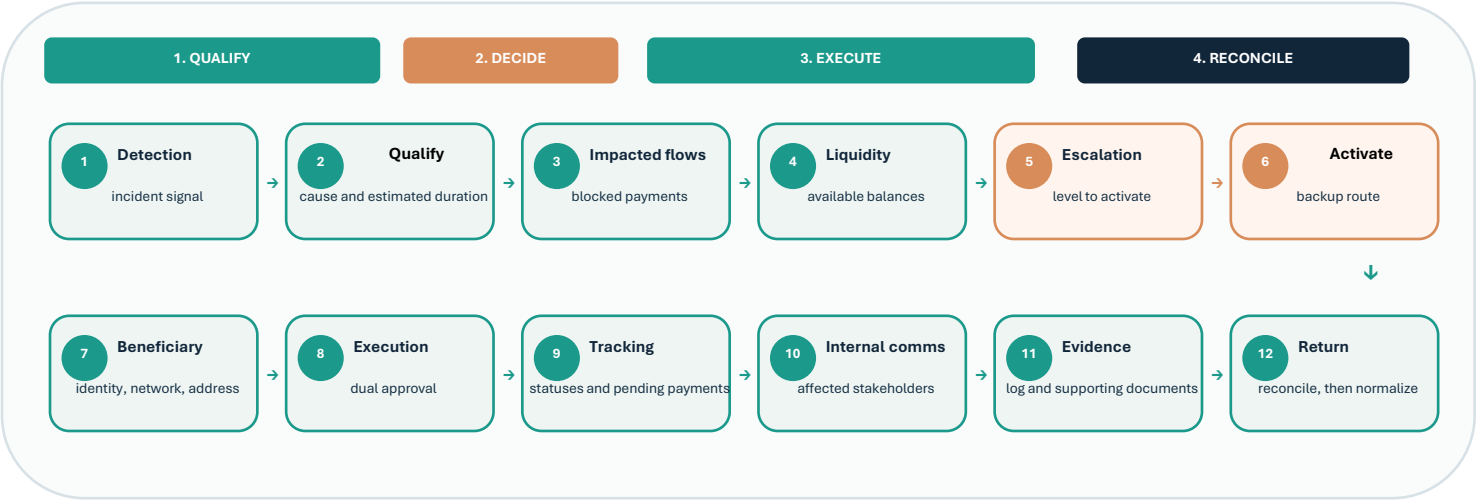
PAGE 08 • CONTINUITY RUNBOOK

# The incident-day runbook

## Urgency does not authorize improvisation.

The runbook turns the incident into an action sequence: who alerts, who qualifies, who decides, who executes, what evidence to keep and how to avoid double payment.

### RUNBOOK — FROM SIGNAL TO RETURN TO NORMAL




## WHO DOES WHAT?

The procedure must separate alerting, decision, execution and control.

**CALLS / ALERTS** — **Treasury · IT · provider**
Reports the blockage and timestamps the incident.

**DECIDES** — **CFO / treasurer + compliance**
Activates the level defined by the matrix.

**EXECUTES** — **Authorized operators**
Uses the authorized route, with four-eye review.

**CONTROLS** — **Accounting / internal control**
Avoids duplicates, missing evidence and balance gaps.

**Preserve even in urgency: authorization, compliance, evidence, reconciliation.**

**NON-NEGOTIABLE CONTROLS**

beneficiary | network | address | authorization | compliance | evidence | anti-double payment

**WHAT EXECUTIVES SHOULD REMEMBER**

**On incident day, the priority is to execute without losing control: every payment must remain authorized, traceable and reconcilable.**

SOURCES

1. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010.
2. ISO — ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements.
3. CPMI — Considerations for the Use of Stablecoin Arrangements in Cross-border Payments, 31 October 2023.
4. ISO — ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance.

PAGE 09 • CONTINUITY TESTS

# Test the plan before you need it

## An untested plan remains an assumption.

The test must prove that the backup route is accessible, authorized people can act, controls hold, and the payment can be tracked then reconciled.

### OBLIGATION OR GOOD PRACTICE?

Ordinary company: resilience and internal-control good practice.
EU financial entity in DORA scope: formal test requirements apply depending on status and proportionality.

**Never present DORA as a universal obligation.**

TEST TABLE — COMPLETE AFTER EACH EXERCISE

| SCENARIO | IMPACT | ALTERNATIVE SOLUTION | SWITCHOVER TIME | TEST RESULT | CORRECTIVE ACTION |
|---|---|---|---|---|---|
| **Stablecoin / redemption unavailable** | Urgent supplier blocked | Approved stablecoin or banking rail | ____ **min/h** | OK / FAIL ___ | _____ |
| **Network unavailable** | On-chain payment impossible | Preconfigured alternative network | ____ **min/h** | OK / FAIL ___ | _____ |
| **Wallet / custodian inaccessible** | Funds or rights inaccessible | Second wallet / independent custodian | ____ **min/h** | OK / FAIL ___ | _____ |
| **Conversion / bank unavailable** | Fiat unavailable at due date | Second off-ramp / account + fiat reserve | ____ **min/h** | OK / FAIL ___ | _____ |
| **Key employee absent** | Signature / access blocked | Delegation + authorized backup person | ____ **min/h** | OK / FAIL ___ | _____ |
| **Beneficiary cannot receive usual route** | Settlement delayed | Address / alternative rail pre-validated | ____ **min/h** | OK / FAIL ___ | _____ |

### A TEST MUST PRODUCE EVIDENCE

Not just a scenario meeting.

1. **SIMULATE**
   Cut off a defined link without warning the executing team.
2. **SWITCH**
   Actually use the alternative route and backup access.
3. **MEASURE**
   Time it, record failures, control gaps and duplicate-payment risks.
4. **CORRECT**
   Assign an owner, a deadline, then replay the scenario.

**REPLAY THE PLAN IF:** provider | wallet / network | authorizations | limits | bank / off-ramp | regulation

**WHAT EXECUTIVES SHOULD REMEMBER**

**Plan B only truly exists when it has been tested, timed, documented and corrected — with the same essential controls as the main route.**

SOURCES

1. EUR-Lex — Regulation (EU) 2022/2554 (DORA), Arts. 24–25, 14 Dec. 2022. Link

2. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010. Link

PAGE 10 • FINAL CHECKLIST

# Can your company keep paying tomorrow morning?

## Eleven simple checks: what is not open, authorized, funded and tested remains an assumption.

Tick “OK” only if the setup is usable on incident day, with an accessible route, an authorized person and retained evidence.

### QUICK DIAGNOSTIC — CHECK BEFORE DEPLOYMENT

| | CRITERION | | OK | PARTIAL | NO |
|---|---|---|---|---|---|
| 1 | Critical flows identified | suppliers, payroll, refunds, deadlines | ☐ | ☐ | ☐ |
| 2 | Dependencies mapped | stablecoin, network, wallet, bank, team | ☐ | ☐ | ☐ |
| 3 | Single points known | no invisible critical link | ☐ | ☐ | ☐ |
| 4 | Alternatives opened | wallet, custodian, conversion or banking route | ☐ | ☐ | ☐ |
| 5 | Access available | rights, keys, API, accounts and limits checked | ☐ | ☐ | ☐ |
| 6 | Backup people authorized | key-person absence covered | ☐ | ☐ | ☐ |
| 7 | Liquidity actually mobilizable | stablecoin, fiat, off-ramp and bank | ☐ | ☐ | ☐ |
| 8 | Switchover thresholds defined | monitoring, degraded, switchover, suspension | ☐ | ☐ | ☐ |
| 9 | Operational runbook | who alerts, decides, executes and controls | ☐ | ☐ | ☐ |
| 10 | Plan tested and corrected | timed scenarios, evidence retained | ☐ | ☐ | ☐ |
| 11 | Return to normal planned | reconciliation, duplicates, balances and reporting | ☐ | ☐ | ☐ |

## RESILIENCE MATRIX

The level depends on the number of criteria that are actually operational.

**RESILIENT** — 10–11 OK
Actionable, tested and controlled plan B.

**RESILIENT WITH CONDITIONS** — 7–9 OK
Switchover possible; targeted fixes required.

**VULNERABLE** — 4–6 OK
Uncertain continuity: dependencies to reduce.

**CRITICAL** — 0–3 OK
First incident = risk of payment blockage.

**Decision: if a critical flow has no tested backup route, it remains a priority to address.**

**WHAT EXECUTIVES SHOULD REMEMBER**

**Continuity is not an intention: it is the proven ability to pay another way without losing authorization, compliance, evidence and reconciliation.**

SOURCES

1. ISO — ISO 22301:2019, Security and resilience — BCMS requirements. Link 2. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010. Link
3. CPMI / Bank for International Settlements — Considerations for the Use of Stablecoin Arrangements in Cross-border Payments, 31 October 2023. Link