

Stablecoin indisponible, wallet bloqué, réseau interrompu :

Votre entreprise peut-elle continuer à payer ?

Préparer un plan de continuité des paiements en stablecoins

Un incident peut affecter le stablecoin, le réseau, le wallet, le dépositaire, la plateforme de conversion, la banque ou les accès internes. La vraie question n'est pas de savoir si l'infrastructure fonctionne aujourd'hui, mais combien de temps votre entreprise peut continuer à payer si elle cesse de fonctionner demain matin.

Objectif

Identifier les dépendances critiques, les points uniques de défaillance et les conditions de bascule afin de construire un plan B réellement activable.

UN INCIDENT. DEUX ISSUES.

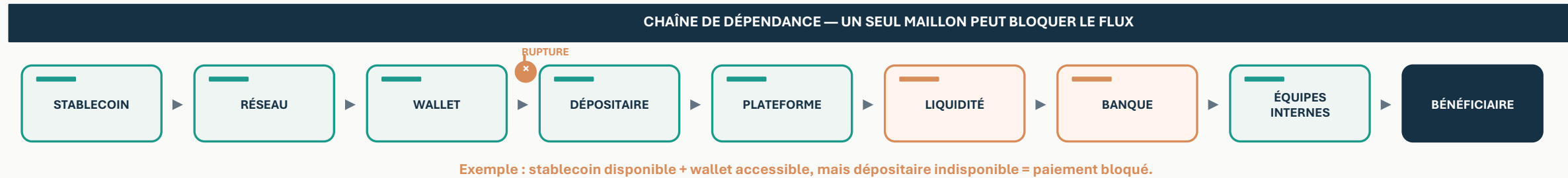


Continuité = solution de secours testée, activable et gouvernée.

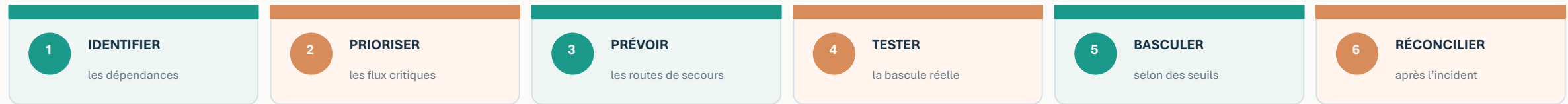
Votre continuité dépend de plusieurs maillons

Un paiement peut devenir impossible même si le stablecoin lui-même continue à fonctionner.

Le point de rupture peut se situer dans l’infrastructure, la liquidité, la banque ou l’organisation interne.



LE GUIDE SUIV 6 ACTIONS



CE QU’UN DIRIGEANT DOIT RETENIR

Ne comptez pas vos prestataires : comptez vos chemins réellement indépendants, testés et activables de bout en bout.

SOURCES

1. CPMI / Banque des règlements internationaux — Considerations for the use of stablecoin arrangements in cross-border payments, 31 octobre 2023. [Lien](#)

2. Financial Stability Board — High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 17 juillet 2023. [Lien](#)

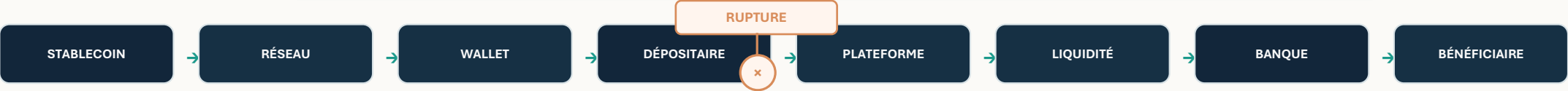
Qualification : le schéma présenté est une bonne pratique de résilience et de contrôle interne. Les recommandations FSB citées s'adressent aux autorités et ne constituent pas, à elles seules, une obligation générale applicable à toute entreprise.

Où votre entreprise peut-elle réellement tomber en panne ?

Un paiement peut être bloqué par un maillon invisible — même si le stablecoin fonctionne encore.

La continuité commence par une cartographie honnête : actif, réseau, accès, garde, conversion, liquidité, banque, équipes et bénéficiaire.
Le risque critique est le point unique de défaillance : un seul blocage suffit à arrêter le paiement.

CHAÎNE À TESTER — CHAQUE MAILLON PEUT ÊTRE LE POINT DE RUPTURE



1 ACTIF & RÉSEAU

Stablecoin indisponible ou mint/redeem suspendu · réseau inutilisable · congestion sévère ou frais exceptionnels.

2 ACCÈS & CONSERVATION

Wallet bloqué · dépositaire indisponible · API en panne · perte ou absence d'un collaborateur habilité.

3 CONVERSION, LIQUIDITÉ & BANQUE

Plateforme indisponible · liquidité insuffisante · retrait fiat impossible · compte bancaire ou rail traditionnel indisponible.

4 CONFORMITÉ & BÉNÉFICIAIRE

Restriction réglementaire nouvelle · alerte KYT/sanctions · bénéficiaire incapable de recevoir sur la route prévue.

CE QU'UN DIRIGEANT DOIT RETENIR

Votre “plan B” n'existe vraiment que si sa route ne partage pas le même point de rupture que la route principale.

SOURCES

- 1. CPMI / Banque des règlements internationaux — Considerations for the use of stablecoin arrangements in cross-border payments, 31 octobre 2023. [Lien](#)
- 2. Financial Stability Board — High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 17 juillet 2023. [Lien](#)
- 3. EUR-Lex — Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, 14 décembre 2022. [Lien](#)
- 4. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, mai 2010. [Lien](#)

Quels paiements doivent continuer en priorité ?

Le plan B protège d’abord les flux dont le retard bloque l’activité.

Avant de choisir une route de secours, classez chaque paiement selon son délai maximum acceptable, son impact financier ou juridique, sa possibilité de report et l’existence d’un moyen de substitution.

CLASSER LES FLUX AVANT L’INCIDENT

1	À MAINTENIR Délai max : immédiat à 24 h	Fournisseur indispensable · paie/prestataire critique · échéance contractuelle avec pénalité.
2	À BASCULER SOUS SEUIL Délai max : 24 à 72 h	Remboursement client sensible · transfert intra-groupe · paiement international urgent.
3	À REPORTER / SUIVRE Délai max : au-delà de 72 h	Paiement non opérationnel · fournisseur non critique · opération sans pénalité immédiate.

LES 6 QUESTIONS À RENSEIGNER POUR CHAQUE FLUX

Criticité	Délai max	Montant	Report possible ?	Substitution ?	Impact juridique
-----------	-----------	---------	-------------------	----------------	------------------

CE QU’UN DIRIGEANT DOIT RETENIR

Le paiement prioritaire n’est pas toujours le plus gros montant : c’est celui dont le retard bloque l’activité, crée une pénalité ou empêche l’entreprise de respecter un engagement essentiel.

MATRICE DE PRIORITÉ

Impact
sur l’activité

FORT

**CRITIQUE
à sécuriser**

**PRIORITAIRE
à basculer**

FAIBLE

À SURVEILLER

REPORTABLE

< 24 h

24–72 h+

Délai maximum acceptable

Le montant seul ne suffit pas : un petit paiement peut être critique s’il bloque une livraison ou une obligation contractuelle.

SOURCES

1. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, mai 2010. [Lien](#)

3. EUR-Lex — Règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier, 14 décembre 2022. [Lien](#)

2. ISO — ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements. [Lien](#)

Ces références fondent une bonne pratique de continuité ; DORA est sectoriel et ne s’applique pas universellement.

Où sont vos concentrations cachées ?

Plusieurs prestataires ne créent pas forcément plusieurs routes indépendantes.

Deux wallets, deux plateformes ou deux banques peuvent dépendre du même stablecoin, du même réseau, du même dépositaire, du même compte bancaire ou de la même personne habilitée.

CARTOGRAPHIER LES CONCENTRATIONS

MAILLON	CONCENTRATION	DÉPENDANCE COMMUNE À VÉRIFIER
Stablecoin	Un seul actif utilisé	Même émetteur, même réserve, même droit de remboursement
Réseau	Un seul rail on-chain	Congestion, arrêt, frais extrêmes ou réseau non supporté
Conservation	Wallets multiples en apparence	Même custodien, même fournisseur technologique ou même accès
Conversion	Un seul off-ramp	Même plateforme, même liquidité, même banque de sortie
Banque	Un seul compte critique	Retrait impossible si incident bancaire ou restriction locale
Équipe	Une seule personne clé	Droits, validations, 2FA, connaissance de la procédure

À TESTER AVANT DE VALIDER LE PLAN B

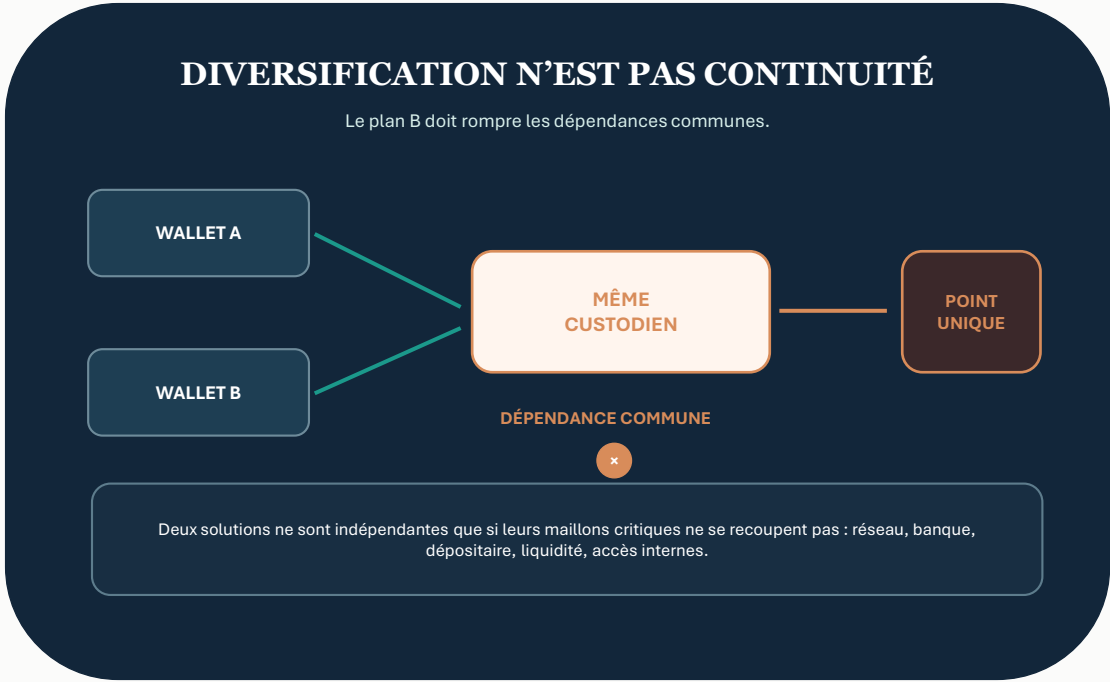
Même stablecoin ?

Même réseau ?

Même dépositaire ?

Même banque ?

Même personne clé ?



CE QU’UN DIRIGEANT DOIT RETENIR

Avoir plusieurs prestataires ne suffit pas : la continuité existe seulement si la route alternative peut fonctionner sans le même maillon critique que la route principale.

SOURCES

- CPMI-IOSCO — Application of the Principles for Financial Market Infrastructures to stablecoin arrangements, juillet 2022. [Lien](#)
- CPMI — Considerations for the Use of Stablecoin Arrangements in Cross-border Payments, octobre 2023. [Lien](#)
- NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, mai 2010. [Lien](#)

- CPMI — Considerations for the Use of Stablecoin Arrangements in Cross-border Payments, octobre 2023. [Lien](#)
- ISO — ISO 22301:2019, Business continuity management systems — Requirements. [Lien](#)

Construire une solution de secours réellement utilisable

Votre plan B n'existe que s'il peut exécuter un paiement réel, avec des contrôles maintenus.

Une alternative ouverte “au cas où” ne suffit pas. Elle doit être activable dans les délais, disposer de liquidité, être conforme, autorisée par les bonnes personnes et ne pas dépendre du même point de rupture que la route principale.

CHOISIR UNE ROUTE DE SECOURS — PAS UNE OPTION THÉORIQUE

OPTION	CE QUE ÇA COUVRE	À VÉRIFIER AVANT DE L'APPROUVER
Stablecoin ou réseau alternatif	Incident actif ou rail	Liquidité réelle, frais, réseau supporté par le bénéficiaire
Second wallet	Accès et exécution	Droits, 2FA, seuils et procédure de paiement testés
Second custodien ou plateforme	Garde, off-ramp, conversion	Dépendances communes, limites transactionnelles et SLA
Route bancaire traditionnelle	Paiement fiat de secours	Compte actif, bénéficiaires enregistrés, cut-off et délais
Réserve bancaire de liquidité	Paiement sans conversion	Montant tampon, règles d'usage et reconstitution

À VALIDER : la solution de secours ne doit pas contourner les contrôles essentiels ni recréer le même point unique de défaillance.

CE QU'UN DIRIGEANT DOIT RETENIR

Une solution de secours n'est pas celle qui existe sur le papier : c'est celle qui peut payer, convertir et documenter l'opération dans le délai acceptable.

SOURCES

1. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, mai 2010. [Lien](#)
3. CPMI — Considerations for the Use of Stablecoin Arrangements in Cross-border Payments, 31 octobre 2023. [Lien](#)

2. ISO — ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements. [Lien](#)
4. FSB — High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 17 juillet 2023. [Lien](#)

LA PREUVE D'ACTIVATION

Une route de secours est valable seulement si elle réunit 4 conditions.

1

OUVERTE

Comptes, wallets et accès prêts

2

FINANCÉE

Liquidité disponible ou crédit confirmé

3

AUTORISÉE

Rôles, seuils et validations connus

4

TESTÉE

Paiement réel ou test documenté

Non testée = non disponible le jour de l'incident

Quand faut-il déclencher le plan B ?

Un plan B se déclenche selon des seuils écrits.

L’objectif n’est pas de basculer trop tôt, ni d’attendre qu’un paiement critique échoue. Chaque niveau doit préciser l’événement

MATRICE DE DÉCLENCHEMENT — DU SIGNAL À LA SUSPENSION

NIVEAU	ÉVÉNEMENT	DÉCISION	AUTORITÉ
SURVEILLANCE	Signaux faibles : lenteurs, frais anormaux, alertes liquidité	Renforcer le suivi ; préparer les preuves et alterna	Trésorerie + SI
MODE DÉGRADÉ	Indisponibilité au-delà du seuil court ou conversion ralentie	Prioriser les flux ; réserver la liquidité ; préparer la	DAF / trésorier
BASCULE PARTIELLE	Transaction critique impossible ou route principale instable	Utiliser la route de secours pour les flux prioritaire	DAF + conformité
BASCULE COMPLÈTE	Wallet, custodien, réseau, plateforme ou banque indisponi	Basculer les paiements autorisés sur l’infrastruct	Direction habilitée
SUSPENSION	Alerte sanctions, sécurité ou conformité non maîtrisée.	Bloquer les paiements concernés jusqu’à décisio	Direction + conformité

À FIXER AVANT L’INCIDENT : durée, montant critique, liquidité minimale, conformité et personne habilitée.

CE QU’UN DIRIGEANT DOIT RETENIR

Le bon moment pour basculer est celui qui a été prévu avant l’incident : seuils, rôles et contrôles doivent déjà être écrits.

SOURCES

1. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, mai 2010. Lien

3. ISO — ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance. Lien
2. ISO — ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements. Lien

4. CPMI — Considerations for the Use of Stablecoin Arrangements in Cross-border Payments, 31 octobre 2023. Lien

QUI PEUT DÉCIDER ?

La bascule doit être gouvernée : détecter n’est pas décider, et décider n’est pas exécuter seul

1 DÉTECTION
Trésorerie, SI ou prestataire signale l’incident.



2 QUALIFICATION
Flux impactés, liquidité, conformité et bénéficiaires.



3 DÉCISION
Niveau activé selon seuils et délégation écrite.



4 EXÉCUTION
Paiement alternatif avec contrôles maintenus.

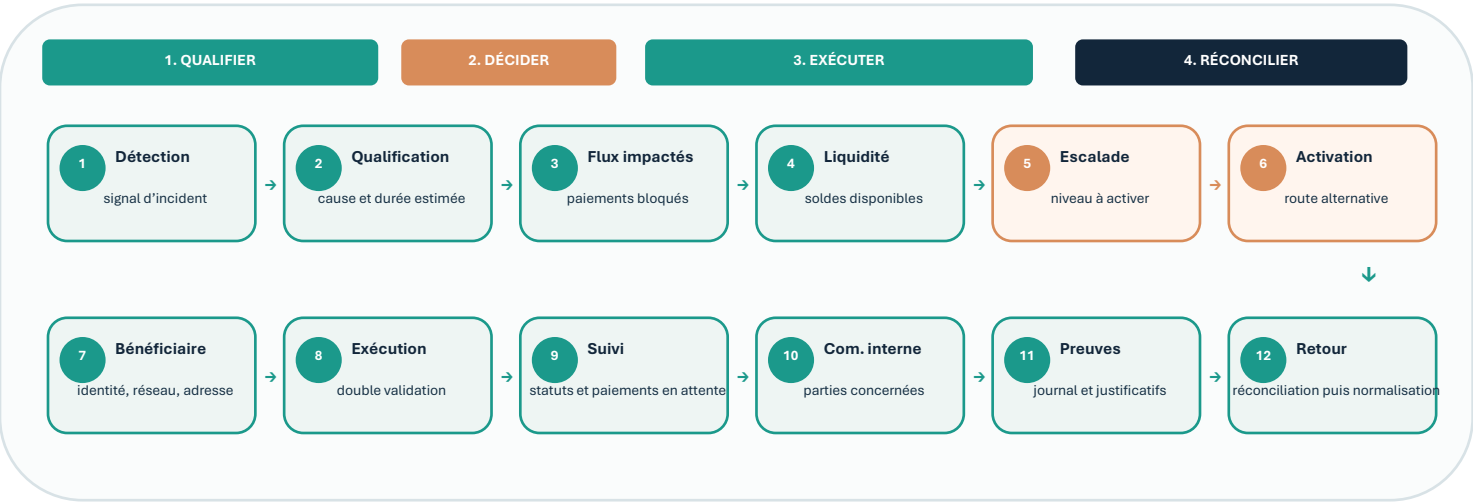
Ja d’urgence sans contrôle bénéficiaire, réseau, adresse, autorisation et preuve con

Le runbook du jour d'incident

L'urgence n'autorise pas l'improvisation.

Le runbook transforme l'incident en séquence d'actions : qui alerte, qui qualifie, qui décide, qui exécute, quelles preuves conserver

RUNBOOK — DU SIGNAL AU RETOUR À LA NORMALE



QUI FAIT QUOI ?

La procédure doit séparer l'alerte, la décision, l'exécution et le contrôle.

APPELLE / ALERTE	Trésorerie • SI • prestataire
Signale le blocage et horodate l'incident.	
DÉCIDE	DAF / trésorier + conformité
Active le niveau prévu par la matrice.	
EXÉCUTE	Opérateurs habilités
Utilise la route autorisée, avec double regard.	
CONTRÔLE	Comptabilité / contrôle interne
Évite doublons, preuves manquantes et écarts de soldes.	
À préserver même en urgence : autorisation, conformité, preuve, rapprochement.	

CONTRÔLES NON NÉGOCIABLES

bénéficiaire

réseau

adresse

autorisation

conformité

preuve

anti-double paiement

CE QU'UN DIRIGEANT DOIT RETENIR

Le jour de l'incident, la priorité est d'exécuter sans perdre le contrôle : chaque paiement doit rester autorisé, tracé et réconciliable.

SOURCES

1. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, mai 2010. Lien

2. ISO — ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements. Lien

3. CPMI — Considerations for the Use of Stablecoin Arrangements in Cross-border Payments, 31 octobre 2023. Lien

4. ISO — ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance. Lien

Tester le plan avant d’en avoir besoin

Un plan non testé reste une hypothèse.

Le test doit prouver que la route de secours est accessible, que les personnes habilitées peuvent agir, que les contrôles tiennent et que le paiement peut être suivi puis réconcilié.

TABLEAU DE TEST — À RENSEIGNER APRÈS CHAQUE EXERCICE

SCÉNARIO	IMPACT	SOLUTION ALTERNATIVE	DÉLAI DE BASCULE	RÉSULTAT DU TEST	ACTION CORRECTIVE
Stablecoin / rachat indisponible	Fournisseur urgent bloqué	Stablecoin ou rail bancaire approuvé	___ min/h	OK / ÉCHEC —	_____
Réseau indisponible	Paiement on-chain impossible	Réseau alternatif pré-configuré	___ min/h	OK / ÉCHEC —	_____
Wallet / custodien inaccessible	Fonds ou droits inaccessibles	Second wallet / custodien indépendant	___ min/h	OK / ÉCHEC —	_____
Conversion / banque indisponible	Fiat non disponible à l'échéance	Second off-ramp / compte + réserve fiat	___ min/h	OK / ÉCHEC —	_____
Collaborateur clé absent	Signature / accès bloqué	Délégation + personne de secours habilitée	___ min/h	OK / ÉCHEC —	_____
Bénéficiaire ne peut recevoir la route usuelle	Règlement retardé	Adresse / rail alternatif validé à l'avance	___ min/h	OK / ÉCHEC —	_____

OBLIGATION OU BONNE PRATIQUE ?

Entreprise ordinaire : bonne pratique de résilience et de contrôle interne.
Entité financière UE dans le champ de DORA : exigences formelles de tests applicables selon le statut et la proportionnalité.

Ne jamais présenter DORA comme une obligation universelle.

UN TEST DOIT PRODUIRE UNE PREUVE

Pas seulement une réunion de scénario.

- 1

SIMULER
Couper un maillon défini sans prévenir l'équipe exécutante.
- 2

BASCULER
Utiliser réellement la route alternative et les accès de secours.
- 3

MESURER
Chronométrer, relever les échecs, écarts de contrôle et doubles risques.
- 4

CORRIGER
Attribuer un responsable, une échéance puis rejouer le scénario.

REJOUER LE PLAN SI :

prestataire

wallet / réseau

habilitations

limites

banque / off-ramp

réglementation

CE QU'UN DIRIGEANT DOIT RETENIR Le plan B n'existe réellement que lorsqu'il a été testé, chronométré, documenté et corrigé — avec les mêmes contrôles essentiels que le circuit principal.

SOURCES

1. EUR-Lex — Règlement (UE) 2022/2554 (DORA), art. 24–25, 14 déc. 2022. [Lien](#)

2. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, mai 2010. [Lien](#)

Votre entreprise peut-elle continuer à payer demain matin ?

Onze contrôles simples : ce qui n’est pas ouvert, habilité, liquidé et testé reste une hypothèse.

Cochez “OK” seulement si le dispositif est utilisable le jour de l’incident, avec une route accessible, une personne habilitée et des preuves conservées.

DIAGNOSTIC RAPIDE — À COCHER AVANT DÉPLOIEMENT

CRITÈRE			OK	PARTIEL	NON
1	Flux critiques identifiés	fournisseurs, salaires, remboursements, échéances	☐	☐	☐
2	Dépendances cartographiées	stablecoin, réseau, wallet, banque, équipe	☐	☐	☐
3	Points uniques connus	aucun maillon critique non visible	☐	☐	☐
4	Alternatives ouvertes	wallet, dépositaire, conversion ou route bancaire	☐	☐	☐
5	Accès disponibles	droits, clés, API, comptes et limites vérifiés	☐	☐	☐
6	Personnes de secours habilitées	absence d'un collaborateur clé couverte	☐	☐	☐
7	Liquidité réellement mobilisable	stablecoin, fiat, off-ramp et banque	☐	☐	☐
8	Seuils de bascule définis	surveillance, dégradé, bascule, suspension	☐	☐	☐
9	Runbook opérationnel	qui alerte, décide, exécute et contrôle	☐	☐	☐
10	Plan testé et corrigé	scénarios chronométrés, preuves conservées	☐	☐	☐
11	Retour à la normale prévu	réconciliation, doublons, soldes et reporting	☐	☐	☐

CE QU’UN DIRIGEANT DOIT RETENIR La continuité n’est pas une intention : c’est la capacité prouvée à payer autrement, sans perdre l’autorisation, la conformité, la preuve et la réconciliation.

SOURCES

1. ISO — ISO 22301:2019, Security and resilience — BCMS requirements. [Lien](#)

2. NIST — SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, mai 2010. [Lien](#)

3. CPMI / Banque des règlements internationaux — Considerations for the Use of Stablecoin Arrangements in Cross-border Payments, 31 octobre 2023. [Lien](#)

MATRICE DE RÉSILIENCE

Le niveau dépend du nombre de critères réellement opérationnels.

RÉSILIENT

10–11 OK

Plan B activable, testé et contrôlé.

RÉSILIENT SOUS CONDITIONS

7–9 OK

Bascule possible, corrections ciblées à traiter.

VULNÉRABLE

4–6 OK

Continuité incertaine : dépendances à réduire.

CRITIQUE

0–3 OK

Premier incident = risque de blocage de paiement.

Décision : si un flux critique n’a pas de route de secours testée, il reste prioritaire à traiter.