Capital Investment Club

Business Continuity and Disaster Recovery Policy

Critical processes, recovery targets, backups, continuity planning, communications, and testing.

Last updated: 04/24/2023

Purpose

This policy defines CIC's requirements for maintaining resilience, recovering from disruptions, and protecting critical business operations.

Scope

This applies to CIC production applications, APIs, databases, cloud infrastructure, communication tools, support operations, financial workflows, repositories, vendor dependencies, and administrative systems.

Objectives

- Identify critical business processes.
- Define recovery expectations.
- Maintain backups or equivalent recovery methods.
- Test recovery capabilities.
- Reduce operational disruption.
- Maintain communication during incidents.

Critical Processes

CIC should classify criticality for:

- User authentication and platform access
- Pitch workflows
- Grant workflows
- Wallet and transaction workflows
- Messaging and notifications
- Public profile and marketplace features
- KYC-adjacent workflows
- Support workflows
- Admin workflows

- Deployment and repository access

Business Impact Analysis

CIC should maintain a business impact analysis for critical services. The analysis should document user impact, financial impact, security impact, legal impact, vendor dependencies, manual workaround, recovery priority, recovery owner, and communication owner.

Recovery Targets

Each critical system should have:

- Recovery time objective
- Recovery point objective
- System owner
- Dependencies
- Recovery procedure
- Communication path

Baseline Recovery Objectives

The following baseline objectives should be used until a formal business impact analysis approves different targets.

Service or process	Target RTO	Target RPO	Priority	Notes
Authentication and account access	4 hours	1 hour	Critical	Required for authenticated users and support.
Wallet, transaction, and ledger workflows	4 hours	15 minutes	Critical	Integrity is more important than speed; validate balances before reopening.
Grant funding and disbursement workflows	8 hours	1 hour	High	Pause high-risk actions if integrity cannot be confirmed.
Pitch investment workflows	8 hours	1 hour	High	Validate equity and payment records before reopening.
Messaging and notifications	24 hours	4 hours	Medium	Manual communication workaround may be used.
Public profiles and marketplace browsing	24 hours	4 hours	Medium	Can remain degraded if financial and identity systems are stable.
Support operations	8 hours	4 hours	High	Alternate contact process should be documented.
CI/CD and repository access	24 hours	24 hours	Medium	Manual freeze may be used during outage.

Business Impact Analysis Procedure

CIC should complete or refresh the business impact analysis annually and after material product changes.

The analysis should:

- Identify the system, owner, users affected, and critical workflows.
- Identify upstream and downstream dependencies.
- Estimate financial, legal, privacy, security, customer, and operational impact.
- Define acceptable downtime and acceptable data loss.
- Document manual workarounds and their limitations.
- Identify recovery personnel and alternates.
- Approve recovery objectives and test expectations.

Backups

Backup and recovery controls should cover critical databases, configuration, source code, and operational records.

Requirements:

- Backups or recovery mechanisms must be documented.
- Access to backups must be restricted.
- Recovery must be tested at least annually for critical systems.
- Failed backup or recovery tests must be remediated.

Restoration Validation

Recovered systems must not be returned to normal operation until the owner validates:

- Application health checks pass.
- Critical API endpoints respond successfully.
- Authentication and authorization behave correctly.
- Wallet, grant, pitch, and ledger balances match expected reconciliation records.
- Recent transactions are present or documented as intentionally replayed or corrected.
- Background jobs, notifications, and scheduled jobs are operating or intentionally paused.
- Monitoring alerts are stable.
- Known temporary workarounds are documented.

Continuity Scenarios

Plans should include response options for:

- Production API outage.
- Database corruption or accidental deletion.
- Wallet or ledger inconsistency.
- Cloud region or service disruption.

- Email or notification provider outage.
- Support tool outage.
- Repository or CI/CD outage.
- Security incident requiring feature shutdown.
- Key personnel unavailable.

Business Continuity Planning

Plans should address:

- Production outage
- Cloud provider disruption
- Database issue
- Vendor outage
- Security incident
- Loss of key personnel
- Support tool outage
- Payment or wallet workflow disruption

Communications

CIC must define internal escalation and external communication paths for material outages or disruptions.

Communication records should identify the incident owner, communication owner, affected users, current impact, workaround, next update time, and final resolution summary.

Manual Workarounds

Where practical, critical workflows should document manual workarounds. Workarounds must include authorization requirements, records to retain, reconciliation requirements, and criteria for returning to automated processing.

For example:

- Support may collect affected user details in an approved ticketing system during a support tool outage.
- Grant or wallet operations may be temporarily paused until balance integrity is validated.
- User-facing updates may be posted through an approved status or support channel if notifications are unavailable.

Testing

CIC should test continuity or recovery at least annually. Testing may include tabletop exercises, backup restoration, failover validation, or operational response drills.

Required Test Scenarios

At minimum, the annual continuity program should cover:

- Database restoration for a critical application dataset.
- Wallet or ledger inconsistency triage and correction.
- Production deployment rollback.
- Vendor outage affecting notifications, payments, hosting, or support.
- Security incident requiring temporary workflow shutdown.
- Loss of key privileged operator.

Test Evidence

Recovery tests should record scope, scenario, date, participants, systems tested, recovery result, issues found, remediation owner, and target date.

Evidence

Required evidence:

- Business continuity plan
- Disaster recovery plan
- Critical system inventory
- Backup records
- Recovery test records
- Tabletop records
- Remediation tracker

Review

This policy must be reviewed at least annually.