# Module XX – Partial Recovery & Grace-Based Capsule Engine

Version: 4.1 | Classification: CTO Mandatory (Resilience & Fault Tolerance)

Scope: Controlled capsule recovery under partial system failure or incomplete trust execution

## 0. Purpose & Recovery Boundary Context

This module defines recovery strategies and capsule downgrade logic in case of partial subsystem failure, degraded execution paths, or incomplete audit visibility. It enables runtime grace periods, fallback capsule paths, and bounded reentry into sovereign operations. It is essential for deployments requiring resilience under partial capsule system degradation or delayed audit reentry.

## 1. Grace Capsule Declaration & Downgrade Envelope

A `Grace Capsule (GC)` is emitted when a capsule subsystem cannot execute or validate as required:  
`{ capsule\_id, failed\_subsystem, impact\_scope[], grace\_ttl, recoverable\_flag, downgrade\_level, escalation\_lock, hash\_anchor }`  
GCs must reference ledger path hash and declare rollback tolerance or partial certification state.

## 2. Recovery Path Classification & Partial Reentry

Recovery types:  
- Passive Delay: retry until subsystem re-available (e.g. Audit Engine outage)  
- Trust Downgrade: operate under Tier-1 fallback with locked policy capsule  
- Fork Isolation: operate with strict capsule scope under sovereign flag  
Partial Reentry only allowed if:  
- Ledger and Trust scope are verified  
- All recovery capsules are signed and included in trace replay  
- Audit Engine (Module 14) issues `Grace Replay Confirmation Capsule (GRCC)`

## 3. Violation Chains & Capsule Bypass Control

Systems must detect and freeze:  
- unauthorized capsules generated under partial trust  
- fake reentry capsules mimicking resolved states  
- bypassed forks without consent trail  
Responses:  
- `Grace Violation Capsule (GVC)` for unapproved capsule flows  
- `Execution Isolation Capsule (EIC)` for downgraded forks

## 4. Certification Impact & Capsule Chain Validity

Systems using grace-based reentry:  
- must declare partial certification tier in CTO Capsule (Module 17)  
- are required to revalidate full capsule path within 30 logical execution cycles  
- are blocked from fork initiation or capsule signing beyond declared trust tier  
Final recovery confirmed via `Recovery Finalization Capsule (RFC)` and grace path hash review.

## 5. Sovereign Reentry Protocol under Degradation

Sovereign reentry under degraded capsule state is bound to:  
- Public trace replay integrity confirmation  
- Frozen ledger segment review  
- Cross-federation consensus (if applicable)  
Failure to complete recovery path locks trust authority and halts audit stream updates.