

Recovery Design Boundary

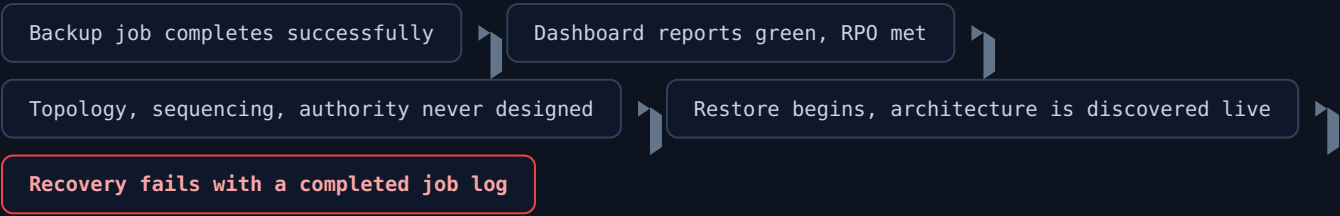
DEFINITION

The line between systems whose recovery characteristics have been intentionally designed and systems whose recovery behavior is only discovered during restoration. Backup exists on both sides. Recoverability only exists on the designed side.

FRAMEWORK FLOW

01 Backup Coverage Data is captured and confirmed. The job succeeded. This is the only thing most recovery metrics actually measure.	02 The Boundary Was recovery intentionally designed? Topology, sequencing, target capacity, and authority either were decided in advance, or weren't.	03 Failure State Recovery-Blind Architecture — backup coverage exists, but recovery behavior was never explicitly designed.	04 Restore Time The architecture is either proven in advance, or discovered live — during the one moment it can't afford to be wrong.
---	--	--	--

Failure State: Recovery-Blind Architecture



THE DIAGNOSTIC SIGNAL

RECOVERY TOPOLOGY

Ask which systems recover to which destination. A backup job confirms data left production — it says nothing about where it lands, or whether that destination can accept it.

DEPENDENCY SEQUENCING

Ask what order multi-tier applications restore in. A database restored after the tier that depends on it is a failed recovery with a completed job log.

RECOVERY TARGET CAPABILITY

Ask whether capacity, identity, networking, tooling, and licensing at the recovery target match what production actually needs today, not what was provisioned at contract signing.

RECOVERY AUTHORITY

Ask who owns execution when normal operating boundaries are broken — and whether that person is reachable independent of the outage that just occurred.

ARCHITECTURAL RELATIONSHIPS

#122

Recovery Dependency Collapse

RELATED MODERATE

Pairs on blast-radius design — both are D1-adjacent questions, one about whether topology was designed, one about what collapses when it wasn't.

#144

Recovery Authority Fragmentation

RELATED MODERATE

Pairs on authority-ownership design — both are D1-adjacent questions, one about whether an owner was assigned, one about what happens when they're unreachable.

#111

Recovery Validity Boundary

DOWNSTREAM ASSUMES DESIGN EXISTS

Asks whether a specific test validates the documented procedure — assumes a recovery design already exists to test against.

#148

Recoverability Gap

DOWNSTREAM ASSUMES DESIGN EXISTS

Asks whether a validated plan survives adversarial, ransomware-class compromise — also assumes the design question is already settled.

ANCHOR /recovery-design-boundary/

FRAMEWORK HOME

D1 — Recovery Architecture Foundations. Stage entry point for the full D1-D6 recovery maturity path.

"Recovery cannot discover its own architecture during an outage. An organization that's never tested whether it can is not more prepared than one that hasn't backed up at all — it's just better documented on the way to the same discovery."