

BUSINESS CONTINUITY
& DISASTER RECOVERY.

Outages, disasters, and attacks are a matter of when, not if — **the difference is how fast the organization gets back up**. Business continuity keeps critical operations running through disruption, and disaster recovery restores the systems behind them within a defined, tested window.

- BUSINESS IMPACT ANALYSIS
- RTO & RPO TARGETS
- FAILOVER & BACKUP
- DR TESTING

01 THE MECHANISM



Business Impact Analysis
Identifying which processes are **critical** and how much disruption each can absorb before real damage sets in.



Recovery Planning
Defining the steps, roles, and systems needed to **restore operations within a target window**.



Failover & Backup
Maintaining redundant systems and data copies that can **take over the moment primary systems fail**.

02 THE FLOW

The Continuity Cycle ONGOING PROGRAM

1

Business impact analysis **ranks processes by criticality** and tolerance for downtime.

2

Recovery time and recovery point objectives are **set for each critical system** based on that tolerance.

3

Plans, backups, and failover paths are **built and kept current** against those targets.

The Disaster Cycle LIVE EVENT

1

An outage or disaster is declared, **activating the continuity plan** and its designated roles.

2

Operations shift to backup systems or alternate sites **while primary systems are restored**.

3

A post-event review checks **whether RTO and RPO targets were actually met**.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Business Impact Analysis	Ranks processes by criticality and quantifies the cost of downtime for each.
Recovery Objectives (RTO/RPO)	Sets the maximum tolerable downtime and data loss for every critical system.
Backup & Failover	Maintains redundant data and systems ready to take over on short notice.
DR Testing	Validates that recovery actually works within target windows before it's needed.

04 CONTINUITY APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Backups With No Recovery Plan	No	Data exists somewhere, but nobody knows how long restoring it takes.
Untested Disaster Recovery Plan	No	A plan that has never been executed is an assumption, not a capability.
Single-Site Infrastructure Only	No	One outage, disaster, or attack can take everything down at once.
Paper-Only Annual DR Test	No	A tabletop walkthrough doesn't prove the failover actually works.
Combined BC/DR Program (BIA + RTO/RPO + Failover)	Yes	Sets a target, builds toward it, and proves the target is met.

BUSINESS CONTINUITY.

PLAN · FAILOVER · RECOVER

05

PROGRAM OPERATIONS

Recovery time objectives are promises to the business, not IT metrics. Every hour of RTO has a cost attached.

A DR plan that has never failed over live is unproven. Tabletop walkthroughs don't test technical failover.

Dependencies cascade. One shared vendor or database can take down every "independent" system at once.

Recovery plans age quickly. New systems, integrations, and staff all need to be folded back into the plan.

06

CONTROL MAPPING

NIST SP 800-34

Contingency planning guide for federal information systems and organizations.

ISO 22301

International standard for business continuity management systems.

NIST CSF 2.0

Recover function coverage for restoration of impaired capabilities.

FFIEC BCM BOOKLET

Business continuity guidance for financial institutions.

07

WHAT THIS DOES NOT SOLVE

A disaster exceeding planned scope

Plans built for one scenario can fail against a larger, compounding event.

Recovery objectives without funding

An aggressive RTO promise means nothing without the infrastructure to hit it.

Key-person dependency

A plan living in one person's head fails the moment that person is unavailable.

Data loss inside the RPO window

Even a well-met RPO still means losing everything since the last backup.

08

MYTHS VS. REALITY

MYTH	REALITY
"We have backups, so we're covered."	Backups without a tested recovery process just mean the data exists somewhere.
MYTH	REALITY
"Business continuity is an IT problem."	Every business function needs its own plan, not just IT systems.
MYTH	REALITY
"Cloud infrastructure means we don't need DR."	Cloud providers fail too, and misconfiguration is still on you.
MYTH	REALITY
"One DR test a year is sufficient."	Systems change constantly; untested change is untested recovery.
MYTH	REALITY
"RTO and RPO are technical details."	They're business decisions about acceptable loss, made before a crisis.

09

SPEAK THE PROGRAM — KEY TERMS

BUSINESS CONTINUITY PLAN (BCP)

The documented strategy for keeping critical operations running through disruption.

DISASTER RECOVERY (DR)

The process of restoring IT systems and data after a disruptive event.

RECOVERY TIME OBJECTIVE (RTO)

The maximum acceptable time to restore a system after disruption.

RECOVERY POINT OBJECTIVE (RPO)

The maximum acceptable amount of data loss, measured in time.

BUSINESS IMPACT ANALYSIS (BIA)

The process of identifying and prioritizing critical business functions.

FAILOVER

The automatic or manual switch to a redundant system when the primary fails.