

OPERATIONAL RESILIENCE PRINCIPLES.

Basel's principles measure success by whether a critical operation keeps running through disruption, not by whether disruption was prevented — **and the principles themselves carry no legal force until a national regulator writes them into binding rules.**

- IMPACT TOLERANCE
- DEPENDENCY MAPPING
- SEVERE-SCENARIO TESTING
- NATIONAL IMPLEMENTATION GAP

01 THE MECHANISM

Outcome-Focused Resilience, Not Just Prevention

The principles define success as continuing to deliver a critical operation through disruption, not just reducing the odds of one occurring — **a bank can pass every preventive control and still fail** to keep the operation running.

Impact Tolerance for Each Critical Operation

Banks must set a measurable limit for how much disruption a critical operation can tolerate before causing intolerable harm — **testing then proves whether that tolerance actually holds** under a severe scenario.

Interconnection & Third-Party Mapping

Once critical operations are identified, banks must map every dependency, including third parties and financial market infrastructure. **Resilience for one system is meaningless if an unmapped dependency fails first.**

02 THE FLOW

The Outcome-Tested Bank CONTAINED

1

The bank identifies its critical operations and sets a specific impact tolerance for each, defining how much disruption is acceptable before real harm occurs.

2

Severe-but-plausible testing, covering mapped third-party and infrastructure dependencies, **proves whether the system can stay inside that tolerance**, not just whether a plan exists.

3

When a real incident hits, the pre-mapped dependencies and rehearsed response let the bank **keep delivering the operation within its stated tolerance**, or recover fast enough to stay inside it.

The Prevention-Only Bank EXPOSED

1

Resilience planning stops at trying to prevent disruption, with no defined tolerance for how much disruption a critical operation could survive.

2

Dependency mapping covers only the bank's own systems, leaving **third-party and infrastructure failures as unmodeled blind spots** until they happen.

3

When a real incident hits, the bank discovers in real time **how much disruption a critical operation can tolerate**, instead of already knowing from testing.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Critical Operations & Impact Tolerance	Requires identifying operations whose disruption could threaten the bank's safety and soundness or the wider financial system, then setting a measurable tolerance for how severely each can be disrupted.
Interconnection & Dependency Mapping	Requires mapping the people, processes, systems, third parties, and financial market infrastructure a critical operation actually depends on, not just the systems the bank directly controls.
Severe-But-Plausible Scenario Testing	Requires testing business continuity and incident response against scenarios extreme enough to actually threaten the stated impact tolerance, not routine drills.
ICT & Cyber Security Resilience	Requires resilient ICT and cyber security controls specifically framed around keeping critical operations running through disruption, not just protecting data.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Traditional BCP Focused on Prevention Only	No	Aims to avoid disruption but doesn't define how much disruption a critical operation could actually survive if prevention fails.
Dependency Mapping Limited to Owned Systems	No	Misses third-party and financial market infrastructure failures that can break a critical operation just as completely as an internal outage.
Routine, Non-Severe Testing Scenarios	No	Confirms a plan works for a mild disruption without ever proving whether it holds up under an event likely to breach the impact tolerance.
Principles Read But Not Implemented Into Rules	No	Basel's principles carry no direct legal force on their own; without a national supervisor converting them into rules, they're guidance, not obligation.
Impact Tolerances + Dependency Mapping + Severe-Scenario Testing + National Rules	Yes	Combines a measurable standard, complete visibility into dependencies, real proof under stress, and actual legal enforceability.

OPERATIONAL RESILIENCE PRINCIPLES. MAP · TEST · TOLERATE

05 PROGRAM OPERATIONS

Basel's principles are supervisory guidance, not law themselves. They only become enforceable once a national regulator writes them into binding rules, such as the UK PRA's Operational Resilience regime.

Impact tolerance is a new concept, not a renamed recovery time objective. It measures the outer limit of acceptable harm to customers and markets, not just how fast a system comes back online.

Testing has to target the tolerance, not just the plan. A scenario that never threatens the stated tolerance doesn't actually validate whether the bank can hold the line.

Cyber security is one of seven principles, not the whole framework. Operational resilience treats ICT risk as one dependency among several, alongside people, processes, and third parties.

06 CONTROL MAPPING

BCBS PRINCIPLES FOR OPERATIONAL RESILIENCE (2021)

The **core seven-principle framework** from the Basel Committee on Banking Supervision, covering governance through ICT and cyber security.

BCBS SOUND MANAGEMENT OF OPERATIONAL RISK

The **broader operational risk framework** operational resilience is explicitly built on top of, rather than replacing.

UK PRA OPERATIONAL RESILIENCE POLICY (PS21/3)

A **binding national implementation** of Basel's principles, requiring UK banks to set impact tolerances for defined "important business services."

EU DORA

A **separate, directly binding EU regulation** covering similar ICT and operational resilience ground for financial entities, layered alongside Basel's principles rather than derived from them.

07 WHAT THIS DOES NOT SOLVE

Direct Legal Enforceability

The principles themselves create **no obligation until a national supervisor adopts binding rules** based on them, unlike a regulation such as DORA.

Credit, Market & Liquidity Risk

Operational resilience is scoped to **keeping operations running through disruption**, not the separate prudential risks a bank's capital and liquidity framework manages.

Consistent Global Implementation

Because each jurisdiction implements the principles independently, **a globally active bank can face materially different binding requirements** across the countries it operates in.

Non-Bank Financial Institutions

The framework is written for **banks supervised under the Basel framework**, not insurers, asset managers, or other financial entities covered by separate regimes.

08 MYTHS VS. REALITY

MYTH "Basel's operational resilience principles are binding international law."	REALITY They're supervisory guidance from the Basel Committee, which has no direct legal enforcement power — obligations only exist once a national regulator writes them into binding rules.
MYTH "Impact tolerance is just another name for recovery time objective."	REALITY RTO measures how fast a system returns; impact tolerance measures the outer limit of harm to customers and markets that's acceptable before a disruption becomes intolerable.
MYTH "Operational resilience is really just about cybersecurity."	REALITY ICT and cyber security is one of seven principles — people, processes, third parties, and infrastructure dependencies matter just as much to keeping an operation running.
MYTH "If a bank has a tested business continuity plan, it meets the operational resilience principles."	REALITY Traditional BCP aims to prevent or minimize disruption; operational resilience additionally requires a defined tolerance and proof, through severe testing, that the bank can stay inside it.
MYTH "All countries have implemented Basel's operational resilience principles the same way."	REALITY Implementation is independent and inconsistent across jurisdictions — the UK's binding PRA rules are considerably more prescriptive than how other regulators approached the same principles.

09 SPEAK THE PROGRAM — KEY TERMS

CRITICAL OPERATION

An activity whose disruption could **threaten a bank's safety and soundness or the wider financial system**, the starting point for scoping the entire framework.

IMPACT TOLERANCE

The **measurable outer limit of disruption** a critical operation can absorb before causing intolerable harm to customers, markets, or the bank itself.

SEVERE-BUT-PLAUSIBLE SCENARIO

A testing scenario extreme enough to **meaningfully threaten the stated impact tolerance**, rather than a routine drill the plan was already known to pass.

INTERCONNECTIONS & INTERDEPENDENCIES

The full map of **people, processes, systems, third parties, and infrastructure** a critical operation actually relies on to function.

FINANCIAL MARKET INFRASTRUCTURE (FMI)

Systems like **payment, clearing, and settlement infrastructure** that many critical operations depend on but that sit outside any single bank's direct control.

NATIONAL IMPLEMENTATION

The process by which a **country's own supervisor converts Basel's principles into binding, enforceable rules** — the step that actually creates legal obligation.