Falconry360™

WHITEPAPER

BUSINESS RESILIENCE & CONTINUITY

# Building resilience that lasts.

Organizational resilience through integrated crisis management, business continuity and disaster recovery planning.

01 Crisis management | 02 Business continuity | 03 Disaster recovery



# In this paper

# Resilience is an operating capability, not a set of documents

Most organizations already have crisis plans, continuity plans and recovery runbooks. What many lack is the connective tissue between them: shared impact analysis, shared ownership, shared evidence, and a single view of readiness that leadership can trust.

This paper sets out a practical model for integrating crisis management, business continuity and disaster recovery into one resilience capability — aligned to ISO 22301 and ISO 22316, and to the expectations of GCC and international regulators.

It is written for boards, risk and resilience leaders, and the practitioners who will operate the capability day to day.

### THREE ARGUMENTS

1. Disruption is a certainty to plan for, not a risk to eliminate.
2. Fragmented plans fail together — integration is what makes them work under pressure.
3. Regulators now examine resilience as an outcome — evidence of readiness, not existence of plans.

# The case for integrated resilience

## 01 Disruption has changed shape

Ransomware, cloud and third-party outages, supply-chain failure and regional events now disrupt operations without touching a building. Plans built around site loss no longer cover the dominant scenarios.

## 02 Regulators expect demonstrable readiness

SAMA, CBUAE, NCA, DORA and international supervisors have moved from "do you have a plan?" to "show us it works" — tested tolerances, exercised teams, evidenced recovery.

## 03 Operations are interdependent

A single critical service can depend on dozens of systems, suppliers and teams. No one plan owns that chain — only an integrated capability can see it end to end.

SECTION 02 / DEFINITIONS

# Three disciplines, one capability

## Crisis management

The leadership discipline. Who decides, who communicates, and how the organization escalates when an event exceeds normal management.

PROTECTS: DECISIONS & REPUTATION

## Business continuity

The operational discipline. How critical services keep running at an acceptable level during disruption — people, workarounds, alternate sites and suppliers.

PROTECTS: CRITICAL SERVICES

## Disaster recovery

The technology discipline. How systems, data and infrastructure are restored to defined recovery time and recovery point objectives.

PROTECTS: SYSTEMS & DATA

Each discipline answers a different question. Resilience is the property that emerges when all three are planned from the same impact analysis and exercised as one.

SECTION 02 / FAILURE PATTERNS

# Where fragmented programs break down

### Plans built on different assumptions

Continuity assumes a system is back in four hours; the recovery team has committed to twenty-four. Nobody discovers the gap until the incident.

### Ownership scattered across silos

Crisis plans sit with corporate affairs, continuity with risk, recovery with IT. Three owners, three documents, three review cycles — no single accountable view.

### Exercises that test documents, not decisions

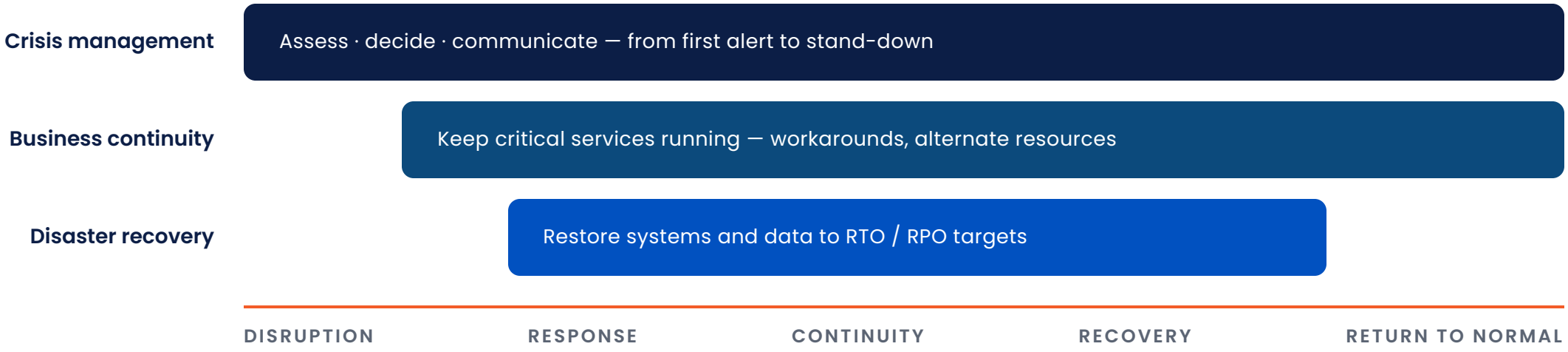
Annual walkthroughs validate that plans exist. They rarely test the handoffs between crisis, continuity and recovery teams — which is where incidents are lost.

### Evidence assembled after the fact

When the regulator asks for proof of readiness, teams reconstruct it from email threads and spreadsheets — slow, incomplete, and hard to defend.

# The integrated operating model

One disruption timeline, three coordinated responses — all planned from a single business impact analysis and governed by one crisis authority.




- **One impact analysis** sets the priorities and tolerances all three respond to.
- **One crisis authority** directs escalation, decisions and communication.
- **One evidence base** records exercises, invocations and improvement actions.

# Decisions under pressure

A crisis is any event that threatens strategic objectives, reputation or viability faster than normal governance can respond. Crisis management gives the organization a pre-agreed way to assess, escalate, decide and communicate — so leadership spends the first hour acting, not organizing.

- **Defined crisis team** — named roles, deputies and authorities, activated by clear triggers.
- **Escalation thresholds** — objective criteria that turn an incident into a crisis, removing hesitation.
- **Communication protocols** — pre-approved holding statements and stakeholder maps for regulators, clients, media and staff.
- **Decision logging** — a live record of what was decided, by whom, on what information.

### THE FIRST HOUR

| | |
|---|---|
| **Verify** | Confirm the event and its scope |
| **Activate** | Convene the crisis team against triggers |
| **Assess** | Impact on services, people, obligations |
| **Direct** | Invoke continuity and recovery plans |
| **Inform** | Notify regulators and stakeholders on time |

# Keeping critical services running

Business continuity starts with the business impact analysis (BIA): which services matter most, how quickly they must resume, and what they depend on. Everything else — strategies, plans, alternate arrangements — flows from those answers.

- **Business impact analysis** — criticality, tolerable downtime and dependencies for every service.
- **Continuity strategies** — workarounds, alternate sites, cross-trained staff, substitute suppliers.
- **Documented plans** — owned by the business, current, and usable under stress.
- **Exercising** — from desktop walkthroughs to full invocation tests, on a defined cycle.

### THE MEASURES THAT MATTER

| | |
|---|---|
| **MTPD** | Maximum tolerable period of disruption before impact becomes unacceptable |
| **RTO** | Recovery time objective — how quickly a service or system must resume |
| **RPO** | Recovery point objective — how much data loss is tolerable |
| **MBCO** | Minimum business continuity objective — the acceptable reduced service level |

# Restoring technology to target

Disaster recovery turns continuity requirements into technical commitments. Every critical system carries an RTO and RPO inherited from the BIA — and the recovery architecture, runbooks and testing regime exist to meet them, not the other way round.

- **Tiered recovery** — systems classified by criticality, each tier with defined RTO / RPO commitments.
- **Recovery runbooks** — step-by-step restoration procedures, current and executable by more than one person.
- **Data protection** — backups and replication designed against the RPO, with immutability for ransomware scenarios.
- **Recovery testing** — actual restorations on a schedule, with results recorded against targets.

### QUESTIONS THE BOARD SHOULD ASK

When did we last **restore** a critical system — not back it up?

Do recovery commitments **match** what continuity plans assume?

Could we recover if our backups were **encrypted** too?

Which third-party services sit **inside** our recovery path?

# The regulatory landscape

| FRAMEWORK | APPLIES TO | FOCUS |
|---|---|---|
| **ISO 22301** | All sectors, international | Certifiable business continuity management system — policy, BIA, strategy, exercising |
| **ISO 22316** | All sectors, international | Principles and attributes of organizational resilience beyond continuity planning |
| **SAMA BCM** | Saudi financial sector | Mandated BCM lifecycle — governance, BIA, plans, exercising and reporting |
| **NCA ECC** | Saudi critical & government entities | Cybersecurity resilience domain — continuity of security operations within the ECC controls |
| **CBUAE standards** | UAE licensed financial institutions | Operational resilience and business continuity expectations for critical functions |
| **DORA** | EU financial entities | Digital operational resilience — ICT risk, incident reporting, resilience testing, third parties |
| **NIST SP 800-34** | Widely adopted practice | Contingency planning guidance for information systems — the reference DR methodology |

SECTION 05 / SELF-ASSESSMENT

# The resilience maturity model

Five levels, assessed per critical service. Most organizations sit at level two or three; regulated entities are increasingly expected to evidence level four.

1

### Reactive

Response improvised per event. No documented plans.

2

### Documented

Plans exist in silos. Reviewed for audit, rarely exercised.

3

### Practised

Plans exercised on a cycle. Owners named. Gaps tracked to closure.

4

### Integrated

One BIA drives crisis, continuity and recovery. Shared evidence base. Cross-team exercises test handoffs.

5

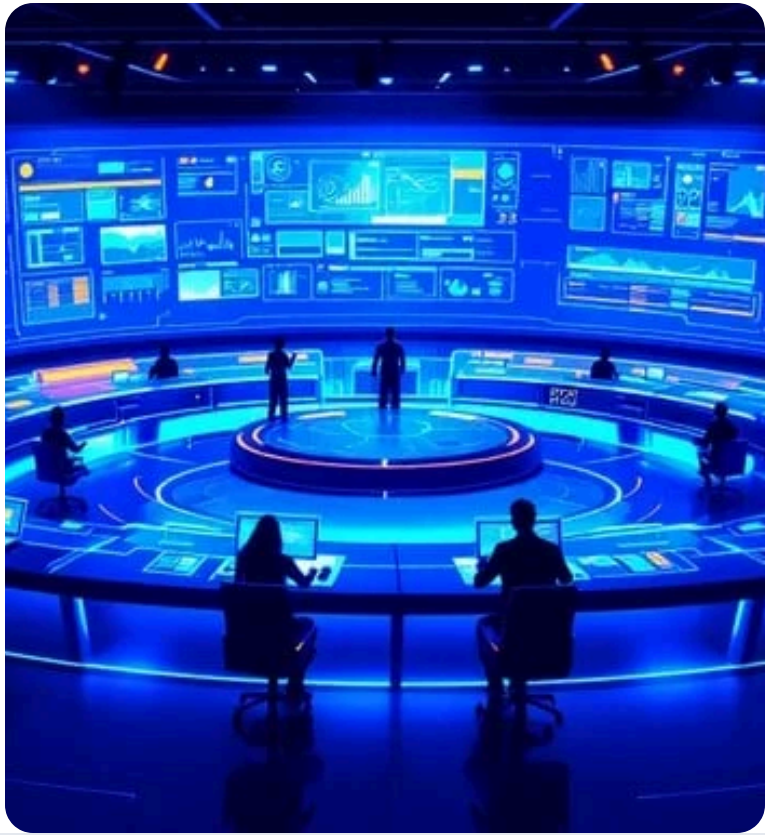
### Adaptive

Resilience informs strategy and change. Tolerances monitored continuously; every disruption improves the model.

# A ransomware event, handled as one capability

| | |
|---|---|
| **Hour 0** | **Detection.** Encryption activity on core systems. Escalation thresholds classify it as a crisis within minutes, not meetings. |
| **Hour 1** | **Crisis team convened.** Pre-agreed roles activate. Regulator notification clock starts; holding statements go out on schedule. |
| **Hours 2–8** | **Continuity invoked.** Critical services switch to documented workarounds at their minimum continuity objectives while systems are isolated. |
| **Day 1–3** | **Tiered recovery.** Systems restore from immutable backups in BIA priority order, each verified against its RTO and RPO. |
| **Day 5+** | **Stand-down and review.** Decision log, invocation records and recovery results feed the post-incident review — and the evidence file. |

*Illustrative sequence only — actual timings depend on your impact tolerances and recovery objectives.*



# Implementation roadmap

## 01

### Assess

MONTHS 1–3

Business impact analysis, dependency mapping, current-state maturity and gap assessment against regulatory obligations.

## 02

### Design

MONTHS 3–6

Resilience strategy and tolerances, crisis governance, continuity strategies and recovery architecture — one design, three disciplines.

## 03

### Implement

MONTHS 6–9

Plans authored and owned by the business, teams trained, recovery capabilities built and platform workflows stood up.

## 04

### Embed

MONTHS 9–12, THEN CONTINUOUS

Exercise across disciplines, measure against tolerances, report to the board, and improve after every test and disruption.

Sequence matters less than ownership: each phase should leave the business — not consultants or the resilience team alone — holding the capability.

SECTION 08 / WITHSTAND

# Resilience on Falconry360

The Withstand pillar operationalizes this model — one of five connected pillars: Govern · Anticipate · Comply · Withstand · Assure.

### BIA & dependency mapping

Impact analysis, tolerances and dependencies captured once — shared by every plan.

### Plan lifecycle management

Crisis, continuity and recovery plans with named owners, review cycles and version control.

### Incident & crisis workflows

Escalation, task assignment, decision logging and stakeholder notifications in one accountable flow.

### Exercising & evidence

Exercises scheduled, results recorded, actions tracked — a defensible audit trail by design.

### Executive dashboards

Board-ready readiness reporting generated from live platform data, not manual decks.

### Framework alignment

Resilience activities mapped to ISO 22301, SAMA, NCA, CBUAE and DORA obligations.

# Glossary

| | |
|---|---|
| **BIA** | Business impact analysis — identifies critical services, tolerable downtime and dependencies |
| **BCMS** | Business continuity management system — the governed program defined by ISO 22301 |
| **CMT** | Crisis management team — the named group with authority to direct crisis response |
| **Exercise** | A planned rehearsal — from desktop walkthrough to full invocation — that tests plans and people |
| **Invocation** | The formal decision to activate a continuity or recovery plan |
| **MTPD** | Maximum tolerable period of disruption before impacts become unacceptable |
| **RTO** | Recovery time objective — target time to resume a service or system |
| **RPO** | Recovery point objective — maximum tolerable data loss, measured in time |
| **MBCO** | Minimum business continuity objective — the acceptable service level during disruption |
| **Tolerance** | Impact tolerance — the maximum acceptable disruption to a critical service, set by the board |

Falconry360™

# Build resilience that lasts.

Talk to us about assessing your resilience maturity — or see the Withstand pillar on Falconry360.

Request a demo

contact@falconry.solutions · falconry360.com ·