Emergency Preparedness & Contingency Planning

When Crisis Hits, Preparation Is Everything

TDW
CYBERSECURITY • IT CONSULTING

WITHOUT A PLAN

“Without a plan, every crisis is a first-time event.”

Operational Chaos

No defined roles, no escalation path, no communication protocol. Responders improvise under pressure while critical systems remain offline.

Extended Downtime

Organizations with tested plans restore services hours faster than those without. Every unplanned hour carries operational, financial, and reputational cost.

Regulatory Exposure

Most critical infrastructure operators face regulatory requirements for documented, tested response capability. An incident without a plan compounds the violation.

What Is Contingency Planning?

Contingency planning is the disciplined process of preparing an organization to respond effectively to disruptions — whether a cyberattack, natural disaster, facility emergency, or operational failure.

Contingency plans — disaster recovery plans, business continuity plans, emergency response plans, crisis management plans, and others — are important tools for organizational resilience. Contingency planning won't prevent a crisis from occurring, but it can mitigate the effects by enabling a quicker, more coordinated response and more efficient recovery.

A complete contingency program is more than one plan. It is an integrated suite of documents, procedures, and trained personnel that covers every dimension of organizational response — from the technical response to a cyber incident, to the continuity of critical business functions, to the corporate communication strategy for a public crisis.

Plans that sit in a drawer are not plans — they are compliance artifacts. Effective contingency planning requires development, review, exercise, and continuous improvement.

The Contingency Planning Journey

Creating a contingency plan is only half the journey. Plans must be reviewed and updated regularly -- at least annually, and more frequently for high-criticality operations. Organizations evolve through restructuring, personnel changes, and shifts in technology and operating conditions -- each requiring a plan update. Plans must also be tested: exercising your plan against a simulated crisis is the best way to measure its real-world effectiveness before an actual crisis demands it.

The Four Core Plans

CIRP

Cyber Incident Response Plan

Defines roles, escalation procedures, containment actions, and recovery steps for cyberattacks on critical systems. The first-response playbook for security incidents.

ERP

Emergency Response Plan

Facility-level emergency procedures covering fires, severe weather, hazmat events, and other physical emergencies. Tiered by facility criticality to operations.

BCP

Business Continuity Plan

Ensures critical business functions continue during disruption. Built on Business Impact Analysis — identifies critical processes, dependencies, and recovery time objectives.

CMP

Crisis Management Plan

Corporate-level coordination and communication framework for significant crises. Defines the crisis team, communication protocols, and decision-making authority.

Regulatory & Framework Requirements

Most critical infrastructure operators have regulatory obligations for documented, tested emergency and continuity plans.

But compliance is a floor, not a ceiling. Regulatory requirements specify the minimum — a functional contingency program goes further by ensuring plans are exercised, current, and understood by the people who must execute them.

FEMA NIMS

National Incident Management System — the federal framework for emergency preparedness. TDW aligns all plan development to NIMS standards.

NERC CIP

Requires documented incident response and recovery plans for bulk electric system operators, with defined testing and reporting requirements.

Sector Standards

Water utilities, municipalities, and other critical infrastructure operators face sector-specific requirements from EPA, DHS, and state regulators.

Benefits of a Strong Contingency Program

Faster Recovery

Documented, practiced plans reduce the time to restore critical services — directly limiting operational and financial impact.

Regulatory Compliance

Meet documented obligations under NERC CIP, FEMA NIMS, and sector-specific requirements with auditable, maintained plans.

Staff Confidence

People who have exercised a plan respond with clarity and purpose. Those who haven't default to improvisation under stress.

Reduced Liability

A documented, tested response capability demonstrates due diligence — relevant for regulatory defense, insurance, and governance.

Organizational Resilience

Plans force organizations to understand their critical dependencies before a crisis reveals them.

Continuous Improvement

Each exercise and real event produces lessons that make the next response more effective. The program gets stronger over time.

The Planning Process

1

Risk Assessment

Identify threats, hazards, and vulnerabilities relevant to the organization's operations and environment.

2

Business Impact Analysis

Identify critical processes, their dependencies, and the operational impact of disruption at varying timeframes.

3

Plan Development

Draft plan documents — CIRP, ERP, BCP, CMP — based on risk assessment and BIA findings, aligned to FEMA NIMS.

4

Review & Approval

Subject matter review, leadership approval, and integration with other plans and vendor agreements.

5

Exercise & Improve

Validate plans through tabletop and functional exercises. Update based on findings, operational changes, and real events.

Business Impact Analysis: The Foundation

The BIA is the analytical foundation of every contingency plan. It answers the questions that determine the entire plan's structure: What are we protecting, why, and how long can we afford to lose it?

Critical Process Identification

Which business functions are essential to operations? Which would cause immediate, severe harm if disrupted?

Dependency Mapping

What systems, personnel, vendors, and facilities does each critical process depend on? Where are the single points of failure?

Impact Analysis

What is the operational, financial, regulatory, and reputational impact of disruption at 1 hour, 24 hours, 72 hours, and longer?

Recovery Objectives

What is the maximum tolerable downtime (MTD)? What is the recovery time objective (RTO)? What data recovery point is acceptable (RPO)?

Plan Review & Maintenance

A plan that isn’t maintained becomes a liability. Outdated contact lists, obsolete procedures, and unreviewed assumptions all degrade plan effectiveness — often without anyone noticing until a crisis reveals the gap.

Annual Review Cycle

Full plan review at least annually — verify contacts, update procedures, reflect organizational changes, confirm vendor commitments.

Trigger-Based Updates

Update plans when triggered by: significant organizational change, new facility or system, regulatory revision, post-exercise findings, or real incident.

Version Control

All plan documents versioned and dated. Prior versions archived. Distribution list documented and current.

What Triggers an Unscheduled Update

- Significant changes to personnel, facilities, or systems
- New regulatory requirements or audit findings
- After-action report from an exercise or real incident
- Changes to key vendor or supplier relationships
- Acquisition, merger, or major organizational change

CRISIS EXERCISES

Testing your plans is not optional. It is how you find out if they work.

Contingency plans need to be tested regularly. The best way to find out how well your plan helps in mitigating crisis events is to practice using it in response to a virtual crisis. A dry run ensures your plan has the information required by personnel responding to a crisis and allows them to practice and refine crisis communications that are critical in response and recovery.

These exercises can vary in realism and complexity. Start with a simple scenario the organization may have encountered, with all participants in the same meeting. Progress to more complex scenarios — virtual crises with multiple simultaneous impacts, requiring personnel to respond and coordinate either locally or remotely. To truly test your crisis response, a complex scenario could include the loss of internet and other communication channels.

Types of Exercises

Tabletop Exercise

Best for: Initial plan validation, leadership familiarization, lower resource commitment

A facilitated, discussion-based exercise where participants walk through a scenario without executing real actions. Teams discuss roles, decisions, and coordination in real time.

- Identify gaps in roles, responsibilities, and escalation paths
- Test decision-making under simulated time pressure
- Surface conflicting assumptions between departments
- Build familiarity with plan content and structure
- Low cost, high value — can be completed in a half day

Functional Exercise

Best for: Validating operational readiness, regulatory compliance, mature programs

A higher-fidelity exercise where teams actually execute plan procedures — activating systems, initiating communication protocols, and operating in real or simulated environments.

- Test actual execution of response and recovery procedures
- Validate technical recovery capabilities and timelines
- Exercise interoperability with external agencies or vendors
- Satisfy regulatory exercise requirements
- Produces the most rigorous after-action findings

After-Action Review & Continuous Improvement

Every exercise and every real incident is an opportunity to improve. The after-action review (AAR) is what converts the experience into a better plan.

1

Document Findings

Record what worked, what didn't, and what was unclear during the exercise or incident. Capture participant feedback immediately.

2

Prioritize Gaps

Categorize findings by severity. Critical gaps (safety, compliance, operational) go to the front of the improvement queue.

3

Update Plans

Revise plan documents to reflect findings. Update procedures, contacts, and assumptions. Re-version and redistribute.

4

Schedule Re-Exercise

Verify significant changes with a follow-up exercise. Establish the next exercise date before closing the current cycle.

TDW

CYBERSECURITY • IT CONSULTING

25 years of embedded critical infrastructure consulting — building and maintaining contingency plans, crisis exercises, and risk programs for energy cooperatives and water utilities for nearly two decades.

- Full contingency plan suite — CIRP, ERP, BCP, CMP — aligned to FEMA NIMS
- Crisis exercise design and facilitation — tabletop and functional
- After-action review and plan improvement programs
- 19-year embedded engagements with energy and water utility clients

tdwco.com