**Tool 1: The 5-Question BCP Check & Program Scope Worksheet**
A workable plan answers five fundamental questions before a disruption forces them. It is built function by function, not department by department. Use this worksheet to establish program scope, define executive accountability, and audit core operational tolerances.

## 1. PROGRAM GOVERNANCE & POLICY REGISTRATION

| | | | |
|---|---|---|---|
| **Organization / Entity:** | *[ Enter entity name ]* | **Executive Sponsor:** | *[ Named C-Suite executive ]* |
| **BCP Coordinator:** | *[ Named program manager ]* | **Plan Version & Review Date:** | *v2026.1 • Oct 31, 2026* |
| **In-Scope Facilities / Sites:** | *[ Primary HQ, branch facilities, warehouse/fulfillment centers, data centers ]* | | |
| **In-Scope Products / Services:** | *[ Regulated customer operations, payment processing, client delivery, core supply chain ]* | | |

## 2. THE 5-QUESTION BCP CRITICALITY AUDIT (FUNCTION BY FUNCTION)

Evaluate your organization's core operations against the 5 questions defined in the guide. Complete one row per critical function.

| 1. CRITICAL FUNCTION<br>WHICH CANNOT WAIT? | 2. TOLERABLE DOWNTIME<br>MTPD & RTO TARGET | 3. WORKAROUND STRATEGY<br>WHAT DO PEOPLE DO INSTEAD? | 4. COMMAND & ACTION<br>WHO DECIDES & WHO ACTS? | 5. STAND DOWN<br>HOW RETURN TO NORMAL? |
|---|---|---|---|---|
| **Function A: Payroll & Disbursements** | MTPD: 5 Days<br>**RTO: 72 Hours** | Process via off-site manual batch files or secondary banking portal from remote laptops. | **Decider:** CFO / VP HR<br>**Actor:** Payroll Lead + Alternate | Dual reconciliation against GL; verify direct deposits. |
| **Function B: Order Intake / Dispatch** | MTPD: 24 Hours<br>**RTO: 4 Hours** | Manual paper order logs, phone-in dispatching, or reroute to secondary branch site. | **Decider:** Operations Dir<br>**Actor:** Order Desk Lead | Back-enter manual tickets; physical inventory recount. |
| **Function C: Client Billing & Invoicing** | MTPD: 10 Days<br>**RTO: 5 Days** | Offline invoice templates; manual receipt logging; hold non-urgent billing runs. | **Decider:** Controller<br>**Actor:** Billing Supervisor | Re-sync ERP database; audit sequential invoice IDs. |
| **Function D: Customer Support / Hotline** | MTPD: 8 Hours<br>**RTO: 2 Hours** | Redirect VoIP telephony to mobile hunt groups; deploy pre-drafted status banner. | **Decider:** Support Dir<br>**Actor:** Support Shift Lead | Restore call queues; log ticket resolution back-history. |
| *[ Enter Function E ]* | *MTPD: RTO:* | *[ Document workaround ]* | *Decider: Actor:* | *[ Stand-down criteria ]* |
| *[ Enter Function F ]* | *MTPD: RTO:* | *[ Document workaround ]* | *Decider: Actor:* | *[ Stand-down criteria ]* |

## 3. THE 4 FATAL TRAPS TO REFUSE ON DAY ONE

**Trap 1: IT-Only Scope**
Disaster recovery restores servers; business continuity is what staff do while servers are down. Ensure manual processes, alternate facilities, and supplier backups are documented.

**Trap 2: Department vs. Function Thinking**
Departments hold multiple activities of differing urgency. Build playbooks around specific functions (e.g. "dispensing medication" vs "the pharmacy department").

**Trap 3: Single Named Responders**
Every role must have a named primary owner AND a named alternate. An alternate who doesn't know they are on the plan is a single point of failure with a title page.

**Trap 4: Inaccessible Storage**
Plans stored solely behind corporate single-sign-on or on internal file shares are inaccessible during a network collapse. Keep offline encrypted copies and physical binders.

**The Threat-Agnostic Principle:** Fires, floods, cyberattacks, severe weather, and pandemics are distinct causes that produce identical operational effects. Good plans are written against the *effect* — Loss of Site, Loss of System, Loss of People, or Loss of Supplier — so one playbook covers threats nobody predicted.

## 1. THE FOUR OPERATIONAL LOSS MODES

### LOSS MODE 1: LOSS OF SITE (Physical Premises)

**Triggers:** Structural damage, fire, localized flooding, power grid blackout, HAZMAT exclusion, denial of access.

**Standard Workarounds:** Relocation to secondary facility, distributed remote work from home, reciprocal space-sharing agreements, mobile workspace trailers.

### LOSS MODE 2: LOSS OF SYSTEM (Technology & Data)

**Triggers:** Ransomware lockup, core ERP database corruption, SaaS outage, telecommunications cut, hardware failure.

**Standard Workarounds:** Paper-based forms, offline local spreadsheets, secondary cloud failover, telephone dispatch, manual tracking ledgers.

### LOSS MODE 3: LOSS OF PEOPLE (Key Personnel)

**Triggers:** Communicable illness / pandemic, transit shutdown, key staff departure, concurrent family emergencies.

**Standard Workarounds:** Pre-identified named alternates, cross-training matrix, documented SOPs, contractor surge staff, emergency delegating of authority.

### LOSS MODE 4: LOSS OF SUPPLIER (Third-Party Partners)

**Triggers:** Vendor insolvency, courier / supply chain strike, single-source part shortage, supplier cybersecurity breach.

**Standard Workarounds:** Pre-negotiated secondary vendor contracts, emergency buffer stock, alternative logistics routes, component substitution.

## 2. THREAT-AGNOSTIC WORKAROUND MATRIX (FILLABLE PLANNER)

| CRITICAL FUNCTION | LOSS OF SITE WORKAROUND | LOSS OF SYSTEM WORKAROUND | LOSS OF PEOPLE WORKAROUND | LOSS OF SUPPLIER WORKAROUND |
|---|---|---|---|---|
| **Function 1: Customer Service / Orders** | Staff shift to pre-configured remote softphones; calls routed to cellular hunt group. | Log incoming customer calls on paper intake sheets; queue orders for manual entry. | Shift leads step in; activate cross-trained sales reps on priority customer queues. | Reroute out-of-stock items to secondary fulfillment vendor under agreed master SLA. |
| **Function 2: Payment Processing** | Finance team operates from secondary branch office or encrypted home workstations. | Switch to offline standalone card terminals or secure telephone authorization. | Secondary authorized signatory steps in; backup payroll specialist executes run. | Switch to secondary payment gateway; utilize emergency merchant backup facility. |
| **Function 3: Shipping & Logistics** | Divert incoming freight to secondary warehouse facility; dispatch from backup dock. | Generate offline bills of lading using standalone thermal printers and printed templates. | Deploy cross-trained receiving staff to primary packing lines; call vetted agency surge. | Engage backup regional carrier bench; spot-hire local dedicated courier fleet. |
| *[ Enter Function 4 ]* | *[ Document site workaround ]* | *[ Document system workaround ]* | *[ Document staffing workaround ]* | *[ Document vendor workaround ]* |
| *[ Enter Function 5 ]* | *[ Document site workaround ]* | *[ Document system workaround ]* | *[ Document staffing workaround ]* | *[ Document vendor workaround ]* |

## 3. WORKAROUND FEASIBILITY & LIMITATION REVIEW

| WORKAROUND CATEGORY | CAPACITY LIMIT (% OF NORMAL VOLUME) | MAXIMUM SUSTAINABLE DURATION |
|---|---|---|
| **Manual Paper Processing** | Typically 25% – 40% of normal transactional speed. | Maximum 3 to 5 business days before backlog creates fatal backlog. |
| **Distributed Remote Work** | Typically 70% – 90% (limited by home bandwidth/hardware). | Sustainable for 2 to 4 weeks provided cybersecurity holds. |
| **Secondary Supplier Bench** | Typically 50% – 80% volume allocation under surge pricing. | Depends on contract reserves and vendor capacity limits. |

**Design Standard:** Written for the person holding it at 3 a.m. — possibly not the person who authored it. Keep playbooks concise, sequential, and threat-agnostic. Deep analysis belongs in the BIA; this document is purely an operational runbook for day one of a disruption.

## 1. FUNCTION HEADER & RECOVERY OBJECTIVES

| | | | |
|---|---|---|---|
| **Function Name:** | *Client Invoicing & Cash Collections* | **Priority Tier / Rank:** | *Tier 2 • Recovery Rank #3* |
| **RTO (Recovery Target):** | *72 Hours (3 Business Days)* | **MTPD (Max Outage):** | *120 Hours (5 Business Days)* |
| **Primary Owner:** | *Jane Doe, AR Supervisor (Ext 401, Cell 555-0144)* | **Named Alternate:** | *Mark Smith, Senior Accountant (Cell 555-0182)* |

## 2. FIRST 3 ACTIONS IN THE FIRST HOUR (00:00 – 01:00)

**MANDATORY IMMEDIATE PROTOCOLS UPON PLAN ACTIVATION:**

☐ **Action 1 (T+15m): Confirm Disruption & Verify Roster:** Primary or Alternate contacts all function team members via mobile signal group; establish who is available and fit to operate.

☐ **Action 2 (T+30m): Check In with BCP Coordinator:** Report operational status (Green / Amber / Red) to Incident Command; declare whether primary site/systems are accessible.

☐ **Action 3 (T+60m): Mobilize Workaround & Retrieve Offline Records:** Access encrypted offline emergency files / paper templates; halt automated batch routines to prevent corruption.

## 3. SEQUENTIAL WORKAROUND PROCEDURES

| STEP | PROCEDURE NAME | STEP-BY-STEP EXECUTION INSTRUCTIONS | RESPONSIBLE ROLE |
|---|---|---|---|
| **1** | Establish Workspace | If primary site unavailable, instruct team to connect via secondary branch facility or secure home broadband VPN. Verify MFA credentials. | Owner / Alternate |
| **2** | Deploy Offline Forms | Retrieve emergency offline invoice templates stored on encrypted offline storage (USB drive or backup drive). Confirm tax calculation tables. | Billing Specialist |
| **3** | Triage Invoicing Queue | Sort pending billing into critical vs non-critical. Prioritize milestone billings exceeding $10,000; defer minor recurring charges until restoration. | Billing Supervisor |
| **4** | Manual Transmission | Generate standalone PDF invoices; transmit via verified secondary email relay or secure courier to client finance contacts. | AR Specialist |
| **5** | Offline Log Entry | Record all manual invoice numbers, amounts, client IDs, and transmission timestamps in the *Manual Incident Ledger*. Maintain sequential control. | AR Specialist |
| **6** | Daily Command Status | Submit end-of-day summary to BCP Coordinator: volume invoiced, backlog volume, cash collections, and any emerging vendor/banking friction. | Owner / Alternate |

## 4. FUNCTION DEPENDENCIES MAP

| DEPENDENCY | PRIMARY RESOURCE REQUIRED | BACKUP / WORKAROUND RESOURCE |
|---|---|---|
| **People (Staffing)** | Minimum 2 billing specialists + 1 supervisor. | Cross-trained AP team members; named contract firm. |
| **Systems (Software)** | Cloud ERP / Billing engine & Corporate Email. | Standalone offline spreadsheet & secondary Gmail domain. |
| **Sites (Workspaces)** | HQ Finance Wing (Floor 3). | Remote home offices with dedicated cellular hotspot. |
| **Vital Records** | Active client master contracts & banking details. | Encrypted monthly offline backup on secure flash drive. |
| **Suppliers (Vendors)** | Primary merchant acquiring bank & clearinghouse. | Secondary merchant bank account with direct wire capability. |

> **Execution Under Command:** Response is what happens in the first hours. Having activation criteria, notification trees, and message templates drafted in advance prevents panic and improvised communications during high-stress hours.

## 1. ACTIVATION CRITERIA & AUTHORITY LOG

Define who possesses the formal authority to declare a continuity event and activate playbooks based on explicit objective thresholds:

| DISRUPTION EVENT | ACTIVATION THRESHOLD CRITERIA | AUTHORIZED DECIDER | ALTERNATE |
|---|---|---|---|
| **Facility Unavailability** | Primary building inaccessible or unsafe for > 2 continuous hours during business day. | Chief Operating Officer | Facilities Director |
| **Core Technology Outage** | Unplanned downtime of primary ERP / customer system projected to exceed 4 hours. | Chief Information Officer | IT Operations Lead |
| **Severe Staff Depletion** | > 35% absenteeism in critical functions due to weather, transit, or contagion. | Chief People Officer | Operations Director |
| **Key Vendor Disruption** | Primary supplier stoppage affecting critical customer deliverables with no ETA < 8h. | Supply Chain Director | Procurement Manager |

## 2. NOTIFICATION & ESCALATION TREE

| COMMAND LEVEL | ROLE & PRIMARY NAMED CONTACT | ALTERNATE NAMED CONTACT | COMMUNICATION CHANNEL & SLA |
|---|---|---|---|
| **Tier 1: Command** | Executive Sponsor: CEO / COO<br>Cell: 555-0101 • Signal App | Executive Alternate: CFO<br>Cell: 555-0102 • Secondary Mobile | Automated emergency broadcast + phone call. Target: within 15 minutes of detection. |
| **Tier 2: Coordination** | BCP Coordinator: Crisis Manager<br>Cell: 555-0120 • Private VoIP | Deputy Coordinator: Ops Specialist<br>Cell: 555-0121 • Direct Cell | Mobilizes function leaders; opens incident bridge line. Target: within 30 minutes. |
| **Tier 3: Functions** | Function Leads (Payroll, AR, CS)<br>Department group channels | Designated Function Alternates<br>Individual emergency lists | SMS broadcast to active roster; account for personnel. Target: within 45 minutes. |

## 3. PRE-DRAFTED CRISIS COMMUNICATION TEMPLATES

**TEMPLATE 1: INTERNAL STAFF ADVISORY (SMS / Emergency App / Email)**

"*ATTENTION ALL EMPLOYEES: [Company Name] has activated its Business Continuity Plan due to [disruption type, e.g. power outage at HQ / network interruption]. All staff assigned to [Site/Department] should [DO NOT REPORT TO BUILDING / SWITCH TO REMOTE WORK PROTOCOLS]. Check in with your department supervisor via [Signal/SMS] by [Time]. Updates will be posted every [2 hours] on [emergency intranet/portal]. Your safety is our highest priority.*"

**TEMPLATE 2: CUSTOMER & CLIENT SERVICE ADVISORY (Email / Web Banner)**

"*IMPORTANT SERVICE UPDATE: [Company Name] is currently experiencing a temporary operational disruption affecting [specific service/facility]. In accordance with our business continuity standards, our teams have transitioned to secondary operating procedures to maintain critical customer operations. Core processing continues, but response times may be extended by [timeframe]. For urgent requests, please contact our dedicated continuity desk at [phone/email]. Next formal update will be provided at [Time].*"

**TEMPLATE 3: REGULATOR & STATUTORY NOTIFICATION (Formal Letter / Portal)**

"*FORMAL NOTICE OF OPERATIONAL EVENT: Pursuant to [applicable regulatory standard / statutory rule], this notice informs [Regulator Name] that [Entity Name] experienced a disruption to [regulated function] commencing at [Timestamp] due to [cause, if known]. Our Business Continuity Management System has been fully activated. Critical activities have transitioned to [workaround/alternate site]. Current customer impact is assessed as [Minor/Contained]. Our BCP Coordinator [Name/Contact] is available for inquiries. A preliminary incident report will follow within [24/48 hours].*"

> **Recovery Closes the Event:** Recovery ends when the business is whole again — not when the workaround starts. Restoring normal operations requires systematic reconciliation of work done during workarounds, formal stand-down authorization, and writing lessons learned directly back into the plan.

## 1. STAND-DOWN AUTHORIZATION & RETURN CRITERIA

Never improvise the end of an incident. All 4 criteria must be satisfied prior to declaring stand-down:

| STAND-DOWN GATE | VERIFICATION STANDARD | STATUS | SIGN-OFF |
|---|---|---|---|
| **1. Environment Stable** | Primary facility inspected, power/HVAC stable, physical security confirmed. | ☐ Verified | *[ Facilities Lead ]* |
| **2. IT Integrity Verified** | Core databases restored, network connectivity solid, cybersecurity cleared. | ☐ Verified | *[ CIO / CISO ]* |
| **3. Backlog Quantified** | Manual workarounds stopped; all unprocessed transactions counted and queued. | ☐ Verified | *[ Ops Coordinator ]* |
| **4. Executive Declaration** | Executive Sponsor formally declares continuity event terminated. | ☐ Declared | *[ Executive Sponsor ]* |

## 2. TRANSACTION & DATA RECONCILIATION PROTOCOL

**Step 1: Freeze Workarounds**
Instruct all function leads to cease manual paper logs and offline spreadsheets. Timestamp the exact transition cutoff time.

**Step 2: Sequential Audit**
Audit all physical and offline records. Verify document sequencing, missing ticket numbers, and manual signatures.

**Step 3: Dual Entry & Recon**
Back-enter manual transactions into primary systems. Perform dual balance checks against GL and inventory counts.

## 3. LESSONS-BACK-INTO-PLAN REMEDIATION LOG

Every real disruption or tabletop exercise reveals deficiencies. Log findings here and assign single-point accountability to update the plan within 30 days:

| ITEM # | OBSERVATION & FAILURE MODE | REQUIRED PLAN / PROCEDURE UPDATE | SINGLE OWNER | TARGET DATE |
|---|---|---|---|---|
| **REC-01** | Staff contact tree had 4 disconnected mobile numbers during overnight alert. | Implement quarterly mandatory contact verification; adopt automated SMS broadcast tool. | HR Director | Nov 30, 2026 |
| **REC-02** | Order desk manual forms lacked field for state sales tax calculation. | Update and reprint offline order forms; embed pre-calculated county tax tables. | Billing Supervisor | Nov 15, 2026 |
| **REC-03** | Backup supplier required 48h to ship components; caused customer delivery halt. | Renegotiate secondary SLA for guaranteed 12-hour dispatch; maintain 3-day on-site buffer. | Supply Chain Lead | Dec 15, 2026 |
| *[ REC-04 ]* | *[ Document observed gap ]* | *[ Document procedure revision ]* | *[ Named Owner ]* | *[ Due Date ]* |
| *[ REC-05 ]* | *[ Document observed gap ]* | *[ Document procedure revision ]* | *[ Named Owner ]* | *[ Due Date ]* |

## 4. DEMOBILIZATION & ADMINISTRATIVE CLOSEOUT

| | | |
|---|---|---|
| ☐ Release temporary facilities & leased hardware | ☐ Settle emergency vendor expenses & OT payroll | ☐ Secure and archive all manual incident logs |
| ☐ Issue stand-down notices to staff & clients | ☐ Conduct 24-hour hot wash debrief session | ☐ Distribute formal After-Action Report (AAR) |

> **Preventing Plan Rot:** Programs die when the cycle is run once and treated as finished. Untested, unmaintained plans rot at a predictable speed. Use this master checklist to audit your 4 pillars and track triggers that require immediate plan maintenance.

## 1. THE 4-PILLAR PROGRAM BALANCE AUDIT

| CONTINUITY PILLAR | CORE HYGIENE CHECK & VERIFICATION CRITERIA | SCORE (1-5) |
|---|---|---|
| **1. Prevention & Mitigation** | Single points of failure identified and mitigated; hardware maintenance contracts active; critical infrastructure hardened; suppliers audited for resilience. | *[ Score ] / 5* |
| **2. Preparedness** | BIA completed and approved; recovery objectives funded by leadership; function playbooks drafted; staff trained; alternate facilities and vendors contracted. | *[ Score ] / 5* |
| **3. Response** | Clear activation thresholds; designated incident commanders; 24/7 call trees verified; pre-drafted comms ready; offline runbooks accessible at 3 a.m. | *[ Score ] / 5* |
| **4. Recovery** | Formal return-to-normal protocols; data reconciliation checklists; demobilization checklists; mandatory post-incident lessons learned feed into plan updates. | *[ Score ] / 5* |

## 2. MAINTENANCE-ON-CHANGE TRIGGER TRACKER

Change invalidates plans silently. Do not wait for the annual review; update the BCP immediately upon any of these events:

| MATERIAL CHANGE EVENT | REQUIRED PLAN MAINTENANCE ACTION | TRIGGER DETECTED | PLAN UPDATED |
|---|---|---|---|
| **New Core IT System / SaaS** | Update loss-of-system workaround; audit data backup frequency; map dependencies. | *Date: _____* | ☐ *Done* |
| **Facility Opening / Move** | Map physical dependencies; establish alternate site arrangements; update logistics. | *Date: _____* | ☐ *Done* |
| **Staff Departure / Reorg** | Update primary owner and alternate roster; verify contact data; re-assign roles. | *Date: _____* | ☐ *Done* |
| **New Critical Supplier** | Audit supplier BCP; negotiate recovery SLAs; establish backup vendor alternatives. | *Date: _____* | ☐ *Done* |
| **New Regulatory Mandate** | Review compliance obligations (e.g. DORA / ISO 22301); update retention & audit logs. | *Date: _____* | ☐ *Done* |

## 3. TESTING & EXERCISING MASTER CALENDAR

| EXERCISE TYPE | SCOPE / SCENARIO | TARGET DATE | COORDINATOR LEAD |
|---|---|---|---|
| **Tabletop Simulation (Q1)** | Scenario: Ransomware attack & loss of corporate ERP. | Q1 2027 (Feb 15) | BCP Coordinator + IT Lead |
| **Tabletop Simulation (Q3)** | Scenario: Severe regional flood & loss of primary facility. | Q3 2027 (Aug 15) | BCP Coordinator + Facilities |
| **Live Workaround Test** | Execution: Run order processing on paper forms for 4 hours. | Q2 2027 (May 10) | Operations & AR Lead |
| **Call Tree & Alert Drill** | Test: Unannounced off-hours SMS broadcast to all alternates. | Q4 2027 (Nov 05) | HR Director |