Agility Recovery

Guide

Mid-Year BC Plan Review Guide

Is your plan still accurate? Here's how to find out fast.

Table of Contents

Introduction

Business continuity plans go stale faster than most organizations realize. Personnel change, vendors shift, technology gets replaced. And real-world events like storms, outages, ransomware attacks, and supply chain failures expose assumptions that looked reasonable when the plan was written.

The halfway point of the year is a practical moment to run a quick check. Not a full plan overhaul; just a structured review to confirm that what's documented still reflects how your organization actually operates.

This guide walks through the five areas most likely to drift between plan reviews, with a checklist you can complete in an afternoon.

Contact Lists and Roles

Outdated contact information is one of the most common plan failures — and one of the easiest to fix. Even a 6-month-old plan may list people who have left the company, been promoted, or taken on different responsibilities.

Check:

- [ ] Every person named in the plan still works there and is in the same role
- [ ] Emergency contact numbers are current (personal cell, not just office lines)
- [ ] Recovery team members know they're on the list
- [ ] There's a documented backup for each critical role
- [ ] Key vendor and supplier contacts have been verified within the last 90 days

> **Quick Test**
> Pick three contacts from your plan at random and try to reach them. If you can't get through on the first attempt, your contact list needs attention.

Recovery Time and Recovery Point Objectives

RTOs and RPOs are the foundation of your recovery strategy. They define how long your organization can tolerate downtime and how much data loss is acceptable. If your operations have changed since those targets were set, the targets may no longer reflect business reality.

Check:

- [ ] RTOs and RPOs are documented for each critical business function
- [ ] RTOs still reflect actual business tolerance (revenue impact, regulatory requirements, customer SLAs)
- [ ] Any new products, services, or processes added in the last 6 months have been assigned RTOs and RPOs
- [ ] Technology changes haven't created gaps between what's recoverable and what's required

> **Worth Asking**
> Has your business grown, added services, or changed operating hours since your RTOs were last set? Growth often increases recovery complexity without a corresponding update to targets.

Technology and Data Recovery

Technology environments change constantly. New systems get added, old ones get retired, and cloud migrations create dependencies that weren't in the original plan. Data backup configurations deserve particular attention — a backup that hasn't been tested is a backup you can't rely on.

Check:

- [ ] Backup configurations cover all critical systems, including any added in the past 6 months
- [ ] Backup restoration has been tested within the last 90 days
- [ ] Cloud services and SaaS applications have documented recovery procedures
- [ ] Cybersecurity response steps are included in or linked from the BC plan
- [ ] Access credentials for recovery systems are current and securely stored
- [ ] Any retired systems have been removed from recovery procedures

> **Keep in Mind**
> According to the IBM Cost of a Data Breach Report 2025 (Ponemon Institute), organizations that experienced breaches lasting over 200 days faced average costs of $5.01M vs. $3.87M for those contained faster. Your technology recovery procedures directly affect that timeline.

Facilities and Alternate Work Locations

If your plan assumes access to a specific building or workspace, verify those assumptions are still valid. Physical locations change — leases end, layouts shift, and building access procedures get updated.

Check:

- [ ] Primary workspace recovery location is still available and under agreement
- [ ] Access procedures and security credentials for alternate sites are current
- [ ] Remote work capabilities have been documented if the plan relies on them
- [ ] Any new facilities or locations have been added to recovery scope
- [ ] Critical equipment inventories are accurate — both what's on-site and what would be needed in recovery

Plan Testing and Training

A plan that hasn't been tested is a plan with unknown gaps. Review testing history and confirm that the people responsible for executing recovery procedures are prepared to do so.

Check:

- [ ] A tabletop exercise or full test has been completed in the last 12 months
- [ ] Test results and any corrective actions are documented
- [ ] New team members have received BC/DR orientation
- [ ] A test is scheduled for the second half of 2026
- [ ] Lessons from any real events in H1 — outages, weather, cyber incidents — have been incorporated

Mid-Year Review Checklist

Use this checklist to track your review progress. A “No” on any item is a gap that needs a remediation owner and a deadline.

Contacts and Roles

Review Item	Yes	No	N/A
All named contacts are still in their listed roles	○	○	○
Emergency contact numbers are verified and current	○	○	○
Each critical role has a documented backup	○	○	○
Recovery team members have been notified of their responsibilities	○	○	○
Key vendor/supplier contacts verified within the last 90 days	○	○	○

RTOs and RPOs

Review Item	Yes	No	N/A
RTOs and RPOs are documented for all critical functions	○	○	○
Targets still align with current business tolerance and SLAs	○	○	○
New products, services, or processes have been assigned targets	○	○	○
Technology changes have not created gaps in recoverability	○	○	○

Technology and Data

Review Item	Yes	No	N/A
Backup configurations cover all critical systems	○	○	○
Backup restoration tested within the last 90 days	○	○	○
Cloud and SaaS applications have documented recovery procedures	○	○	○
Cyber incident response steps are in the plan or linked	○	○	○
Recovery credentials are current and securely stored	○	○	○
Retired systems have been removed from recovery procedures	○	○	○

Facilities and Alternate Locations

Review Item	Yes	No	N/A
Primary alternate workspace is still available and under agreement	○	○	○
Access procedures and credentials for alternate sites are current	○	○	○
Remote work capabilities are documented if the plan relies on them	○	○	○
New facilities have been added to recovery scope	○	○	○

Testing and Training

Review Item	Yes	No	N/A
A tabletop or full test was completed in the last 12 months	○	○	○
Test results and corrective actions are documented	○	○	○
New team members have received BC/DR orientation	○	○	○
A test is scheduled for H2 2026	○	○	○
Lessons from H1 real-world events have been incorporated	○	○	○

Agility Recovery

This report presents information of a general nature, and Agility Recovery is not, using this publication, rendering any professional advice or services. This publication should not replace a professional counsel or services, nor should it be used as a sole guiding principle for any decision or action that may affect your organization. Before making any business decision or taking any action that may affect your business, you should consult a professional. Agility shall not be responsible for any loss resulted from relying on this publication.

Agility Recovery takes action to get your business back on its feet after any disaster, providing you with comprehensive support and resources when you need it most. Our end-to-end solutions are fully customizable to meet the unique needs of your business and protect against interruptions large and small – from major natural disasters to planned renovations. Whatever it takes to keep you in business, that's what we do.

Visit our website for more information.