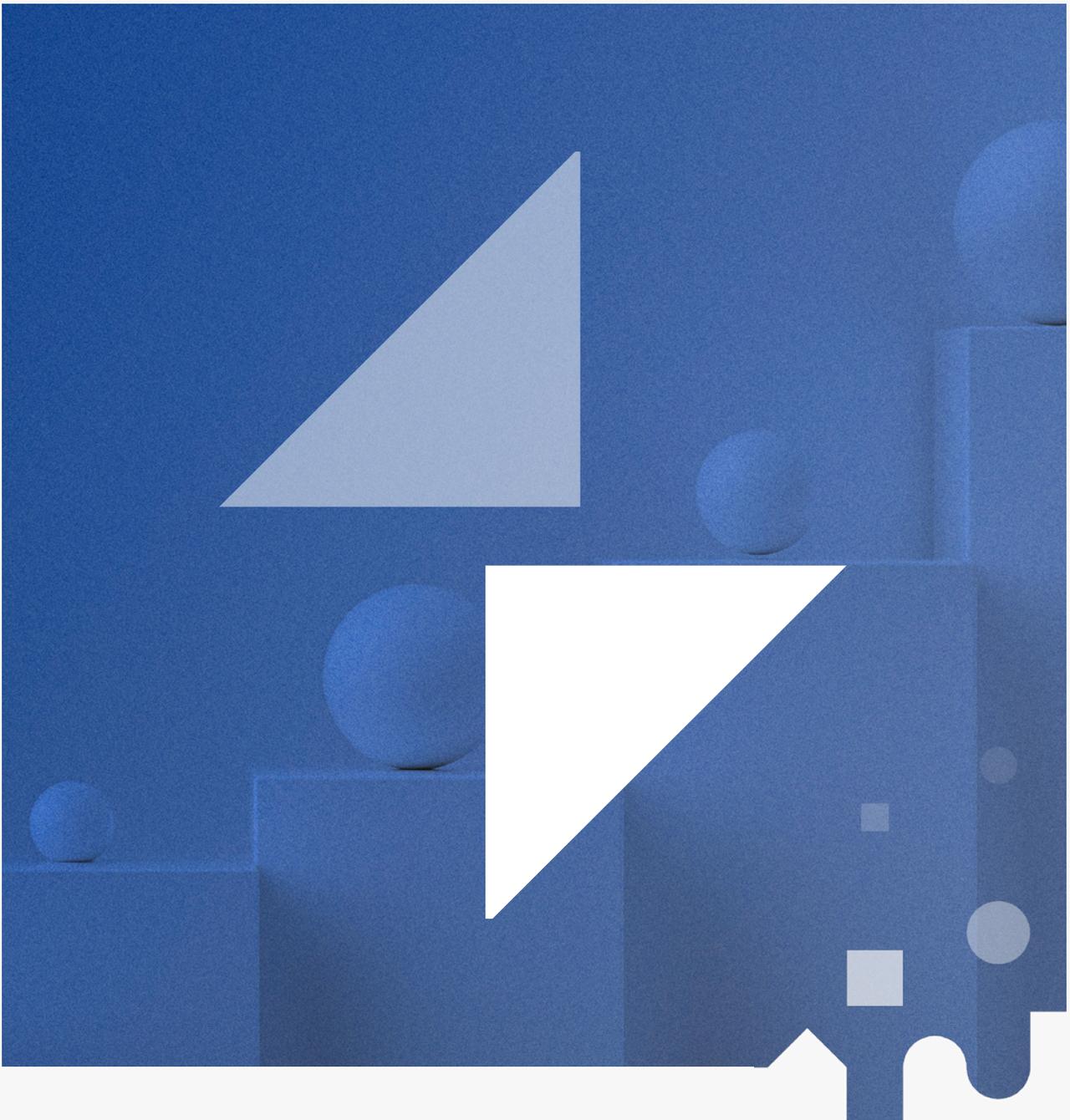
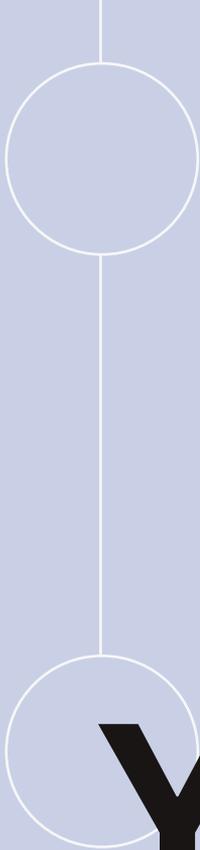


# 21 steps

**to executing an IT disaster recovery  
plan that actually works**





**Y**ou'd think that by now, in a time of inevitable power outages, cyber attacks, global crises, and complex technology estates, organizations would have fortified their technology by developing solid IT disaster recovery plans. But the reality is, according to [securitymagazine.com](http://securitymagazine.com), 54% of them still don't have a company-wide IT DR policy in place, which can expose business operations to serious risks.

Those that do have IT DR plans in place may be overestimating their effectiveness. A recent Gartner survey found that while 86% of information and operations leaders said their recovery capabilities met or exceeded CIO expectations, "only 27% of that group consistently undertook three of the most basic elements expected of a (disaster recovery) program — formalizing scope, performing a (business impact analysis)...and creating detailed recovery procedures."

Although disaster recovery tests are often successful in delivering the expected outcome, this rarely relates to their actual ability to recover in a crisis.

## Walking blindly through tests

Another issue that fuels overconfidence in IT DR plans is too much faith in testing. [In a Cutover discussion](#) entitled “Have we been fooling ourselves about testing?” at DRJ’s March conference, Northpointe Bank CTO Michael Gibeaut recalled drawbacks he encountered with traditional, time-consuming testing: “We walk through these exercises blindly...we check the boxes, we work with risk, we work with our compliance partners but (the test) truly isn’t what would happen in an actual event, so we have to change the way we think.”

The need for new ways of thinking about IT DR planning and testing is growing more urgent. Data breach costs reached \$4.24 million in 2022, the highest average total cost in 17 years, power supply threats surged, and software issues caused major disruptions and recalls - such as Atlassian’s major cloud outage and Tesla’s recall of 594,717 vehicles due to a technical issue.

“Technology is now at the center of company operations,” says Darren Lea, Cutover Product Manager for Operational Resilience. “Along with increased focus and attention on having the right technology, there should be equivalent focus and attention on ensuring those technology services are resilient. That starts with a plan to recover if things go wrong.”

We’ve gathered insights from Lea and other experts to help you create a resilient, realistic, and effective IT disaster recovery plan.

# These 21 steps to creating an IT DR plan can help you:

- ◇ Prepare more effectively for increased regulatory scrutiny
- Define and prioritize risks properly
- Better meet customer expectations
- Trim costs and save time



Figure 1: Savings from reduced incidents with Cutover

# I. FIRST STEPS: KNOW THY ORGANIZATION

---

## 1. To begin building your IT DR plan, confirm the technology services and infrastructure that underpin the services you provide to customers.

If you make use of ITIL (Information Technology Infrastructure Library) to manage and detail your IT activities and technologies, familiarize yourself with it. If not, try to get an understanding of IT services and IT assets in your company and assess which are most critical to business functions and which may be vulnerable to disruption. This inventory is critical — you can't make a good IT disaster recovery plan until you know the IT services your business depends upon.

## 2. Take a frank look at gaps in your current ability to handle a crisis.

What are both the human and technological gaps you have from moving operations from a primary to a secondary site? Do you know the failover will work within the timeframe you need to restore operations? And how do you know this? Examine what prior testing, if any, was done to determine these gaps.

## 3. Consider different scenarios you might face.

"We see more customers thinking outside the bounds of 'I'm going to test for the loss of my primary data center or site,'" Lea says. "That's a nuclear scenario. There's more complexity and subtlety in real-world events. A more likely scenario is a hard disk failing on a database server. You need to be more creative in the types of scenarios you want to test." Lea suggests thinking not only about large versus small tests but about timing — should a test be announced and planned for ahead of time or would it be more realistic if it was unannounced?

#### **4. Examine the risk versus reward of testing your plan.**

Will your test create a lot of disruption and take a lot of time for an unlikely scenario? Would more specific, real-world tests be more worthwhile?

#### **5. Make sure every person involved in your plan embraces it.**

The pandemic and other events have persuaded many C-suite and IT leaders about the importance of IT disaster recovery plans, Lea says. “Where I have seen reluctance is on the front lines, where people can sometimes pay lip service to testing or perform a recovery process that has minimal steps but needs more.” Leaders should create a culture in which employees at every level will know what’s expected of them and understand the part they play in creating and managing resilient services.

#### **6. Create a plan that everyone sees and understands.**

A common mistake made by plan owners is creating an IT DR process that only they can fully understand, which depends on the expertise of individuals for certain steps, and involves processes that are not fully documented. If you make the plan highly transparent and visible, you eliminate these knowledge and redundancy gaps, Lea says “as well as seeing opportunities for automation, you may be able to move people away from low value activities and towards higher value work.”

#### **7. Understand when to be flexible in your plan — and when not to be.**

If you are in the middle of a crisis event, too much flexibility can cause confusion. If teams know precisely what they need to do and when, that will speed recovery. Where you need to be flexible is in having an IT DR plan that accounts for different recovery scenarios.

## II. TESTING YOUR IT DR PLAN: PRACTICE HOW YOU PLAY

---

### 8. Determine when and how often you need to test your IT DR plans.

Financial services firms typically test a data center at least once a year and some have 15-20 data centers but many Cutover customers are looking to test more often and broaden the scale of what a test should encompass. “There are going to be limits by way of cost and by what your staff can support,” Lea says, “but you should test as often as you feel comfortable and can support without disruption to your business.”

### 9. Make your tests as real as possible.

A weeks- or months-long test with hundreds of people isn’t going to prepare you for an actual incident. To do that, CTO Gibeaut advocates the “practice like you play” method — conducting a weekend failover exercise from a primary to a secondary system, then using the next testing weekend to fail back. While this “failover and stay” may seem risky, it actually uses fewer resources and surfaces more potential problems than traditional testing, he says.

### 10. Make enough time for testing.

In many traditional test processes, just 20% of the time spent is on actual testing, with most of the time being spent on routine administration. Testing methods that use runbooks, as Cutover does, allow you to spend more time on testing rather than on administrative tasks.

### 11. Be mindful of accuracy.

To avoid mistakes later, make sure the scale of testing is right and that the breadth of testing will cover all the incident types you think are going to happen. Consider a surprise test — incidents happen unannounced all the time in the real world, so by springing a sudden test on your teams, you may be more likely to get real-world results.

## **12. Involve stakeholders at all levels of the test activity to more accurately replicate what would happen in an actual incident.**

To avoid mistakes later, make sure the scale of testing is right and that the breadth of testing will cover all the incident types you think are going to happen. Consider a surprise test — incidents happen unannounced all the time in the real world, so by springing a sudden test on your teams, you may be more likely to get real-world results.

## **13. Most importantly — practice, practice, practice how you play.**

Repeated activity builds muscle memory, which helps you become more resilient. Having a variety of IT DR scenarios that you rehearse for will build a flexible response for when incidents occur, so even if you can't predict every possible scenario you may need to respond to, you can still have confidence in your response.

# **III. IT'S GO TIME: EXECUTING YOUR IT DR PLAN**

---

## **14. Communication and transparency are key to making the disaster recovery process run smoothly.**

Make sure there is a central, visible, reliable way for everyone on your team to know what's going on. Handing out a manual or holding meetings might lead to more delays. People in crisis need to get information as quickly as possible. Cutover's Collaborative Automation platform provides a single, immediate source of truth, so that everyone can connect with each other and see who's doing what during an incident, which reduces stress and organizes chaos.

## **15. Keep interference to a minimum.**

Let your technology teams do what they're good at — they've tested and rehearsed the IT DR plan and they must be allowed to put it into action. IT leaders should be a buffer between those teams and business leaders, colleagues, and customers who can slow up or even stall the process with questions, comments, and requests.

## **16. Watch the clock.**

A quick recovery equals a less costly recovery and a better experience for customers and employees. Know what your Recovery Time Objective (RTO) is. Cutover has the unique ability to measure RTO against Actual Recovery Time (RTA) to help you gain insight during and after an IT DR event, showing where your recovery process is ahead of target or falling behind.

## **17. Remember, it's company first — not "me" first.**

IT DR plans should account for which business operations are most critical and those priorities should be adhered to — even if some stakeholders want to elbow their way to the front of the line. "Teams have to understand priorities, sequence their recovery activities, and be unselfish," Lea says.

## IV. AFTER THE DISASTER: LEARN FROM MISTAKES AND SUCCESSES

---

### 18. Once your recovery is complete, revisit your IT DR plans.

What were the differences between the scenarios you planned for and tested and what actually happened? And how can you incorporate those differences into revised plans?

### 19. Dig into the details of timing.

Compare your RTA with your RTO and see where you might have saved time or where there are other opportunities for improved execution efficiency. Cutover's automated system of record can help you zero in on where you can improve and where there is opportunity to recover wasted time.

### 20. Look at both how your people and your technology performed.

Did both behave in the way you thought they would? Was orchestration between them seamless or were there technical difficulties and delayed handovers? Again, this exploration will help you pinpoint what should be modified, if anything, in your IT DR plans.

### 21. Get feedback.

How does your own team assess its performance in the incident? How did business leaders and managers outside the team assess performance and what lessons may be learned from the incident? Did you receive any customer feedback, or do you have any insights on how other businesses fare during similar incidents? Some outside feedback may not be useful, but on the flip side, some can give you excellent ideas on evolving your IT DR strategy.

## V. SUMMARY AND SILVER LININGS

---

IT disaster recovery incidents are inevitable — it's never a question of if, it's always a case of when they will happen. But with solid IT DR plans and a platform like Cutover, you can minimize outages and save on the costs associated with them.

There are also many intangible benefits to creating IT DR plans using runbooks. Both the testing time and actual incident recovery time can be greatly reduced and that can give employees their weekends back. In an era where companies are struggling to retain IT talent, the right IT DR strategy and platform can provide an environment where people can do more high-value tasks, have more free time, and can empower your tech team do what they are most motivated to do.

“We still come across firms that don't have adequate IT DR plans,” Lea says, “but they get that they should have plans and that their spreadsheet-based planning isn't enough. When you have many people doing many things in a time-pressured and time-precious scenario, Cutover is a highly effective way to sequence and orchestrate your activities.”

[Find out how Cutover can help you move to unplanned testing.](#)

### Contact us for more information

@ Contact us

@gocutover

in follow us on LinkedIn

www.cutover.com

Ready to see how Cutover can help your organization plan, test, and execute a successful IT DR plan?

SCHEDULE A DEMO NOW