

How to build your IT DR plan with Cutover



What makes an IT disaster recovery plan effective and what steps can you take to improve your planning, testing, and recovery?

[In this paper](#), we outlined the first steps to building an effective IT disaster recovery plan, which include:

- ◆ Understanding the technology and infrastructure that underpin the services you provide to customers
- Making your tests as realistic as possible so you can practice how you play
- Ensuring you have an effective communications strategy in place
- ◆ Reviewing post-event to learn from your mistakes and successes
- Treating your plans as living documents that are constantly being used and improved, not static plans buried in a file somewhere

Our in-house resilience experts have shared these 10 detailed tips for how to build and run the most effective IT disaster recovery.

Jul 22 - DC1 Failover Live run (dynamic)

Pages Dashboards Tasks PIR Set Timezone

My tasks 910/910 tasks

This version was completed at 5 Mar 03:13

Stream Summary

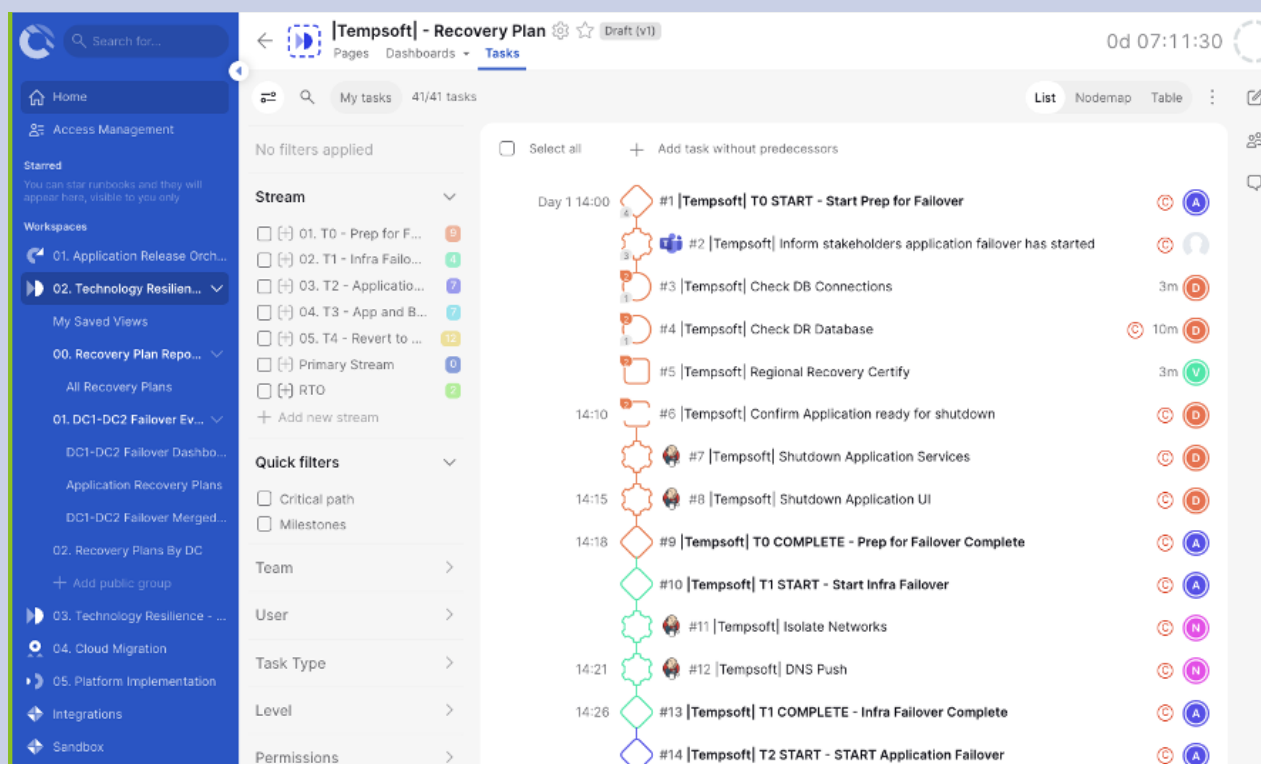
Title	Progress	Start	Finish	Duration
01. T0 - Prep For Failover	✓ COMPLETE	3 Mar 10:55 +25m 15s	4 Mar 03:56 +4h 33m	17h 1m
02. T1 - Infra Failover	✓ COMPLETE	3 Mar 11:05 +17m 12s	4 Mar 03:58 +4h 27m	16h 52m
03. T2 - Application Failovers	✓ COMPLETE	3 Mar 11:16 +20m 10s	4 Mar 10:02 -1h 18m	22h 45m
04. T3 - App and Business Validation	✓ COMPLETE	3 Mar 11:27 +15m 52s	5 Mar 03:12 +14h 51m	1d 15h
05. T4 - Revert to Primary Location	✓ COMPLETE	3 Mar 12:34 +23m 2s	5 Mar 03:13 +13h 7m	1d 14h
RTO	✓ COMPLETE	3 Mar 11:16 +20m 10s	4 Mar 10:02 -1h 18m	22h 45m
Aor - 4 Hours	✓ COMPLETE	3 Mar 19:11 +6h 33m	3 Mar 20:48 +4h 10m	1h 36m
Bytecard - 4 Hours	✓ COMPLETE	3 Mar 19:11 +6h 33m	3 Mar 20:48 +4h 10m	1h 36m
Crayze - 24 Hours	✓ COMPLETE	4 Mar 03:58 +4h 27m	4 Mar 10:02 -1h 18m	6h 4m
Deskget - 4 Hours	✓ COMPLETE	3 Mar 13:33 +55m 18s	3 Mar 19:11 +2h 33m	5h 38m
Fdeam - 4 Hours	✓ COMPLETE	3 Mar 23:18 +5h 14m	4 Mar 03:09 +5h 4m	3h 50m
Gembucket - 15 Mins	✓ COMPLETE	3 Mar 11:33 +37m 19s	3 Mar 11:36 +24m 50s	2m 31s

1

Keep track of the criticality of your IT infrastructure

A lot of things can go wrong when an outage hits your organization, so it's important that the documentation of which networks and applications are mission critical so that their recovery can be prioritized is easily accessible and up to date. Having defined the different tiers that your networks and applications fall into and assigned appropriate recovery time objectives (RTOs) based on how critical they are to the business, you can structure your recovery plans accordingly.

Cutover runbooks allow you to document all this information and automatically calculate and track your RTOs against RTAs, whether you're rehearsing or actually recovering from an incident.

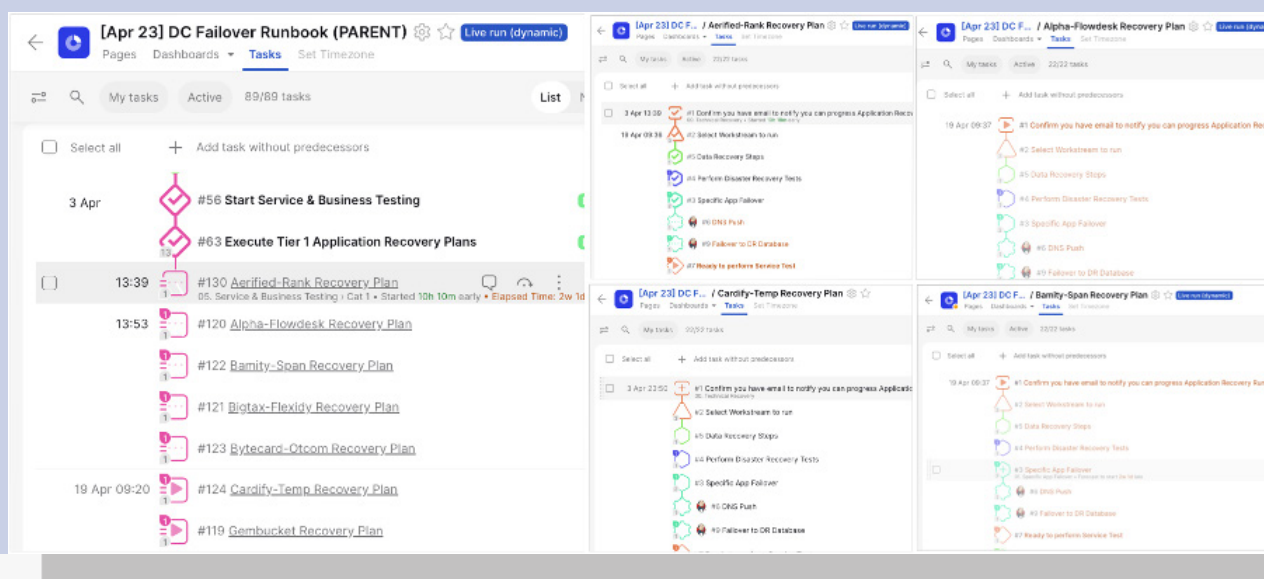


2

Build your service-oriented recovery plans

No matter what recovery tier you are addressing, the first step to effective recovery is building out your recovery plans. These should describe how to recover the functions you are responsible for and the steps required to bring each function back online, including both the technical and business steps that will need to be taken. These plans can then be used to test on a recurring basis to prove you have an effective recovery process and are prepared for an actual event or incident.

Cutover's dynamic, automated runbooks enable you to collaboratively build recovery plans that are executable in the same format for both tests and actual recoveries. Ingest data from your existing ITSM or CMDB solution into your Cutover runbooks via integrations to ensure data is consistent.

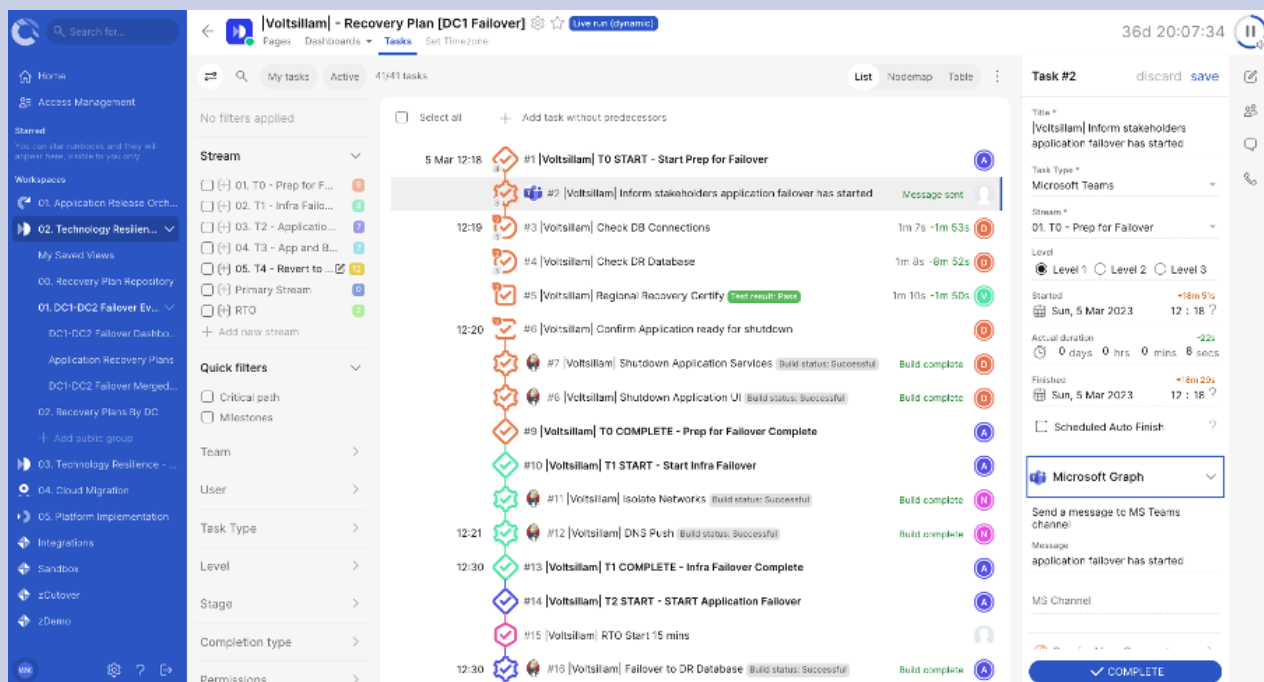


3

Structure your runbooks for efficiency and visibility

Whether you build out your individual service recovery plans and use those to feed into a larger event runbook, or build out the main runbook first and then drill down into the detail of individual plans, these service recovery plans form parts of the recovery test or event as a whole.

When using Cutover, we advise that users have a [main runbook](#) (or parent runbook) set up for the event which is overseen by the event organizer, who can start the runbook when an actual event or incident occurs and oversee the progress of the various individual linked service or application runbooks (or child runbooks) which are delegated out to each service owner or application team. When these are linked in Cutover, it is then easy to see the progress of the recovery as a whole and dig down into the detail of each individual recovery and quickly find problem areas that could cause delays.

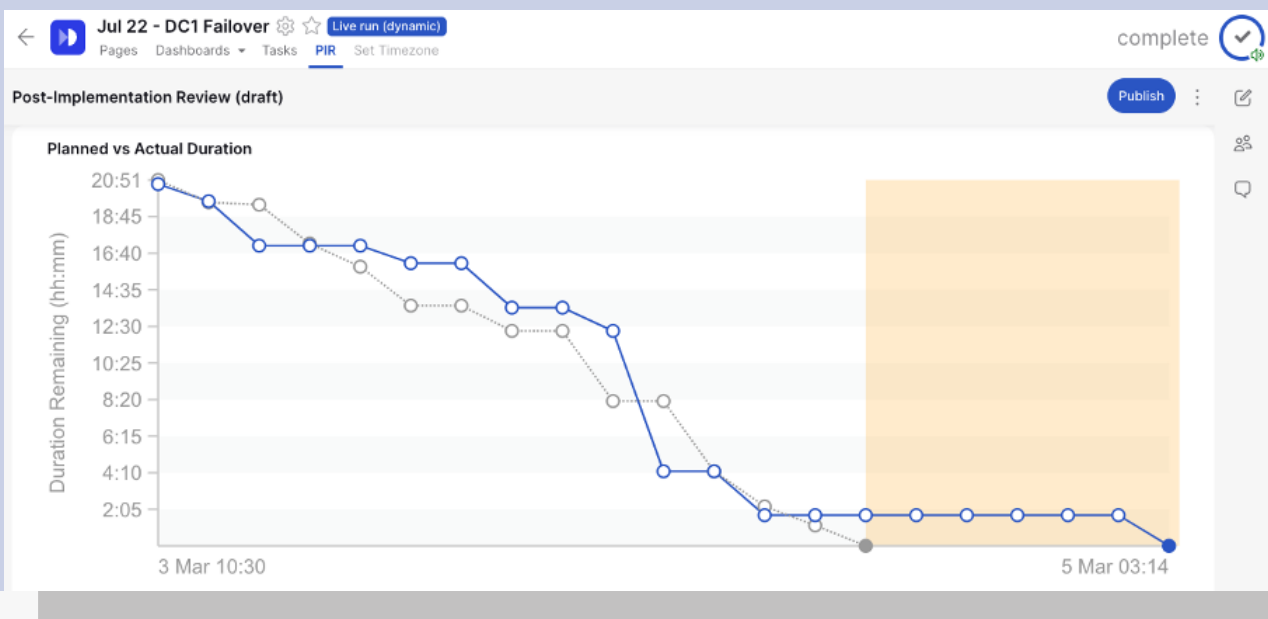


4

Enhance with automation and integrations

When undergoing a test or live recovery, you will likely need to use data from various IT service management (ITSM) or business continuity management (BCM) tooling such as ServiceNow, Remedy, or Fusion RM. By integrating these with Cutover, you can bring in data that is mastered elsewhere into your recovery plans - this could include the last known configurations of infrastructure that you're failing over, RTOs, and more.

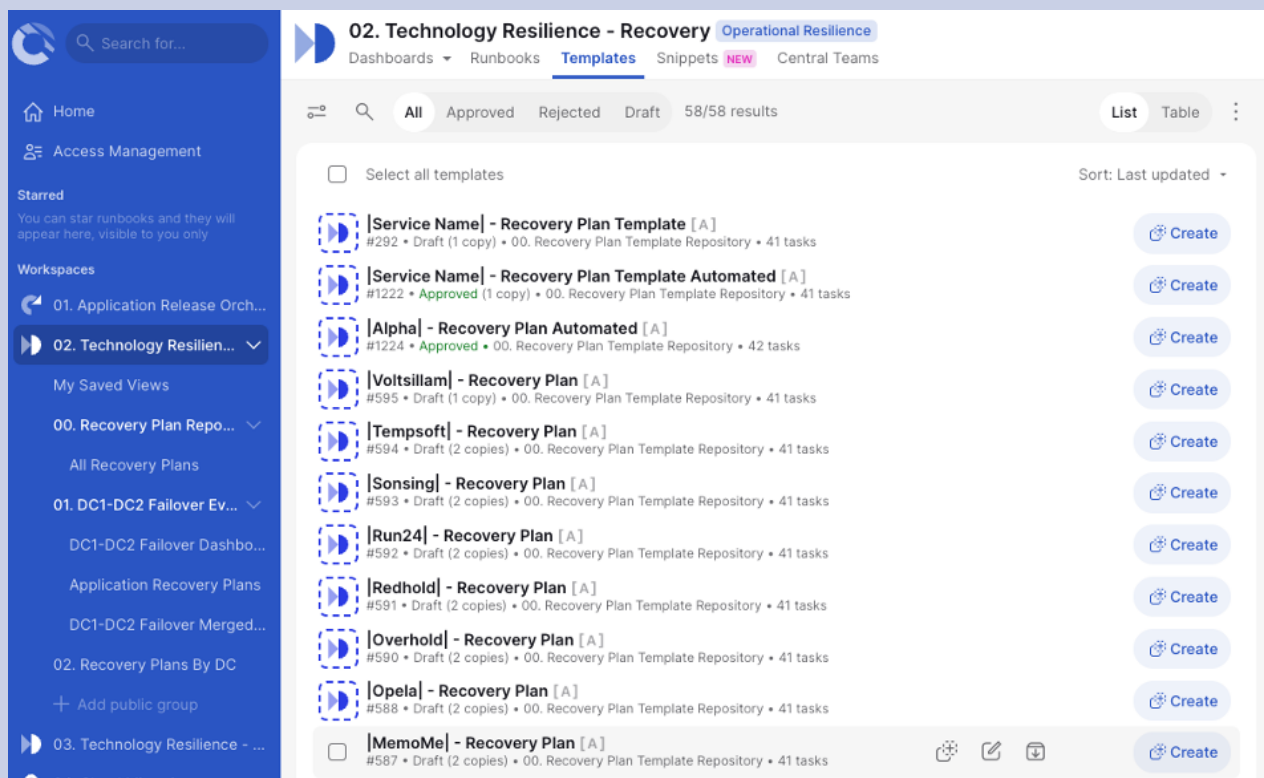
We would also recommend having your mass communications such as Microsoft Teams or Slack integrated into Cutover to keep everyone updated on status and when they need to initiate their tasks.



5

Measure recovery time actuals (RTAs) against RTOs

As you define the critical recovery tiers and associated RTOs for the various functions in your network, you should think about how you would separate out those activities to calculate RTAs - this might be all the activities in your recovery tiers or just a subset. Cutover provides a clear view via customizable real-time dashboards of how long these activities actually took against RTOs, whether these were met, and where delays may have happened.



6

Practice how you play

One way to ensure standardization and the most up-to-date plans is to define them in template form and then review them on a regular basis. You should be reviewing your plans every time you make a significant change to your IT service to ensure that they still hold up. Regularly reviewing your plans means you're ahead when it comes time to do a test as you don't have to worry about reviewing all your plans as part of that exercise

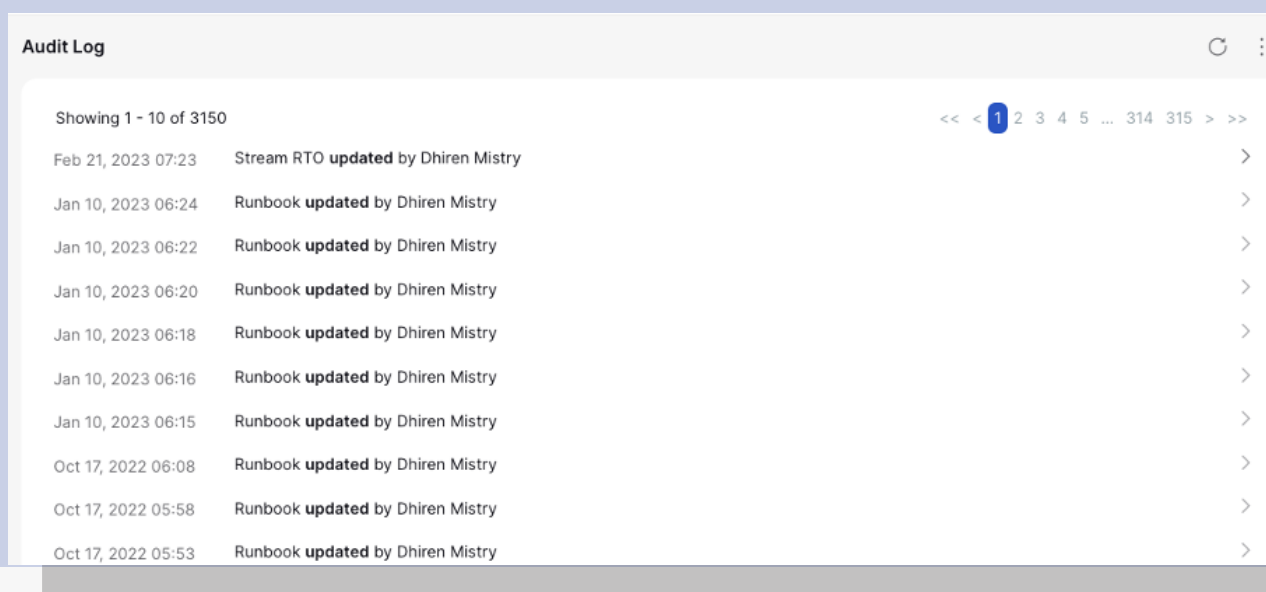
How often you review and run your tests is down to your level of risk appetite and maturity. We would advocate that you structure your tests to as closely mimic what you would actually do in response to an incident. To achieve this you can store pre-approved templates in Cutover to reduce the amount of preparation you do before the test as much as possible (this is where regularly updating your templates comes in), involving your major incident managers in your testing process so they're familiar with how everything works, and, in time, having major incident managers run the tests as well.

7

Prepare for every eventuality

When it comes to how you structure the content of your recovery plans, consider multiple scenarios and how your recovery would be different based on different challenges, such as having to do a bare metal recovery from a ransomware attack which would require a different plan from a regular recovery.

Similarly, while some organizations [mistakenly believe that resilience is automatic in the cloud](#), it's important to also have scenarios in place to recover or fail over services that are hosted on the cloud. For example, what will you do in the unlikely scenario that an entire cloud provider's region fails? Or how do you know you are recovering an immutable database after a ransomware attack?



The screenshot shows an 'Audit Log' window with a table of events. The table has three columns: a timestamp, an action description, and a right-hand icon. The first row shows 'Feb 21, 2023 07:23' for 'Stream RTO updated by Dhiren Mistry'. Subsequent rows show 'Runbook updated by Dhiren Mistry' with timestamps from Jan 10, 2023, down to Oct 17, 2022. A pagination bar at the top indicates 'Showing 1 - 10 of 3150' and includes navigation arrows and page numbers (1, 2, 3, 4, 5, ..., 314, 315).

Audit Log		
Showing 1 - 10 of 3150		
Feb 21, 2023 07:23	Stream RTO updated by Dhiren Mistry	>
Jan 10, 2023 06:24	Runbook updated by Dhiren Mistry	>
Jan 10, 2023 06:22	Runbook updated by Dhiren Mistry	>
Jan 10, 2023 06:20	Runbook updated by Dhiren Mistry	>
Jan 10, 2023 06:18	Runbook updated by Dhiren Mistry	>
Jan 10, 2023 06:16	Runbook updated by Dhiren Mistry	>
Jan 10, 2023 06:15	Runbook updated by Dhiren Mistry	>
Oct 17, 2022 06:08	Runbook updated by Dhiren Mistry	>
Oct 17, 2022 05:58	Runbook updated by Dhiren Mistry	>
Oct 17, 2022 05:53	Runbook updated by Dhiren Mistry	>

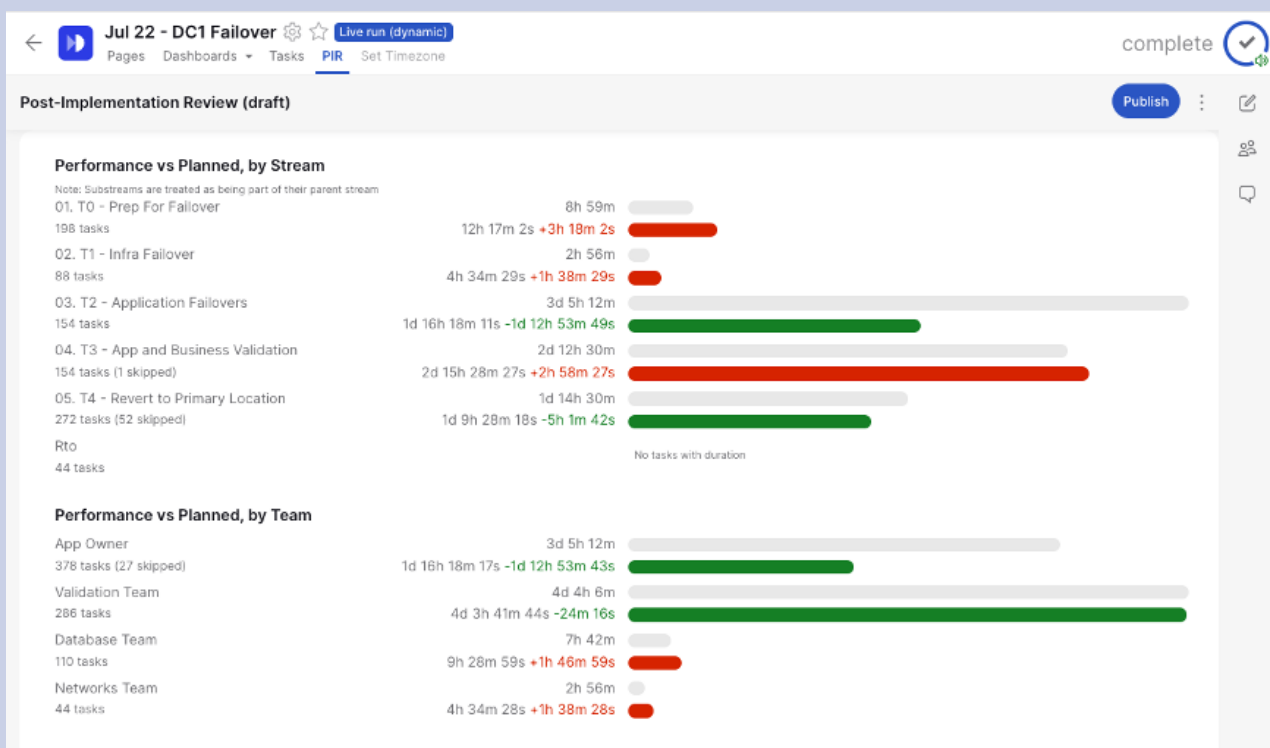
8

Set yourself up for success to meet regulatory requirements

Think ahead about what regulators will need to see and structure your plans with the outputs you will need for regulators in mind. If you put your plans together in a way that takes post-event audits and reporting into account it will be much quicker, easier, and more

straightforward to prove your company's ability to recover from an outage.

Cutover's automated audit trail tracks every action taken in Cutover, when it happened, and who completed it, giving you all the data you need for post-event audit and review without having to search for it or reconstruct what happened post-event.



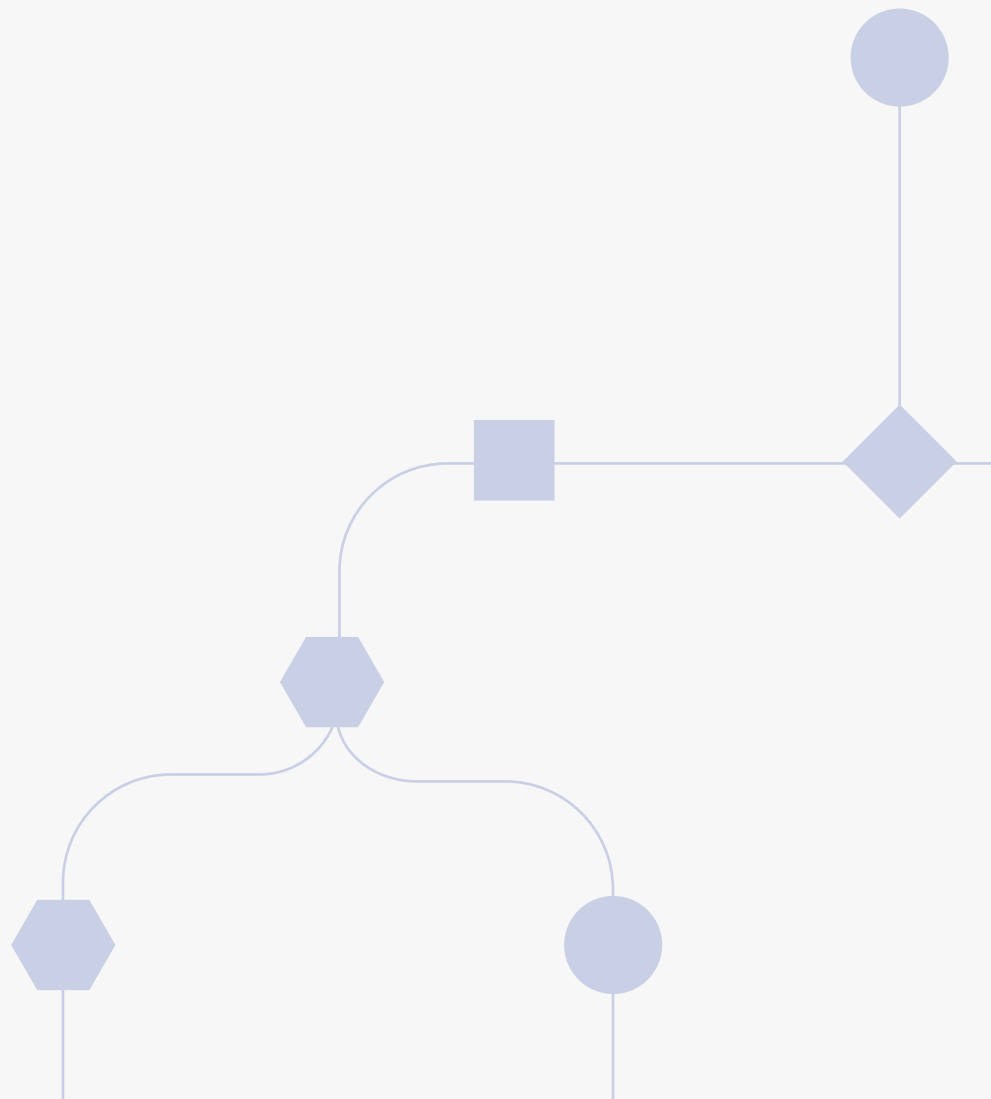
9

Continuously review and improve

Post-event reviews are essential to continuously improving your process. Assessing your successes and failures based on real data will enable you to both pinpoint potential roadblocks for future events and better understand realistic recovery timelines. Cutover's detailed analytics and audit trails make post-event analysis simple for all stakeholders.

10 Use an automated recovery platform

An automated recovery platform provides you with a foundational platform to host and execute all of your recovery plans. Whether the tasks are automated or manual, you need a central system of execution to accurately monitor and manage all the activities needed to enact a test or live recovery. An automated recovery platform such as Cutover can also be triggered from monitoring systems that track the health of the network and associated applications. You can use it to orchestrate when mass communications are sent to stakeholders and integrate with your ITSM platform to address ticketing and updates to the configuration management database (CMDB).



CASE STUDY

Multinational bank improves IT disaster recovery with Cutover



An American investment bank needed to implement a comprehensive resilience solution that enabled them to pull together thousands of standardized technical recovery plans (TRPs) into **test scenarios in minutes rather than weeks**. The technology resilience testing function involved thousands of people globally and up to 2,000 applications that needed to be tested every year and the existing home-grown system for this process was inadequate.

Cutover provides a comprehensive technology resilience platform that hosts thousands of TRPs that can be configured into various test scenarios in minutes.

Having TRPs in Cutover allows the bank to standardize them using a template so that there is minimal work to finalize DCR test runbooks. Cutover provides users with the status information and updates they need during the test to ensure success without manual effort, such as being able to visualize the critical path.

Using Cutover, the bank was able to **reduce event planning time by 70%** and easily facilitated and recorded all 143,000 completed tasks across its 10,000 users.

Want to find out how an automated recovery platform can help you?

[WATCH THIS VIDEO](#)

[READ THIS FACT SHEET](#)