cutover

# The 6 technologies you need for successful technology resilience

The digital-first economy we are now entering is creating greater complexity and vulnerability in enterprises due to the proliferation of new applications that, although they come with significant benefits, also create a host of new and increased threats. The increased reliance on a host of new tools that all require technical support, often not accompanied by increased resources for IT, is also creating additional risk to digital services.

Disruptions to business - whether environmental, cyber, or geo-political - are inevitable. That is why it is critically important for enterprises to understand the impact of the important digital services they provide and to invest in their resilience to protect themselves, consumers, and markets. Adverse events can't always be predicted, but they can be planned and rehearsed for. Planning can make the difference between a minor stumble and an enormous and damaging incident that threatens the health of the business.

# What are the major components needed for an IT disaster recovery plan to work?

In the event of an unplanned disaster, understanding and implementing the proper stack of recovery tooling is essential to successful recovery. Let's explore the six major components for recovering from disasters and outages.

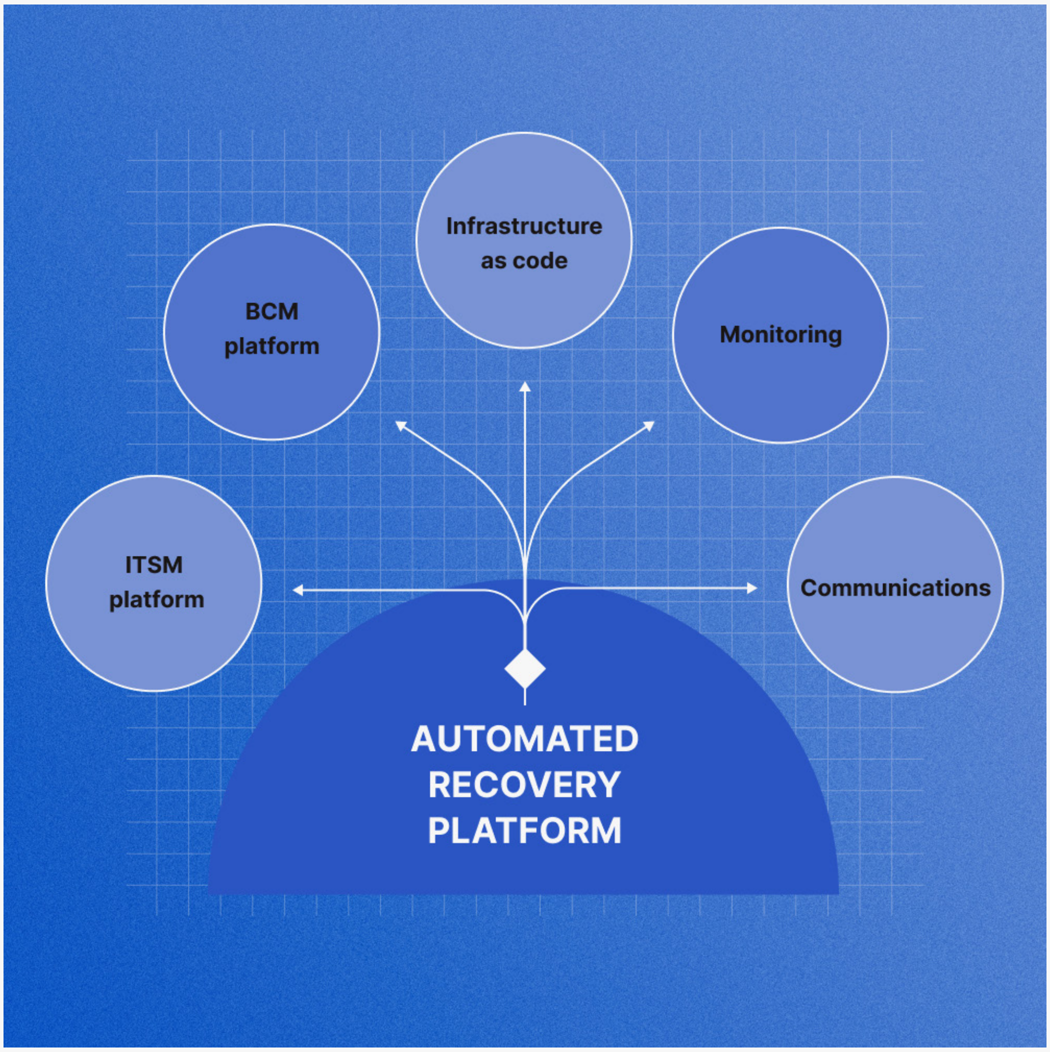

Figure 1: The major components of the technology resilience recovery stack

## Automated recovery platform

The automated recovery platform is the foundational platform that hosts the set of automated recovery plans to be executed based on the particular scenario. The plans are made up of sets of automated and manual activities needed to enact the recovery of an enterprise's applications and/or network. They are executable for testing recovery capabilities and live invocation in an actual disaster. They contain the live execution data following the event and are the golden source of truth for recovery plans and of the Recovery Time Actuals (RTAs) - the data on the actual performance of the plan. These are not document-based plans which are only indicative of what might be done in a disaster and they are not simple task models to be utilized after an event, they are used to actively orchestrate recoveries. They are typically stored at an application or service level and gathered in different configurations for different scenarios. The RTA data is often taken from these and imported into a business continuity management (BCM) platform. Automated recovery platforms are often triggered by monitoring tools. Conversely, the platform can also trigger monitoring from the recovery plans to determine system health and they can orchestrate when mass communications are sent. They also integrate with the IT service management (ITSM) platform to address ticketing and updates to the configuration management database (CMDB).

## ITSM Platform

An ITSM platform typically has two important components related to recovering the technology services that underpin critical business processes:

- The CMDB holds the definitions of what services run on what infrastructure and other important details, e.g. if a cloud region went down you could use the CMDB to understand which technology services were impacted and organize the recovery of those assets.

- The ticketing system ensures that appropriate governance has been enacted to change the configuration of the organization's IT assets, e.g. moving an application to different infrastructure for recovery. The tickets require the appropriate approvals for activities to get underway and, on closing the ticket, the CMDB should be updated. For recovery, this is a system of record and a system of governance.

## BCM platforms

BCM platforms offer the ability for organizations to do the following things: map out the set of business processes and assess the associated risks based on how critical they are to customers, which resources they require (people, places, systems, third parties), and what their impact tolerances are to ensure operations are maintained. This is typically the golden source of the organization's Recovery Time Objectives (RTOs) - the target times to recover technology assets and ensure that impact tolerances are not exceeded. For the purposes of recovery, the BCM platform is a key system of record.

## Infrastructure as code

Infrastructure as code tools, such as Ansible and Terraform, are often used as part of recovery plans to instantiate fresh infrastructure and stand up applications as needed. To avoid complex sets of configuration problems, they work best as modular components integrated into the executable automated recovery plans. Interaction between these tools and the automated recovery platform is essential to avoid delays and potential revenue loss from failures. For example, IT operations teams will map out how they will deal with a scenario and where they have to recreate their environment because the alternate site is also unusable, due to data corruption being transferred to that alternate site. This is particularly pertinent for cyber recovery.

## Monitoring

Monitoring tools, such as Datadog and NewRelic, are used as the starting point to execute recoveries in scenarios where alarms on monitoring software are well-defined, actionable triggers for a recovery plan.

## Communications

Communications, for example, via text, Microsoft Teams, or Slack, are used to ensure that everyone involved in the test or recovery is up to date.

# What does success look like for an IT disaster recovery?

To prepare for cyberattacks, network outages, and other unplanned incidents, your disaster recovery tests should simulate real incidents as closely as possible. Incidents are never planned, so effective disaster recovery testing should mirror that and be conducted unannounced.

In order to have true confidence in your ability to recover quickly, surprise tests are the best predictor of disaster recovery success and can offer the most insight into how to modify processes and technology to better protect IT infrastructure.

Deciding how to move forward across the recovery technology stack is always a challenge.  However, it is important to know that no one vendor addresses all six pillars. Therefore, it is important to evaluate best-of-breed solutions that go beyond vendors saying they have the complete stack.

Cutover's Collaborative Automation cloud solution provides you with an automated recovery platform capability for a complete system of execution across your teams and automation technology. Cutover's proven solution is most commonly used to support the operational resilience strategies and IT DR capabilities of the most demanding financial institutions in the world.

With Cutover, you can seamlessly provide the recovery capabilities you need, including hosting multi-team and technology recovery plans, performing planned or unplanned resilience testing, and recovering from actual events, all with visibility into execution analytics and audit logs.

Unavoidable resilience risks, whether natural disasters or cyberattacks, have unfortunately hit organizations harder than ever in the last few years. Now regulators want to be able to see organizations' operational risk and resilience practices in action so they can be sure that they are able to recover quickly and effectively in a real scenario. Underpinning your operational resilience strategies with Cutover allows you to thrive and not just survive under resilience events.

## Contact us for more information

@ Contact

@gocutover

follow us on LinkedIn

visit www.cutover.com

SEE CUTOVER FOR ITDR IN ACTION

cutover