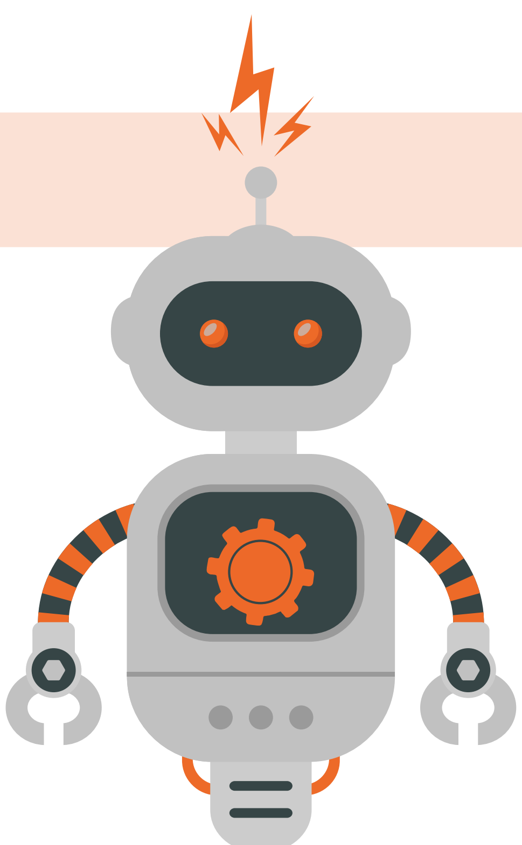
How to test your DR plan: At-a-glance essentials

Without testing, your disaster recovery plan is just a piece of paper – and how useful is that during a continuity crisis? No matter how advanced your software, meticulous your planning or well-briefed your people, it is impossible to know if untested DR is fit for purpose. Working through these 3 levels will ensure that business-critical IT, applications and data are available and resilient when disaster strikes.

LEVEL 1 Automated DR testing



IT can be used to regularly test whether systems involved in DR are functioning as intended. Automated testing forces individual tasks to occur – such as data backups and restorations or connecting to a failover system and running applications – which are not specific to any scenario. The most common automated DR test methods are:

PARALLEL TEST

Recovery systems are implemented and tested to see if they can perform actual business functions and processes. Primary systems still carry the full production workload. **This can happen during hours of operation.**

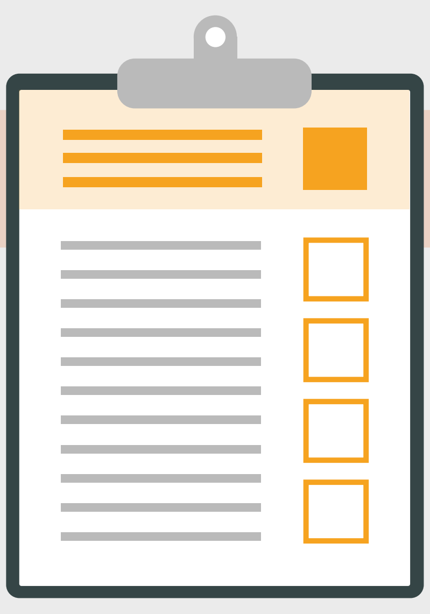
CUTOVER TEST

Recovery systems are implemented to assume the full production workload. Primary systems are disconnected and technology is tested. **This must happen overnight or outside of trading hours.**

Automated testing with DRaaS

Disaster Recovery as a Service (DRaaS) automates the testing of functionality and availability of systems, applications and data involved in DR. K3 delivers tailored DRaaS including strategies for all DR infrastructure, which you can read about here.

LEVEL 2 Paper and walkthrough testing



To supplement DRaaS functions, IT DR should undergo periodic paper testing and walkthrough testing. Think of these processes as intermediary spot-checks to supplement a simulation.

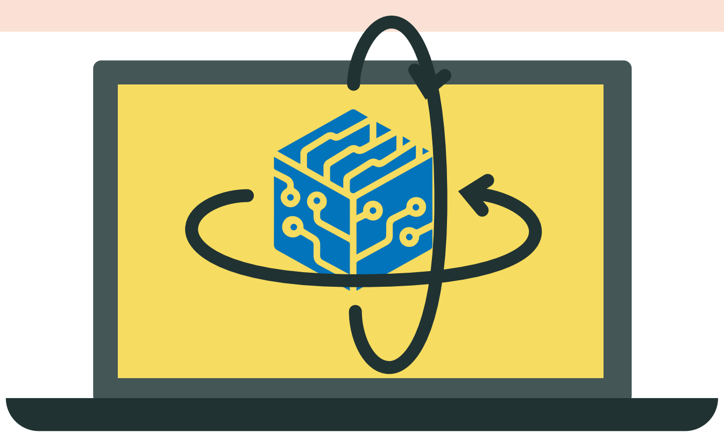
PAPER TEST

A refresher of the current DR plan. This will involve all members of the DR team meeting to read and annotate the plan – including an analysis of IT provision – and making any obvious changes.

WALKTHROUGH TEST

The DR team plus an observer meet to tackle a hypothetical disaster scenario using the DR plan. As the name suggests, the group will walk through the plan in tandem with the scenario to identify issues and updates prior to a full simulation.

LEVEL 3 Simulation testing



A simulation test is the closest thing to invoking the DR plan and is the most effective step in determining if the plan and technology are adequate. It is typically run no more than twice a year depending on plan complexity and changes to business circumstances, the business impact analysis or the economy.

The DR team will work through a disaster scenario using the real DR procedures, technology and allocated resources

This usually involves sending the team to a separate disaster recovery location to restart IT or operational functions

The use of alternative equipment and third-party services is another common requirement

93% of businesses without DR plans would shut down within 1 year of a major breach

CLOSED

50% of organisations lack budget to recover from a cyberattack

50% of companies experienced a event in the last 5 years exceeding 1 day

96% of businesses with a tested DR plan can survive ransomware attacks

61% of companies say inadequate resources prevent DR testing

The first step to building a DR testing strategy is a consultancy session with a specialist. This service will assist you in determining testing schedules and metrics, testing types and much more.

To arrange a session, contact Starcom on **0844 579 0800**

starcom
A Node4 Company